MALICIOUS

Classifications: Phishing

Threat Names: Mal/HTMLGen-A

Verdict Reason: -

Sample Type	URL
File Name	**https://dlscordjbost.com/csi**
ID	#6177580
MD5	8ee713e4284cc2061f0010e093fd65e4
SHA1	7183eef7e14d3af2545dc885a87c3fd6342dd75c
SHA256	e65bdd5244c5f0d3957599244738c4511e8dd574cbd101af9e65a6946562eb20
File Size	28 bytes
Report Created	2022-11-21 11:53 (UTC+1)
Target Environment	win10_64_th2_en_web | web_root

OVERVIEW

VMRay Threat Identifiers (5 rules, 28 matches)

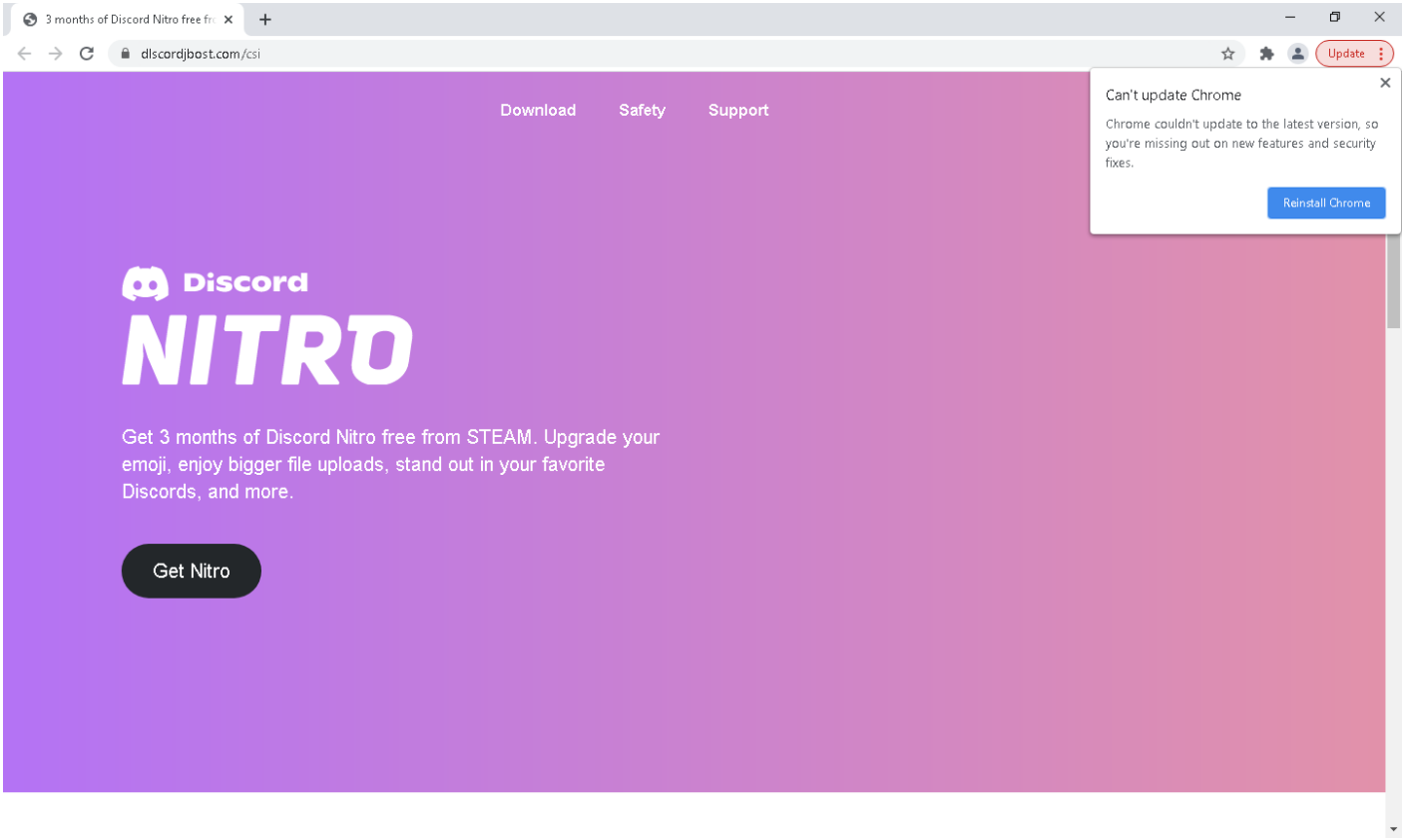
Score	Category	Operation	Count	Classification
4/5	Machine Learning	Phishing page detected	1	Phishing
	• Phishing attempt detected by ML module (StingRay).			
4/5	Reputation	Known malicious URL	1	-
	• Reputation analysis labels the submitted URL "https://dlscordjbost.com/csi" as Mal/HTMLGen-A.			
4/5	Reputation	Contacts known malicious URL	14	-
	• Reputation analysis labels the contacted URL "https://dlscordjbost.com/ddbd2431e283688ab878e6...0586e9c099a58488ec03d.js" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/metrica.php?method=AuthOpen&url=https%3A%2F%2Fdlscordjbost.com%2Fcsi%23" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/metrica.php?method=AuthOpen&url=https%3A%2F%2Fdlscordjbost.com%2Fcsi" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/ddbd2431e283688ab878e6...535777e4e6a2aaf15e84.css" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/csi-auth?openid.ns=mkbl5i04http%3A%2F%2Fspecs.openid.net%2F... ... 2Fauth%2F2.0%2Fidentifier_select&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/ddbd2431e283688ab878e6...19b59d330e0a32fba45f9.js" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/ddbd2431e283688ab878e6...ed300f49bbba4c1757e0.css" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/c287634f0a24c2946eafa5...02970a971532a01292d46.js" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/ddbd2431e283688ab878e6...803ac72d04baff5fb508.css" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/ddbd2431e283688ab878e6...37ac1da6dbe2746c96d0.css" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/ddbd2431e283688ab878e6...c726dda244d50aa0f909.css" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/ddbd2431e283688ab878e6...9b59d330e0a32fba45f9.css" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/metrica.php?method=LoadedCount&url=https%3A%2F%2Fdlscordjbost.com%2Fcsi" as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "https://dlscordjbost.com/csi#" as Mal/HTMLGen-A.			
2/5	Heuristics	Page is hosted on a recently registered domain	1	-
	• Domain dlscordjbost.com was registered just 8 days ago.			
1/5	Heuristics	Resource is loaded from a service commonly used for temporary hosting	11	-
	• Resource at https://cdn.discordapp.com/attachments/880449376957390941/889581462108639263/pososi_mudila.webm loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/818120722869911602/884000156729630780/11.png loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/818120722869911602/884000187708747836/33.png loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/818120722869911602/884000214405496832/55.png loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/818120722869911602/884000199557677076/44.png loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/818120722869911602/884000234466869299/66.png loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/818120722869911602/884001809654484993/e6d6b255259ac878d00819a9555072ad.png loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/818120722869911602/884002677346943047/847541504914fd33810e70a0ea73177e.png loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/818120722869911602/884000175457185842/22.png loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/818120722869911602/883999740071657542/nitro.png loaded from Discord. • Resource at https://cdn.discordapp.com/attachments/880449376957390941/880495556596744252/779a770c34fcb823a598a7277301adaf.png loaded from Discord.			
-	Trusted	Known clean file	1	-
	• Embedded file "" is a known clean file.			

