ID: 756170
Cookbook: urldownload.jbs
Time: 19:03:59
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

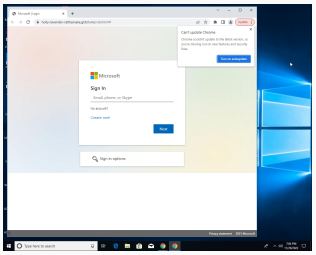
Windows Analysis Report

https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nb...

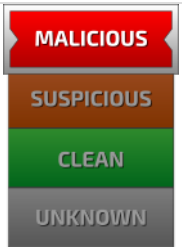
Overview

General Information

Sample URL:	http://https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s
Analysis ID:	756170
Infos:	



Detection



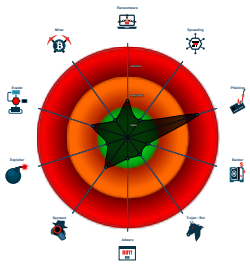
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Misleading page title found
- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Queries the volume information (nam…
- Yara signature match
- Found iframes
- Very long cmdline option found, this…
- No HTML title found
- Detected potential crypto function
- HTML body contains low number of …

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6032 cmdline: C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s" > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 5988 cmdline: wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s" MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- chrome.exe (PID: 5132 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\download\index.html@url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2288 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=1944 --field-trial-handle=1616,i,5292400896411780733,13825633785752334259,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
29025.1.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x497d8:$c8: while(!![]) • 0xb1f4c:$c8: while(!![]) • 0x497f9:$d1: parseInt(_0xc8185d(0x1ee))/0x1+parseInt(_0xc8185d(0x1f9))/0x2*(-parseInt(_0xc8185d(0x207))/0x3)+parseInt(_0xc8185d(0x206))/0x4+-parseInt(_0xc8185d(0x1ef))/0x5*(parseInt(_0xc8185d(0x1fe))/0x6)+- • 0x49818:$d1: parseInt(_0xc8185d(0x1f9))/0x2*(-parseInt(_0xc8185d(0x207))/0x3)+parseInt(_0xc8185d(0x206))/0x4+-parseInt(_0xc8185d(0x1ef))/0x5*(parseInt(_0xc8185d(0x1fe))/0x6)+-parseInt(_0xc8185d(0x1fa))/0x7*(• 0x49839:$d1: parseInt(_0xc8185d(0x207))/0x3)+parseInt(_0xc8185d(0x206))/0x4+-parseInt(_0xc8185d(0x1ef))/0x5*(parseInt(_0xc8185d(0x1fe))/0x6)+-parseInt(_0xc8185d(0x1fa))/0x7*(parseInt(_0xc8185d(0x200))/0x8)+- • 0x49859:$d1: parseInt(_0xc8185d(0x206))/0x4+-parseInt(_0xc8185d(0x1ef))/0x5*(parseInt(_0xc8185d(0x1fe))/0x6)+-parseInt(_0xc8185d(0x1fa))/0x7*(parseInt(_0xc8185d(0x200))/0x8)+-parseInt(_0xc8185d(0x201))/0x9*(- • 0x49879:$d1: parseInt(_0xc8185d(0x1ef))/0x5*(parseInt(_0xc8185d(0x1fe))/0x6)+-parseInt(_0xc8185d(0x1fa))/0x7*(parseInt(_0xc8185d(0x200))/0x8)+-parseInt(_0xc8185d(0x201))/0x9*(-parseInt(_0xc8185d(0x1fb))/0xa)+ • 0xb1f6a:$d1: parseInt(_0x5d57ec(0x1d9))/0x1+parseInt(_0x5d57ec(0x1c7))/0x2*(-parseInt(_0x5d57ec(0x1f1))/0x3)+-parseInt(_0x5d57ec(0x1dd))/0x4*(parseInt(_0x5d57ec(0x1cb))/0x5)+parseInt(_0x5d57ec(0x1ca))/0x6*(- • 0xb1f89:$d1: parseInt(_0x5d57ec(0x1c7))/0x2*(-parseInt(_0x5d57ec(0x1f1))/0x3)+-parseInt(_0x5d57ec(0x1dd))/0x4*(parseInt(_0x5d57ec(0x1cb))/0x5)+parseInt(_0x5d57ec(0x1ca))/0x6*(-parseInt(_0x5d57ec(0x1da))/0x7)+ • 0xb1faa:$d1: parseInt(_0x5d57ec(0x1f1))/0x3)+-parseInt(_0x5d57ec(0x1dd))/0x4*(parseInt(_0x5d57ec(0x1cb))/0x5)+parseInt(_0x5d57ec(0x1ca))/0x6*(-parseInt(_0x5d57ec(0x1da))/0x7)+parseInt(_0x5d57ec(0x1fd))/0x8*(- • 0xb1fcb:$d1: parseInt(_0x5d57ec(0x1dd))/0x4*(parseInt(_0x5d57ec(0x1cb))/0x5)+parseInt(_0x5d57ec(0x1ca))/0x6*(-parseInt(_0x5d57ec(0x1da))/0x7)+parseInt(_0x5d57ec(0x1fd))/0x8*(-parseInt(_0x5d57ec(0x1d1))/0x9)+- • 0xb1feb:$d1: parseInt(_0x5d57ec(0x1cb))/0x5)+parseInt(_0x5d57ec(0x1ca))/0x6*(-parseInt(_0x5d57ec(0x1da))/0x7)+parseInt(_0x5d57ec(0x1fd))/0x8*(-parseInt(_0x5d57ec(0x1d1))/0x9)+-parseInt(_0x5d57ec(0x1e1))/0xa+- • 0xb200b:$d1: parseInt(_0x5d57ec(0x1ca))/0x6*(-parseInt(_0x5d57ec(0x1da))/0x7)+parseInt(_0x5d57ec(0x1fd))/0x8*(-parseInt(_0x5d57ec(0x1d1))/0x9)+-parseInt(_0x5d57ec(0x1e1))/0xa+-parseInt(_0x5d57ec(0x1c6))/0xb*(-
29025.1.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing

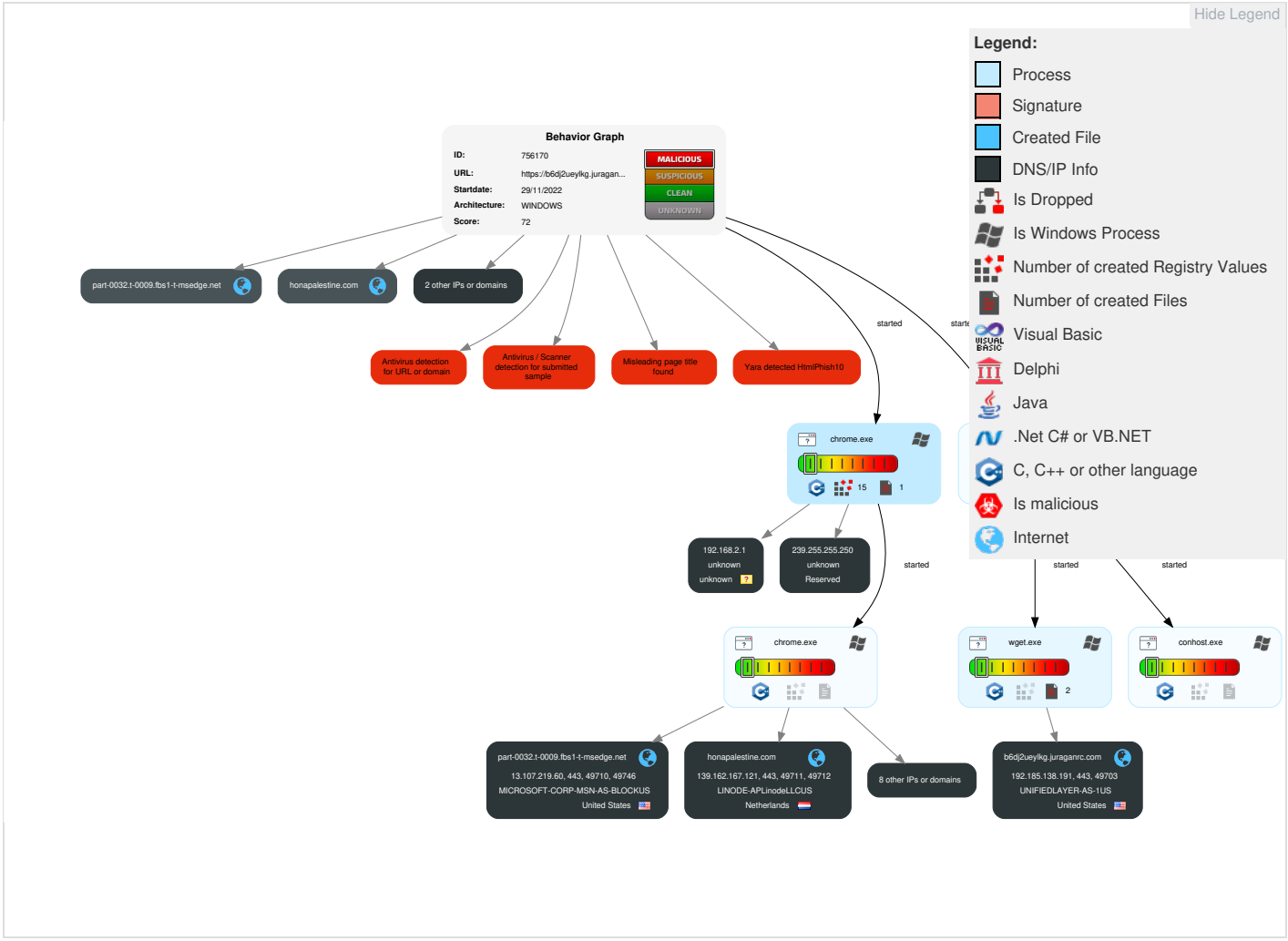
Misleading page title found

Yara detected HtmlPhish10

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
1 Drive-by Compromise	1 Command and Scripting Interpreter	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	1 2 System Information Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 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	1 Remote System Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

