

JOeSandbox Cloud BASIC



ID: 715076

Cookbook:

defaultwindowsinteractivecookbook.jbs

Time: 15:59:09

Date: 03/10/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report https://smilodon-bat-m9ct.squarespace.com/	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	4
AV Detection	4
Mitre Att&ck Matrix	4
Screenshots	4
Thumbnails	4
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	6
Contacted Domains	6
Contacted URLs	6
World Map of Contacted IPs	6
Public IPs	6
Private	7
General Information	7
Warnings	7
Created / dropped Files	7
Static File Info	7

Windows Analysis Report

https://smilodon-bat-m9ct.squarespace.com/

Overview

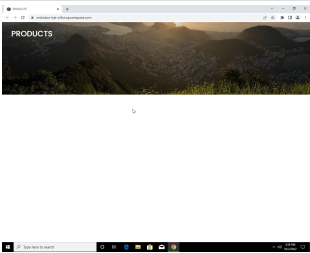
General Information

Sample URL:

https://smilodon-bat-m9ct.squarespace.com/

Analysis ID:

715076



Detection

MALICIOUS

SUSPICIOUS

CLEAN

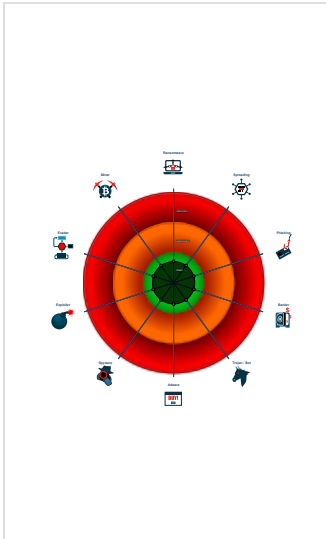
UNKNOWN

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

Signatures

Antivirus / Scanner detection for sub...

Classification



Process Tree

- System is w10x64_ra
- chrome.exe (PID: 2340 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://smilodon-bat-m9ct.squarespace.com/ MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
 - chrome.exe (PID: 4180 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=2044 --field-trial-handle=1744,i,6067084562247289383,4305548710663750486,131072 --disable-features=Optimizati onGuideModelDownloading,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

