MALICIOUS

Classifications: Phishing

Threat Names: -

Verdict Reason: -

Sample Type	**HTML Document**
File Name	**Advice Ref Priority payment Customer RefSep19092023.htm**
ID	#8861751
MD5	76ddcf9746b2bf27799893a802842ed0
SHA1	fe3af38e966497a285d8108a9b66c5096e3db632
SHA256	9b0a1e902ca833c6c9adf6fdd3cd0e1f30e232ba439fcafc5fe0fcd6087527c6
File Size	251.81 KB
Report Created	2023-09-19 19:13 (UTC+2)
Target Environment	win10_64_th2_en_web | web_root

OVERVIEW

VMRay Threat Identifiers (5 rules, 6 matches)

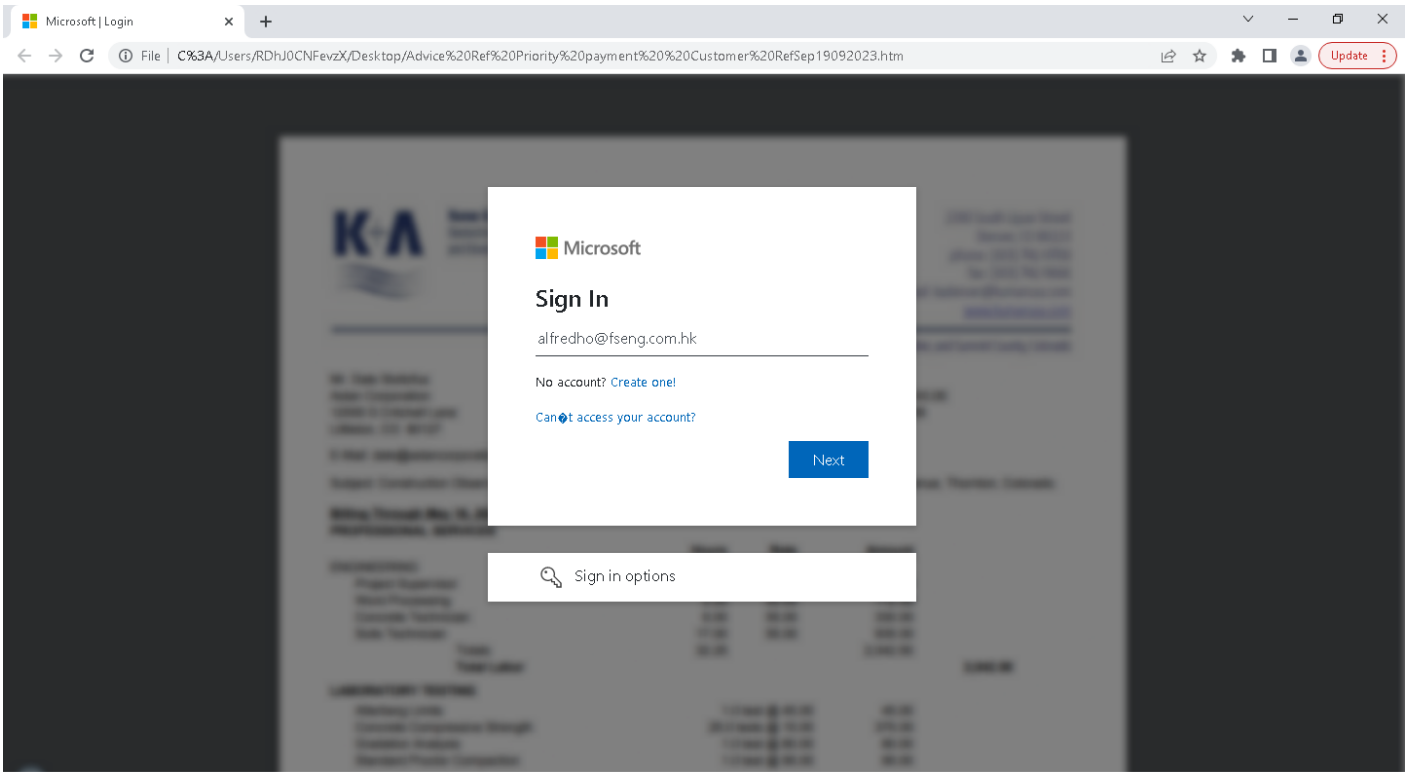
Score	Category	Operation	Count	Classification
5/5	Heuristics	Combination of other detections indicates a phishing website	1	Phishing
	• Heuristics determined that the page is a phishing website, based on combination of other detections.			
4/5	Machine Learning	Phishing page detected	1	Phishing
	• Phishing attempt detected by ML module (Osprey).			
3/5	Heuristics	Page contains a Microsoft logon form	1	-
	• Page contains a Microsoft logon form.			
2/5	Heuristics	The HTML file contains logon form.	1	-
	• Initial HTML file contains a logon form.			
1/5	Heuristics	Page presents itself as a logon page	2	-
	• Page title indicates it is a logon page. • Page contains a logon form.			

