ID: 800697
Cookbook: browseurl.jbs
Time: 18:21:07
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

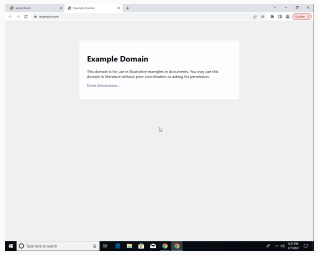
Windows Analysis Report

https://server.1ksat.com/?ufov&qrc=jneal@heniff.com&c=E,1,b3hl6R7LYWai95TidY7oKofIoKw3DsF4Po..

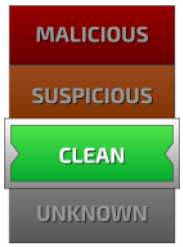
Overview

General Information

Sample URL:	https://server.1ksat.com/?ufov&qrc=jneal@heniff.com&c=E,1,b3hl6R7LYWai95Tid...EwdMkQ_Szrum_7168W7bTNHjC2nzWdEhCHm4HwED1LIkrBAldy8iRpLM7NZotqaK-Q,,&typo=1
Analysis ID:	800697
Infos:	



Detection

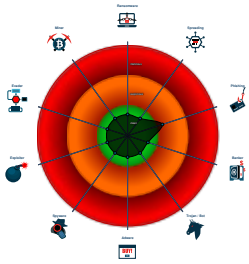


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

URL contains potential PII (phishing…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5920 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 3128 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1724 --field-trial-handle=1708,i,17388265217453813 83,15185311736595585432,131072 --disable-features =OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5624 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://server.1ksat.com/?ufov&qrc=jneal@heniff.com&c=E,1,b3hl6R7LYWai95TidY7oKofIoKw3DsF4PoHXJGBO0t7029g1ST6sdhPuEwdMkQ_Szrum_7168W7bTNHjC2nzWdEhCHm4HwED1LIkrBAldy8iRpLM7NZotqaK-Q,,&typo=1 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

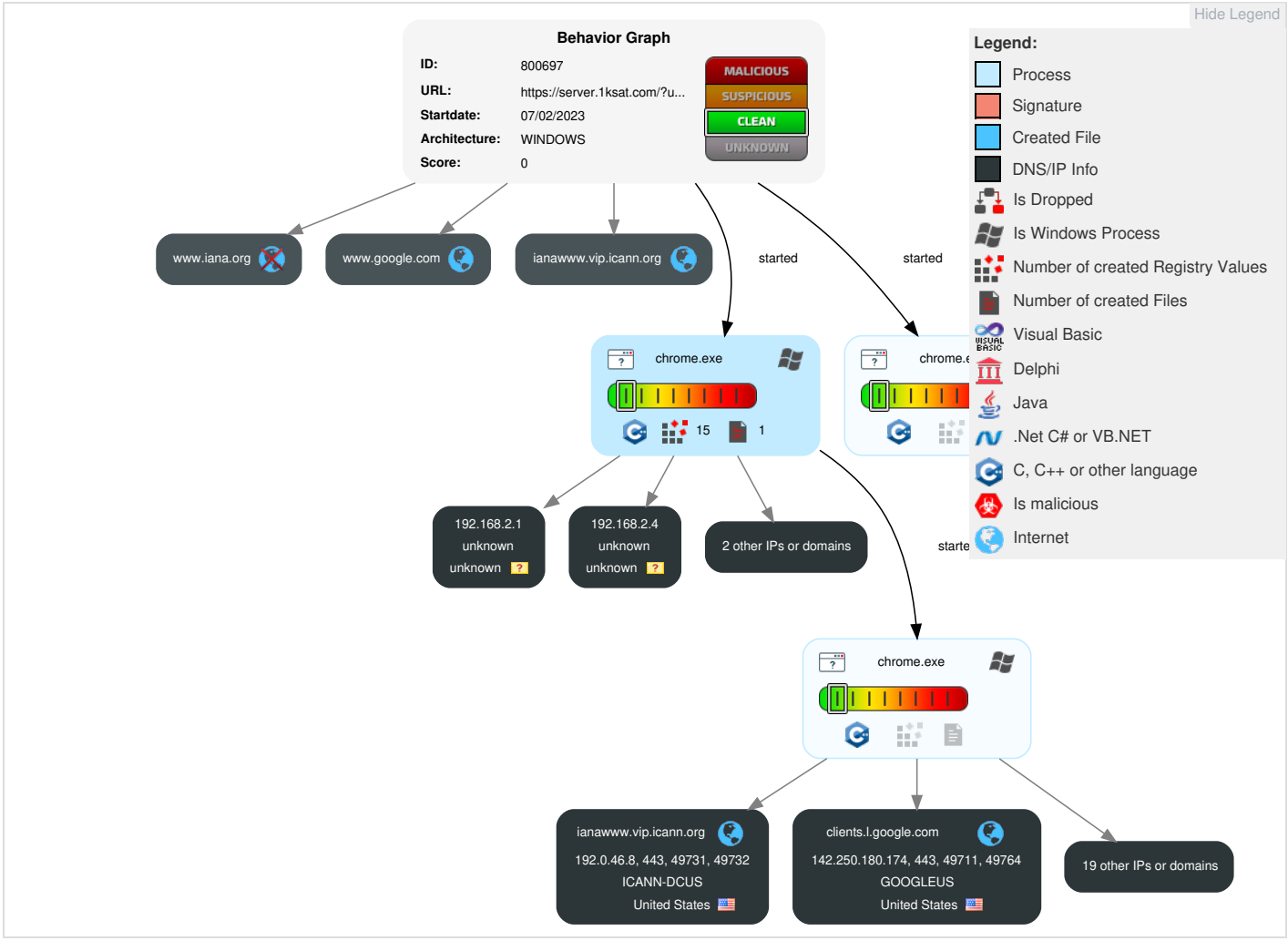
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	5 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	6 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
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	4 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

