MALICIOUS

Classifications: Phishing

Threat Names: -

Verdict Reason: -

Sample Type	URL
File Name	**hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html**
ID	#10636114
MD5	15593b64d263eda2a910ea0338050d11
SHA1	b3b82443a95915791ea9ead99b3f64a8cb58a32f
SHA256	73c6d9f166d83269bd1b608f3f1704715d779e1332573adc5b563a7ab5d0d57e
File Size	60 bytes
Report Created	2024-06-13 12:03 (UTC)
Target Environment	windows 10 (64bit TH2 -EN- WEB_ANALYSIS) | web_root

OVERVIEW

VMRay Threat Identifiers (11 rules, 13 matches)

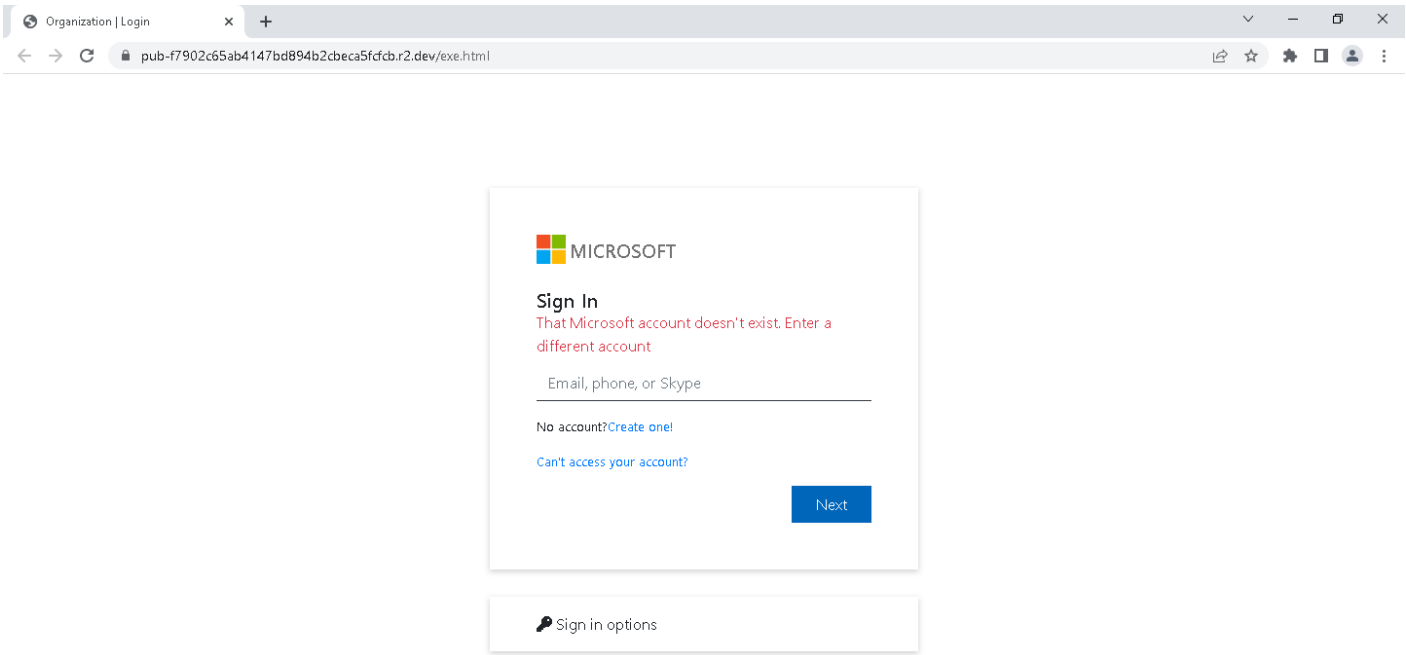
Score	Category	Operation	Count	Classification
5/5	Heuristics	Combination of other detections indicates a phishing website	1	Phishing
	• Heuristics determined that the page is a phishing website, based on combination of other detections.			
4/5	Reputation	Malicious host or URL detected via reputation	2	-
	• Submitted URL "hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html" is a known malicious URL and was reported as "Phishing". • Contacted URL "hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/favicon.ico" is a known malicious URL and was reported as "Phishing".			
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 hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html contains a Microsoft logon form.			
3/5	Machine Learning	Highly suspicious page detected	1	-
	• ML module (StingRay) detects the page to be highly suspicious.			
2/5	Heuristics	Page is served from a service commonly used for temporary hosting	1	-
	• Page at hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html served from Cloudflare Pages.			
2/5	Heuristics	Page secured via a Domain Validated SSL certificate	1	-
	• Host pub-f7902c65ab4147bd894b2cbeca5fcfcb.r2.dev uses DV certificate issued by Let's Encrypt to *.r2.dev.			
1/5	Heuristics	Resource is loaded from a service commonly used for temporary hosting	1	-
	• Resource at hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/favicon.ico loaded from Cloudflare Pages.			
1/5	Heuristics	Page presents itself as a logon page	2	-
	• Page title of hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html indicates it is a logon page. • Page hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html contains a logon form.			
1/5	Heuristics	Page contents are loaded dynamically	1	-
	• The contents the page hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html are loaded dynamically via JavaScript.			
1/5	Masquerade	Page contains Microsoft copyright text	1	-
	• Page https://pub-f7902c65ab4147bd894b2cbeca5fcfcb.r2.dev/exe.html contains a Microsoft copyright text.			

