ID: 715086
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 16:07:27
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

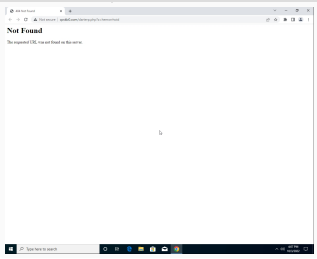
Windows Analysis Report

http://www.cpskb0.com/darterp.php?z=hemorrhoid

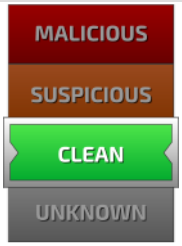
Overview

General Information

Sample URL:	http://www.cpskb0.com/darterp.php?z=hemorrhoid
Analysis ID:	715086
Infos:	



Detection

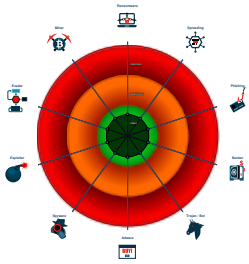


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

No high impact signatures.

Classification



Analysis Advice

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Some HTTP requests failed (404). It is likely that the sample will exhibit less behavior.

Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 6000 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://www.cpskb0.com/darterp.php?z=hemorrhoid MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 2312 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=2036 --field-trial-handle=1824,i,11055943044610990432,15687841212519678928,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

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.

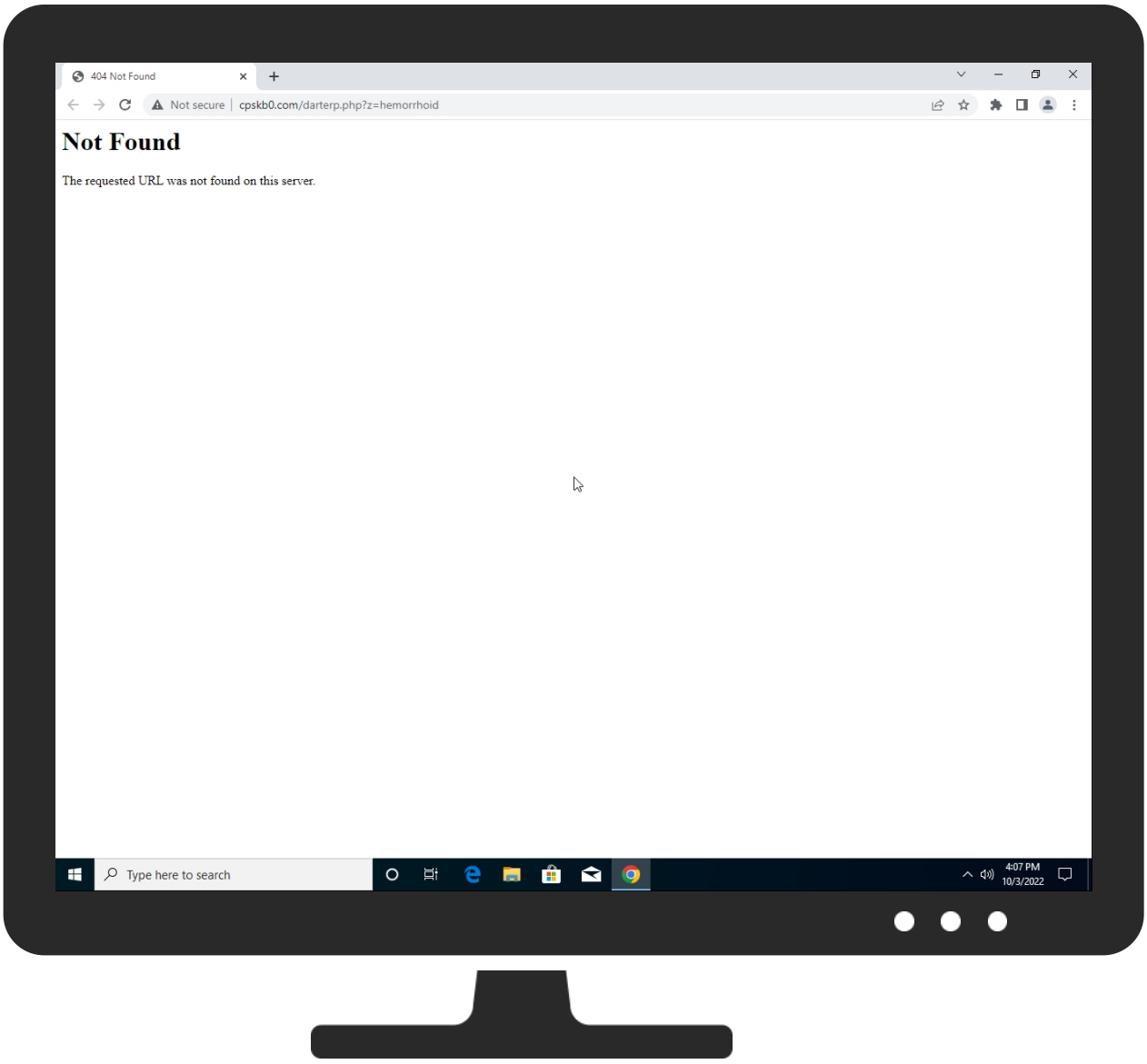
Mitre Att&ck Matrix

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	2 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	3 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	4 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

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://www.cpskb0.com/darterp.php?z=hemorrhoid	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.cpskb0.com/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

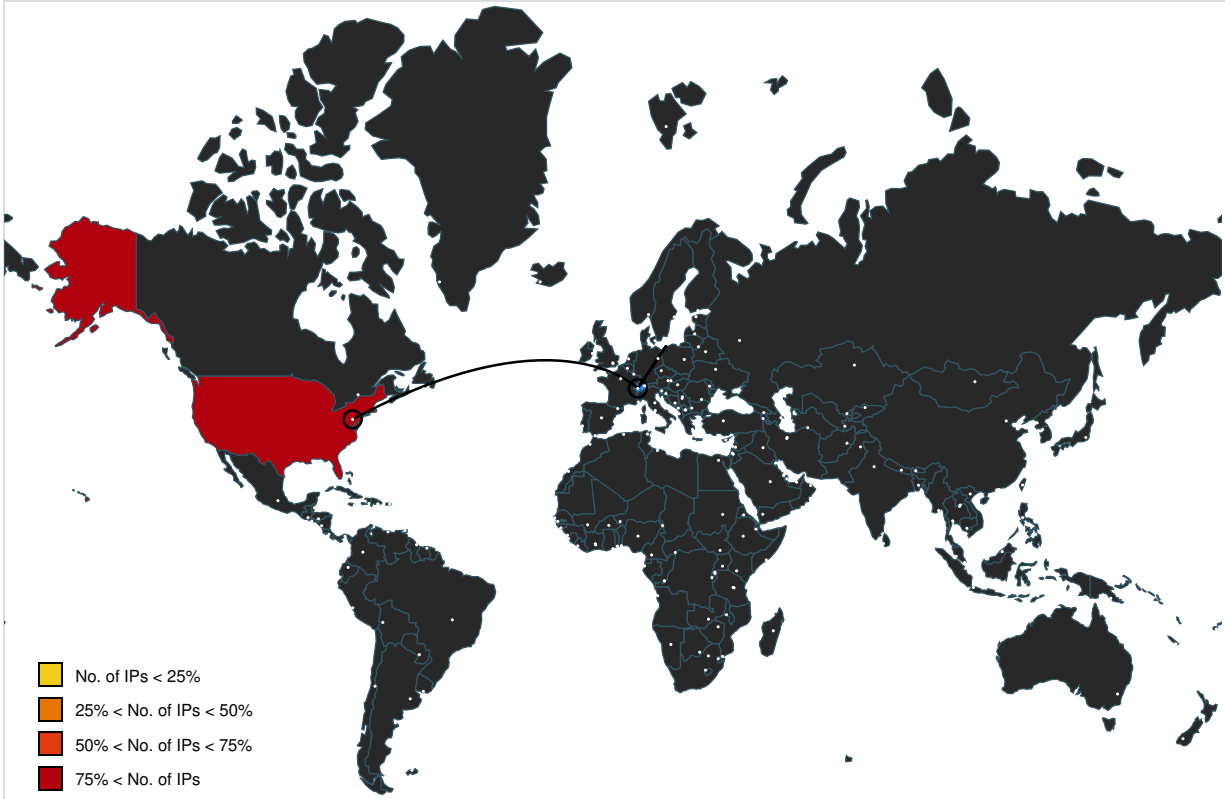
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.185.109	true	false		high
www.cpskb0.com	104.233.253.189	true	false		unknown
www.google.com	172.217.16.132	true	false		high
clients.l.google.com	142.250.186.110	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.cpskb0.com/darterp.php?z=hemorrhoid	false		unknown
http://www.cpskb0.com/darterp.php?z=hemorrhoid	false		unknown
http://www.cpskb0.com/favicon.ico	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.109	accounts.google.com	United States		15169	GOOGLEUS	false
104.233.253.189	www.cpskb0.com	United States		137443	ANCHGLOBAL-AS-APAnchnetAsiaLimitedHK	false
142.250.186.68	unknown	United States		15169	GOOGLEUS	false
142.250.186.35	unknown	United States		15169	GOOGLEUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.195	unknown	United States		15169	GOOGLEUS	false
142.250.186.110	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.132	unknown	United States		15169	GOOGLEUS	false

Private

IP

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715086
Start date and time:	2022-10-03 16:07:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://www.cpskb0.com/darterp.php?z=hemorrhoid
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	12
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@25/0@5/111

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe
- Excluded IPs from analysis (whitelisted): 20.190.159.75, 40.126.31.69, 20.190.159.68, 40.126.31.67, 20.190.159.4, 40.126.31.73, 20.190.159.71, 20.190.159.64, 142.250.185.195, 34.104.35.123
- Excluded domains from analysis (whitelisted): fs.microsoft.com, prda.aadg.msidentity.com, edgedl.me.gvt1.com, slscr.update.microsoft.com, login.live.com, ctldl.windowsupdate.com, clientservices.googleapis.com, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Created / dropped Files

No created / dropped files found

Static File Info

No static file info