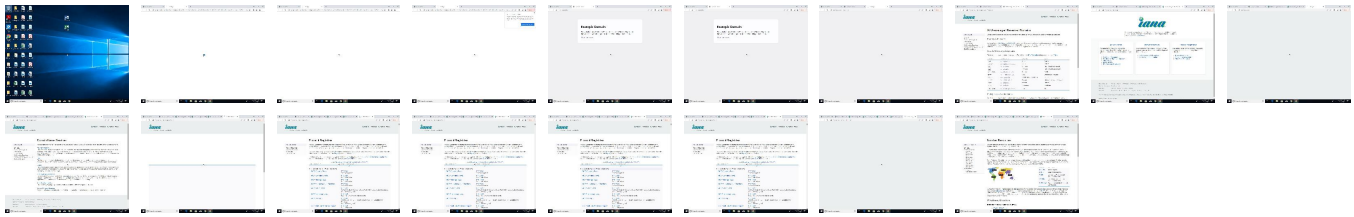
Behavior Graph

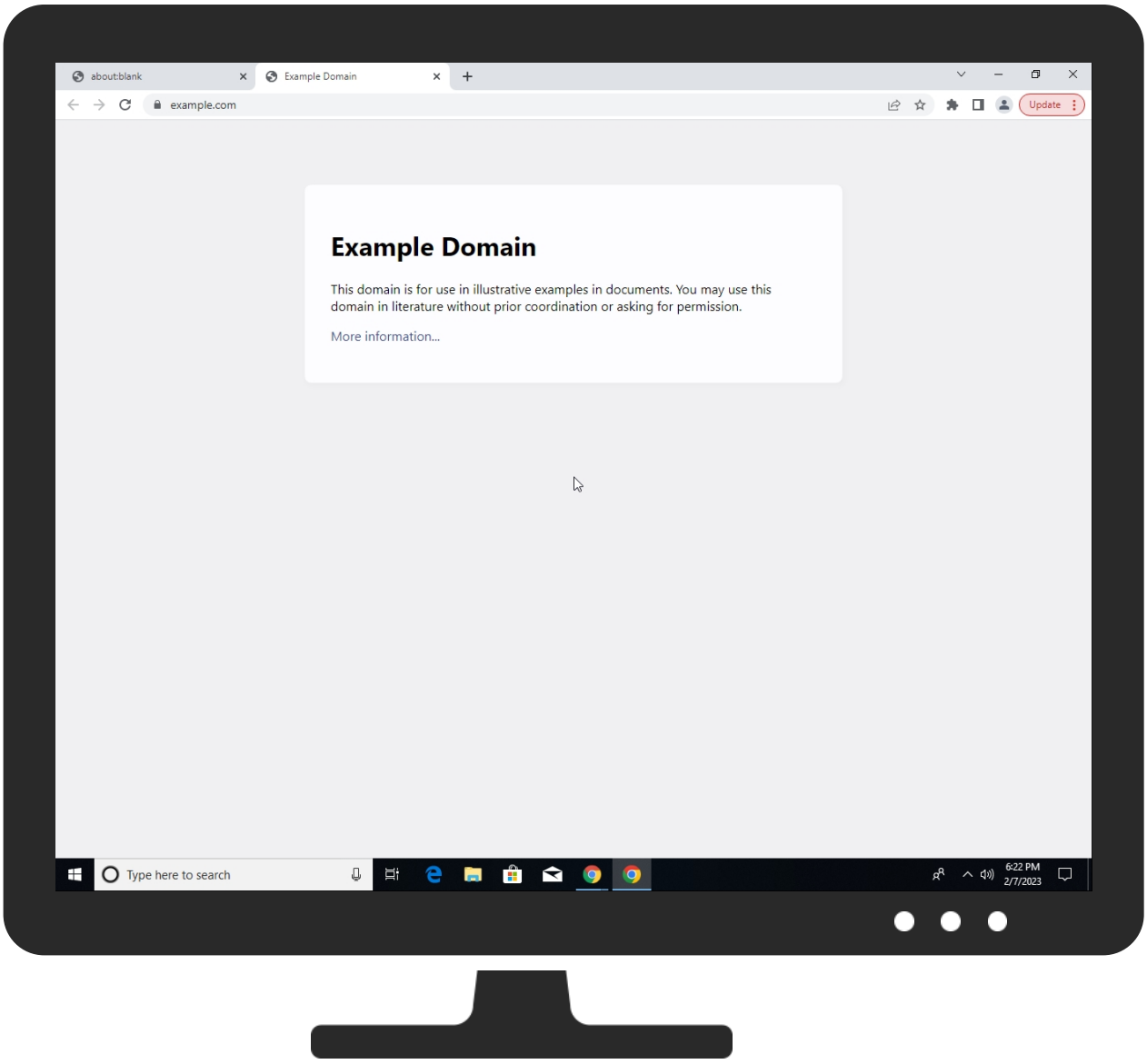


Screenshots

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
http://https://server.1ksat.com/?ufov&qrc=jneal@heniff.com&c=E,1,b3hl6R7LYWai95TidY7oKofIoKw3DsF4PoHXJGBO0t7029g1ST6sdhPuEwdMkQ_Szrum_7168W7bTNHjC2nzWdEhCHm4HwED1LIkrBAldy8iRpLM7NZotqaK-Q,,&typo=1	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