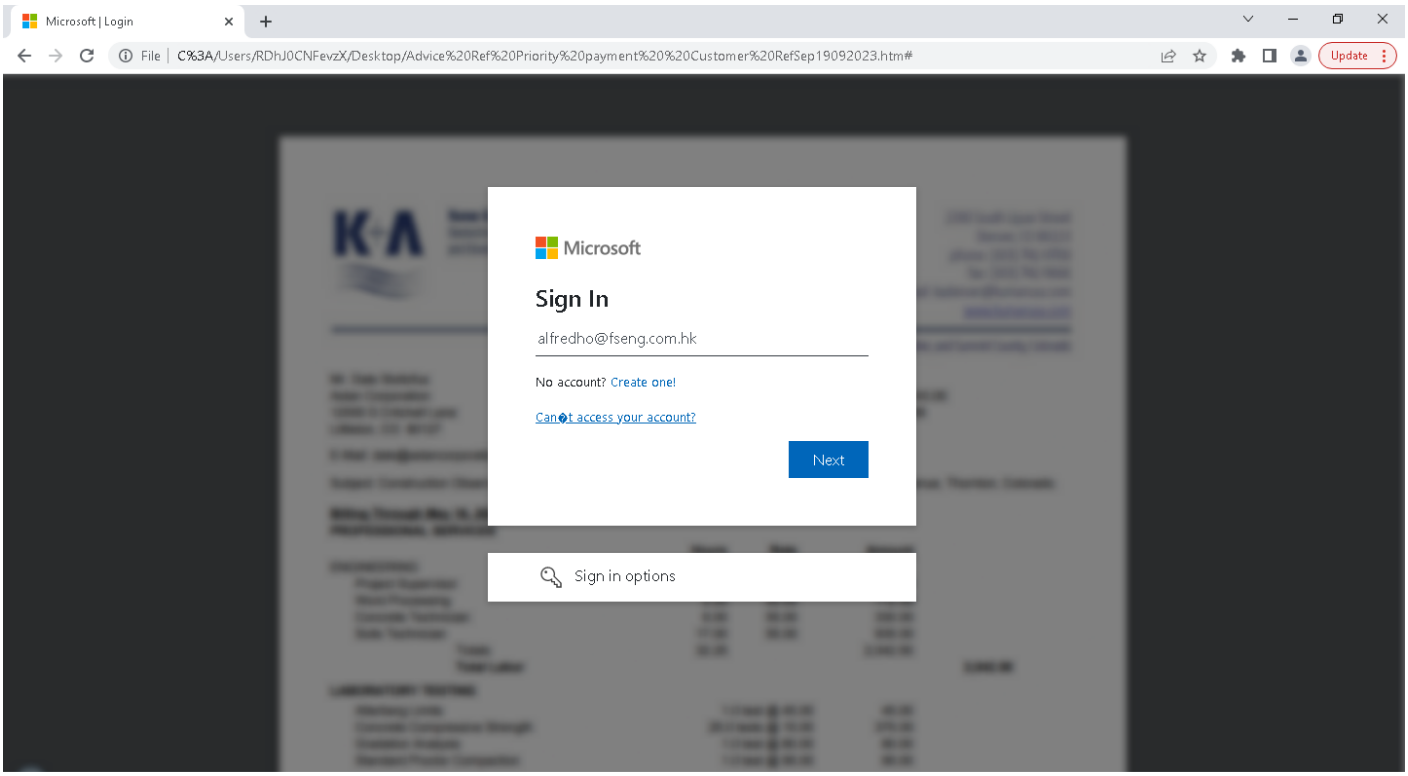
Sample Information

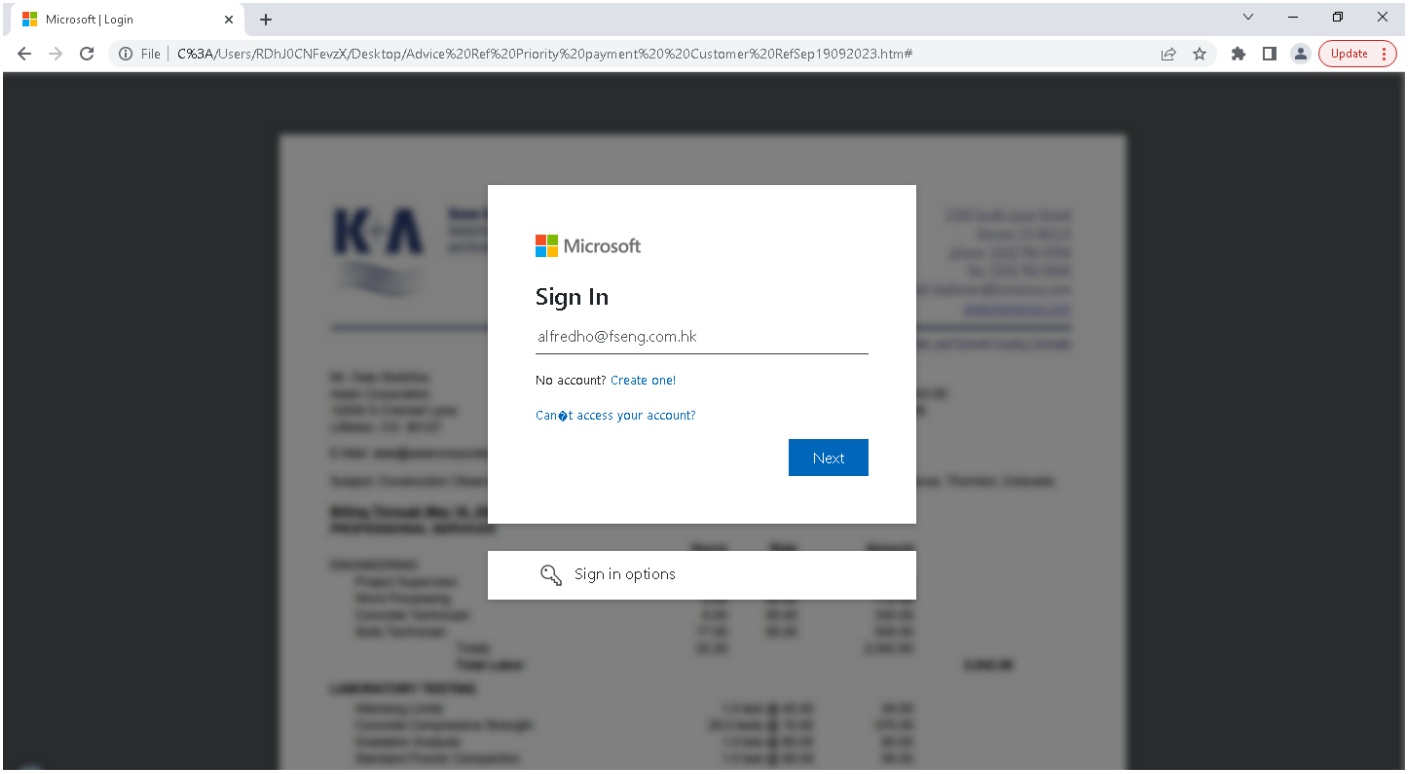
ID	#8861751
MD5	76ddcf9746b2bf27799893a802842ed0
SHA1	fe3af38e966497a285d8108a9b66c5096e3db632
SHA256	9b0a1e902ca833c6c9adf6fdd3cd0e1f30e232ba439fcafc5fe0fcd6087527c6
SSDeep	6144:fV16hqFDCkcKuPJQa0w9vm1dFrM9XikDaNELw:bLFeXKGKa0w9vWF44ke2Lw
File Name	Advice Ref Priority payment Customer RefSep19092023.htm
File Size	251.81 KB
Sample Type	HTML Document
Has Macros	✔