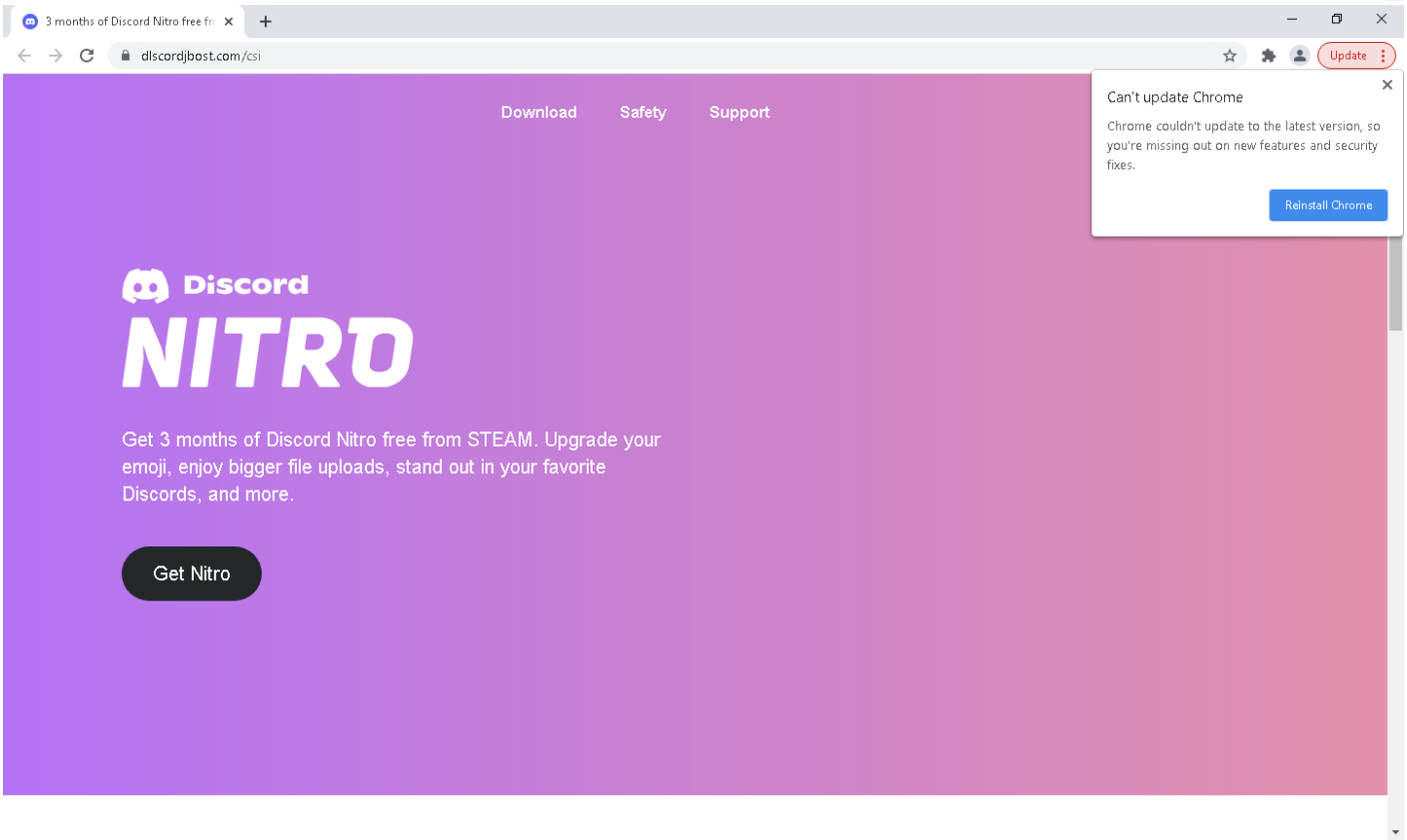
Sample Information

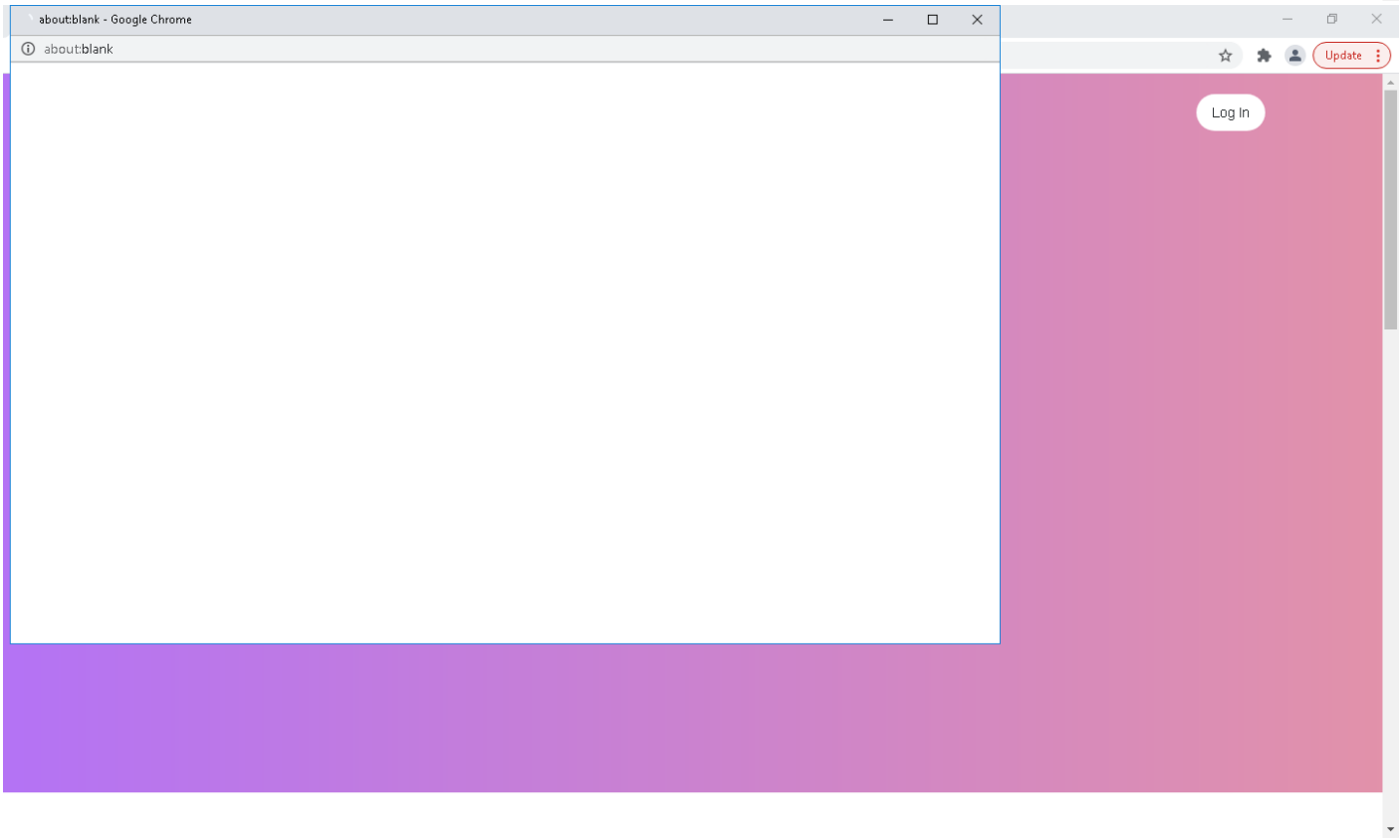
ID	#6177580
MD5	8ee713e4284cc2061f0010e093fd65e4
SHA1	7183eef7e14d3af2545dc885a87c3fd6342dd75c
SHA256	e65bdd5244c5f0d3957599244738c4511e8dd574cbd101af9e65a6946562eb20
SSDeep	3:N8RW/aUMn:2E/aV
File Name	https://dlscordjbost.com/csi
File Size	28 bytes
Sample Type	URL
Has Macros	✔