AV Detection



Antivirus / Scanner detection for submitted sample

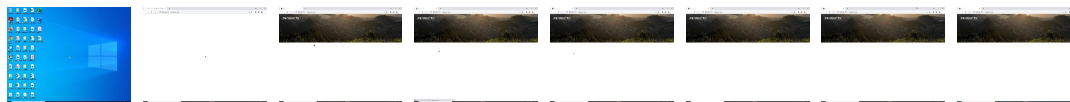
Mitre Att&ck Matrix

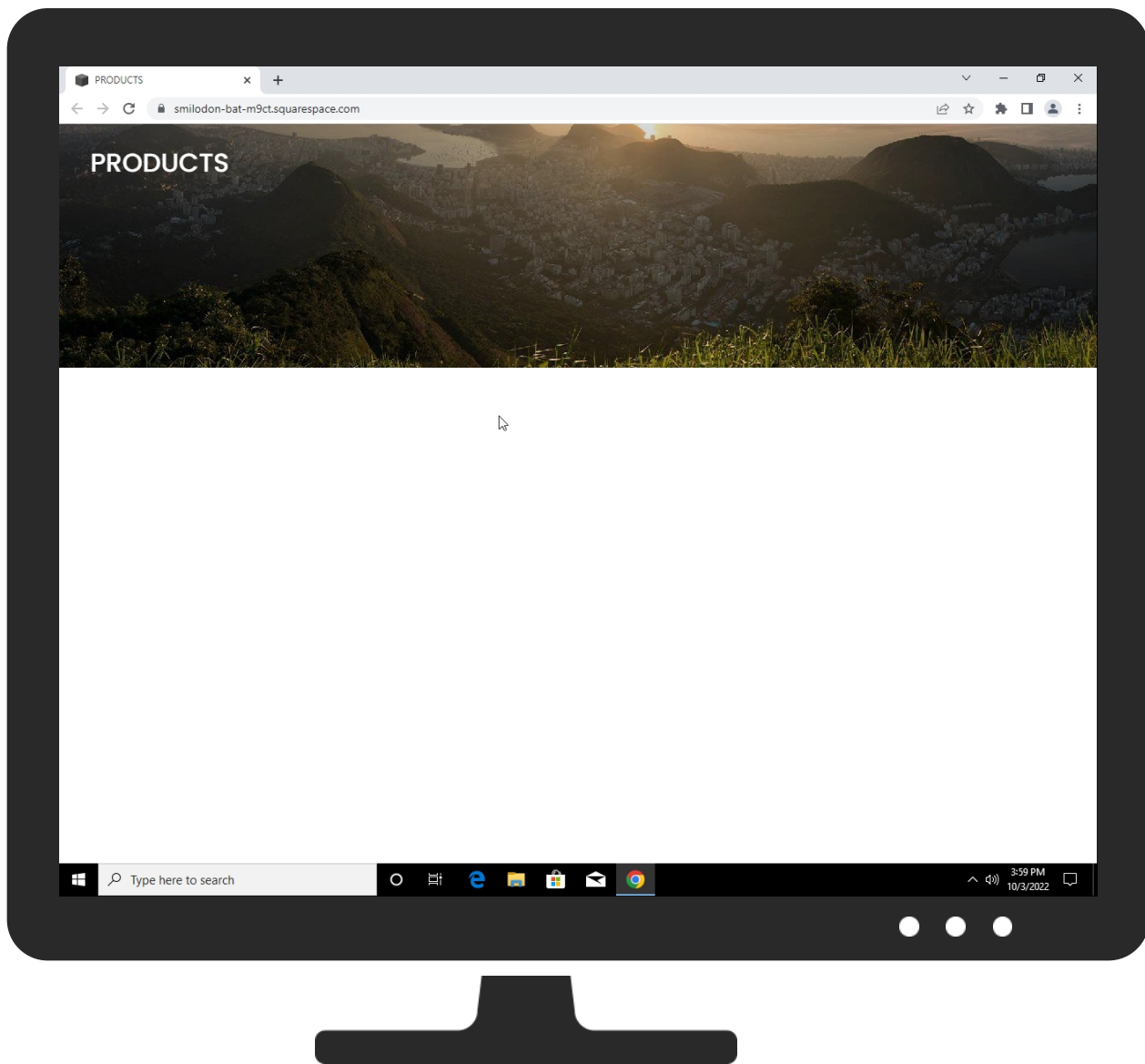
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	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://smilodon-bat-m9ct.squarespace.com/	0%	Virustotal		Browse
https://smilodon-bat-m9ct.squarespace.com/	100%	Avira URL Cloud	phishing	