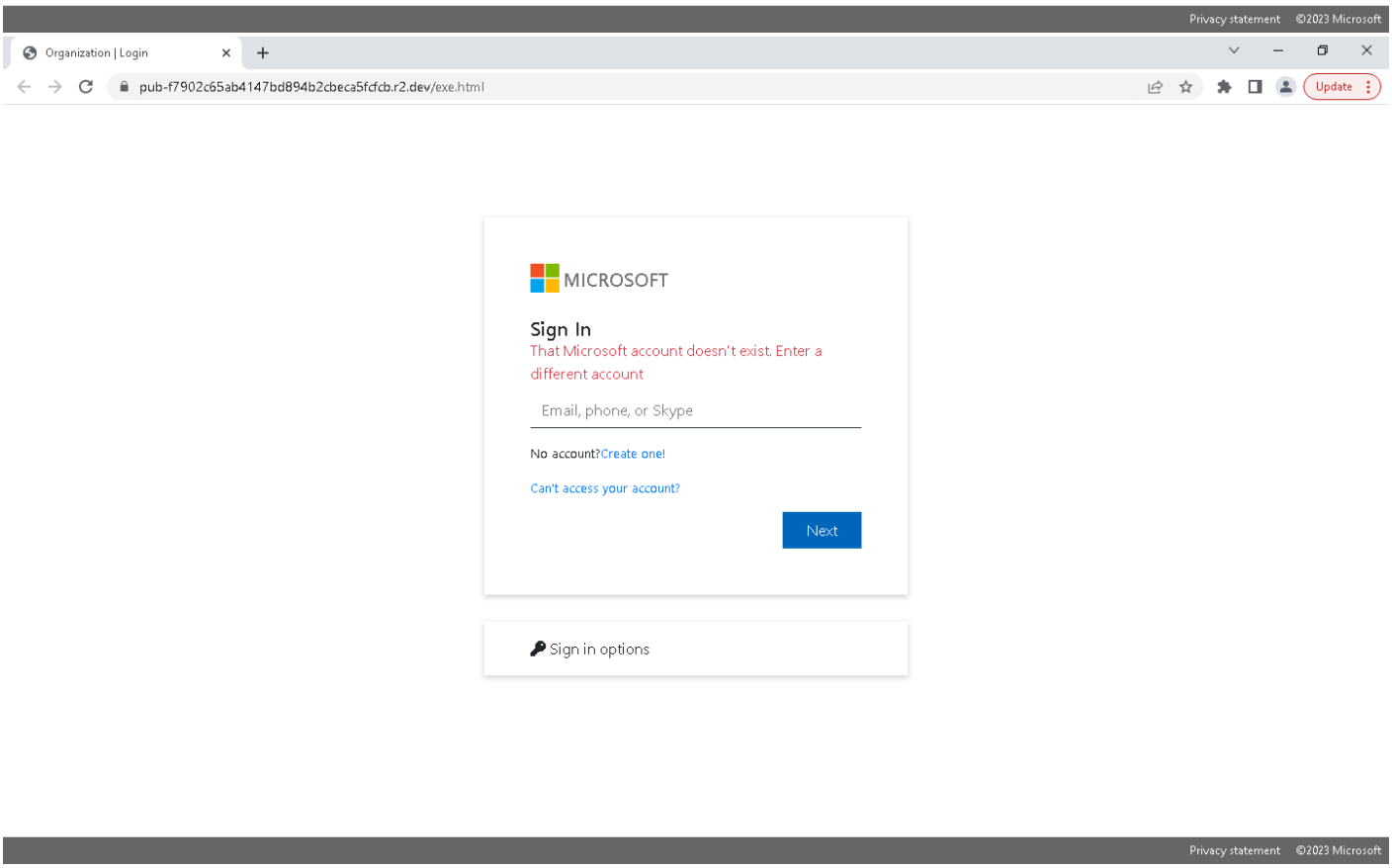
Sample Information

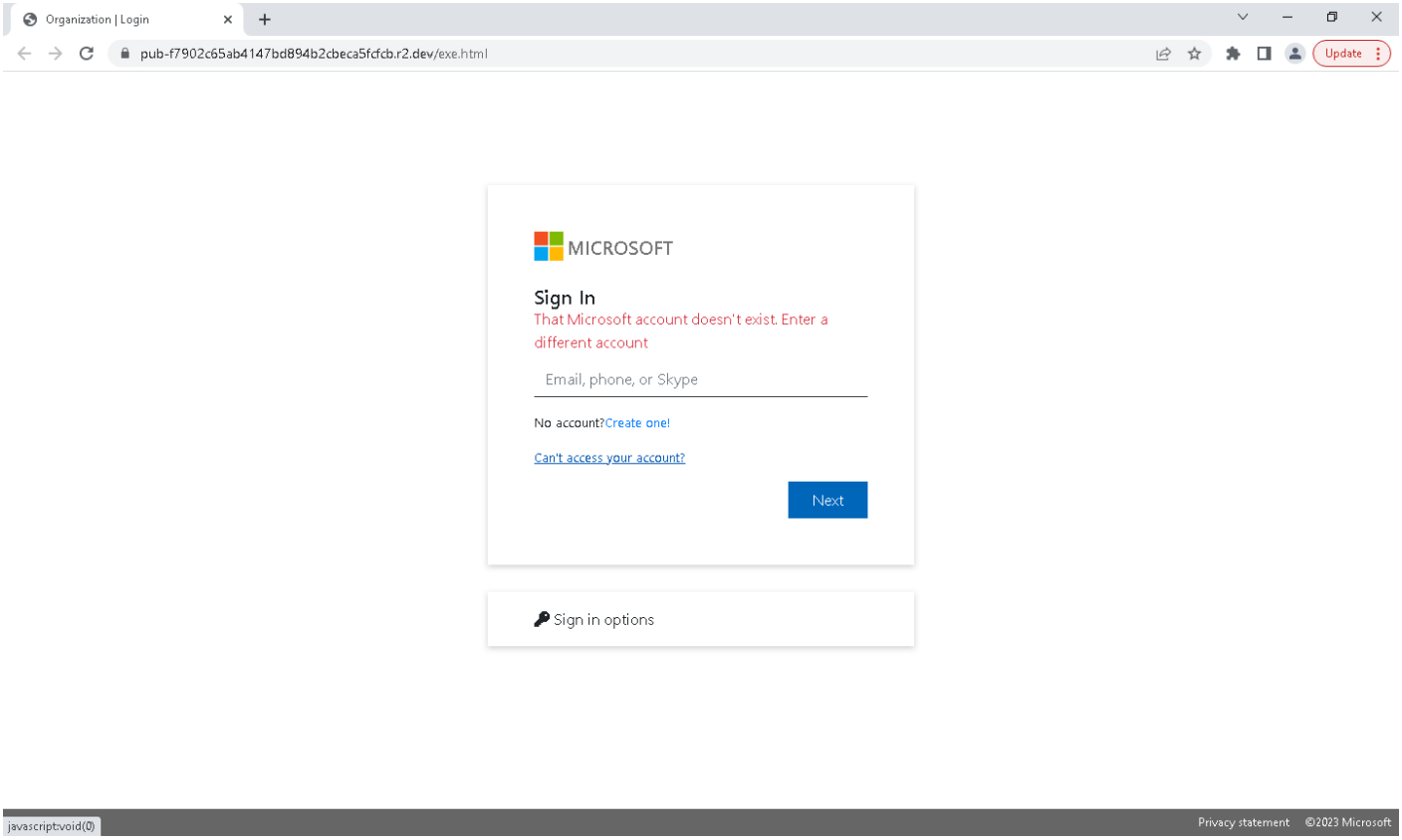
ID	#10636114
MD5	15593b64d263eda2a910ea0338050d11
SHA1	b3b82443a95915791ea9ead99b3f64a8cb58a32f
SHA256	73c6d9f166d83269bd1b608f3f1704715d779e1332573adc5b563a7ab5d0d57e
SSDeep	3:N8UeNWNy0HBKGH4QDfHLVAGzR0:2UeNcaGxuGzG
File Name	hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html
File Size	60 bytes
Sample Type	URL
Has Macros	✔

