Cyberint
A Check Point Company

Hezi Rash: A Rising DDoS Threat

October 2025

TABLE OF CONTENTS

INTRODUCTION

Check Point External Risk Management, has identified Hezi Rash, a nationalist hacktivist group that has rapidly gained traction in the DDoS threat landscape. Established in 2023, Hezi Rash positions itself as a digital defender of Kurdish society, combining strong ideological messaging with targeted cyber operations.

Hezi Rash has claimed or been linked to DDoS attacks (Distributed Denial-of-Service) across a wide range of countries, including Japan, Turkey, Israel, Iran, Iraq, and Germany. These operations demonstrate a clear ideological motive, often tied to real-world provocations blending nationalist and religious themes into their digital warfare.

Although technical details about their attack infrastructure remain limited, DDoS is clearly their primary tactic. Notably, the group appears to align with other well-known hacktivist collectives such as Keymous+, Killnet, and NoName057(16). These alliances likely grant Hezi Rash access to a broader ecosystem of tools, including DDoS-as-a-Service (DaaS) platforms like EliteStress and attack toolkits such as DDoSia and Abyssal DDoS v3.

This report explores the group's origins, ideological motives, and attack patterns. It also provides statistical insights into their operations and examines the DDoS tools most plausibly associated with Hezi Rash based on open-source intelligence and observed affiliations, followed by actionable recommendations for cyber security professionals.

BACKGROUND

Hezi Rash (Kurdish: “Black Force”) is a nationalist hacktivist group, established in 2023. They describe themselves as a digital collective aiming to protect Kurdish society and fight perceived threats online.

Figure 1: Hezi Rash Logo

On their public page, they state: “A Kurdish national team working to help and protect Kurdish society and raise awareness against cyber violence aims to eliminate threats and evildoers on social media and fights evildoers in order to improve Kurdish society and help Kurds in all four parts and all Kurds. Our team was established in 2023 and continues to serve for the sake of God, religion and nation.”

Operationally, Hezi Rash has focused its campaigns against countries and organizations viewed as hostile to the Kurdish people or to Muslims more broadly, without targeting any specific sector. In one example, the group responded to a depiction of a burning Kurdish flag in a Japanese anime series by launching DDoS attacks against anime-related websites, studios, and associated services.

Figure 2: Burning of Kurdish flag

Hezi Rash has claimed that Japanese society and authorities are becoming increasingly hostile toward Kurds, referencing both the symbolic act of the burning flag and recent incidents where Kurdish migrants reportedly faced hostility.