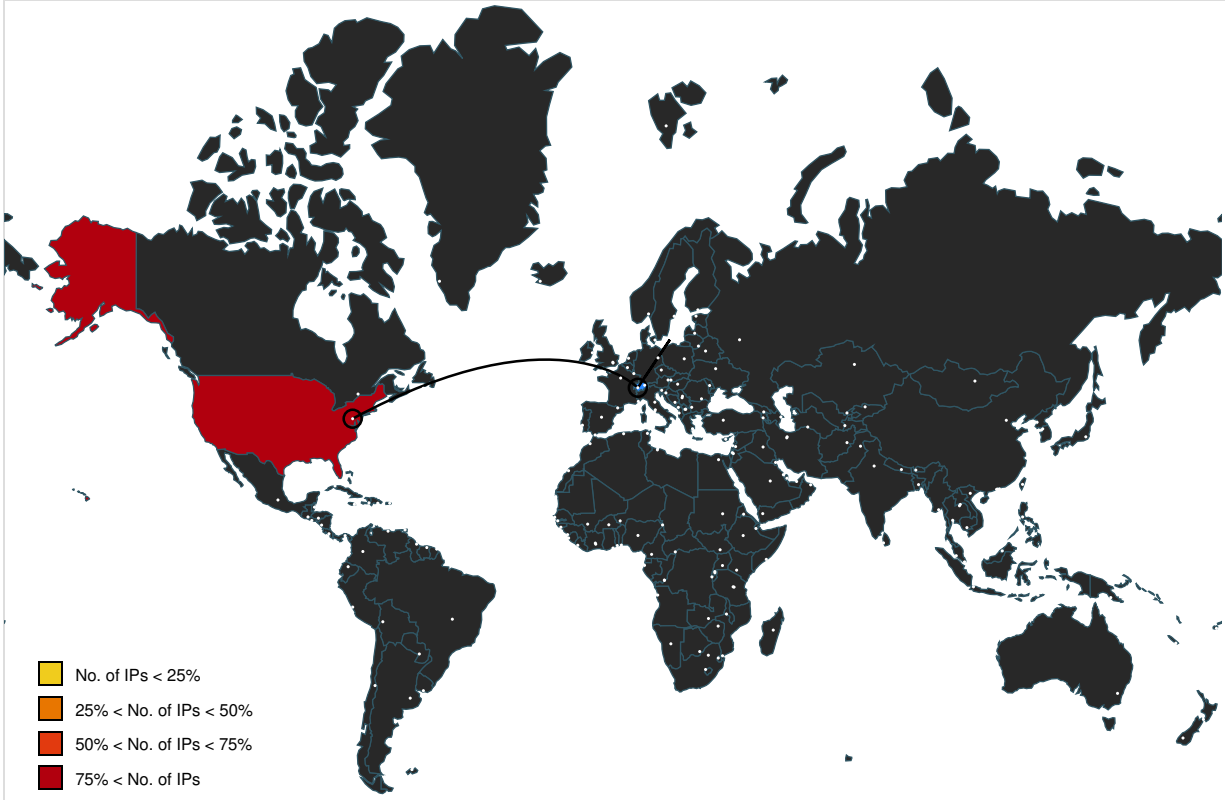
Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.arin.net	199.43.0.47	true	false		high
www.nro.net	193.0.19.65	true	false		unknown
accounts.google.com	216.58.209.45	true	false		high
www.afrinic.net	196.216.2.6	true	false		high
ianawww.vip.icann.org	192.0.46.8	true	false		high
href.li	192.0.78.26	true	false		high
www.vip.icann.org	192.0.47.7	true	false		high
www.lacnic.net	200.3.14.184	true	false		high
server.1ksat.com	34.214.99.116	true	false		unknown
cse.google.com	142.250.180.174	true	false		high
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
example.com	93.184.216.34	true	false		high
www.apnic.net	unknown	unknown	false		high
www.ietf.org	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.iana.org	unknown	unknown	false		high
pti.icann.org	unknown	unknown	false		high
www.ripe.net	unknown	unknown	false		high
www.icann.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.iana.org/_img/2022/fonts/SourceCodePro-Regular.woff	false		high
http://https://www.iana.org/_img/2022/fonts/NotoSans-Italic.woff	false		high
http://https://cse.google.com/cse.js?cx=010470622406686203020:boq_dnseony	false		high
http://https://www.iana.org/_img/2022/iana-logo-header.svg	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://www.iana.org/domains/reserved	false		high
http://https://www.iana.org/_img/bookmark_icon.ico	false		high
http://https://www.iana.org/_css/2022/iana_website.css	false		high
http://www.iana.org/_img/bookmark_icon.ico	false		high
http://www.iana.org/	false		high
http://www.iana.org/domains	false		high
http://www.iana.org/	false		high
http://www.iana.org/_img/2013.1/rir-map.svg	false		high
http://https://www.iana.org/_img/2022/fonts/NotoSans-Bold.woff	false		high
http://https://server.1ksat.com/?ufov&qrc=jneal@heniff.com&c=E,1,b3hl6R7LYWai95TidY7oKofIoKw3DsF4PoHXJGBO0t7029g1ST6sdhPuEwdMkQ_Szrum_7168W7bTNHjC2nzWdEhCHm4HwED1LIkrBAldy8iRpLM7NZotqaK-Q,,&typo=1	false		unknown
http://www.iana.org/domains/reserved	false		high
http://https://example.com/	false		high
http://https://href.li/?https://example.com	false		high
http://https://www.iana.org/_js/iana.js	false		high