Analysis Information

Creation Time	2023-09-19 19:13 (UTC+2)
Analysis Duration	00:01:11
Termination Reason	No Recent or Pending Activity
Number of Monitored Processes	0
Execution Successful	True
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Microsoft | Login
File | C%3A/Users/RDhJ0CNFevzX/Desktop/Advice%20Ref%20Priority%20payment%20%20Customer%20RefSep19092023.htm
Update
Microsoft
Sign In
alfredho@fseng.com.hk
No account? Create one!
Can't access your account?
Next
Sign in options
Terms of use
Privacy & cookies


Microsoft | Login
File | C%3A/Users/RDhJ0CNFevzX/Desktop/Advice%20Ref%20Priority%20payment%20%20Customer%20RefSep19092023.htm#
Update
Microsoft
Sign In
alfredho@fseng.com.hk
No account? Create one!
Can't access your account?
Next
Sign in options
/C%3A/Users/.../Advice Ref Priority payment Customer RefSep19092023.htm
Terms of use
Privacy & cookies


Microsoft | Login
File | C%3A/Users/RDhJ0CNFevzX/Desktop/Advice%20Ref%20Priority%20payment%20%20Customer%20RefSep19092023.htm#
Update
Microsoft
Sign In
alfredho@fseng.com.hk
No account? Create one!
Can't access your account?
Next
Sign in options
Terms of use
Privacy & cookies
...

NETWORK

General

22.10 KB total sent

257.84 KB total received

2 ports 443, 53

8 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

16 DNS requests for 8 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

12 URLs contacted, 9 servers

7 sessions, 25.03 KB sent, 548.71 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://cdnjs[.]cloudflare[.]com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	-	-	-	0 bytes	CLEAN
GET	hxxps://ajax[.]googleapis[.]com/ajax/libs/jquery/2.2.4/jquery.min.js	-	-	-	0 bytes	CLEAN
GET	hxxps://maxcdn[.]bootstrapcdn[.]com/bootstrap/4.0.0/css/bootstrap.min.css	-	-	-	0 bytes	CLEAN
GET	hxxps://maxcdn[.]bootstrapcdn[.]com/bootstrap/4.0.0/js/bootstrap.min.js	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]office[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://use[.]fontawesome[.]com/releases/v5.7.0/css/all.css	-	-	-	0 bytes	CLEAN
GET	hxxps://fonts[.]googleapis[.]com/css?family=Archivo+Narrow&display=swap	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]google[.]com/s2/favicons?domain=microsoft.com	-	-	-	0 bytes	CLEAN
GET	hxxps://logincdn[.]msauth[.]net/shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg	-	-	-	0 bytes	CLEAN
GET	hxxps://code[.]jquery[.]com/jquery-3.3.1.js	-	-	-	0 bytes	CLEAN
GET	hxxps://code[.]jquery[.]com/jquery-3.1.1.min.js	-	-	-	0 bytes	CLEAN
GET	hxxps://code[.]jquery[.]com/jquery-3.2.1.slim.min.js	-	-	-	0 bytes	CLEAN
GET	hxxps://t1[.]gstatic[.]com/faviconV2?client=SOCIAL&type=FAVICON&fallback_opts=TYPE,SIZE,URL&url=http://microsoft.com&size=16	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	ajax[.]googleapis[.]com	NO_ERROR	-	-	CLEAN