Analysis Information

Creation Time	2024-06-13 12:03 (UTC)
Analysis Duration	00:00:31
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


Organization | Login
pub-f7902c65ab4147bd894b2cbeca5fcfcb.r2.dev/exe.html
MICROSOFT
Sign In
That Microsoft account doesn't exist. Enter a different account
Email, phone, or Skype
No account?Create one!
Can't access your account?
Next
Sign in options


Privacy statement ©2023 Microsoft
Organization | Login
pub-f7902c65ab4147bd894b2cbeca5fcfcb.r2.dev/exe.html
Update
MICROSOFT
Sign In
That Microsoft account doesn't exist. Enter a different account
Email, phone, or Skype
No account?Create one!
Can't access your account?
Next
Sign in options
Privacy statement ©2023 Microsoft


Organization | Login
pub-f7902c65ab4147bd894b2cbeca5fcfcb.r2.dev/exe.html
Update
MICROSOFT
Sign In
That Microsoft account doesn't exist. Enter a different account
Email, phone, or Skype
No account?Create one!
Can't access your account?
Next
Sign in options
javascript:void(0)
Privacy statement
©2023 Microsoft

NETWORK

General

19.27 KB total sent

832.96 KB total received

2 ports 443, 53

9 contacted IP addresses

0 URLs extracted

0 files downloaded

1 malicious hosts detected

DNS

9 DNS requests for 9 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

11 URLs contacted, 9 servers

8 sessions, 20.47 KB sent, 403.10 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://aadcdn[.]msauth[.]net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	-	-	-	0 bytes	CLEAN
GET	hxxps://todosec[.]org/images/bg.jpg	-	-	-	0 bytes	CLEAN
GET	hxxps://api[.]ipify[.]org/?format=json	-	-	-	0 bytes	CLEAN
GET	hxxps://use[.]fontawesome[.]com/releases/v5.7.0/webfonts/fa-solid-900.woff2	-	-	-	0 bytes	CLEAN
GET	hxxps://use[.]fontawesome[.]com/releases/v5.7.0/css/all.css	-	-	-	0 bytes	CLEAN
GET	hxxps://code[.]jquery[.]com/jquery-3.6.0.min.js	-	-	-	0 bytes	CLEAN
GET	hxxps://fonts[.]googleapis[.]com/css?family=Archivo+Narrow&display=swap	-	-	-	0 bytes	CLEAN
GET	hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/favicon.ico	-	-	-	0 bytes	MALICIOUS
GET	hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html	-	-	-	0 bytes	MALICIOUS
GET	hxxps://maxcdn[.]bootstrapcdn[.]com/bootstrap/4.0.0/js/bootstrap.min.js	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	aadcdn[.]msauth[.]net, aadcdnoriginwus2[.]azureedge[.]net, aadcdnoriginwus2[.]afd[.]azureedge[.]net, firstparty-azurefd-prod[.]tra... ...zurefd-t-fb-prod[.]trafficmanager[.]net, dual[.]s-part-0017[.]t-0009[.]fb-t-msedge[.]net, s-part-0017[.]t-0009[.]fb-t-msedge[.]net	NO_ERROR	13.107.253.45	aadcdnoriginwus2[.]azureedge[.]net, aadcdnoriginwus2[.]afd[.]azureedge[.]net, firstparty-azurefd-prod[.]trafficmanager[.]net, shed... ...zurefd-t-fb-prod[.]trafficmanager[.]net, dual[.]s-part-0017[.]t-0009[.]fb-t-msedge[.]net, s-part-0017[.]t-0009[.]fb-t-msedge[.]net	CLEAN
A	code[.]jquery[.]com	NO_ERROR	151.101.66.137, 151.101.2.137, 151.101.194.137, 151.101.130.137	-	CLEAN
A	api[.]ipify[.]org	NO_ERROR	104.26.12.205, 172.67.74.152, 104.26.13.205	-	CLEAN
A	pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev	NO_ERROR	104.18.2.35, 104.18.3.35	-	CLEAN
A	todosec[.]org	NO_ERROR	103.224.212.213	-	CLEAN
A	maxcdn[.]bootstrapcdn[.]com	NO_ERROR	104.18.11.207, 104.18.10.207	-	CLEAN
A	fonts[.]googleapis[.]com	NO_ERROR	-	-	CLEAN
A	cdnjs[.]cloudflare[.]com	NO_ERROR	104.17.25.14, 104.17.24.14	-	CLEAN
A	use[.]fontawesome[.]com, use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	NO_ERROR	104.21.27.152, 172.67.142.245	use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	CLEAN