Analysis Information

Creation Time	2022-11-21 11:53 (UTC+1)
Analysis Duration	00:03:59
Termination Reason	Timeout
Number of Monitored Processes	0
Execution Successful	False
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


3 months of Discord Nitro free fr
dlscordjbost.com/csi
Update
Download
Safety
Support
Can't update Chrome
Chrome couldn't update to the latest version, so you're missing out on new features and security fixes.
Reinstall Chrome
Discord
NITRO
Get 3 months of Discord Nitro free from STEAM. Upgrade your emoji, enjoy bigger file uploads, stand out in your favorite Discords, and more.
Get Nitro


3 months of Discord Nitro free fr
dlscordjbost.com/csi
Update
Download
Safety
Support
Can't update Chrome
Chrome couldn't update to the latest version, so you're missing out on new features and security fixes.
Reinstall Chrome
Discord
NITRO
Get 3 months of Discord Nitro free from STEAM. Upgrade your emoji, enjoy bigger file uploads, stand out in your favorite Discords, and more.
Get Nitro



Screenshots truncated

NETWORK

General

113.32 KB total sent

2105.51 KB total received

2 ports 443, 53

10 contacted IP addresses

0 URLs extracted

16 files downloaded

0 malicious hosts detected

DNS

11 DNS requests for 11 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

71 URLs contacted, 9 servers

14 sessions, 479.82 KB sent, 6098.14 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://steamstore-a.akamaihd.net/public/shared/css/buttons.css?v=l3li_MNwxNDv&l=russian	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/css/v6/store.css?v=PNn6rEomR33m&l=russian	-	-		0 bytes	NA
GET	https://dlscordjbost.com/c287634f0a24c2946eafa53c8bc7be45802a1154e5c9/f222f0fef03d30b6b2cebc702970a971532a01292d46.js	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/shared/css/motiva_sans.css?v=GvhJzpHNW-hA&l=russian	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/javascript/main.js?v=x1ds_vlJBv32&l=russian	-	-		0 bytes	NA
GET	https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/5402ea41ab4861e107b66986803ac72d04baff5fb508.css	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/shared/css/shared_responsive.css?v=AKHr_xXe1lDr&l=russian	-	-		0 bytes	NA
GET	https://dlscordjbost.com/metrica.php?method=LoadedCount&url=https%3A%2F%2Fdlscordjbost.com%2Fcsi	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/javascript/dynamicstore.js?v=uBXbyztlCe1q&l=russian	-	-		0 bytes	NA
GET	https://steamcommunity-a.akamaihd.net/public/shared/images/responsive/logo_valve_footer.png	-	-		0 bytes	NA
GET	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/images/footerLogo_valve_new.png	-	-		0 bytes	NA
GET	https://discord.com/assets/0.1fafb1729b3e11fa547c.css	-	-		0 bytes	NA
GET	https://discord.com/assets/91a561ed8fe1c491df40.js	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://steamstore-a.akamaihd.net/public/css/v6/cart.css?v=4QI8ScFus6Kr&l=russian	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/880449376957390941/889581462108639263/pososi_mudila.webm	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/images/ico/ico_twitter.gif	-	-		0 bytes	NA
GET	https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/b4512d6a903aba23eb2b30c19b59d330e0a32fba45f9.css	-	-		0 bytes	NA
GET	https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/4e7c0b1bf41a2db46da58bdc37ac1da6dbe2746c96d0.css	-	-		0 bytes	NA
GET	https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/69abcd73d5078d41c2e007d0535777e4e6a2aaf15e84.css	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/818120722869911602/884000156729630780/11.png	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/818120722869911602/884000187708747836/33.png	-	-		0 bytes	NA
GET	https://discord.com/assets/be0060dafb7a0e31d2a1ca17c0708636.woff	-	-		0 bytes	NA
GET	https://store.cloudflare.steamstatic.com/public/shared/images/responsive/header_logo.png	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/818120722869911602/884000214405496832/55.png	-	-		0 bytes	NA
GET	https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/528332455e5780e963a9ed1ac726dda244d50aa0f909.css	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/images/ico/ico_facebook.gif	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/shared/javascript/shared_global.js?v=nWHYEn6G1KtO&l=russian	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/818120722869911602/884000199557677076/44.png	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/css/v6/browse.css?v=7hoqLVcZ7KVq&l=russian	-	-		0 bytes	NA
GET	https://discord.com/assets/ae7c84783ad48b6d1c8e2bfbe707e0d4.woff2	-	-		0 bytes	NA
GET	https://discord.com/assets/41b19499e43362e694db.js	-	-		0 bytes	NA
GET	https://store.akamai.steamstatic.com/public/shared/fonts/MotivaSans-Regular.ttf?v=4.015	-	-		0 bytes	NA
GET	https://discord.com/assets/92e32db984c8577d8b81548b43b9c061.woff	-	-		0 bytes	NA
GET	https://steamcommunity.com/favicon.ico	-	-		0 bytes	NA