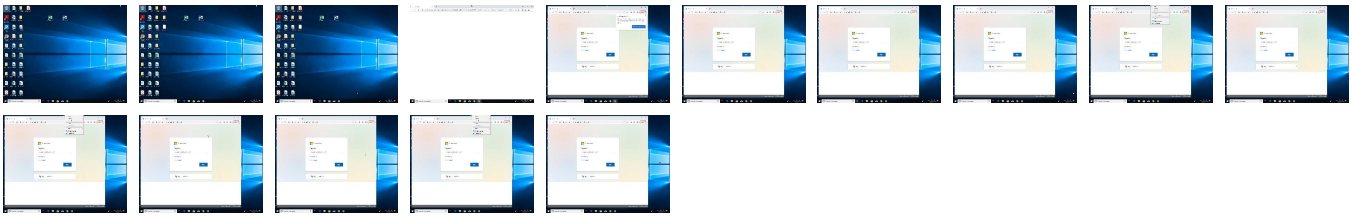
Behavior Graph

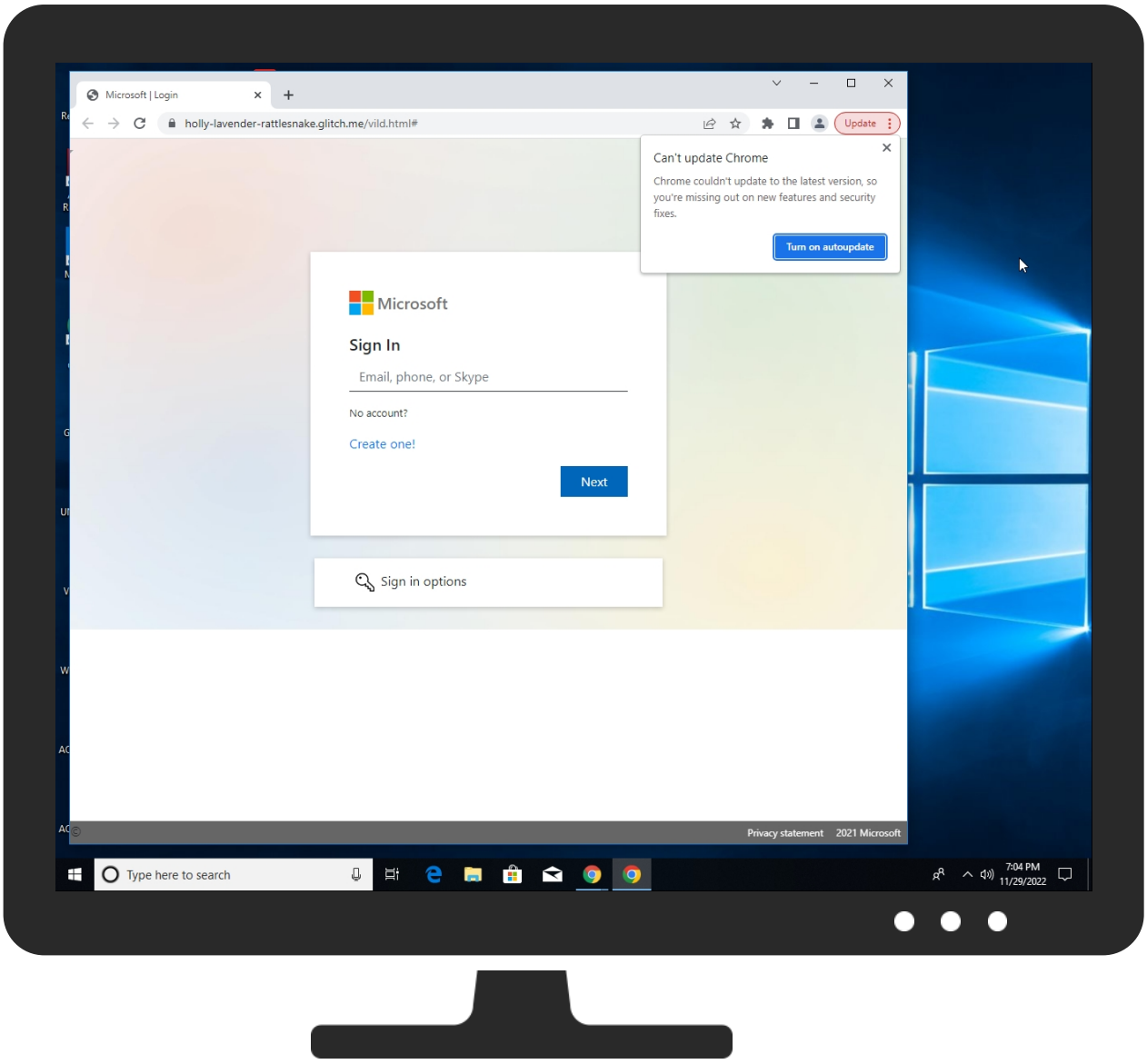


Screenshots

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://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s	0%	Virustotal		Browse
http://https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s	0%	Avira URL Cloud	safe	
http://https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://holly-lavender-rattlesnake.glitch.me/vild.html#	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://honapalestine.com/1/frontend/web/css/FrutigerLTArabic-55Roman.ttf	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/images/playstore.png	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/images/icons.png	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/index.php?/	2%	Virustotal		Browse
http://https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvd	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/images/appstore.png	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/assets/e189e3b3/js/bootstrap.js	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/images/listenlive.png	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/css/site.css	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/images/searchenglishbgar.png	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/assets/df38217b/yii.js	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/assets/493c98da/jquery.js	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/images/logo-en.png	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/images/bg.jpg	0%	Avira URL Cloud	safe	
http://https://honapalestine.com/1/frontend/web/assets/e189e3b3/css/bootstrap.css	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
holly-lavender-rattlesnake.glitch.me	44.199.49.219	true	false		high
honapalestine.com	139.162.167.121	true	false		unknown
b6dj2ueylkg.juraganrc.com	192.185.138.191	true	false		unknown
www.google.com	172.217.168.36	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
part-0032.t-0009.fbs1-t-msedge.net	13.107.219.60	true	false		unknown
clients2.google.com	unknown	unknown	false		high