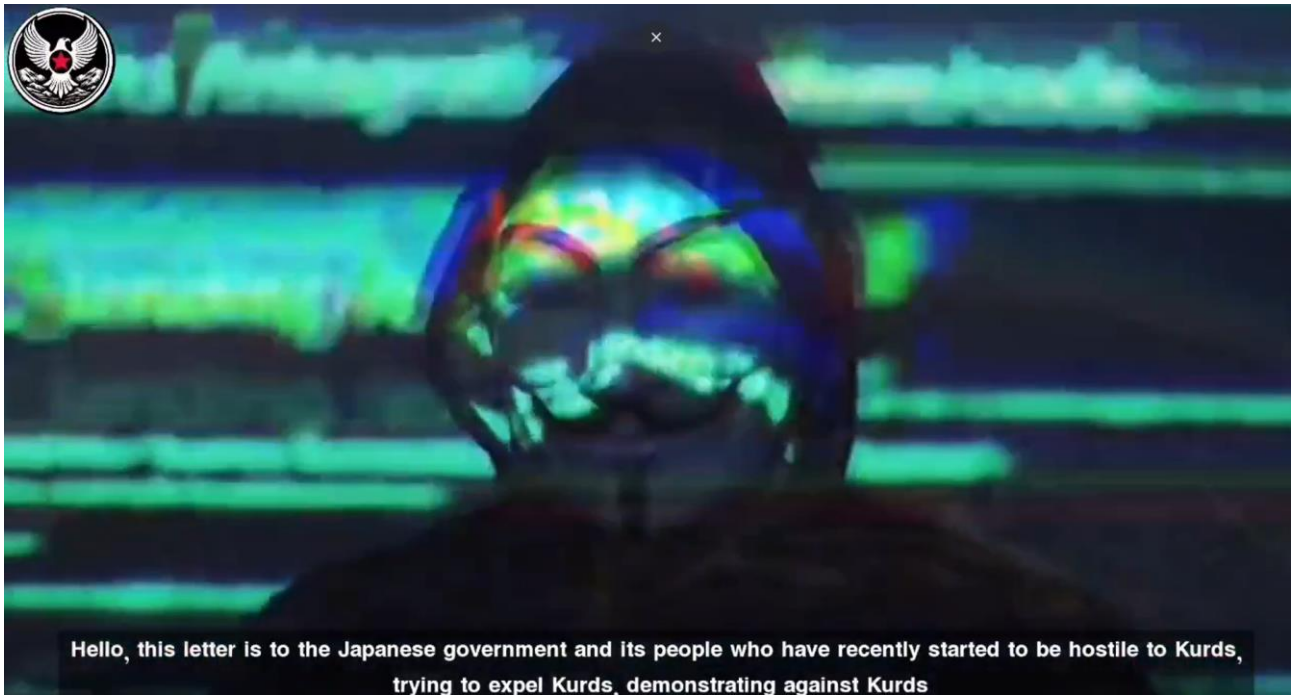

Figure 3: Video by Hezi Rash on the Japanese "Hostility" from X platform

For Hezi Rash, dignity and national symbolism, particularly the Kurdish flag, carry deep cultural importance. However, it is important to note that such incidents appear to be isolated and do not necessarily reflect an official Japanese policy or a coordinated national stance toward the Kurdish population. Similarly, during the #OpIsrael campaign, Hezi Rash targeted Israeli platforms, aligning with broader Islamic hacktivist narratives.

INDICATORS OF COMPROMISE (IOCS):

The following IOCs are attributed to, or associated with, the Hezi Rash threat actor group:

Table 1: IOCs Table

IOC	Description
Guns[.]lol/hezirash	Linktree
hezi-rash[.]ct[.]ws	Main Website
Facebook.com/hezirashkrd	Facebook Account
tiktok.com/@hezi_rash2	TikTok Account

youtube.com/@hezirash	YouTube Account
x.com/hezi_rash	Twitter/X Account
t.me/hezi_rash	Main Telegram Account
t.me/+zk8Mri50AA9kYjZi	Archive Telegram Account

STATISTICS

From early August to early October, Check Point External Risk Management documented approximately **350 DDoS attacks** attributed to Hezi Rash. This volume marks a **notable increase** compared to the typical output of similarly sized hacktivist groups over a comparable time frame. While some of these incidents may have been coordinated with allied groups, the bulk of activity is assessed as originating directly from Hezi Rash.

The sharp rise in attack volume may reflect the group's efforts to establish a stronger presence and reputation in the hacktivist ecosystem. Threat actors often escalate operations aggressively in their early or semi-new phases to gain visibility, credibility, or perceived legitimacy, especially when motivated by ideological or religious narratives. It's also possible that regional developments or symbolic triggers (such as incidents involving Kurdish representation or Muslim identity) contributed to a surge in activity.

Attacks were mapped by date, domain, and geography. The resulting heat map and pie chart (see visual assets) show the distribution of attacks by country, with Japan, Turkey, and Israel as primary targets. Appendix A includes a table of the Country and the distribution of DDoS attacks attributed to Hezi Rash.

Pie Chart of DDoS attacks by country with over 11 incidents:

