MALICIOUS

Classifications: Phishing

Threat Names: -

Verdict Reason: -

Sample Type	URL
File Name	**hxxps://send-us[.]page-review[.]com**
ID	#10321187
MD5	9c617bf8e1148eb8e6a94ab5e611d03f
SHA1	e5b7591cf59c47806cefc5888f628aaff32787d5
SHA256	b009ae0ac23da7086fc55448af0fd5f615397b86eb3785c25356072d2f44bf65
File Size	31 bytes
Report Created	2024-04-28 10:55 (UTC)
Target Environment	windows 10 (64bit TH2 -EN- WEB_ANALYSIS) | web_root

OVERVIEW

VMRay Threat Identifiers (5 rules, 8 matches)

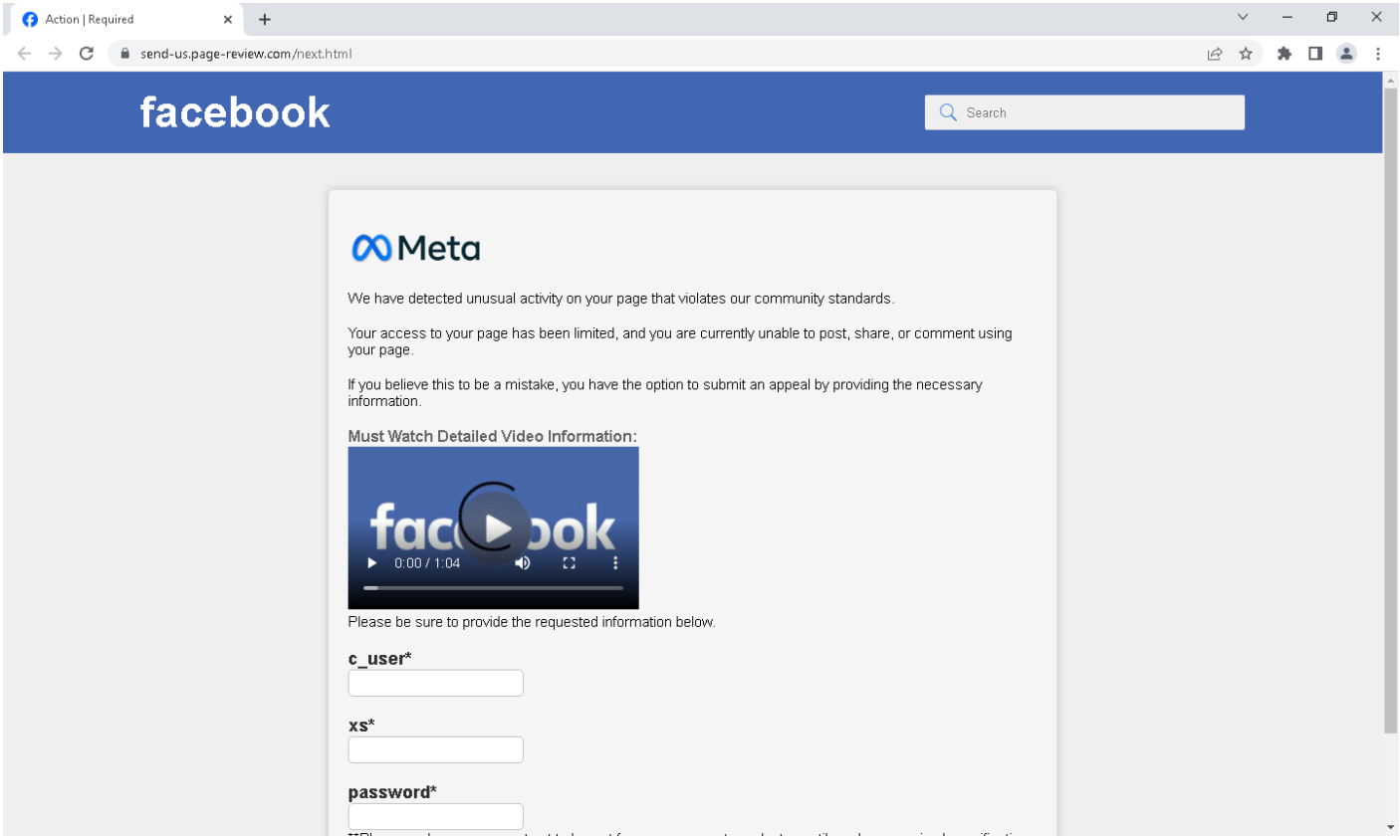
Score	Category	Operation	Count	Classification
5/5	Heuristics	Combination of other detections indicates a phishing website	1	Phishing
	• Heuristics determined that the page is a phishing website, based on combination of other detections.			
4/5	Reputation	Malicious host or URL detected via reputation	4	-
	• Submitted URL "hxxps://send-us[.]page-review[.]com" is a known malicious URL and was reported as "Phishing". • Contacted URL "hxxps://send-us[.]page-review[.]com" is a known malicious URL and was reported as "Phishing". • Contacted URL "hxxps://send-us[.]page-review[.]com/next.html" is a known malicious URL and was reported as "Phishing". • Contacted URL "hxxps://send-us[.]page-review[.]com/styles.css" is a known malicious URL and was reported as "Phishing".			
2/5	Heuristics	Page secured via a Domain Validated SSL certificate	1	-
	• Host send-us.page-review.com uses DV certificate issued by Google Trust Services LLC to page-review.com.			
2/5	Heuristics	Page is hosted on a recently registered domain	1	-
	• Domain send-us.page-review.com was registered just 2 days ago.			
1/5	Heuristics	Page presents itself as a logon page	1	-
	• Page hxxps://send-us[.]page-review[.]com/next.html contains a logon form.			