Contacted URLs

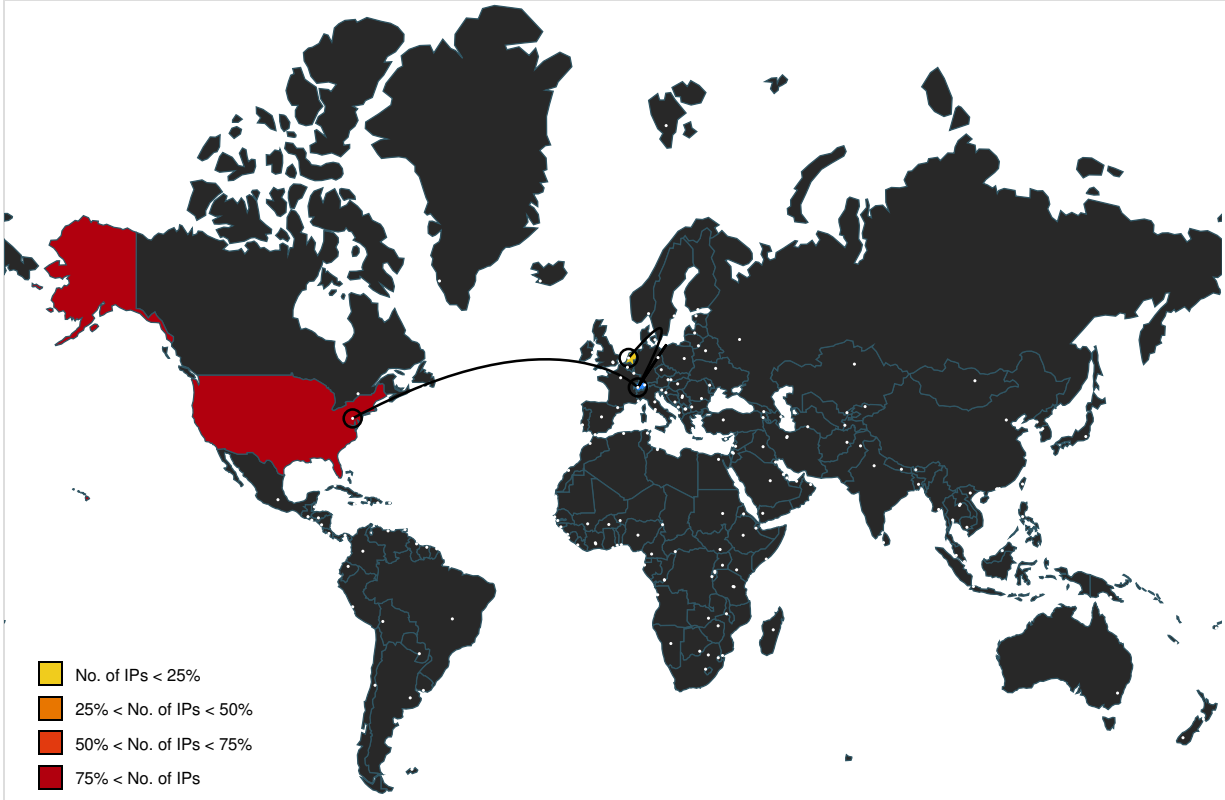
Name	Malicious	Antivirus Detection	Reputation
http://https://holly-lavender-rattlesnake.glitch.me/vild.html#	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s	true		unknown
http://https://honapalestine.com/1/frontend/web/index.php?/	false	• 2%, Virustotal, Browse	unknown
http://https://holly-lavender-rattlesnake.glitch.me/favicon.ico	false		high
http://https://honapalestine.com/1/frontend/web/css/FrutigerLTArabic-55Roman.ttf	false	• Avira URL Cloud: safe	unknown
http://https://honapalestine.com/1/frontend/web/images/icons.png	false	• Avira URL Cloud: safe	unknown
http://https://honapalestine.com/	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://honapalestine.com/1/frontend/web/images/playstore.png	false	• Avira URL Cloud: safe	unknown
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
http://https://honapalestine.com/1/frontend/web/images/appstore.png	false	• Avira URL Cloud: safe	unknown
http://https://honapalestine.com/1/frontend/web/assets/e189e3b3/js/bootstrap.js	false	• Avira URL Cloud: safe	unknown
http://https://holly-lavender-rattlesnake.glitch.me/vild.html	false		high
http://https://honapalestine.com/1/frontend/web/index.php?/	false	• 2%, Virustotal, Browse	unknown
http://https://honapalestine.com/1/frontend/web/images/listenlive.png	false	• Avira URL Cloud: safe	unknown
http://https://honapalestine.com/1/frontend/web/css/site.css	false	• Avira URL Cloud: safe	unknown
http://https://honapalestine.com/1/frontend/web/assets/df38217b/yii.js	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://honapalestine.com/1/frontend/web/images/searchenglishbgar.png	false	• Avira URL Cloud: safe	unknown
http://https://honapalestine.com/1/frontend/web/assets/493c98da/jquery.js	false	• Avira URL Cloud: safe	unknown
http://https://honapalestine.com/1/frontend/web/images/logo-en.png	false	• Avira URL Cloud: safe	unknown