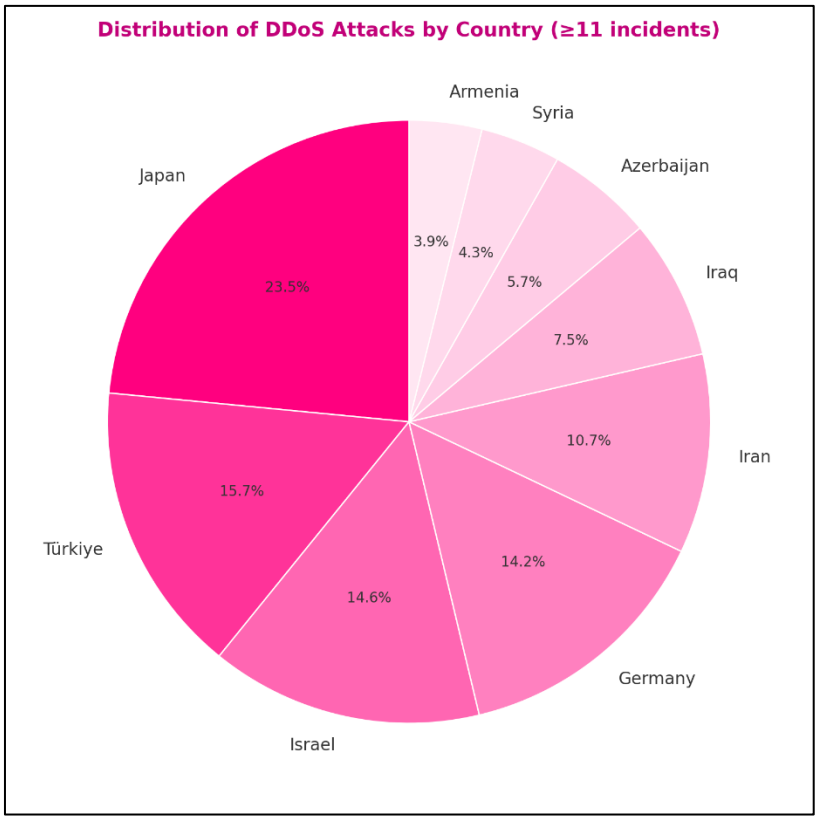

Figure 4: Distribution of DDoS attacks by country

POTENTIAL DDOS TOOLKITS AND SERVICES USED BY HEZI RASH

Hezi Rash does not publicly disclose the means or tools used to carry out their DDoS attacks. However, by analyzing patterns within the broader DDoS threat landscape and examining their known alliances, we can develop informed hypotheses about their operational capabilities and thus derive potential mitigation strategies.

First and foremost, it is important to recognize that threat actors evolve constantly. The tools and techniques they use today may change tomorrow, adapting to new vulnerabilities or bypassing existing defenses. Broadly, DDoS attacks can be categorized into two operational models:

1. Custom Toolkits developed or maintained by threat actors themselves
2. DDoS-as-a-Service (DaaS) platforms, which offer attack capabilities to paying users via subscriptions or pay-per-use schemes

Well established threat groups often operate or leverage DaaS infrastructure, while smaller actors, or ideologically motivated groups like Hezi Rash, frequently rely on services offered by those larger entities. This ecosystem creates a layered web of access, where smaller threat actors tap into the firepower and tools of more organized cybercrime collectives.

In the case of Hezi Rash, no confirmed tool or platform has been publicly attributed to their campaigns. However, several reasonable assumptions can be made:

Alliances with Other Threat Actors: Hezi Rash has demonstrated ideological and operational alignment with other hacktivist groups such as Keymous+. This alliance points to the possible use of EliteStress, a DDoS-as-a-Service platform associated with Keymous+. EliteStress has been linked to hundreds of attacks in recent years, particularly by smaller hacktivist cells.

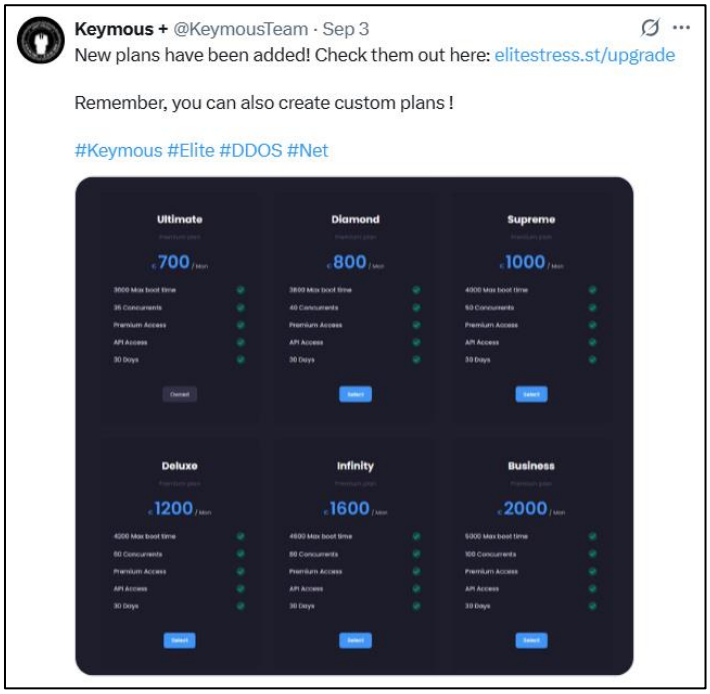

Figure 5: Elitestress promotion through Keymous+ Twitter account

Killnet as a Potential Infrastructure Provider: Another possibility is that Hezi Rash, like other threat actors, leverages infrastructure or botnet access from Killnet, a pro-Russian collective known for orchestrating large-scale DDoS campaigns and operating commercialized booter services.