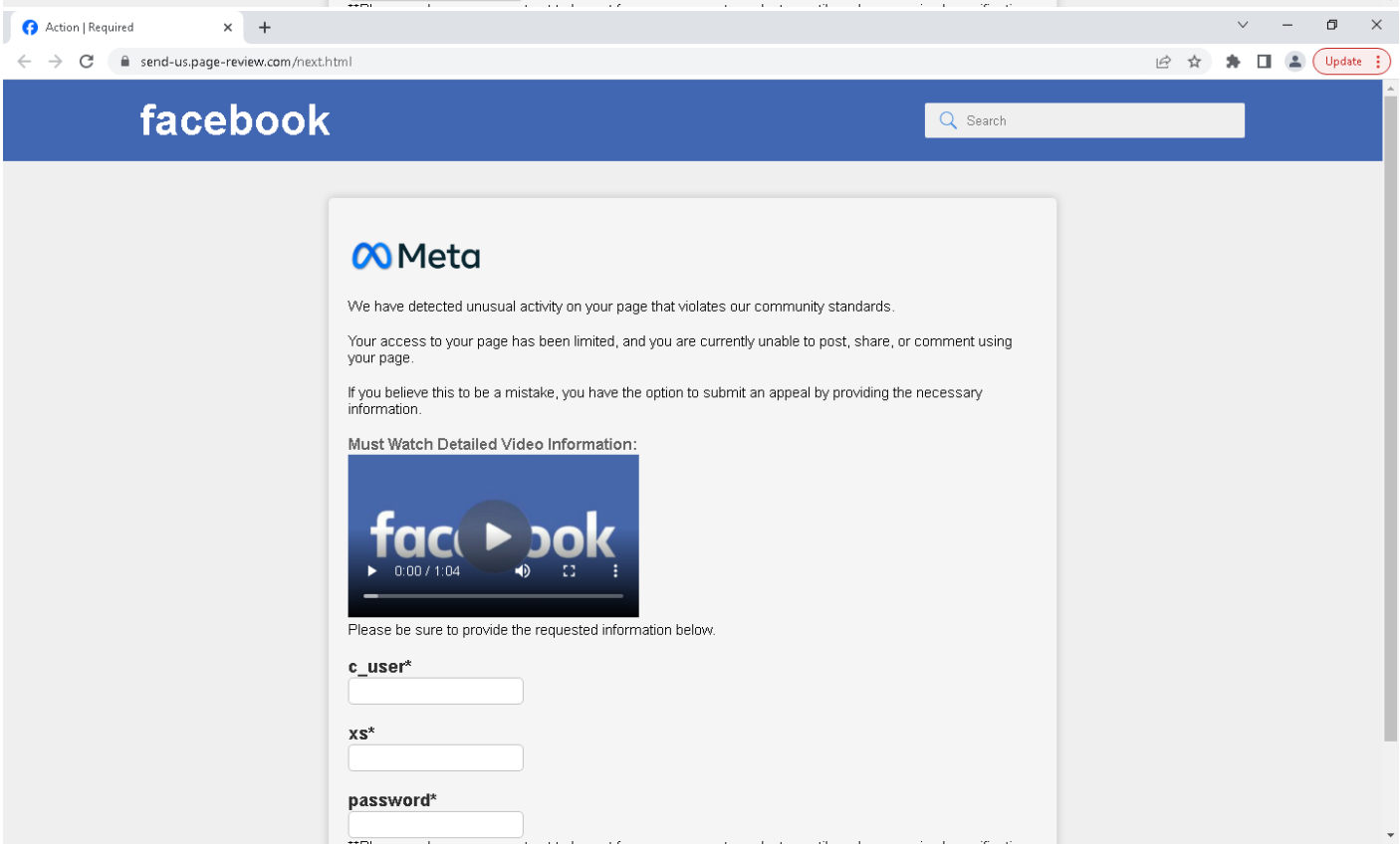
Sample Information

ID	#10321187
MD5	9c617bf8e1148eb8e6a94ab5e611d03f
SHA1	e5b7591cf59c47806cefc5888f628aaff32787d5
SHA256	b009ae0ac23da7086fc55448af0fd5f615397b86eb3785c25356072d2f44bf65
SSDeep	3:N8NTdUXATMJI:21dUQT9
File Name	hxxps://send-us[.]page-review[.]com
File Size	31 bytes
Sample Type	URL
Has Macros	✔

Analysis Information

Creation Time	2024-04-28 10:55 (UTC)
Analysis Duration	00:00:30
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


Action | Required
send-us.page-review.com/next.html
facebook
Search
Meta
We have detected unusual activity on your page that violates our community standards.
Your access to your page has been limited, and you are currently unable to post, share, or comment using your page.
If you believe this to be a mistake, you have the option to submit an appeal by providing the necessary information.
Must Watch Detailed Video Information:
0:00 / 1:04
Please be sure to provide the requested information below.
c_user*
xs*
password*


Action | Required
send-us.page-review.com/next.html
Update
facebook
Search
Meta
We have detected unusual activity on your page that violates our community standards.
Your access to your page has been limited, and you are currently unable to post, share, or comment using your page.