http://https://honapalestine.com/1/frontend/web/images/bg.jpg	false	• Avira URL Cloud: safe	unknown
http://https://honapalestine.com/1/frontend/web/assets/e189e3b3/css/bootstrap.css	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://holly-lavender-rattlesnake.glitch.me/vild.html#	index.html@url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s.2.dr	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvd	wget.exe, 00000002.00000003.237761279.0000000002BE9000.00000004.00000800.00020000.00000000.sdmp, cmdline.out.0.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.219.60	part-0032.t-0009.fbs1-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
139.162.167.121	honapalestine.com	Netherlands		63949	LINODE-APLinodeLLCUS	false
44.199.49.219	holly-lavender-rattlesnake.glitch.me	United States		14618	AMAZON-AESUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
192.185.138.191	b6dj2ueylkg.juraganrc.com	United States		46606	UNIFIEDLAYER-AS-1US	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756170
Start date and time:	2022-11-29 19:03:59 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s
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:	16
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.phis.win@30/2@8/10
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123, 216.58.215.234, 172.217.168.74, 142.250.203.106, 172.217.168.10
- Excluded domains from analysis (whitelisted): fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, ajax.googleapis.com, aadcdnoriginwus2.azureedge.net, update.googleapis.com, clientservices.googleapis.com, aadcdnoriginwus2.afd.azureedge.net, aadcdn.msauth.net, firstparty-azurefd-prod.trafficmanager.net, global-entry-afdthirdparty-fallback.trafficmanager.net
- Execution Graph export aborted for target wget.exe, PID 5988 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.
- 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