GET	https://store.akamai.steamstatic.com/public/shared/images/popups/btn_arrow_down_padded.png	-	-		0 bytes	NA
GET	https://code.jquery.com/ui/1.11.3/jquery-ui.js	-	-		0 bytes	NA
GET	https://store.akamai.steamstatic.com/public/shared/fonts/MotivaSans-Thin.ttf?v=4.015	-	-		0 bytes	NA
GET	https://store.akamai.steamstatic.com/public/shared/images/header/btn_header_installsteam_download.png?v=1	-	-		0 bytes	NA
GET	https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/48ef06e313c1e0e1a256a0b0586e9c099a58488ec03d.js	-	-		0 bytes	NA
GET	https://dlscordjbost.com/metrica.php?method=AuthOpen&url=https%3A%2F%2Fdlscordjbost.com%2Fcsi	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://discord.com/assets/5c9406522a805df295db.js	-	-		0 bytes	NA
GET	https://discord.com/assets/c8d1fec4ad144f280f54.js	-	-		0 bytes	NA
GET	https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/b4512d6a903aba23eb2b30c19b59d330e0a32fba45f9.js	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/818120722869911602/884000234466869299/66.png	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/images/ico/ico_rss2.gif	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/818120722869911602/884001809654484993/e6d6b255259ac878d00819a9555072ad.png	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/shared/css/shared_global.css?v=tMXeUkoXL8fe&l=russian	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/images/v6/logo_steam_footer.png	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/shared/javascript/jquery-1.8.3.min.js?v=.TZ2NKhB-nliU	-	-		0 bytes	NA
GET	https://discord.com/assets/00a0131a221e58790dd0.js	-	-		0 bytes	NA
GET	https://discord.com/assets/8e12fb4f14d9c4592eb8ec9f22337b04.woff	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/818120722869911602/884002677346943047/847541504914fd33810e70a0ea73177e.png	-	-		0 bytes	NA
GET	https://code.jquery.com/jquery-3.6.0.min.js	-	-		0 bytes	NA
GET	https://dlscordjbost.com/csi-auth?openid.ns=mkbl5i04http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&openid.mode=checkid_setup&openid.re... ...2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/shared/javascript/tooltip.js?v=.9Z1XDV02xrml	-	-		0 bytes	NA
GET	https://discord.com/assets/3bdef1251a424500c1b3a78dea9b7e57.woff	-	-		0 bytes	NA
GET	https://dlscordjbost.com/csi	-	-		0 bytes	NA
GET	https://dlscordjbost.com/metrica.php?method=AuthOpen&url=https%3A%2F%2Fdlscordjbost.com%2Fcsi%23	-	-		0 bytes	NA
GET	https://discord.com/assets/e8acd7d9bf6207f99350ca9f9e23b168.woff	-	-		0 bytes	NA
GET	https://store.akamai.steamstatic.com/public/shared/images/joinsteam/acct_creation_bg.jpg	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/shared/javascript/shared_responsive_adapter.js?v=DA2EvSkOoJao&l=russian	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/shared/images/responsive/header_menu_hamburger.png	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/818120722869911602/884000175457185842/22.png	-	-		0 bytes	NA
GET	https://community.cloudflare.steamstatic.com/public/shared/images/header/logo_steam.svg?t=962016	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/818120722869911602/883999740071657542/nitro.png	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/880449376957390941/880495556596744252/779a770c34fcb823a598a7277301adaf.png	-	-		0 bytes	NA
GET	https://discord.com/assets/220d6edab61258b8bec9.js	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://steamstore-a.akamaihd.net/public/shared/images/login/join_pc.png?v=1	-	-		0 bytes	NA
GET	https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/fd9f4de7201b2848c97b902fed300f49bbba4c1757e0.css	-	-		0 bytes	NA
GET	https://steamstore-a.akamaihd.net/public/images/blank.gif	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	discord.com	NO_ERROR	162.159.137.232, 162.159.128.233, 162.159.136.232, 162.159.138.232, 162.159.135.232		NA
A	steamcommunity-a.akamaihd.net, steamcommunity-a.akamaihd.net.edgesuite.net, a1697.b.akamai.net	NO_ERROR	88.221.110.201, 88.221.110.219	steamcommunity-a.akamaihd.net.edgesuite.net, a1697.b.akamai.net	NA
A	community.cloudflare.steamstatic.com	NO_ERROR	172.64.150.233, 104.18.37.23		NA
A	dlscordjbost.com	NO_ERROR	188.114.96.3, 188.114.97.3		NA
A	cdn.discordapp.com	NO_ERROR	162.159.133.233, 162.159.130.233, 162.159.129.233, 162.159.134.233, 162.159.135.233		NA
A	steamcommunity.com	NO_ERROR	2.23.49.250		NA
A	store.akamai.steamstatic.com	NO_ERROR	88.221.110.209, 88.221.110.137		NA
A	cdnjs.cloudflare.com	NO_ERROR	104.17.24.14, 104.17.25.14		NA
A	store.cloudflare.steamstatic.com	NO_ERROR	172.64.150.233, 104.18.37.23		NA
A	code.jquery.com, cds.s5x3j6q5.hwcdn.net	NO_ERROR	69.16.175.42, 69.16.175.10	cds.s5x3j6q5.hwcdn.net	NA
A	steamstore-a.akamaihd.net, steamstore-a.akamaihd.net.edgesuite.net, a1737.b.akamai.net	NO_ERROR	88.221.110.209, 88.221.110.137	steamstore-a.akamaihd.net.edgesuite.net, a1737.b.akamai.net	NA