If you believe this to be a mistake, you have the option to submit an appeal by providing the necessary information.
Must Watch Detailed Video Information:
0:00 / 1:04
Please be sure to provide the requested information below.
c_user*
xs*
password*

NETWORK

General

49.32 KB total sent

6601.91 KB total received

2 ports 443, 53

5 contacted IP addresses

0 URLs extracted

0 files downloaded

1 malicious hosts detected

DNS

4 DNS requests for 4 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

8 URLs contacted, 4 servers

3 sessions, 59.38 KB sent, 7002.72 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://cdn[.]glitch[.]global/d08141de-e7af-45a5-916b-2f09d06ac286/search-icon-lob.png?v=1712422050841	-	-	-	0 bytes	CLEAN
GET	hxxps://cdn[.]glitch[.]global/d08141de-e7af-45a5-916b-2f09d06ac286/Meta-Logo.png?v=1712422024289	-	-	-	0 bytes	CLEAN
GET	hxxps://i[.]pinimg[.]com/originals/97/95/69/979569a2dedd37573974ceebc05b4a4e.png	-	-	-	0 bytes	CLEAN
GET	hxxps://cdn[.]glitch[.]global/d08141de-e7af-45a5-916b-2f09d06ac286/Facebook_Logo_2023.png?v=1712421903497	-	-	-	0 bytes	CLEAN
GET	hxxps://send-us[.]page-review[.]com/next.html	-	-	-	0 bytes	MALICIOUS
GET	hxxps://send-us[.]page-review[.]com/styles.css	-	-	-	0 bytes	MALICIOUS
GET	hxxps://send-us[.]page-review[.]com	-	-	-	0 bytes	MALICIOUS