ARTIFACTS

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/exe.html	Sample, Contacted	104.18.2.35, 104.18.3.35	-	GET	MALICIOUS
hxxps://pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev/favicon.ico	Contacted	104.18.2.35, 104.18.3.35	-	GET	MALICIOUS
hxxps://fonts[.]googleapis[.]com/css?family=Archivo+Narrow&display=swap	Contacted	-	-	GET	CLEAN
hxxps://use[.]fontawesome[.]com/releases/v5.7.0/css/all.css	Contacted	172.67.142.245, 104.21.27.152	-	GET	CLEAN
hxxps://code[.]jquery[.]com/jquery-3.6.0.min.js	Contacted	151.101.130.137, 151.101.194.137, 151.101.66.137, 151.101.2.137	United States	GET	CLEAN
hxxps://aadcdn[.]msauth[.]net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	Contacted	13.107.253.45	United States	GET	CLEAN
hxxps://cdnjs[.]cloudflare[.]com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	Contacted	104.17.25.14, 104.17.24.14	-	GET	CLEAN
hxxps://maxcdn[.]bootstrapcdn[.]com/bootstrap/4.0.0/js/bootstrap.min.js	Contacted	104.18.11.207, 104.18.10.207	-	GET	CLEAN
hxxps://todosec[.]org/images/bg.jpg	Contacted	103.224.212.213	Australia	GET	CLEAN
hxxps://use[.]fontawesome[.]com/releases/v5.7.0/webfonts/fa-solid-900.woff2	Contacted	172.67.142.245, 104.21.27.152	-	GET	CLEAN
hxxps://api[.]ipify[.]org/?format=json	Contacted	104.26.13.205, 104.26.12.205, 172.67.74.152	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev	104.18.2.35, 104.18.3.35	-	HTTPS, TLS, DNS, TCP	CLEAN
fonts[.]googleapis[.]com	-	-	-	CLEAN
use[.]fontawesome[.]com	172.67.142.245, 104.21.27.152	-	HTTPS, TCP, UDP, TLS, DNS	CLEAN
use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	172.67.142.245, 104.21.27.152	-	HTTPS, TCP, UDP, TLS, DNS	CLEAN
code[.]jquery[.]com	151.101.130.137, 151.101.194.137, 151.101.66.137, 151.101.2.137	United States	HTTPS, DNS, TCP	CLEAN
aadcdn[.]msauth[.]net	13.107.253.45	United States	HTTPS, DNS, TCP	CLEAN
aadcdnoriginwus2[.]azureedge[.]net	13.107.253.45	United States	HTTPS, DNS, TCP	CLEAN
aadcdnoriginwus2[.]afd[.]azureedge[.]net	13.107.253.45	United States	HTTPS, DNS, TCP	CLEAN
firstparty-azurefd-prod[.]trafficmanager[.]net	13.107.253.45	United States	HTTPS, DNS, TCP	CLEAN
shed[.]dual-low[.]s-part-0017[.]t-0009[.]t-msedge[.]net	13.107.253.45	United States	HTTPS, DNS, TCP	CLEAN
azurefd-t-fb-prod[.]trafficmanager[.]net	13.107.253.45	United States	HTTPS, DNS, TCP	CLEAN
dual[.]s-part-0017[.]t-0009[.]fb-t-msedge[.]net	13.107.253.45	United States	HTTPS, DNS, TCP	CLEAN
s-part-0017[.]t-0009[.]fb-t-msedge[.]net	13.107.253.45	United States	HTTPS, DNS, TCP	CLEAN
cdnjs[.]cloudflare[.]com	104.17.25.14, 104.17.24.14	-	HTTPS, DNS, TCP	CLEAN