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	cdnjs[.]cloudflare[.]com	NO_ERROR	104.17.25.14, 104.17.24.14	-	CLEAN
UNKNOWN	logincdn[.]msauth[.]net, lgincdn[.]trafficmanager[.]net, lgincdnvzeuno[.]azureedge[.]net, lgincdnvzeuno[.]ec[.]azureedge[.]net, cs1227[.]wpc[.]alphacdn[.]net	NO_ERROR	-	lgincdn[.]trafficmanager[.]net, lgincdnvzeuno[.]azureedge[.]net, lgincdnvzeuno[.]ec[.]azureedge[.]net, cs1227[.]wpc[.]alphacdn[.]net	CLEAN
UNKNOWN	code[.]jquery[.]com	NO_ERROR	-	-	CLEAN
UNKNOWN	t1[.]gstatic[.]com	NO_ERROR	-	-	CLEAN
A	maxcdn[.]bootstrapcdn[.]com	NO_ERROR	104.18.10.207, 104.18.11.207	-	CLEAN
UNKNOWN	fonts[.]googleapis[.]com	NO_ERROR	-	-	CLEAN
UNKNOWN	use[.]fontawesome[.]com, use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	NO_ERROR	-	use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	CLEAN

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9b0a1e902ca833c6c9adf6fdd3cd0e1f30e232ba439fcafc5fe0fcd6087527c6	C:\Users\RDhJ0CNFevzX\Desktop\Advice Ref Priority payment Customer RefSep19092023.htm, Advice Ref Priority payment Customer RefSep19092023.htm	Sample File	251.81 KB	text/html	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\Advice Ref Priority payment Customer RefSep19092023.htm	Sample File	-	MALICIOUS
Advice Ref Priority payment Customer RefSep19092023.htm	Sample File	-	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\images\success.PNG	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Advice Ref Priority payment Customer RefSep19092023.htm#	Miscellaneous File	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://maxcdn[.]bootstrapcdn[.]com/bootstrap/4.0.0/js/bootstrap.min.js	Extracted, Contacted	104.18.10.207, 104.18.11.207	-	GET	CLEAN
hxxps://www[.]office[.]com	Extracted	-	-	-	CLEAN
hxxps://logincdn[.]msauth[.]net/shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg	Extracted, Contacted	192.229.221.185	United States	GET	CLEAN
hxxps://cdnjs[.]cloudflare[.]com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	Extracted, Contacted	104.17.24.14, 104.17.25.14	-	GET	CLEAN
hxxps://t1[.]gstatic[.]com/faviconV2?client=SOCIAL&type=FAVICON&fallback_opts=TYPE,SIZE,URL&url=http://microsoft.com&size=16	Extracted, Contacted	142.250.181.228	United States	GET	CLEAN
hxxps://maxcdn[.]bootstrapcdn[.]com/bootstrap/4.0.0/css/bootstrap.min.css	Extracted, Contacted	104.18.10.207, 104.18.11.207	-	GET	CLEAN
hxxps://ajax[.]googleapis[.]com/ajax/libs/jquery/2.2.4/jquery.min.js	Extracted, Contacted	142.250.185.74	-	GET	CLEAN
hxxps://code[.]jquery[.]com/jquery-3.1.1.min.js	Extracted, Contacted	151.101.194.137, 151.101.130.137, 151.101.66.137, 151.101.2.137	United States	GET	CLEAN
hxxps://www[.]google[.]com/s2/favicons?domain=microsoft.com	Extracted, Contacted	142.250.185.164	United States	GET	CLEAN
hxxps://code[.]jquery[.]com/jquery-3.2.1.slim.min.js	Extracted, Contacted	151.101.194.137, 151.101.130.137, 151.101.66.137, 151.101.2.137	United States	GET	CLEAN
hxxps://use[.]fontawesome[.]com/releases/v5.7.0/css/all.css	Extracted, Contacted	172.64.103.11, 172.64.102.11	United States	GET	CLEAN
hxxps://fonts[.]googleapis[.]com/css?family=Archivo+Narrow&display=swap	Extracted, Contacted	142.250.186.42	-	GET	CLEAN
hxxps://code[.]jquery[.]com/jquery-3.3.1.js	Extracted, Contacted	151.101.194.137, 151.101.130.137, 151.101.66.137, 151.101.2.137	United States	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
logincdn[.]trafficmanager[.]net	192.229.221.185	United States	TCP, DNS, HTTPS	CLEAN