Toolkits from Larger Affiliates: Beyond DaaS platforms, there are tools like Project DDoSia, maintained by NoName057(16), and Abyssal DDoS v3, developed by Mr. Hamza,

both well-known players in the hacktivist ecosystem. Hezi Rash's indirect connections to these actors suggest a reasonable likelihood that such tools may also be used in their operations.

Figure 6: Hezi Rash collabortation with Noname057(16) through Telegram

While none of these links provide definitive attribution, the convergence of shared ideologies, alliances, and tactics helps form a picture of what tools may be accessible to Hezi Rash.

Although it is not currently possible to confirm the exact DDoS tools or services used by Hezi Rash, the group's known affiliations suggest a high likelihood that they rely on capabilities from prominent DDoS actors such as Keymous+, Killnet, NoName057(16), and Mr. Hamza. Mapping these potential connections provides valuable context for defenders to anticipate the scale and method of future attacks and to deploy appropriate mitigation measures in advance.

It is also important to note that many of these hacktivist alliances appear to be built less on shared ideology and more on mutual interest. Despite operating under different political or religious narratives, these groups frequently collaborate, not necessarily due to aligned motives, but rather as a means of mutual gain. For example, Hezi Rash may use DDoSisa to further its cause, while Noname057(16) benefits from increased exposure and

recognition. This pragmatic, interest-based cooperation is a recurring pattern among ideologically diverse hacktivist actors.

RECOMMENDATIONS

To defend against Hezi Rash's DDoS activity and tools likely used through their alliances, apply the following:

- Use a DDoS mitigation provider (Cloudflare, Akamai, AWS Shield) with pre-built protections for volumetric and HTTP-layer attacks.
- Rate-limit HTTP requests to key endpoints (e.g., /login, /api/search) to mitigate EliteStress and DDoSia request floods.
- Enable WAF challenge pages (e.g., JavaScript challenge, CAPTCHA) to filter bots used by EliteStress.
- Set short connection timeouts and limit concurrent connections per IP to block Abyssal DDoS v3 slow HTTP attacks.
- Block requests from outdated or spoofed user agents, often used by stresser bots.
- Geo-block or challenge requests from regions with no business justification (e.g., via firewall or CDN rules).
- Monitor for abnormal spikes from residential IPs, a sign of volunteer-based tools like DDoSia.

About Check Point External Risk Management

Check Point External Risk Management (Formerly Cyberint) reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web.
A team of global cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including

vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

Together with Check Point's prevention and detection technologies, External Risk Management gives organizations a clearer, more proactive stance against modern ransomware campaigns — helping them spot threats early, manage exposure, and respond before damage escalates.

APPENDIX A

DDoS Attacks by Hezi Rash, from early August to early October, 2025.

Table 2: DDoS attacks per country list

Country	Count
Japan	66
Turkey	47
Israel	42
Germany	39
Iran	30
Iraq	21
Azerbaijan	16
Syria	12
Armenia	11
Georgia	6
Pakistan	4
Ukraine	4
Turkmenistan	4
Norway	4
Czechia	4
European Union	3
USA	3
Yemen	3
Cyprus	2
Lithuania	2
Micronesia	2
Switzerland	2
British Indian Ocean Territory	2
Tuvalu	2
Greece	2
Colombia	1

Kazakhstan	1
China	1
Egypt	1

Contact us

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL
Tel: +972-73-226-4555
5 Shlomo Kaplan Street
6789159

UNITED KINGDOM
Tel: +972-73-226-4555
5 Shlomo Kaplan Street
6789159

USA – TX
Tel: +1-646-568-7813
7250 Dallas Parkway STE 400
Plano, TX 75024-4931

SINGAPORE
Tel: +65-3163-5760
Level 42, Suntec Tower 3,
8 Temasek Boulevard. Singapore 038988

USA – MA
Tel: +1-646-568-7813
22 Boston Wharf Road
Boston, MA 02210

JAPAN
Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com