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a73c922331dd9ca4692e0663eea1a6328cd3cae53682a14b5db97c9cb938174e	-	Downloaded File	126.08 KB	text/plain	-	CLEAN
d8bbe461137d50211568449468a1981ef189248200eadd48c3141a9df0b8f7fc	-	Downloaded File	2.52 KB	image/png	-	CLEAN
fee9c5438f2b9c6cc0bceaba92e1e00c320981f0e51a0e5715d7059573b62f91	-	Downloaded File	24.43 KB	text/plain	-	CLEAN
3dfbda507ea5fb1ed6c358bcc2e595c170ed4293ccb135545f05be3e30f7a0c0	-	Downloaded File	1.39 KB	image/gif	-	CLEAN
3d0874ab563803918741edfd0204aa756df378544bf81e1874a538b17839500d	-	Downloaded File	32.74 KB	text/plain	-	CLEAN
8b97ba0dac22fe6704c1f6d95fe79613f33017804f256abb9006df0442491787	-	Downloaded File	1.80 KB	image/png	-	CLEAN
ba6eda7945ab8d7e57b34cc5a3dd292fa2e4c60a5ced79236ecf1a9e0f0c2d32	-	Downloaded File	91.44 KB	text/plain	-	CLEAN
5f97cfe4186b827737324c19df2fa7f98bb465e6e0893092c683c4ad76d9495b	-	Downloaded File	1.14 KB	image/gif	-	CLEAN
de0871b3da5b1cd9c00a2a9e5abb89b32750d411d35d19786ee02316ecfeab3b	-	Downloaded File	85.75 KB	text/plain	-	CLEAN
8f73ef54efc672061f69ca881fe318dccc6dd67d993cbb8e76e53e52c84ee493	-	Downloaded File	807 bytes	image/gif	-	CLEAN
e2d4e0e1d3e162fdc815f16dfff9ae9b0a967949f0f3ae371f947d730a3f0661	-	Downloaded File	15.71 KB	text/html	-	CLEAN
218bedd2a2817dfde5f3a900b6204c7e378e1b747ff98ae89aedff2391e4429c	-	Downloaded File	2.58 KB	text/plain	-	CLEAN
56b34b332b0bba4c9a3bf6337b836da709cf968bb779c9ce6a2d96cd6e3a9e87	-	Downloaded File	17.81 KB	text/plain	-	CLEAN
97e05e9dafe42fc4ea95403d5e584f48e0f5438b52129c52c56d492fce017bd9	-	Downloaded File	11.04 KB	text/plain	-	CLEAN
2772850b98923d3dcde7942c03c76f088cba2f9f50d0ac69a83a45bd1d6be430	-	Downloaded File	55.86 KB	text/plain	-	CLEAN
4f22ae53003ddf733732137f6325523ae9adbaf32d09daae2b092707f09e1684	-	Downloaded File	83.90 KB	text/plain	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/48ef06e313c1e0e1a256a0b0586e9c099a58488ec03d.js	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/metrica.php?method=AuthOpen&url=https%3A%2F%2Fdlscordjbost.com%2Fcsi%23	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/metrica.php?method=AuthOpen&url=https%3A%2F%2Fdlscordjbost.com%2Fcsi	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/69abcd73d5078d41c2e007d0535777e4e6a2aaf15e84.css	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/csi-auth?openid.ns=mkbl5i04http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&openid.mode=checkid_setup&openid.re... ...2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/b4512d6a903aba23eb2b30c19b59d330e0a32fba45f9.js	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/fd9f4de7201b2848c97b902fed300f49bbba4c1757e0.css	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/c287634f0a24c2946eafa53c8bc7be45802a1154e5c9/f222f0fef03d30b6b2cebc702970a971532a01292d46.js	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/csi	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/5402ea41ab4861e107b66986803ac72d04baff5fb508.css	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/4e7c0b1bf41a2db46da58bdc37ac1da6dbe2746c96d0.css	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/528332455e5780e963a9ed1ac726dda244d50aa0f909.css	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/ddbd2431e283688ab878e61e32428ef25923e16a3e28/b4512d6a903aba23eb2b30c19b59d330e0a32fba45f9.css	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://dlscordjbost.com/metrica.php?method=LoadedCount&url=https%3A%2F%2Fdlscordjbost.com%2Fcsi	-	188.114.96.3, 188.114.97.3	-	GET	MALICIOUS
https://cdn.discordapp.com/attachments/818120722869911602/884000214405496832/55.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN
https://discord.com/assets/5c9406522a805df295db.js	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/images/ico/ico_rss2.gif	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://discord.com/assets/ae7c84783ad48b6d1c8e2bfbe707e0d4.woff2	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	-	CLEAN
https://store.cloudflare.steamstatic.com/public/shared/images/responsive/header_logo.png	-	172.64.150.233, 104.18.37.23	-	GET	CLEAN
https://discord.com/assets/3bdef1251a424500c1b3a78dea9b7e57.woff	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	-	CLEAN
https://steamstore-a.akamaihd.net/public/images/footerLogo_valve_new.png	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://steamstore-a.akamaihd.net/public/css/v6/store.css?v=PNn6rEomR33m&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/shared/css/shared_responsive.css?v=AKHr_xXe1lDr&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/css/v6/cart.css?v=4QI8ScFus6Kr&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://discord.com/assets/0.1fafb1729b3e11fa547c.css	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	-	CLEAN