Dropped Files

⊘ No Antivirus matches

Unpacked PE Files

⊘ No Antivirus matches

Domains

⊘ No Antivirus matches

URLs

⊘ No Antivirus matches

Domains and IPs

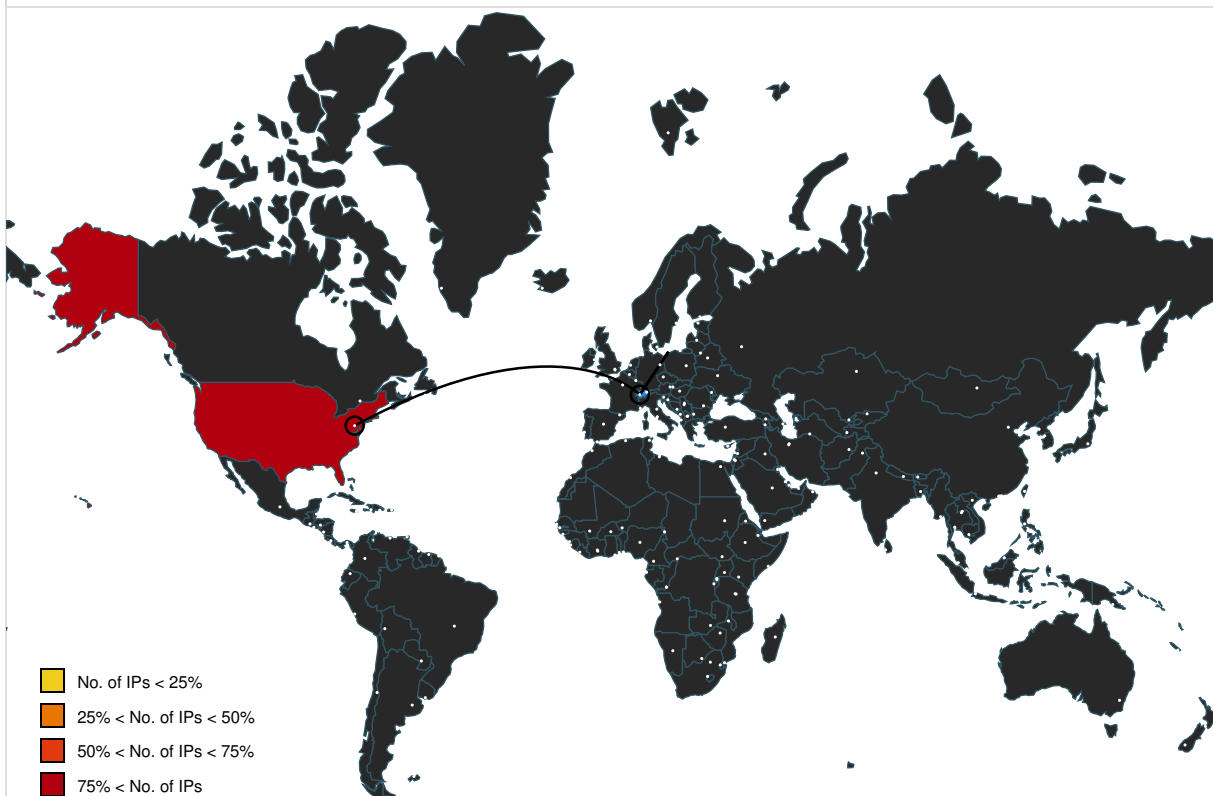
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.184.237	true	false		high
static.squarespace.map.fastly.net	151.101.0.237	true	false		unknown
www.google.com	142.250.74.196	true	false		high
smilodon-bat-m9ct.squarespace.com	198.185.159.177	true	false		high
clients.l.google.com	172.217.18.14	true	false		high
squarespace.map.fastly.net	151.101.192.238	true	false		unknown
prod.squarespace.map.fastly.net	151.101.0.238	true	false		unknown
clients2.google.com	unknown	unknown	false		high
images.squarespace-cdn.com	unknown	unknown	false		unknown
assets.squarespace.com	unknown	unknown	false		high
static1.squarespace.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://smilodon-bat-m9ct.squarespace.com/	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
151.101.192.238	squarespace.map.fastly.net	United States		54113	FASTLYUS	false
172.217.18.14	clients.l.google.com	United States		15169	GOOGLEUS	false
151.101.0.237	static.squarespace.map.fastly.net	United States		54113	FASTLYUS	false
151.101.0.238	prod.squarespace.map.fastly.net	United States		54113	FASTLYUS	false
142.251.36.10	unknown	United States		15169	GOOGLEUS	false
198.185.159.177	smilodon-bat-m9ct.squarespace.com	United States		53831	SQUARESPACEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved	🇵🇸	unknown	unknown	false
142.250.185.131	unknown	United States	🇺🇸	15169	GOOGLEUS	false
142.250.185.195	unknown	United States	🇺🇸	15169	GOOGLEUS	false
142.250.184.237	accounts.google.com	United States	🇺🇸	15169	GOOGLEUS	false
142.250.186.132	unknown	United States	🇺🇸	15169	GOOGLEUS	false
142.250.184.227	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:	715076
Start date and time:	2022-10-03 15:59:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://smilodon-bat-m9ct.squarespace.com/
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:	MAL
Classification:	mal48.win@22/0@10/114

Warnings
- Exclude process from analysis (whitelisted): SIHClient.exe - Excluded IPs from analysis (whitelisted): 40.126.31.67, 40.126.31.71, 20.190.159.4, 40.126.31.73, 20.190.159.64, 20.190.159.75, 20.190.159.0, 20.190.159.23, 142.250.185.195, 142.250.136.10, 34.104.35.123, 142.250.184.195, 142.250.185.131 - Excluded domains from analysis (whitelisted): fonts.googleapis.com, fs.microsoft.com, prda.aadg.msidentity.com, edgedl.me.gvt1.com, slscr.update.microsoft.com, login.live.com, font.s.gstatic.com, www.tm.lg.prod.aadmsa.akadns.net, ctldl.windowsupdate.com, clientservices.googleapis.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net - 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