http://www.iana.org/protocols	false		high
http://https://www.iana.org/_img/2022/fonts/NotoSans-Regular.woff	false		high
http://https://example.com/favicon.ico	false		high
http://https://www.iana.org/_img/2013.1/rir-map.svg	false		high
http://www.iana.org/protocols	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/sorry/index?continue=https://cse.google.com/cse.js%3Fcx%3D010470622406686203020:boq_dnseony&q=EgRUETQNGOORip8GIjCfzYmwLuKcy4IAIwbs2Qk2pKJdI6TLau-PLMIWh6D5iMBjkYX4NLuYSVAPF0L8ud0yAXI	false		high
http://www.iana.org/numbers	false		high
http://www.iana.org/_img/2022/iana-logo-header.svg	false		high
http://https://www.iana.org/domains/example	false		high
http://https://www.iana.org/_img/2015.1/iana-logo-homepage.svg	false		high
http://www.iana.org/numbers	false		high
http://https://www.iana.org/_js/jquery.js	false		high
http://https://example.com/	false		high
http://www.iana.org/domains	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.46.8	ianawww.vip.icann.org	United States		16876	ICANN-DCUS	false
93.184.216.34	example.com	European Union		15133	EDGECASTUS	false
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
192.0.78.26	href.li	United States		2635	AUTOMATTICUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
34.214.99.116	server.1ksat.com	United States		16509	AMAZON-02US	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	cse.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.4
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800697
Start date and time:	2023-02-07 18:21:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://server.1ksat.com/?ufov&qrc=jneal@heniff.com&c=E,1,b3hl6R7LYWai95TidY7oKofIoKw3DsF4PoHXJGBO0t7029g1ST6sdhPuEwdMkQ_Szrum_7168W7bTNHjC2nzWdEhCHm4HwED1LIkrBAldy8iRpLM7NZotqaK-Q,,&typo=1
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
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:	CLEAN
Classification:	clean0.win@35/0@21/12
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://www.iana.org/domains/example • Browse: http://www.iana.org/ • Browse: http://www.iana.org/domains • Browse: http://www.iana.org/protocols • Browse: http://www.iana.org/numbers