Domain	IP Address	Country	Protocols	Verdict
code[.]jquery[.]com	151.101.194.137, 151.101.130.137, 151.101.66.137, 151.101.2.137	United States	TCP, DNS, TLS, HTTPS	CLEAN
lgincdnvzeuno[.]azureedge[.]net	192.229.221.185	United States	TCP, DNS, HTTPS	CLEAN
maxcdn[.]bootstrapcdn[.]com	104.18.10.207, 104.18.11.207	-	TCP, DNS, UDP, HTTPS	CLEAN
www[.]google[.]com	142.250.185.164	United States	TCP, DNS, TLS, HTTPS, UDP	CLEAN
www[.]office[.]com	-	-	-	CLEAN
fonts[.]googleapis[.]com	142.250.186.42	-	DNS	CLEAN
cs1227[.]wpc[.]alphacdn[.]net	192.229.221.185	United States	TCP, DNS, HTTPS	CLEAN
lgincdnvzeuno[.]ec[.]azureedge[.]net	192.229.221.185	United States	TCP, DNS, HTTPS	CLEAN
ajax[.]googleapis[.]com	142.250.185.74	-	DNS	CLEAN
use[.]fontawesome[.]com	172.64.103.11, 172.64.102.11	United States	TCP, DNS, HTTPS	CLEAN
logincdn[.]msauth[.]net	192.229.221.185	United States	TCP, DNS, HTTPS	CLEAN
t1[.]gstatic[.]com	142.250.181.228	United States	TCP, DNS, HTTPS	CLEAN
cdnjs[.]cloudflare[.]com	104.17.24.14, 104.17.25.14	-	TCP, DNS, HTTPS	CLEAN
use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	172.64.103.11, 172.64.102.11	United States	TCP, DNS, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
172.64.103.11	use[.]fontawesome[.]com, use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	United States	DNS	CLEAN
151.101.194.137	code[.]jquery[.]com	United States	DNS	CLEAN
172.64.102.11	use[.]fontawesome[.]com, use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	United States	TCP, DNS, HTTPS	CLEAN
104.18.11.207	maxcdn[.]bootstrapcdn[.]com	-	DNS	CLEAN
104.17.24.14	cdnjs[.]cloudflare[.]com	-	DNS	CLEAN
104.18.10.207	maxcdn[.]bootstrapcdn[.]com	-	TCP, DNS, UDP, HTTPS	CLEAN
142.250.181.228	t1[.]gstatic[.]com	United States	TCP, DNS, HTTPS	CLEAN
142.250.185.164	www[.]google[.]com	United States	TCP, DNS, TLS, HTTPS, UDP	CLEAN
151.101.130.137	code[.]jquery[.]com	United States	TCP, DNS, TLS, HTTPS	CLEAN
192.229.221.185	lgincdnvzeuno[.]azureedge[.]net, logincdn[.]msauth[.]net, cs1227[.]wpc[.]alphacdn[.]net, lgincdnvzeuno[.]ec[.]azureedge[.]net, lgincdn[.]trafficmanager[.]net	United States	TCP, DNS, HTTPS	CLEAN
104.17.25.14	cdnjs[.]cloudflare[.]com	-	TCP, DNS, HTTPS	CLEAN
151.101.66.137	code[.]jquery[.]com	United States	DNS	CLEAN
151.101.2.137	code[.]jquery[.]com	United States	DNS	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_web
Description	win10_64_th2_en_web
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2023.3.1
Web Engine Version	1.5.0 / 07/17/2023 04:23
Static Engine Version	2023.3.1.0 / 2023-07-17 03:00:15
AV Exceptions Version	2023.3.1.2 / 2023-07-01 17:20:29
ML Detection Models Version	2023.3.1.18 / 2023-08-10 15:33:22
Link Detonation Heuristics Version	2023.3.1.24 / 2023-08-31 16:59:16
Signature Trust Store Version	2023.3.1.2 / 2023-07-01 17:20:29
VMRay Threat Identifiers Version	2023.3.1.32 / 2023-09-11 09:59:25
Web Engine Auto UI Rules Version	2023.3.1.24 / 2023-08-31 16:59:16
YARA Built-in Ruleset Version	2023.3.1.24

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	Not installed
Microsoft Office Version	Not installed
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	106.0.5249.119
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows