Notable DDoS Attack Tools and Services Supporting Hacktivist Operations in 2023

blog.cyble.com/2023/05/24/notable-ddos-attack-tools-and-services-supporting-hacktivist-operations-in-2023/

May 24, 2023

Increased Adoption of Affordable DDoS Services

Executive Summary

Hacktivism, a combination of hacking and uncontrolled activism supported by political or social goals, has been spreading societal concerns and aiming its attention at both public and private institutions. In 2022, Cyble Research and Intelligence Labs (CRIL) observed that pro-Russian hacktivist groups such as Killnet, UserSec, GhostSec, Noname057, and various pro-Ukrainian anonymous collectives were highly concentrated in launching coordinated DDoS, breaches, and other cyber-attacks impacting state and private entities around the globe.

The beginning of 2023 highlighted another stream of groups, such as Anonymous Sudan, Team Mysterious Bangladesh, Team Insane Pk, Hacktivist Indonesia, Ganosec team, Anonymous India, Indian Cyber Force, Kerala Cyber Xtractors that were observed aggravating DDoS attacks and defacements, for their religious beliefs and political agendas driven by either state or non-state actors.

Evidently, DDoS attacks have become a prime tactic for hacktivist groups, among all the other attack methods, for causing disruptions of any internet-facing digital infrastructure or services. Subsequently, various groups continue to emerge catering to the requirement for convenient and cost-friendly tools and resources for launching DDoS attacks. This report provides an overview of the most active and newly introduced DDoS tools and services used by threat actors and hacktivist groups during 2023 for their malicious campaigns against states and private entities.

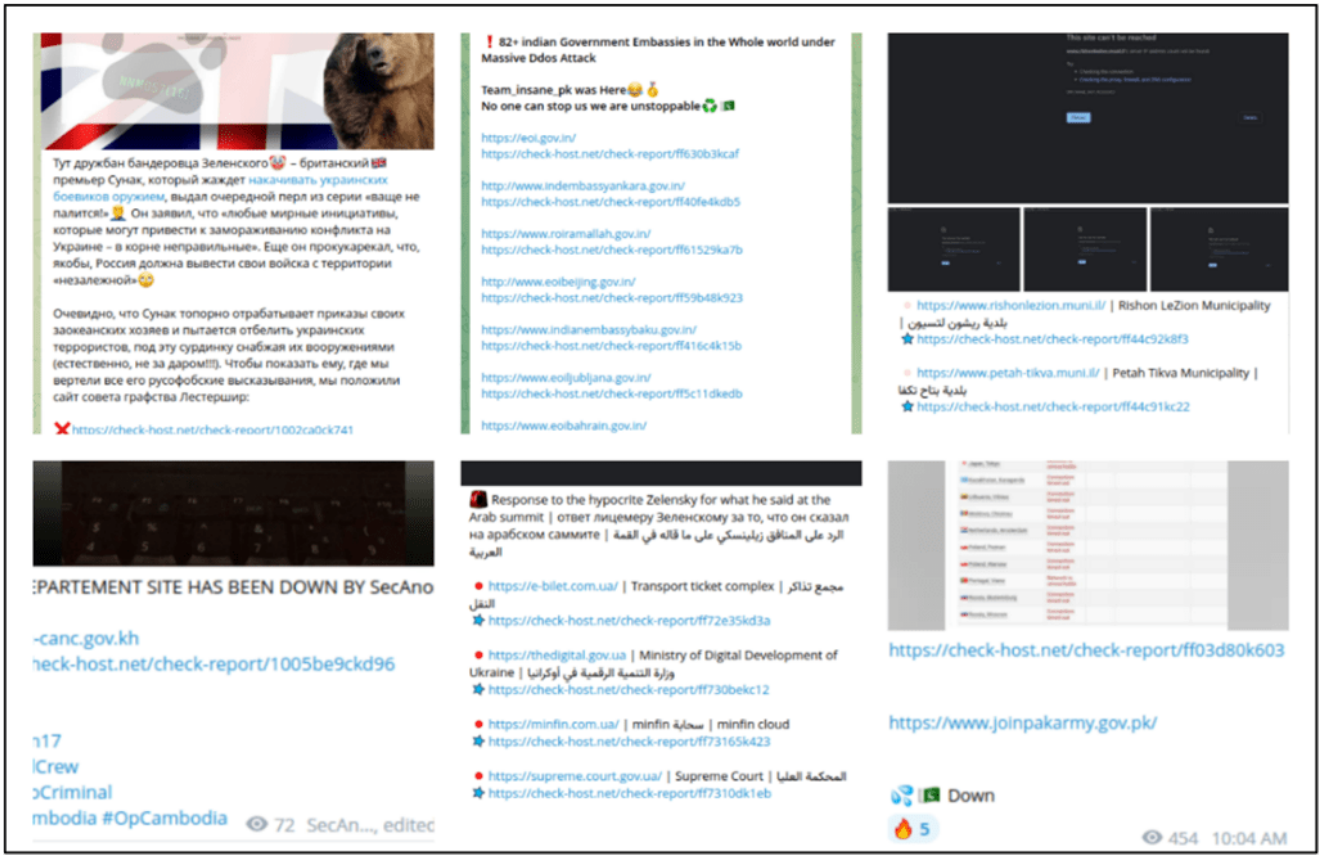

Figure 1: Recent hacktivist campaigns

RedStress.io DDoS Panel

RedStress, a web-based IP stresser service, offers a convenient panel to launch anonymous DDoS attacks on a target server/website/IP, starting from USD 35 per month.

The service is accessible via the website and is operated by the threat actor behind the pseudonym **Mercado**. The threat actors also operate a Telegram channel and Discord server to promote their DDoS service. The Telegram channel had 10,753 subscribers at the time of conducting this analysis.

There are three pricing packages in their plans – Normal network (300K Packet Per Second Per concurrent) & VIP network (600K Packet Per Second Per concurrent) & Private network (1 million Packet Per Second Per concurrent).

Their service plans start from an affordable pricing of USD 35 per month with the capability to launch an attack for a maximum of 1,200 seconds and go up to USD 9,800 per month with the capability to launch an attack for 86,400 seconds (24Hrs.) via 150 nodes concurrently. The service claims to have 40 dedicated servers to support their methods.

Apart from paid subscriptions, the service also offers a free method dubbed 'HTTP-Killer' for threat actors to target small home networks or unsecured websites.

The dashboard of the service suggests that 21,043 users have registered on the website, and the DDoS panel has launched 1,261,855 attacks to date.

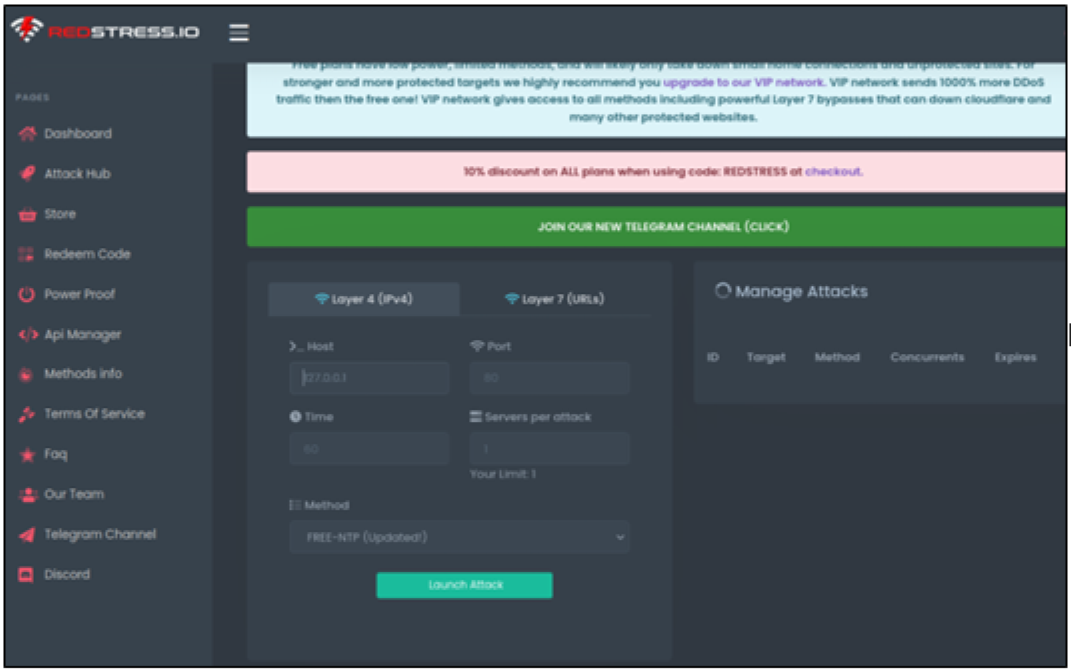

Figure 2: Redstress attack Interface

The DDoS attack methods offered by Redstress are as follows:

Amplification Attacks:

- *CLDAP*
- *NTP*
- *ARD*
- *DVR*
- *SNMP*
- *DNS*

Layer 4 Attacks:

- *UDP-ROCKET*
- *UDP-BYPASS*
- *UDP-GAME*
- *SYN*

- *TCP-PRO (SYN+ACK)*
- *ACK*
- *TCP-GAME (For TCP protocol game servers)*

Layer 7 Attacks:

- *GAME-REKT (Targets CS: GO, ARMA 3, PUBG, ARK)*
- *HTTP-KILLER (Method for free users)*
- *HTTP-BYPASS (Hits with over 20,000 different IPs located worldwide)*
- *HTTP-RAW*

Bypass Methods:

- *OVH-UDP*
- *OVH-TCP*
- *OVH-PACKET*
- *TCP-BYPASS (Firewall Bypass)*
- *CLOUDFLARE-BYPASS (Sends requests using Chrome browser and acts like a real visitor, can bypass Cloudflare UAM and other JS challenges and protections)*
- *CAPTCHA-BYPASS (Can go through Cloudflare Under Attack Mode (5 second challenge), Cloudflare HCAPTCHA and RECAPTCHA, DDoS-Guard, and most other JavaScript-based protections, it only works on HTTPS websites)*

Private Methods:

- *TCP-RED (Sends custom TCP botnet requests)*
- *TCP-REDV2*
- *TCP-REDV3*
- *TCP-THOR*
- *FIVEM-BYPASS*
- *RUST-BYPASS (UDP based)*
- *Minecraft*
- *WSD*

The operators of RedStress have previously targeted game streaming services and cryptocurrency websites to demonstrate their capabilities.

DDosia Project

DDosia is a project started by a pro-Russian threat group dubbed ‘NoName057(16)’ to launch DDoS attacks against those who obliquely or overtly support Ukraine in the war.

A volunteer can download a ZIP archive containing a Windows bot binary and a unique identifier file dubbed 'client_id.txt.' via Telegram. Users are also expected to register at a cryptocurrency wallet to receive monetary benefits at a later stage of the project.

Open-source research suggests that following the agent's execution on the volunteer's computer, the bot registers with the authors' command-and-control (C2) infrastructure. After the C2 servers feed the bot a list of targets, the malicious software starts launching TLS-encrypted Layer 7 and TCP-SYN Denial-of-Service attacks on the specified targets.

The group also releases guides to help the volunteers contribute to the project by targeting adversaries using Android devices.

NoName057(16) operates two Telegram channels, one for Russian and the other for the English-speaking community, to radicalize their subscribers to use their tool in support of Russia.

The Russian language channel has 43,489 subscribers, while the DDosia project group has 9,505 members at the time of conducting our analysis.

Figure 3: NoName057(16)'s advertisement thread on their Telegram channel

Tesla Botnet

Tesla is a newly-launched DDoS botnet active since April 28, 2023, and offers services starting from USD 50 per month.

The pro-Russian threat actor **Radis** operates the Telegram channel to publicize their tool and two other channels for their buyers to post reviews on their DDoS tool. The TA's channel had 765 subscribers at the time. On May 19, 2023, **Radis** also launched an official website to promote their tool.

On May 23, the TA announced the commencement of development of version three of their botnet service, which comes with improved bypass methods and a newly-introduced mode dubbed 'DOOMINATE'.

The service claims to specialize in launching DDoS attacks targeting onion websites with their private method dubbed the 'TOR-KILLER' method.

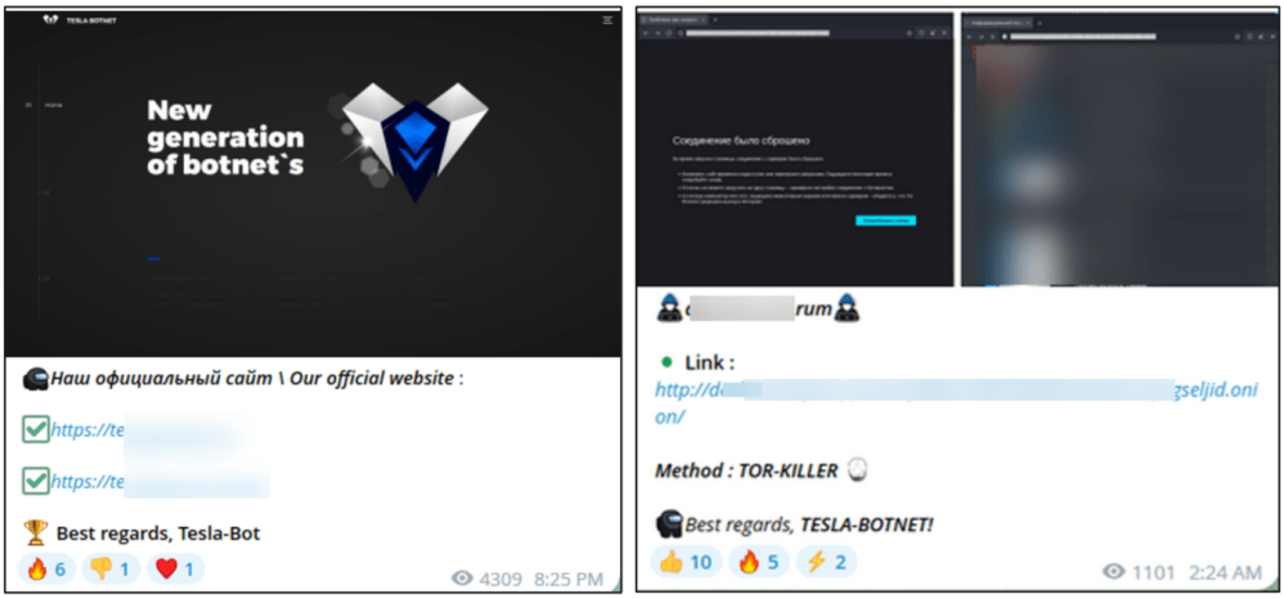

Figure 4: Tesla Bot Advertisements

The other DDoS attack methods offered by Tesla Bot are as follows:

Private Methods:

- *MACAN-TLS*
- *HTTP-FLOOD*
- *TOR-KILLER*
- *SMYKL-FLOOD*

The operators of Tesla Bot recently launched a browser plugin feature to enable DDoS attacks on any target from the browser. The TA has targeted websites of the United States Department of Defense (defense.gov), a Russia-based payment and financial services provider (qiwi.com), and the Central Intelligence Agency (cia.gov) to promote and demonstrate the capabilities of their tools.

The number of views at the bottom of the advertisement suggests that the group is gaining decent popularity in a short span of time, as shown below.

Figure 5: TA's claim of launching a DDoS attack on the US Government

The TA **Radis** also administrates the Telegram channel dubbed **Infinity Hackers,** which was originally established on January 16, 2023, by members of the *infinity.ink* – a cybercrime forum reportedly launched by Russia-aligned hacktivist group **KillMilk**and **Deanon Club**, suggesting an association with Radis.

Stressbot.io DDoS Panel

Stressbot, under the pretense of a legitimate web-based IP stresser service, offers malicious actors and groups a convenient way to launch DDoS attacks on a target server/website/IP, starting from USD 30 per month.

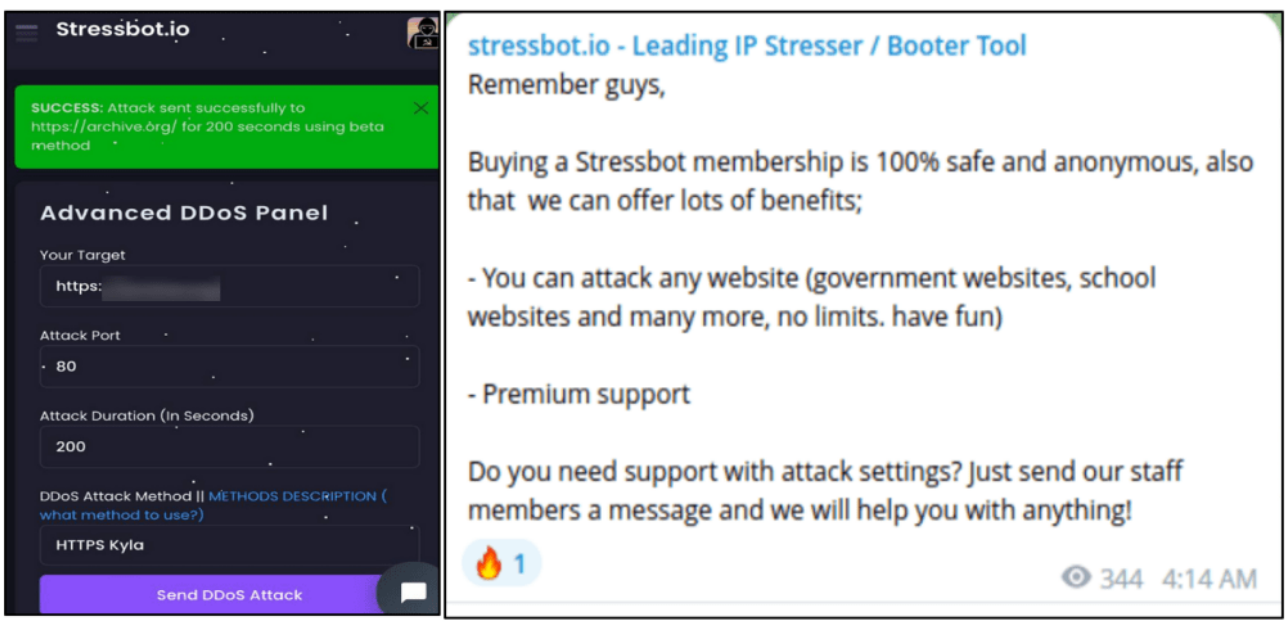

Figure 6: Stressbot tool & TA's advertisement thread on their Telegram channel

The service is accessible via the website and is operated by the threat actor behind the pseudonym **Aleksey Chekaldin**. The TA also operates a Telegram channel to promote their DDoS service to anonymously target government and private entities. The Telegram channel had 1,284 subscribers at the time.

The DDoS attack methods offered by Stressbot are as follows:

Layer 4 Attacks:

- *NTP*
- *ARD*
- *DVR*
- *LDAP*
- *TCP-BYPASS*
- *UDP-BYPASS*

Layer 7 Attacks:

- *HTTP-GET*
- *HTTP POST*
- *HTTPS Ky*
- *xEmulator (bypass)*

Our research also found artifacts suggesting that the pro-Pakistani hacktivist group **Team_insane_pk** has been using DDoS services offered by stressbot.io to launch attacks targeting India and Israel. The TA also promotes Stressbot on their Telegram channel and has been observed recommending others to use it.

Team_insane_pk is a hacktivist group allegedly operated by a team of Threat Actors (TAs) and led by ‘Mr Insane’ aka ‘xxINSANExx’. The group usually claims to launch DDoS attacks on Government and private entities while sharing a link to a status-check website as Proof of Compromise (POC).

Ziyaettin DDoS Botnet

Ziyaettin is a Telegram-based DDoS bot service available from June 2022 within a price range of USD 30 to USD 150 per month.

Figure 7: Ziyaettin DDoS Advertisement (L) and Ziyaettin Bot in Operation (R)

The owner of the botnet, the TA **ziyaettin**, operates a public Telegram channel, “Ziyaettin – Power Proofs”, to share updates and promote their tool. The Telegram channel has 1,573 subscribers at the time of our analysis.

Ziyaettin’s DDoS service offers the following methods:

Amplification Attacks:

- *LDAP*
- *NTP (12 GB concurrent)*
- *DVR*
- *DNS (10+ GB concurrent)*

Layer 4 Attacks:

- *SYNAMP*
- *SYNACK (SYN-TCP+ACK)*
- *SYN (SYN WITH HIGH PPS)*
- *TCPMIX (TCP Mix Flood)*
- *TCPWRA (TCP Bypass)*

Layer 7 Attacks:

- *HTTPGET*
- *TLS-DETECT*
- *TLS-BYPASS (150K RPS)*
- *ZIYBYPASS*
- *ZIYSHAKE*
- *ZIYBYPASS2*
- *TLS-DETECT (AUTO TLS DETECT)*
- *TLS-BYPASS (AUTO BYPASS)*

Bypass Methods:

- *OVH-TCP (OVH Bypass)*
- *UDPBYPASS (UDP flood)*
- *VALVE (UDP with fragmented source query packets)*
- *GAME-UDP (UDP Bypass with crafted payloads)*
- *GAME-NUKE (Steam UDP Bypass with crafted payloads v2)*
- *TCPBYPASS (HIGH PPS)*
- *FIVEM (Bypass for FiveM Servers)*
- *DISCORD (Bypass Discord Call)*

Private Methods:

- *ZIYBYPASS*
- *ZIYBYPASS2*
- *ZIYSHAKE (300K RPS)*

Recently, the TA launched a new functionality dubbed 'ZIYBROWSER', a browser-enabled plugin for the convenient launch of DDoS attacks on a target with a capability of 20-30K Requests Per Second (RPS).

The DDoS services by Ziyaettin have been endorsed in various Telegram channels and groups where notable hacktivist groups such as GhostSec collaborate.

Neferian Empire DDoS Botnet

Neferian Empire offers a command line-based DDoS tool purportedly capable of bypassing DDoS attack protection services offered by Akamai, Cloudflare UAM, BFM, DDoS-Guard, Google Shield, OVH, FiveM, and Amazon DDoS Protection.

According to their posts, their tool was capable of launching 50 Million requests per second for a Layer 7 attack and 1 – 1.2 Terabytes per second (TB/s) for a Layer 4 attack method.

On May 8th, the group posted a visual statistic claiming to have hit 583 Million requests per second against the Cloudflare DDoS protection.

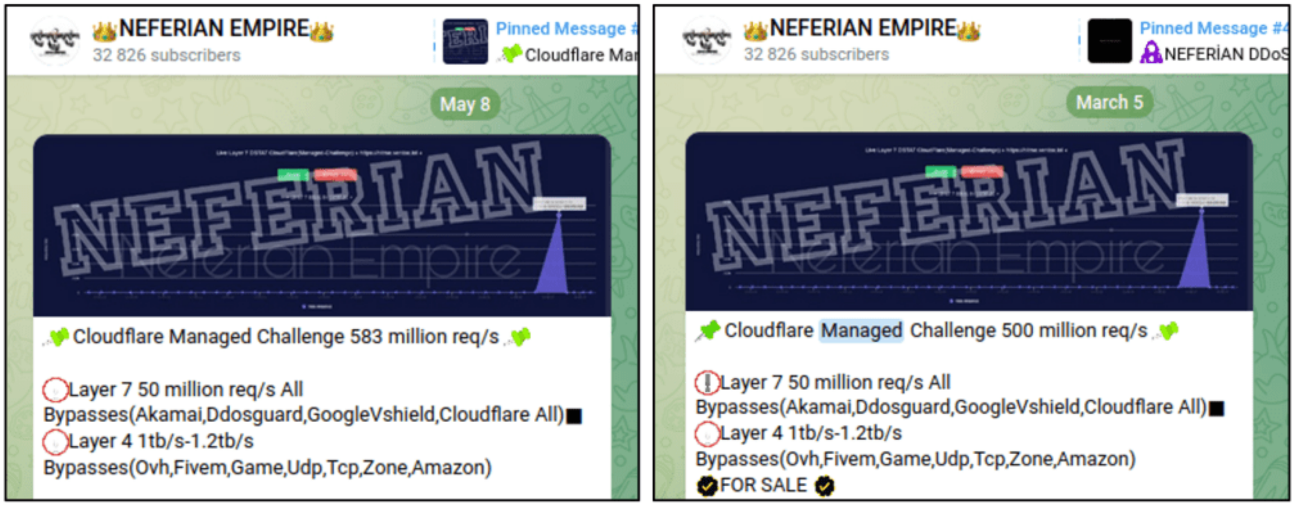

Figure 8: Neferian's Cloudflare Managed Challenge Stats

The DDoS services are operated by the TA **NEFERiAN** and have been marketed on their Telegram channel, established in May 2022, also offering malicious tools, web shells, and stealer logs. The channel had 32,860 subscribers at the time of writing this advisory.

It was observed that the **Neferian Empire** has a tendency similar to the Tesla Bot, to market its DDoS tool by demonstrating live attacks on high-value organizations or targets. In a recent instance, the TA launched DDoS attacks on the websites of Interpol (interpol.int) and the United States Department of Defense (defense.gov) to promote the capabilities of their DDoS tool.

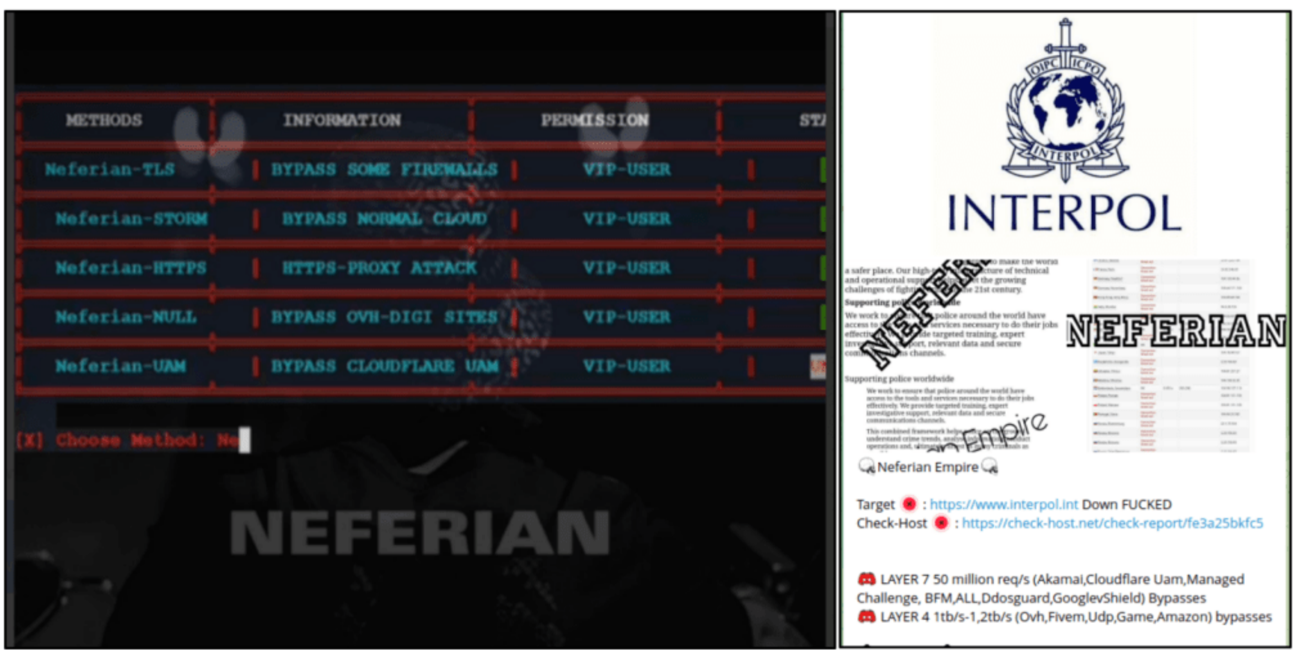

Figure 9: Neferian DDoS tool & the TA's recent advertisement on their Telegram channel

Artemis C2 DDoS Botnet

Artemis C2 is a newly established DDoS botnet operating since May 1, 2023, and offers services starting from USD 15 per month. The service claims to specialize in launching DDoS attacks targeting Rainbow Six Siege and Minecraft servers.

Artemis C2 is maintained and operated by the threat actors **cryptopsycho**and **ritz**. They maintain a Telegram channelto promote their tool and a private group for discussion with other threat actors and potential buyers.

The Telegram channel, at the time of writing this advisory, has 141 subscribers. They also plan to launch their own Discord server, an Onion website, and a store on Sellix.

The DDoS attack methods offered by Artemis are as follows:

Amplification Attacks:

DNS

Layer 4 Attacks:

- *TCP*
- *UDP*

Layer 7 Attacks:

- *Https*
- *Httpv2*
- *TLS*

Private Methods:

- *OVH Bypass*
- *FiveM Bypass*
- *Socket*

Our research revealed that pro-Pakistani hacktivist group **Team_insane_pk** has been promoting on their Telegram channel to leverage Artemis C2 for their DDoS campaigns targeting India. This indicates a potential association with the owner of the tools. However, our sources suggest that the hacktivist group does not have any links with the developer of Artemis C2.

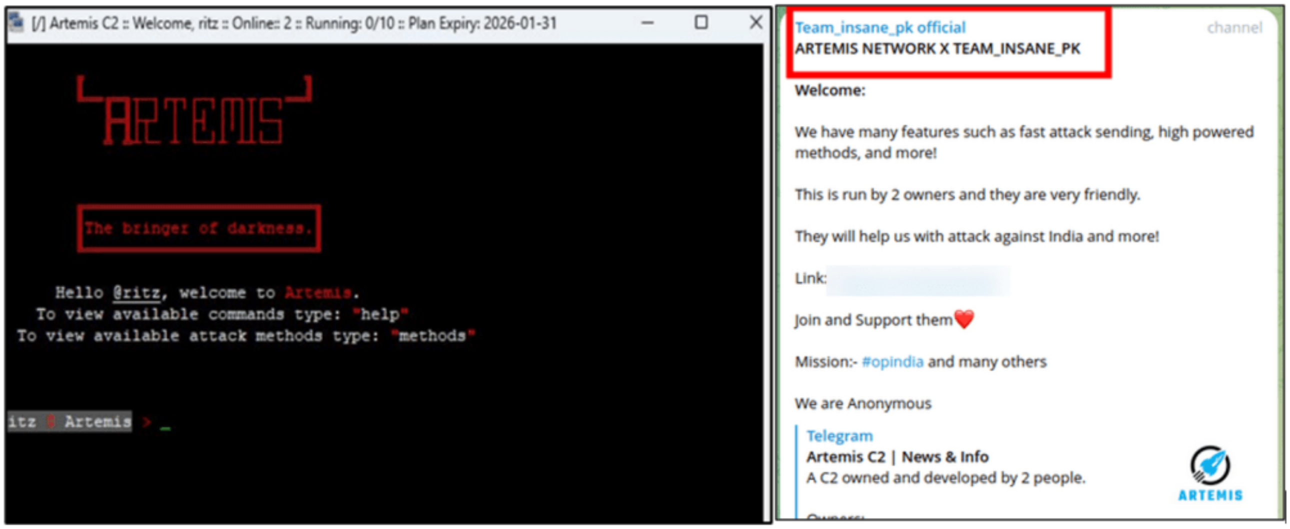

Figure 10: Artemis tool & Team_insane_pk promoting their tool on their Telegram channel

SkyElite-Net DDoS

SkyElite-Net is a newly launched DDoS bot started on May 8, 2023, by the TA **skyzz**.

The TA **skyzz** operates two Telegram channels; the first one has 57 subscribers and offers private DDoS methods along with offering DDoS service to its users, and the second one is used to post reviews received from buyers.

On May 22, 2023, the TA launched a new method dubbed 'Sky-Bypass' while claiming that it is a Layer 7 attack that can bypass OVH and Cloudflare DDoS protection.

Private Methods:

- *SkyElite-TLS*
- *SkyElye-Flood*

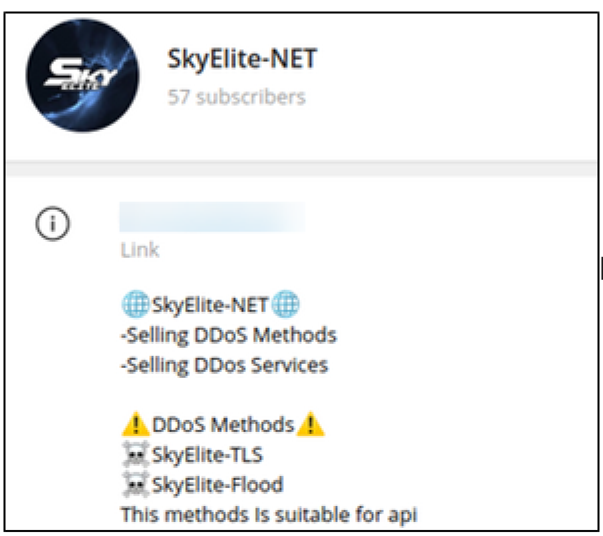

Figure 11: SkyElite-Net's Telegram channel

Open-source research revealed that the TA **skyzz746** is also a member of the private group operated by the **Khalifah cyber community,** a group of Malaysian and Indonesian hacktivists**.**

Recommendations

DDoS has been a mainstay of hacktivists, along with defacements, and are difficult to predict by nature. However, a proactive threat intelligence capability for understanding the adversary and an efficient Denial-of-Service response plan can counter and minimize the impact of an attack.

CERT-IN released the following recommendations to prevent and disrupt web attacks:

Measures for prevention of Denial of Service (DoS/DDoS) attacks:

1. Identify critical services and their priorities. Have a Business Continuity Plan and Disaster Recovery Plan ready for activation in case of emergency.
2. Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.
3. Employ defense-in-depth strategies: emphasize multiple, overlapping and mutually supportive defensive systems to guard against single point failures in any specific technology and protection method.
4. Enable adequate logging mechanisms at perimeter level, server and system level and review the logs at frequent intervals. Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks.
5. Thoroughly scan the network and online applications and plug any existing vulnerability in the network devices, Operating Systems, Server software and application software and apply latest patches/updates as applicable.
6. Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks. Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common attack tools.
7. Continuously monitor the network activities; server logs to detect and mitigate suspicious and malicious activities in your network. Review the traffic patterns [RESTRICTED – Not for Hosting in Public Domain] and logs of perimeter devices to detect anomalies in traffic, network level floods (TCP, UDP, SYN, etc.) and application floods (HTTP GET) etc.
8. Maintain and regularly examine logs of webservers to detect malformed requests/traffic.
9. Preserve all logs indicating type of attack and attack sources.
10. Ensure that Intrusion/DDoS Prevention System contains signatures to detect the attacks launched from common DDoS tools.
11. Maintain list of contacts of ISPs, vendors of network and security devices and contact them as appropriate.

12. Sudden surge in inbound traffic to any critical server or services, such as ICMP floods, UDP/TCP flood etc. could be due to Distributed Denial of Service (DDoS) attacks. If such attacks are observed, implement appropriate response measures in coordination with Internet Service Provider (ISP). In case of high volume of DDoS, consult your ISP to block attack sources and apply appropriate rate limiting strategies.
13. Implement Egress and Ingress filtering at router level.
14. Implement a bogon block list at the network boundary.
15. In case your SLA with ISP includes DDoS mitigation services instruct your staff about the requirements to be sent to ISP.
16. Identify the attack sources. Block the attack sources at Router/Packet filtering device/DDoS prevention solutions. Disable non-essential ports/services.
17. To counter attacks on applications, check the integrity of critical application files periodically and in case of suspicion of attack restore applications and content from trusted backups.
18. Allocate traffic to unaffected available network paths, if possible, to continue the service

References

https://phoenixnap.com/blog/prevent-ddos-attacks
https://www.radware.com/security/threat-advisories-and-attack-reports/project-ddosia-russias-answer-to-disbalancer/
https://flashpoint.io/blog/killnets-infinity-forum-cybercriminals/