maxcdn[.]bootstrapcdn[.]com	104.18.11.207, 104.18.10.207	-	HTTPS, DNS, TCP	CLEAN
api[.]ipify[.]org	104.26.13.205, 104.26.12.205, 172.67.74.152	-	HTTPS, DNS, TCP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
todosec[.]org	103.224.212.213	Australia	HTTPS, TLS, DNS, TCP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
103.224.212.213	todosec[.]org	Australia	HTTPS, TLS, DNS, TCP	CLEAN
104.18.2.35	pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev	-	HTTPS, TLS, DNS, TCP	CLEAN
13.107.253.45	aadcdnoriginwus2[.]azureedge[.]net, dual[.]s-part-0017[.]t-0009[.]fb-t-msedge[.]net, aadcdnoriginwus2[.]afd[.]azureedge[.]net, aad...-0009[.]fb-t-msedge[.]net, shed[.]dual-low[.]s-part-0017[.]t-0009[.]t-msedge[.]net, firstparty-azurefd-prod[.]trafficmanager[.]net	United States	HTTPS, DNS, TCP	CLEAN
104.17.25.14	cdnjs[.]cloudflare[.]com	-	HTTPS, DNS, TCP	CLEAN
104.18.11.207	maxcdn[.]bootstrapcdn[.]com	-	HTTPS, DNS, TCP	CLEAN
104.21.27.152	use[.]fontawesome[.]com, use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	-	HTTPS, TCP, UDP, TLS, DNS	CLEAN
104.26.12.205	api[.]ipify[.]org	-	HTTPS, DNS, TCP	CLEAN
151.101.66.137	code[.]jquery[.]com	United States	HTTPS, DNS, TCP	CLEAN
104.18.3.35	pub-f7902c65ab4147bd894b2cbeca5fcfcb[.]r2[.]dev	-	DNS	CLEAN
172.67.142.245	use[.]fontawesome[.]com, use[.]fontawesome[.]com[.]cdn[.]cloudflare[.]net	-	DNS	CLEAN
151.101.2.137	code[.]jquery[.]com	United States	DNS	CLEAN
151.101.194.137	code[.]jquery[.]com	United States	DNS	CLEAN
151.101.130.137	code[.]jquery[.]com	United States	DNS	CLEAN
104.17.24.14	cdnjs[.]cloudflare[.]com	-	DNS	CLEAN
104.18.10.207	maxcdn[.]bootstrapcdn[.]com	-	DNS	CLEAN
172.67.74.152	api[.]ipify[.]org	-	DNS	CLEAN
104.26.13.205	api[.]ipify[.]org	-	DNS	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_web
Description	windows 10 (64bit TH2 -EN- WEB_ANALYSIS)
Architecture	-
Operating System	-
Kernel Version	-
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.3.1
Web Engine Version	1.5.0 / 06/10/2024 04:30
Static Engine Version	2024.3.1.0 / 2024-06-10 03:00:36
AV Exceptions Version	2024.3.1.2 / 2024-06-08 13:32:38
ML Detection Models Version	2024.3.1.2 / 2024-06-08 13:32:38
Link Detonation Heuristics Version	2024.3.1.2 / 2024-06-08 13:32:38
Signature Trust Store Version	2024.3.1.2 / 2024-06-08 13:32:38
VMRay Threat Identifiers Version	2024.3.1.2 / 2024-06-08 13:32:38
Web Engine Auto UI Rules Version	2024.3.1.2 / 2024-06-08 13:32:38
YARA Built-in Ruleset Version	2024.3.1.0

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