ID: 756241
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 21:33:28
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

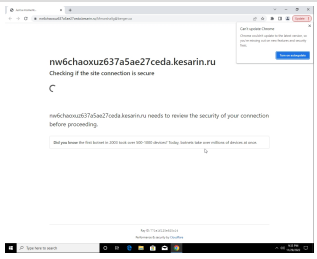
Windows Analysis Report

https://tmsnp.page.link/?link=https%3A%2F%2Fbonsalpaint.com%2Fnicas%2F%3Fe%3Dmarshallg%..

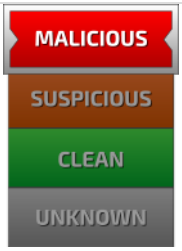
Overview

General Information

Sample URL:	https://tmsnp.page.link/?link=https%3A%2F%2Fbonsalpaint.com%2Fnicas%2F%3Fe%3Dmarshallg%40berger.ca
Analysis ID:	756241



Detection



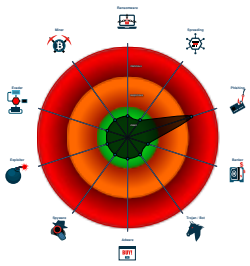
HTMLPhisher

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- HTML body contains low number of ...
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 6792 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://tmsnp.page.link/?link=https%3A%2F%2Fbonsalpaint.com%2Fnicas%2F%3Fe%3Dmarshallg%40berger.ca MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6964 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=1808,i,2143788816404629539,6530415847919180823,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
06625.5.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

Phishing

Yara detected HtmlPhish10

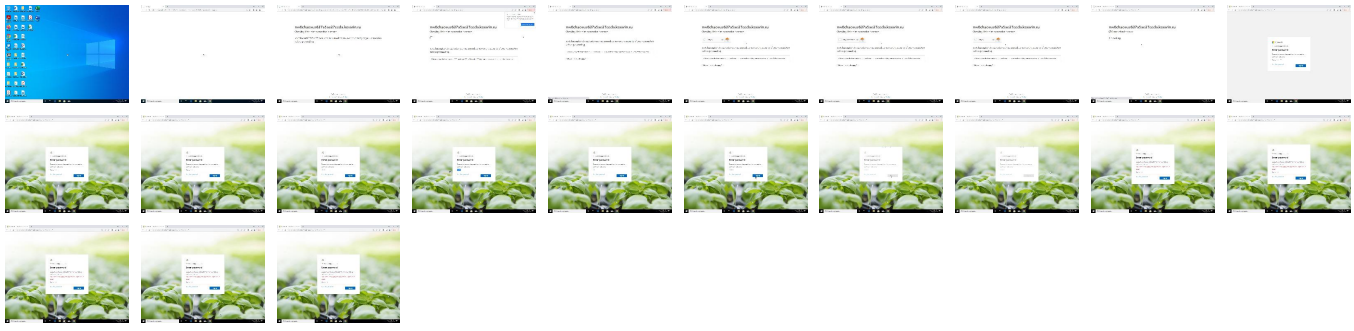
Mitre Att&ck Matrix

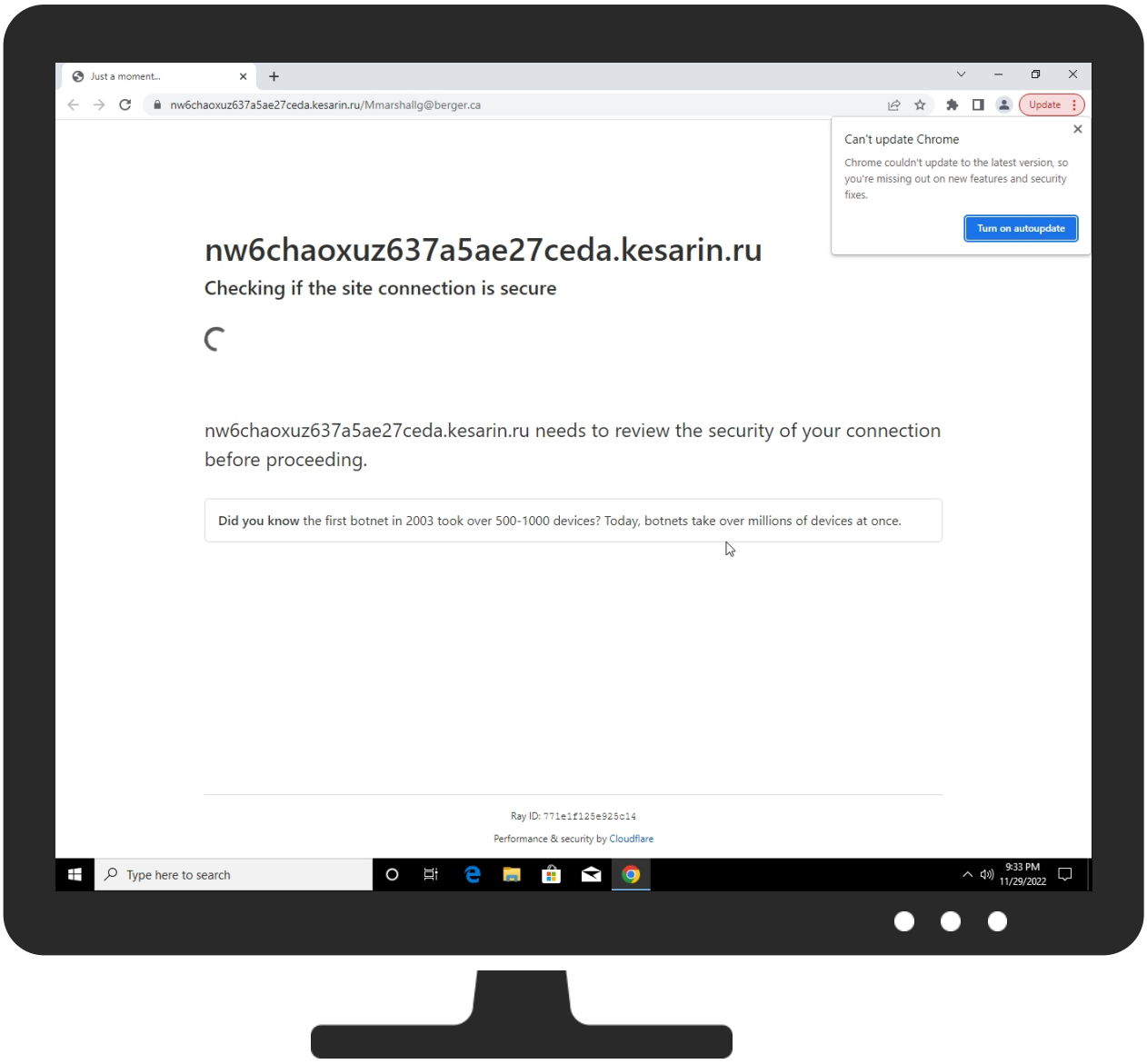
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	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	1 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	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

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
https://tmsnp.page.link/?link=https%3A%2F%2Fbonsalpaint.com%2Fnicas%2F%3Fe%3Dmarshallg%40berger.ca	0%	Avira URL Cloud	safe	
https://tmsnp.page.link/?link=https%3A%2F%2Fbonsalpaint.com%2Fnicas%2F%3Fe%3Dmarshallg%40berger.ca	1%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

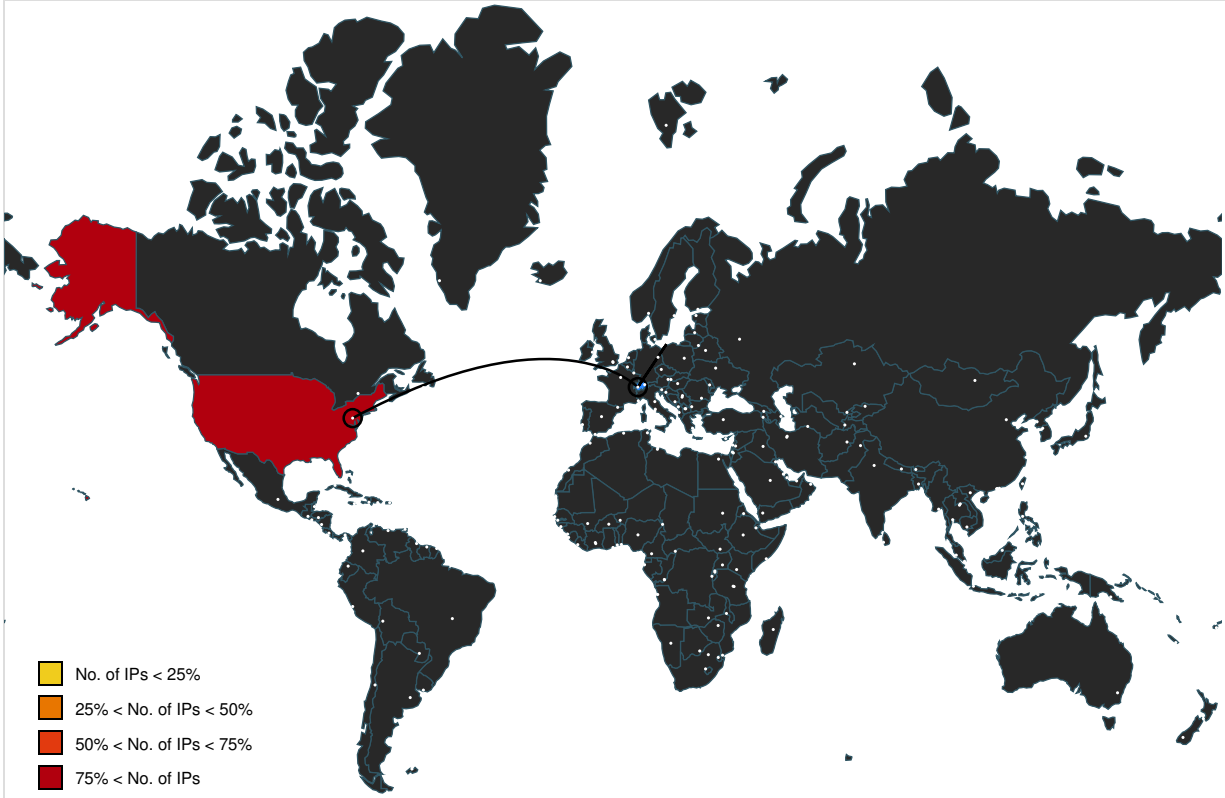
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bonsalpaint.com	67.222.136.231	true	false		unknown
tmsnp.page.link	142.250.184.225	true	false		unknown
a.nel.cloudflare.com	35.190.80.1	true	false		high
accounts.google.com	142.250.186.45	true	false		high
challenges.cloudflare.com	104.18.7.185	true	false		high
www.google.com	142.250.185.196	true	false		high
clients.l.google.com	172.217.23.110	true	false		high
unpkg.com	104.16.125.175	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
cloudflare.hcaptcha.com	104.18.19.132	true	false		unknown
nw6chaoxuz637a5ae27ceda.kesarin.ru	104.21.72.10	true	false		unknown
aadcdn.msauthimages.net	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://nw6chaoxuz637a5ae27ceda.kesarin.ru/Mmarshallg@berger.ca	false		unknown
https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/wjk86/0x4AAAAAAAAjq6WYeRDKmebM/light/normal	false		high
https://nw6chaoxuz637a5ae27ceda.kesarin.ru/PS-63866cc2c5621	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.45	accounts.google.com	United States		15169	GOOGLEUS	false
104.18.19.132	cloudflare.hcaptcha.com	United States		13335	CLOUDFLARENETUS	false
142.250.74.202	unknown	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.7.185	challenges.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
142.250.185.227	unknown	United States		15169	GOOGLEUS	false
104.16.125.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
172.217.23.110	clients.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
67.222.136.231	bonsalpaint.com	United States		393398	ASN-DISUS	false
142.250.184.225	tmsnp.page.link	United States		15169	GOOGLEUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
104.21.72.10	nw6chaoxuz637a5ae27ceda.kesarin.ru	United States		13335	CLOUDFLARENETUS	false
172.217.16.132	unknown	United States		15169	GOOGLEUS	false
142.250.74.195	unknown	United States		15169	GOOGLEUS	false
172.217.18.100	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756241
Start date and time:	2022-11-29 21:33:28 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://tmsnp.page.link/?link=https%3A%2F%2Fbonsalpaint.com%2Fnicas%2F%3Fe%3Dmarshallg%40berger.ca
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:	10
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:	MAL
Classification:	mal48.phis.win@24/0@16/124

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe
- Excluded IPs from analysis (whitelisted): 142.250.185.227, 34.104.35.123, 142.250.74.202, 172.217.23.106, 216.58.212.170, 142.250.184.234, 142.250.185.170, 142.250.186.106, 142.250.185.138, 142.250.184.202, 172.217.18.106, 142.250.185.234, 142.250.185.74, 142.250.185.202, 142.250.186.74, 142.250.185.106, 172.217.16.202, 142.250.186.170
- Excluded domains from analysis (whitelisted): fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, login.live.com, slscr.update.microsoft.com, aadcdn.azureedge.net, aadcdn.ec.azureedge.net, ctldl.windowsupdate.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Created / dropped Files

No created / dropped files found

Static File Info

No static file info