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 142.250.180.163, 104.18.235.68, 104.18.236.68, 104.16.44.99, 104.16.45.99, 104.18.21.44, 104.18.20.44
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, www.ietf.org.cdn.cloudflare.net, fs.microsoft.com, edgedl.me.gvt1.com, login.live.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, www.ripe.net.cdn.cloudflare.net, www.apnic.net.cdn.cloudflare.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

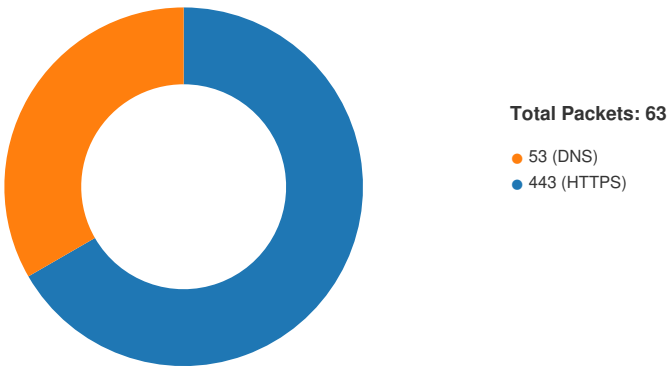
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:22:16.871933937 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:16.872023106 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:16.872128010 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:16.872423887 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:16.872472048 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:16.872546911 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:16.873469114 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:16.873537064 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:16.873596907 CET	49714	443	192.168.2.7	34.214.99.116

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:22:16.874842882 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:16.874890089 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:16.875627041 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:16.875659943 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:16.937477112 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:16.937531948 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:16.981443882 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:16.990067959 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:17.028006077 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:17.033960104 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:17.043283939 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:17.043330908 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:17.043889999 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:17.043915033 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:17.044622898 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:17.044734001 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:17.046113014 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:17.046185970 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:17.046578884 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:17.046688080 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:17.338491917 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:17.379996061 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:18.615642071 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:18.615684986 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:18.617130995 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:18.617281914 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:18.734719038 CET	49715	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:22:18.734785080 CET	443	49715	142.250.184.100	192.168.2.7
Feb 7, 2023 18:22:18.734874010 CET	49715	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:22:18.735313892 CET	49715	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:22:18.735332966 CET	443	49715	142.250.184.100	192.168.2.7
Feb 7, 2023 18:22:18.806797981 CET	443	49715	142.250.184.100	192.168.2.7
Feb 7, 2023 18:22:18.811039925 CET	49715	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:22:18.811083078 CET	443	49715	142.250.184.100	192.168.2.7
Feb 7, 2023 18:22:18.812521935 CET	443	49715	142.250.184.100	192.168.2.7
Feb 7, 2023 18:22:18.812594891 CET	49715	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:22:18.818392038 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:18.818445921 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:18.818667889 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:18.818757057 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:18.818769932 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:18.818893909 CET	49715	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:22:18.818907976 CET	443	49715	142.250.184.100	192.168.2.7
Feb 7, 2023 18:22:18.819149971 CET	443	49715	142.250.184.100	192.168.2.7
Feb 7, 2023 18:22:18.819262028 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:18.819288969 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:18.819475889 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:18.819536924 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:18.819567919 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:18.819684982 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:18.819742918 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:18.819761038 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:18.820318937 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:18.820336103 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:18.862545967 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:18.862626076 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:18.862658978 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:18.862780094 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:18.862848043 CET	49711	443	192.168.2.7	142.250.180.174