https://steamstore-a.akamaihd.net/public/shared/javascript/shared_global.js?v=nWHYEn6G1KtO&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://discord.com/assets/220d6edab61258b8bec9.js	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	GET	CLEAN
https://store.akamai.steamstatic.com/public/shared/fonts/MotivaSans-Thin.ttf?v=4.015	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://cdn.discordapp.com/attachments/818120722869911602/884000187708747836/33.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN
https://cdn.discordapp.com/attachments/818120722869911602/883999740071657542/nitro.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/javascript/main.js?v=x1ds_vlJBv32&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://code.jquery.com/ui/1.11.3/jquery-ui.js	-	69.16.175.42, 69.16.175.10	-	GET	CLEAN
https://cdn.discordapp.com/attachments/818120722869911602/884001809654484993/e6d6b255259ac878d00819a9555072ad.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN
https://discord.com/assets/41b19499e43362e694db.js	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/shared/css/motiva_sans.css?v=GvhJzpHNW-hA&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://store.akamai.steamstatic.com/public/shared/fonts/MotivaSans-Regular.ttf?v=4.015	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/css/v6/browse.css?v=7hoqLVcZ7KVq&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/images/v6/logo_steam_footer.png	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/javascript/dynamicstore.js?v=uBXbyztICe1q&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/shared/javascript/jquery-1.8.3.min.js?v=.TZ2NKhB-nliU	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/images/ico/ico_facebook.gif	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://cdn.discordapp.com/attachments/818120722869911602/884000234466869299/66.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://discord.com/assets/be0060dafb7a0e31d2a1ca17c0708636.woff	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	-	CLEAN
https://discord.com/assets/00a0131a221e58790dd0.js	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	GET	CLEAN
https://discord.com/assets/8e12fb4f14d9c4592eb8ec9f22337b04.woff	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	-	CLEAN
https://steamstore-a.akamaihd.net/public/shared/images/login/join_pc.png?v=1	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://discord.com/assets/e8acd7d9bf6207f99350ca9f9e23b168.woff	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	-	CLEAN
https://cdn.discordapp.com/attachments/818120722869911602/884002677346943047/847541504914fd33810e70a0ea73177e.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN
https://discord.com/assets/c8d1fec4ad144f280f54.js	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/images/blank.gif	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/images/ico/ico_twitter.gif	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/shared/javascript/shared_responsive_adapter.js?v=DA2EvSkOoJao&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/shared/css/shared_global.css?v=tMXeUkoXL8fe&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://discord.com/assets/92e32db984c8577d8b81548b43b9c061.woff	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	-	CLEAN
https://community.cloudflare.steamstatic.com/public/shared/images/header/logo_steam.svg?t=962016	-	172.64.150.233, 104.18.37.23	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/shared/javascript/tooltip.js?v=.9Z1XDV02xrmI	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://cdn.discordapp.com/attachments/818120722869911602/884000156729630780/11.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN
https://store.akamai.steamstatic.com/public/shared/images/joinsteam/acct_creation_bg.jpg	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://steamcommunity-a.akamaihd.net/public/shared/images/responsive/logo_valve_footer.png	-	88.221.110.219, 88.221.110.201	-	GET	CLEAN
https://store.akamai.steamstatic.com/public/shared/images/popups/btn_arrow_down_padded.png	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://cdn.discordapp.com/attachments/818120722869911602/884000175457185842/22.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://cdn.discordapp.com/attachments/880449376957390941/889581462108639263/pososi_mudila.webm	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN
https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js	-	104.17.25.14, 104.17.24.14	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/shared/images/responsive/header_menu_hamburger.png	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://cdn.discordapp.com/attachments/818120722869911602/884000199557677076/44.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN
https://steamcommunity.com/favicon.ico	-	2.23.49.250	-	GET	CLEAN
https://store.akamai.steamstatic.com/public/shared/images/header/btn_header_installsteam_download.png?v=1	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN
https://code.jquery.com/jquery-3.6.0.min.js	-	69.16.175.42, 69.16.175.10	-	GET	CLEAN
https://discord.com/assets/91a561ed8fe1c491df40.js	-	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	GET	CLEAN
https://cdn.discordapp.com/attachments/880449376957390941/880495556596744252/779a770c34fcb823a598a7277301adaf.png	-	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	GET	CLEAN
https://steamstore-a.akamaihd.net/public/shared/css/buttons.css?v=l3li_MNwxNDv&l=russian	-	88.221.110.137, 88.221.110.209	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
dlscordjbost.com	188.114.96.3, 188.114.97.3	-	TCP, TLS, HTTPS, DNS, UDP	SUSPICIOUS
store.cloudflare.steamstatic.com	172.64.150.233, 104.18.37.23	-	TLS, HTTPS, TCP, DNS	CLEAN
steamstore-a.akamaihd.net	88.221.110.137, 88.221.110.209	-	TLS, HTTPS, TCP, DNS	CLEAN
community.cloudflare.steamstatic.com	172.64.150.233, 104.18.37.23	-	TLS, HTTPS, TCP, DNS	CLEAN
steamcommunity.com	2.23.49.250	-	TLS, HTTPS, TCP, DNS	CLEAN
steamstore-a.akamaihd.net.edgesuite.net	88.221.110.137, 88.221.110.209	-	TLS, HTTPS, TCP, DNS	CLEAN
store.akamai.steamstatic.com	88.221.110.137, 88.221.110.209	-	TLS, HTTPS, TCP, DNS	CLEAN
a1737.b.akamai.net	88.221.110.137, 88.221.110.209	-	TLS, HTTPS, TCP, DNS	CLEAN
a1697.b.akamai.net	88.221.110.219, 88.221.110.201	-	HTTPS, TCP, DNS	CLEAN
cds.s5x3j6q5.hwcdn.net	69.16.175.42, 69.16.175.10	-	TLS, HTTPS, TCP, DNS	CLEAN
cdn.discordapp.com	162.159.129.233, 162.159.133.233, 162.159.130.233, 162.159.134.233, 162.159.135.233	-	UDP, HTTPS, TCP, DNS	CLEAN
discord.com	162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232, 162.159.136.232	-	TCP, TLS, HTTPS, DNS, UDP	CLEAN
steamcommunity-a.akamaihd.net.edgesuite.net	88.221.110.219, 88.221.110.201	-	HTTPS, TCP, DNS	CLEAN
code.jquery.com	69.16.175.42, 69.16.175.10	-	TLS, HTTPS, TCP, DNS	CLEAN
steamcommunity-a.akamaihd.net	88.221.110.219, 88.221.110.201	-	HTTPS, TCP, DNS	CLEAN
cdnjs.cloudflare.com	104.17.25.14, 104.17.24.14	-	HTTPS, TCP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
88.221.110.219	steamcommunity-a.akamaihd.net, steamcommunity-a.akamaihd.net.edgesuite.net, a1697.b.akamai.net	Germany	DNS	CLEAN
104.17.25.14	cdnjs.cloudflare.com	-	DNS	CLEAN
104.17.24.14	cdnjs.cloudflare.com	-	HTTPS, TCP, DNS	CLEAN
162.159.128.233	discord.com	-	DNS	CLEAN
162.159.137.232	discord.com	-	TCP, TLS, HTTPS, DNS, UDP	CLEAN
88.221.110.209	steamstore-a.akamaihd.net, steamstore-a.akamaihd.net.edgesuite.net, store.akamai.steamstatic.com, a1737.b.akamai.net	Germany	TLS, HTTPS, TCP, DNS	CLEAN
162.159.133.233	cdn.discordapp.com	-	UDP, HTTPS, TCP, DNS	CLEAN
69.16.175.42	code.jquery.com, cds.s5x3j6q5.hwcdn.net	United States	TLS, HTTPS, TCP, DNS	CLEAN
88.221.110.201	steamcommunity-a.akamaihd.net, steamcommunity-a.akamaihd.net.edgesuite.net, a1697.b.akamai.net	Germany	HTTPS, TCP, DNS	CLEAN
188.114.96.3	dlscordjbost.com	Netherlands	TCP, TLS, HTTPS, DNS, UDP	CLEAN
162.159.136.232	discord.com	-	DNS	CLEAN
162.159.130.233	cdn.discordapp.com	-	DNS	CLEAN
88.221.110.137	steamstore-a.akamaihd.net, steamstore-a.akamaihd.net.edgesuite.net, store.akamai.steamstatic.com, a1737.b.akamai.net	Germany	DNS	CLEAN
104.18.37.23	community.cloudflare.steamstatic.com, store.cloudflare.steamstatic.com	-	DNS	CLEAN
188.114.97.3	dlscordjbost.com	Netherlands	DNS	CLEAN
2.23.49.250	steamcommunity.com	Germany	TLS, HTTPS, TCP, DNS	CLEAN
162.159.138.232	discord.com	-	DNS	CLEAN
162.159.135.232	discord.com	-	DNS	CLEAN
69.16.175.10	code.jquery.com, cds.s5x3j6q5.hwcdn.net	United States	DNS	CLEAN
162.159.135.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.134.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.129.233	cdn.discordapp.com	-	DNS	CLEAN
172.64.150.233	community.cloudflare.steamstatic.com, store.cloudflare.steamstatic.com	United States	TLS, HTTPS, TCP, 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	4.7.0
Web Engine Version	1.5.0 / 10/11/2022 03:25
Static Engine Version	4.7.0.0 / 2022-10-11 02:00:18
AV Exceptions Version	4.7.1.7 / 2022-10-27 16:01:27
ML Detection Models Version	4.7.1.7 / 2022-10-27 16:01:27
Link Detonation Heuristics Version	4.7.1.8 / 2022-10-30 09:01:20
Signature Trust Store Version	4.7.1.8 / 2022-10-30 09:01:20
VMRay Threat Identifiers Version	4.7.1.12 / 2022-11-15 10:04:31
Web Engine Auto UI Rules Version	4.7.1.7 / 2022-10-27 16:01:27
YARA Built-in Ruleset Version	4.7.1.10

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	90.0.4430.85
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

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