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	cdn[.]glitch[.]global, j[.]sni[.]global[.]fastly[.]net	NO_ERROR	146.75.118.132	j[.]sni[.]global[.]fastly[.]net	CLEAN
A	send-us[.]page-review[.]com	NO_ERROR	172.67.138.236, 104.21.70.196	-	SUSPICIOUS
A	i[.]pinimg[.]com, i[.]pinimg[.]com[.]gslb[.]pinterest[.]com, image[.]gslb[.]pinterest[.]net, dualstack[.]pinterest[.]map[.]fastly[.]net	NO_ERROR	146.75.120.84	i[.]pinimg[.]com[.]gslb[.]pinterest[.]com, image[.]gslb[.]pinterest[.]net, dualstack[.]pinterest[.]map[.]fastly[.]net	CLEAN
A	detailed-video-29b30[.]web[.]app	NO_ERROR	199.36.158.100	-	CLEAN

ARTIFACTS

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://send-us[.]page-review[.]com	Sample, Contacted	104.21.70.196, 172.67.138.236	United States	GET	MALICIOUS
hxxps://send-us[.]page-review[.]com/next.html	Contacted	104.21.70.196, 172.67.138.236	United States	GET	MALICIOUS
hxxps://send-us[.]page-review[.]com/styles.css	Contacted	104.21.70.196, 172.67.138.236	United States	GET	MALICIOUS
hxxps://cdn[.]glitch[.]global/d08141de-e7af-45a5-916b-2f09d06ac286/Facebook_Logo_2023.png?v=1712421903497	Contacted	146.75.118.132	Germany	GET	CLEAN
hxxps://cdn[.]glitch[.]global/d08141de-e7af-45a5-916b-2f09d06ac286/search-icon-lob.png?v=1712422050841	Contacted	146.75.118.132	Germany	GET	CLEAN
hxxps://cdn[.]glitch[.]global/d08141de-e7af-45a5-916b-2f09d06ac286/Meta-Logo.png?v=1712422024289	Contacted	146.75.118.132	Germany	GET	CLEAN
hxxps://i[.]pinimg[.]com/originals/97/95/69/979569a2dedd37573974ceebc05b4a4e.png	Contacted	146.75.120.84	Germany	GET	CLEAN
hxxps://detailed-video-29b30[.]web[.]app/detailed%20video.mp4	Contacted	199.36.158.100	United States	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
send-us[.]page-review[.]com	104.21.70.196, 172.67.138.236	United States	TCP, HTTPS, UDP, TLS, DNS	SUSPICIOUS
cdn[.]glitch[.]global	146.75.118.132	Germany	TCP, DNS, HTTPS	CLEAN
j[.]sni[.]global[.]fastly[.]net	146.75.118.132	Germany	TCP, DNS, HTTPS	CLEAN
detailed-video-29b30[.]web[.]app	199.36.158.100	United States	TCP, DNS, TLS	CLEAN
i[.]pinimg[.]com	146.75.120.84	Germany	TCP, DNS, HTTPS	CLEAN
i[.]pinimg[.]com[.]gslb[.]pinterest[.]com	146.75.120.84	Germany	TCP, DNS, HTTPS	CLEAN
image[.]gslb[.]pinterest[.]net	146.75.120.84	Germany	TCP, DNS, HTTPS	CLEAN
dualstack[.]pinterest[.]map[.]fastly[.]net	146.75.120.84	Germany	TCP, DNS, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
172.67.138.236	send-us[.]page-review[.]com	United States	TCP, HTTPS, UDP, TLS, DNS	CLEAN
146.75.118.132	j[.]sni[.]global[.]fastly[.]net, cdn[.]glitch[.]global	Germany	TCP, DNS, HTTPS	CLEAN
146.75.120.84	image[.]gslb[.]pinterest[.]net, i[.]pinimg[.]com[.]gslb[.]pinterest[.]com, dualstack[.]pinterest[.]map[.]fastly[.]net, i[.]pinimg[.]com	Germany	TCP, DNS, HTTPS	CLEAN
199.36.158.100	detailed-video-29b30[.]web[.]app	United States	TCP, DNS, TLS	CLEAN
104.21.70.196	send-us[.]page-review[.]com	-	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	2024.2.1
Web Engine Version	1.5.0 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
ML Detection Models Version	2024.2.1.16 / 2024-04-14 09:07:46
Link Detonation Heuristics Version	2024.2.1.18 / 2024-04-18 14:31:08
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.23 / 2024-04-25 06:55:37
Web Engine Auto UI Rules Version	2024.2.1.22 / 2024-04-22 18:03:52
YARA Built-in Ruleset Version	2024.2.1.18

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