C:\Users\user\Desktop\cmdline.out

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	793
Entropy (8bit):	5.549472422410998
Encrypted:	false
SSDEEP:	12:HFL27Rjjg1rRT1De5RhKkk1DbBKj9B27RjjgMvCrfiBKj9B27RjjgD8:9ORferJxePgJ1pW9BORfz6jEW9BORff
MD5:	03186240F0270BA8CCC373860E489805
SHA1:	6960D9433CEDFE2B3977D8BD451C927A2199E16C
SHA-256:	AE86B4EA6F9CF6366E3337D79ED12A9D7BEA0BD9C38067500F5223AF1CECAF44
SHA-512:	03B62CE1693AD364054984E955BF9DF506BE9517CF78FEC22242F49783EB2269A3475FF880ADA2B648FA6AE30B1C60027740FF732DD444B899AC7AB13A89E4FE
Malicious:	false
Reputation:	low
Preview:	--2022-11-29 19:04:46-- https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s..Resolving b6dj2ueylkg.juraganrc.com (b6dj2ueylkg.juraganrc.com)... 192.185.138.191..Connecting to b6dj2ueylkg.juraganrc.com (b6dj2ueylkg.juraganrc.com)|192.185.138.191|:443... connected...HTTP request sent, awaiting response... 200 OK..Length: unspecified [text/html]..Saving to: 'C:/Users/user/Desktop/download/index.html@url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s'.... 0K 56.9K=0.007s... .2022-11-29 19:04:47 (56.9 KB/s) - 'C:/Users/user/Desktop/download/index.html@url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s' saved [392]....

C:\Users\user\Desktop\download\index.html@url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s

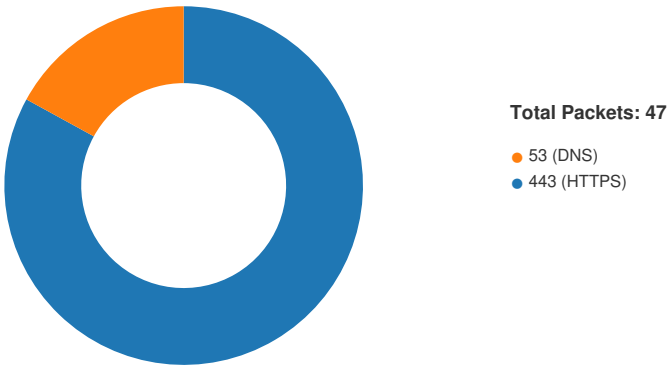
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	392
Entropy (8bit):	5.101991386762123
Encrypted:	false
SSDEEP:	6:vW4QW3tSUOj8yrUi4ePORzQZgwEABm2E3PORzQZgwuGbxBHRWVMwdwoRXfGb:OPgkTlyrUipORUZdc9ORUZqG9OMl0Gb
MD5:	848A7C7C382B42DD1206F4979DE6C2E1
SHA1:	78F46B14C6909877657AA18AAFDF2681965E0AC1
SHA-256:	37E7C3DF45AB788C21033FB290A17EFBA5C439CCA4E01F1B0A787967AA1FC491
SHA-512:	AFD4805012E8B1431D005408E4A7751D4DC59350F74B48D3DB57D336DE4A731881C9BE25EAC62E03B63E760405EED52808765A438F8ED4BAC52548E1DBF7487
Malicious:	false
Reputation:	low
Preview:	..<!DOCTYPE html>..<html>..<head>.. <title>Loading.....</title>..</head>..<meta HTTP-Equiv='refresh' content='0; URL=https://holly-lavender-rattlesnake.glitch.me/vild.html#'>..<script type='text/javascript'>..loc = 'https://holly-lavender-rattlesnake.glitch.me/vild.html#'..self.location.replace(loc);..window.location = loc;..</script>.....<body onload="Fired()">....</body>..</html>

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:04:48.526634932 CET	49703	443	192.168.2.3	192.185.138.191
Nov 29, 2022 19:04:48.526681900 CET	443	49703	192.185.138.191	192.168.2.3
Nov 29, 2022 19:04:48.526793003 CET	49703	443	192.168.2.3	192.185.138.191
Nov 29, 2022 19:04:48.529531956 CET	49703	443	192.168.2.3	192.185.138.191
Nov 29, 2022 19:04:48.529563904 CET	443	49703	192.185.138.191	192.168.2.3
Nov 29, 2022 19:04:48.801815987 CET	443	49703	192.185.138.191	192.168.2.3
Nov 29, 2022 19:04:48.802047968 CET	49703	443	192.168.2.3	192.185.138.191
Nov 29, 2022 19:04:48.806216955 CET	49703	443	192.168.2.3	192.185.138.191
Nov 29, 2022 19:04:48.806251049 CET	443	49703	192.185.138.191	192.168.2.3
Nov 29, 2022 19:04:48.807008982 CET	443	49703	192.185.138.191	192.168.2.3
Nov 29, 2022 19:04:48.809533119 CET	49703	443	192.168.2.3	192.185.138.191
Nov 29, 2022 19:04:48.809571028 CET	443	49703	192.185.138.191	192.168.2.3
Nov 29, 2022 19:04:49.070445061 CET	443	49703	192.185.138.191	192.168.2.3
Nov 29, 2022 19:04:49.070576906 CET	443	49703	192.185.138.191	192.168.2.3
Nov 29, 2022 19:04:49.070683002 CET	49703	443	192.168.2.3	192.185.138.191
Nov 29, 2022 19:04:49.353719950 CET	49703	443	192.168.2.3	192.185.138.191
Nov 29, 2022 19:04:53.489209890 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:53.489234924 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:53.489310980 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:53.490328074 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:53.490351915 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:53.490845919 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.490919113 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.490988016 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.491210938 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.491234064 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.494088888 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.494132996 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.494204044 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.494549990 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.494580030 CET	443	49707	172.217.168.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:04:53.627681017 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.628238916 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.628318071 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.629087925 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.629179955 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.630342960 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.630393028 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.630527973 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.673816919 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.673877954 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.678003073 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.678102970 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.903798103 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.903861046 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.903980017 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.903996944 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.904203892 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.904273987 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.904310942 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.904351950 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.904366016 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.904644012 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.941519976 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.941620111 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.941679955 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.941788912 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.941862106 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.947391033 CET	49706	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:04:53.947439909 CET	443	49706	142.250.203.110	192.168.2.3
Nov 29, 2022 19:04:53.960284948 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.960395098 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.960426092 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.960661888 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:53.960736036 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.962016106 CET	49707	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:04:53.962044001 CET	443	49707	172.217.168.45	192.168.2.3
Nov 29, 2022 19:04:54.012840986 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.013361931 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.013425112 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.015105963 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.015279055 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.019273043 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.019309044 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.019433022 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.019473076 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.019490004 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.107942104 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.107981920 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.207972050 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.362062931 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362123966 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362142086 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362178087 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362194061 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362206936 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362303019 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.362303019 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.362303019 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.362303019 CET	49705	443	192.168.2.3	44.199.49.219

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:04:54.362303972 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.362364054 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362406969 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362456083 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.362456083 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.362521887 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362539053 CET	443	49705	44.199.49.219	192.168.2.3
Nov 29, 2022 19:04:54.362592936 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.362615108 CET	49705	443	192.168.2.3	44.199.49.219
Nov 29, 2022 19:04:54.362628937 CET	443	49705	44.199.49.219	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:04:48.389060020 CET	57840	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:04:48.513338089 CET	53	57840	8.8.8.8	192.168.2.3
Nov 29, 2022 19:04:53.459043980 CET	52387	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:04:53.460686922 CET	56924	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:04:53.461493969 CET	60625	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:04:53.485054016 CET	53	52387	8.8.8.8	192.168.2.3
Nov 29, 2022 19:04:53.488692045 CET	53	56924	8.8.8.8	192.168.2.3
Nov 29, 2022 19:04:53.488954067 CET	53	60625	8.8.8.8	192.168.2.3
Nov 29, 2022 19:04:54.949067116 CET	52955	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:04:55.149802923 CET	53	52955	8.8.8.8	192.168.2.3
Nov 29, 2022 19:04:56.629014015 CET	55638	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:04:56.646708012 CET	53	55638	8.8.8.8	192.168.2.3
Nov 29, 2022 19:04:57.853391886 CET	65320	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:04:58.239686012 CET	53	65320	8.8.8.8	192.168.2.3
Nov 29, 2022 19:05:56.679845095 CET	53623	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:05:56.699873924 CET	53	53623	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 19:04:48.389060020 CET	192.168.2.3	8.8.8.8	0xbb75	Standard query (0)	b6dj2ueylkg.juraganrc.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:53.459043980 CET	192.168.2.3	8.8.8.8	0x3fdd	Standard query (0)	holly-lavender-rattlesnake.glitch.me	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:53.460686922 CET	192.168.2.3	8.8.8.8	0xe2	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:53.461493969 CET	192.168.2.3	8.8.8.8	0x7497	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:54.949067116 CET	192.168.2.3	8.8.8.8	0xe743	Standard query (0)	honapalestine.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:56.629014015 CET	192.168.2.3	8.8.8.8	0x4d99	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:57.853391886 CET	192.168.2.3	8.8.8.8	0xb355	Standard query (0)	honapalestine.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:05:56.679845095 CET	192.168.2.3	8.8.8.8	0xfdcb	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
Nov 29, 2022 19:04:48.513338089 CET	8.8.8.8	192.168.2.3	0xbb75	No error (0)	b6dj2ueylkg.juraganrc.com		192.185.138.191	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:53.485054016 CET	8.8.8.8	192.168.2.3	0x3fdd	No error (0)	holly-lavender-rattlesnake.glitch.me		44.199.49.219	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:53.485054016 CET	8.8.8.8	192.168.2.3	0x3fdd	No error (0)	holly-lavender-rattlesnake.glitch.me		44.196.165.201	A (IP address)	IN (0x0001)	false