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:22:18.865916967 CET	49711	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:22:18.865950108 CET	443	49711	142.250.180.174	192.168.2.7
Feb 7, 2023 18:22:18.891599894 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:18.891726017 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:18.891748905 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:18.892057896 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:18.892126083 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:18.893532038 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:22:18.893558025 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:22:18.928117037 CET	49715	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:22:18.928150892 CET	443	49715	142.250.184.100	192.168.2.7
Feb 7, 2023 18:22:18.983227968 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:19.028069973 CET	49715	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:22:21.397209883 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:21.397331953 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:21.397437096 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:21.399687052 CET	49714	443	192.168.2.7	34.214.99.116
Feb 7, 2023 18:22:21.399724960 CET	443	49714	34.214.99.116	192.168.2.7
Feb 7, 2023 18:22:21.426561117 CET	49717	443	192.168.2.7	192.0.78.26
Feb 7, 2023 18:22:21.426615953 CET	443	49717	192.0.78.26	192.168.2.7
Feb 7, 2023 18:22:21.426707983 CET	49717	443	192.168.2.7	192.0.78.26
Feb 7, 2023 18:22:21.427263975 CET	49717	443	192.168.2.7	192.0.78.26
Feb 7, 2023 18:22:21.427284002 CET	443	49717	192.0.78.26	192.168.2.7
Feb 7, 2023 18:22:21.481267929 CET	443	49717	192.0.78.26	192.168.2.7
Feb 7, 2023 18:22:21.481805086 CET	49717	443	192.168.2.7	192.0.78.26
Feb 7, 2023 18:22:21.481859922 CET	443	49717	192.0.78.26	192.168.2.7
Feb 7, 2023 18:22:21.482784986 CET	443	49717	192.0.78.26	192.168.2.7
Feb 7, 2023 18:22:21.482943058 CET	49717	443	192.168.2.7	192.0.78.26
Feb 7, 2023 18:22:21.483762026 CET	443	49717	192.0.78.26	192.168.2.7
Feb 7, 2023 18:22:21.483880997 CET	49717	443	192.168.2.7	192.0.78.26
Feb 7, 2023 18:22:21.500237942 CET	49717	443	192.168.2.7	192.0.78.26
Feb 7, 2023 18:22:21.500276089 CET	443	49717	192.0.78.26	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:22:16.252435923 CET	50505	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:16.280538082 CET	53	50505	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:16.683895111 CET	61178	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:16.712114096 CET	53	61178	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:16.755249023 CET	63926	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:16.788966894 CET	53	63926	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:18.629657984 CET	50513	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:18.658341885 CET	53	50513	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:21.407033920 CET	50024	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:21.425173044 CET	53	50024	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:22.722906113 CET	62679	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:22.742183924 CET	53	62679	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:30.861478090 CET	51526	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:30.881716013 CET	53	51526	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:33.172885895 CET	57970	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:33.192981005 CET	53	57970	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:33.229687929 CET	64608	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:33.479877949 CET	53	64608	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:35.960926056 CET	61248	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:35.979289055 CET	53	61248	8.8.8.8	192.168.2.7
Feb 7, 2023 18:22:43.538346052 CET	51436	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:22:43.564634085 CET	53	51436	8.8.8.8	192.168.2.7
Feb 7, 2023 18:23:28.532838106 CET	56345	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:23:28.532838106 CET	59112	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:23:28.532999039 CET	55303	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:23:28.550726891 CET	53	56345	8.8.8.8	192.168.2.7
Feb 7, 2023 18:23:28.558995962 CET	53952	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:23:28.584702969 CET	53	55303	8.8.8.8	192.168.2.7
Feb 7, 2023 18:23:28.668144941 CET	64501	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:23:28.677006006 CET	51311	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:23:28.683913946 CET	53859	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:23:28.720637083 CET	53	64501	8.8.8.8	192.168.2.7
Feb 7, 2023 18:23:28.753750086 CET	53	51311	8.8.8.8	192.168.2.7
Feb 7, 2023 18:23:34.053257942 CET	61896	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:23:34.053257942 CET	57940	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:23:34.160751104 CET	53	57940	8.8.8.8	192.168.2.7
Feb 7, 2023 18:23:34.307271004 CET	53	61896	8.8.8.8	192.168.2.7
Feb 7, 2023 18:24:18.595200062 CET	58875	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:24:18.624335051 CET	53	58875	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:22:16.252435923 CET	192.168.2.7	8.8.8.8	0x277d	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:16.683895111 CET	192.168.2.7	8.8.8.8	0x138a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:16.755249023 CET	192.168.2.7	8.8.8.8	0x520f	Standard query (0)	server.1ksat.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:18.629657984 CET	192.168.2.7	8.8.8.8	0xa4bb	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:21.407033920 CET	192.168.2.7	8.8.8.8	0x3c75	Standard query (0)	href.li	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:22.722906113 CET	192.168.2.7	8.8.8.8	0x8df8	Standard query (0)	example.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:30.861478090 CET	192.168.2.7	8.8.8.8	0xe6b	Standard query (0)	www.iana.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:33.172885895 CET	192.168.2.7	8.8.8.8	0xccbf	Standard query (0)	www.icann.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:33.229687929 CET	192.168.2.7	8.8.8.8	0xcfc3	Standard query (0)	pti.icann.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:35.960926056 CET	192.168.2.7	8.8.8.8	0x40a8	Standard query (0)	www.iana.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:43.538346052 CET	192.168.2.7	8.8.8.8	0x4906	Standard query (0)	cse.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.532838106 CET	192.168.2.7	8.8.8.8	0xe7be	Standard query (0)	www.afrinic.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.532838106 CET	192.168.2.7	8.8.8.8	0x63d3	Standard query (0)	www.apnic.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.532999039 CET	192.168.2.7	8.8.8.8	0x323e	Standard query (0)	www.arin.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.558995962 CET	192.168.2.7	8.8.8.8	0xbacd	Standard query (0)	www.ietf.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.668144941 CET	192.168.2.7	8.8.8.8	0xd2f5	Standard query (0)	www.lacnic.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.677006006 CET	192.168.2.7	8.8.8.8	0x5b2a	Standard query (0)	www.nro.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.683913946 CET	192.168.2.7	8.8.8.8	0x796b	Standard query (0)	www.ripe.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:34.053257942 CET	192.168.2.7	8.8.8.8	0x65b	Standard query (0)	pti.icann.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:34.053257942 CET	192.168.2.7	8.8.8.8	0x3ee	Standard query (0)	www.icann.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:18.595200062 CET	192.168.2.7	8.8.8.8	0xb8c2	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:22:16.280538082 CET	8.8.8.8	192.168.2.7	0x277d	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:22:16.280538082 CET	8.8.8.8	192.168.2.7	0x277d	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:16.712114096 CET	8.8.8.8	192.168.2.7	0x138a	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:16.788966894 CET	8.8.8.8	192.168.2.7	0x520f	No error (0)	server.1ksat.com		34.214.99.116	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:18.658341885 CET	8.8.8.8	192.168.2.7	0xa4bb	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:21.425173044 CET	8.8.8.8	192.168.2.7	0x3c75	No error (0)	href.li		192.0.78.26	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:21.425173044 CET	8.8.8.8	192.168.2.7	0x3c75	No error (0)	href.li		192.0.78.27	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:22.742183924 CET	8.8.8.8	192.168.2.7	0x8df8	No error (0)	example.com		93.184.216.34	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:30.881716013 CET	8.8.8.8	192.168.2.7	0xe6b	No error (0)	www.iana.org	ianawww.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:22:30.881716013 CET	8.8.8.8	192.168.2.7	0xe6b	No error (0)	ianawww.vip.icann.org		192.0.46.8	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:33.192981005 CET	8.8.8.8	192.168.2.7	0xccbf	No error (0)	www.icann.org	www.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:22:33.192981005 CET	8.8.8.8	192.168.2.7	0xccbf	No error (0)	www.vip.icann.org		192.0.47.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:33.479877949 CET	8.8.8.8	192.168.2.7	0xcfc3	No error (0)	pti.icann.org	www.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:22:33.479877949 CET	8.8.8.8	192.168.2.7	0xcfc3	No error (0)	www.vip.icann.org		192.0.47.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:35.979289055 CET	8.8.8.8	192.168.2.7	0x40a8	No error (0)	www.iana.org	ianawww.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:22:35.979289055 CET	8.8.8.8	192.168.2.7	0x40a8	No error (0)	ianawww.vip.icann.org		192.0.46.8	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:43.564634085 CET	8.8.8.8	192.168.2.7	0x4906	No error (0)	cse.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.550726891 CET	8.8.8.8	192.168.2.7	0xe7be	No error (0)	www.afrinic.net		196.216.2.6	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.555237055 CET	8.8.8.8	192.168.2.7	0x63d3	No error (0)	www.apnic.net	www.apnic.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:23:28.581576109 CET	8.8.8.8	192.168.2.7	0xbacd	No error (0)	www.ietf.org	www.ietf.org.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:23:28.584702969 CET	8.8.8.8	192.168.2.7	0x323e	No error (0)	www.arin.net		199.43.0.47	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.584702969 CET	8.8.8.8	192.168.2.7	0x323e	No error (0)	www.arin.net		192.136.136.47	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.706823111 CET	8.8.8.8	192.168.2.7	0x796b	No error (0)	www.ripe.net	www.ripe.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:23:28.720637083 CET	8.8.8.8	192.168.2.7	0xd2f5	No error (0)	www.lacnic.net		200.3.14.184	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:28.753750086 CET	8.8.8.8	192.168.2.7	0x5b2a	No error (0)	www.nro.net		193.0.19.65	A (IP address)	IN (0x0001)	false

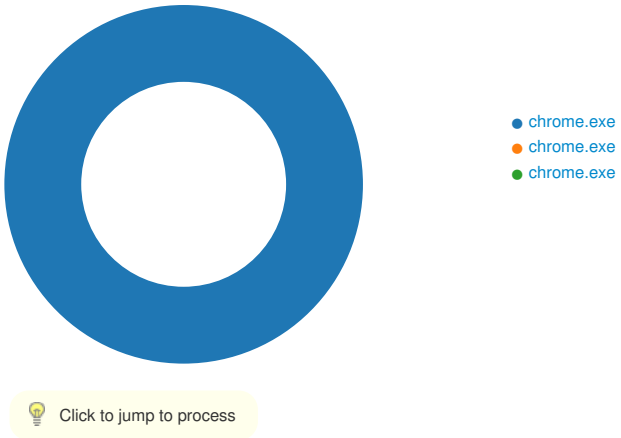
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:23:34.160751104 CET	8.8.8.8	192.168.2.7	0x3ee	No error (0)	www.icann.org	www.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:23:34.160751104 CET	8.8.8.8	192.168.2.7	0x3ee	No error (0)	www.vip.icann.org		192.0.47.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:34.307271004 CET	8.8.8.8	192.168.2.7	0x65b	No error (0)	pti.icann.org	www.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:23:34.307271004 CET	8.8.8.8	192.168.2.7	0x65b	No error (0)	www.vip.icann.org		192.0.47.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:18.624335051 CET	8.8.8.8	192.168.2.7	0xb8c2	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- server.1ksat.com
- href.li
- example.com
- https:
  - www.iana.org
- cse.google.com
- www.google.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5920**, Parent PID: **1616**

General

Target ID:	0
Start time:	18:22:11
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff7c2920000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **3128**, Parent PID: **5920**

General

Target ID:	1
Start time:	18:22:12
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1724 --field-trial-handle=1708,i,17388265217453813 83,15185311736595585432,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7c2920000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **5624**, Parent PID: **1616**

General	
Target ID:	2
Start time:	18:22:13
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://server.1ksat.com/?ufov&qrc=jneal@heniff.com&c=E,1,b3hl6R7LYWai95TidY7oKofIoKw3DsF4PoHXJGBO0t7029g1ST6sdhPuEwdMkQ_Szrum_7168W7bTNHjC2nzWdEhCHm4HwED1LIkrBAldy8iRpLM7NZotqaK-Q,,&typo=1
Imagebase:	0x7ff7c2920000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Disassembly

No disassembly