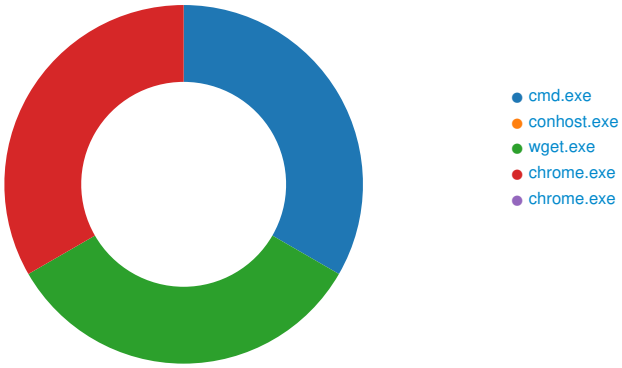
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 19:04:53.485054016 CET	8.8.8.8	192.168.2.3	0x3fdd	No error (0)	holly-lavender-rattlesnake.glitch.me		54.209.182.143	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:53.485054016 CET	8.8.8.8	192.168.2.3	0x3fdd	No error (0)	holly-lavender-rattlesnake.glitch.me		52.4.141.177	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:53.488692045 CET	8.8.8.8	192.168.2.3	0xe2	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:04:53.488692045 CET	8.8.8.8	192.168.2.3	0xe2	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:53.488954067 CET	8.8.8.8	192.168.2.3	0x7497	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:55.109987974 CET	8.8.8.8	192.168.2.3	0x388f	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:04:55.109987974 CET	8.8.8.8	192.168.2.3	0x388f	No error (0)	dual.part-0032.t-0009.fbs1-t-msedge.net	part-0032.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:04:55.109987974 CET	8.8.8.8	192.168.2.3	0x388f	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:55.109987974 CET	8.8.8.8	192.168.2.3	0x388f	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:55.149802923 CET	8.8.8.8	192.168.2.3	0xe743	No error (0)	honapalestine.com		139.162.167.121	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:56.646708012 CET	8.8.8.8	192.168.2.3	0x4d99	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:58.239686012 CET	8.8.8.8	192.168.2.3	0xb355	No error (0)	honapalestine.com		139.162.167.121	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:59.261404991 CET	8.8.8.8	192.168.2.3	0xc690	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:04:59.261404991 CET	8.8.8.8	192.168.2.3	0xc690	No error (0)	dual.part-0032.t-0009.fbs1-t-msedge.net	part-0032.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:04:59.261404991 CET	8.8.8.8	192.168.2.3	0xc690	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:04:59.261404991 CET	8.8.8.8	192.168.2.3	0xc690	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:05:56.699873924 CET	8.8.8.8	192.168.2.3	0xfdcb	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- b6dj2ueylkg.juraganrc.com
- accounts.google.com
- clients2.google.com
- holly-lavender-rattlesnake.glitch.me
- https:
  - aadcdn.msauth.net
  - honapalestine.com

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: **6032**, Parent PID: **416**

General

Target ID:	0
Start time:	19:04:46
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s" > cmdline.out 2>&1
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: conhost.exe PID: **6012**, Parent PID: **6032**

General

Target ID:	1
Start time:	19:04:46
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

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

Analysis Process: wget.exe PID: 5988, Parent PID: 6032

General

Target ID:	2
Start time:	19:04:46
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\wget.exe
Wow64 process (32bit):	true
Commandline:	wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://b6dj2ueylkg.juraganrc.com/?url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s"
Imagebase:	0x400000
File size:	3895184 bytes
MD5 hash:	3DADB6E2ECE9C4B3E1E322E617658B60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\index.html@url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	46596C	fopen

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 5132, Parent PID: 3452

General

Target ID:	3
Start time:	19:04:49
Start date:	29/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\download\index.html@url=aHR0cHM6Ly9ob2xseS1sYXZlbmRlci1yYXR0bGVzbmFrZS5nbGl0Y2gubWUvdmlsZC5odG1s.html
Imagebase:	0x7ff614650000
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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF6146AA143	RegSetValueExW

Analysis Process: chrome.exe PID: **2288**, Parent PID: **5132**

General

Target ID:	4
Start time:	19:04:50
Start date:	29/11/2022
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=1944 --field-trial-handle=1616,i,5292400896411780733,13825633785752334259,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly