December 2, 2024

Pro-Russian and Pro-Palestinian Hacktivists Targeting Australian Organizations

Key Insights:

- Over 60 DDoS attacks were conducted by pro-Russian and pro-Palestinian hacktivist groups targeting 39 websites of Australian government institutions, transportation, organization, financial, legal, educational, and insurance entities.
- Pro-Russian group NoName057(16) claimed responsibility for more than half of the attacks, including over a dozen attacks on November 30, 2024, marking the peak of the campaign.
- The attacks were primarily triggered by Australia's decision to provide 14 military boats worth over $9 million to Ukraine, aligning the country with Western support against Russia.
- NoName057(16), Cyber Army of Russia Reborn, and Z-Pentest framed these actions as Australia's escalation in the Ukraine conflict, directly challenging Russian strategic interests.
- RipperSec and allied groups targeted Australia due to its perceived support for Israel in the Israel-Palestine conflict, accusing the nation of complicity in Palestinian oppression.
- By aligning with groups like Fighter Blackhat and the Pro-Palestinian Hacker Movement (PPHM), RipperSec amplified the scale and visibility of its actions as part of a broader campaign.

DDoS Attacks Targeting Australia

Last month, several pro-Russian and pro-Palestinian hacktivists took responsibility for conducting more than 60 cyberattacks against 39 websites of government institutions, transportation, organization[1], financial, legal, education and insurance organizations in Australia. The attacks culminated in the last week with NoName057(16) claiming more than a dozen attacks on Saturday, November 30.

[1] The organization vertical refers to associations organized around a particular industry, profession, or interest group

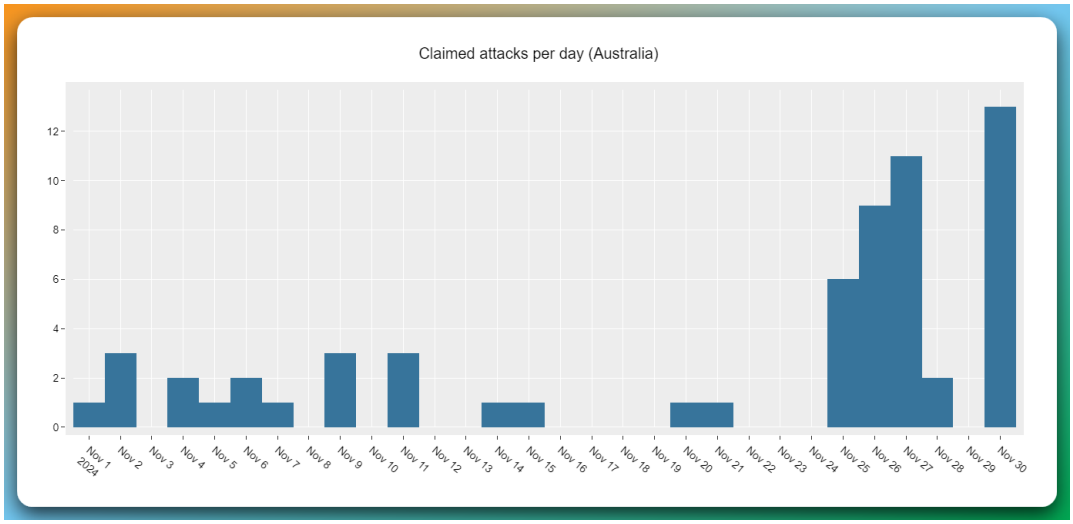

Figure 1: DDoS attack claims per day targeting Australian organizations in November 2024 [source: Radware]

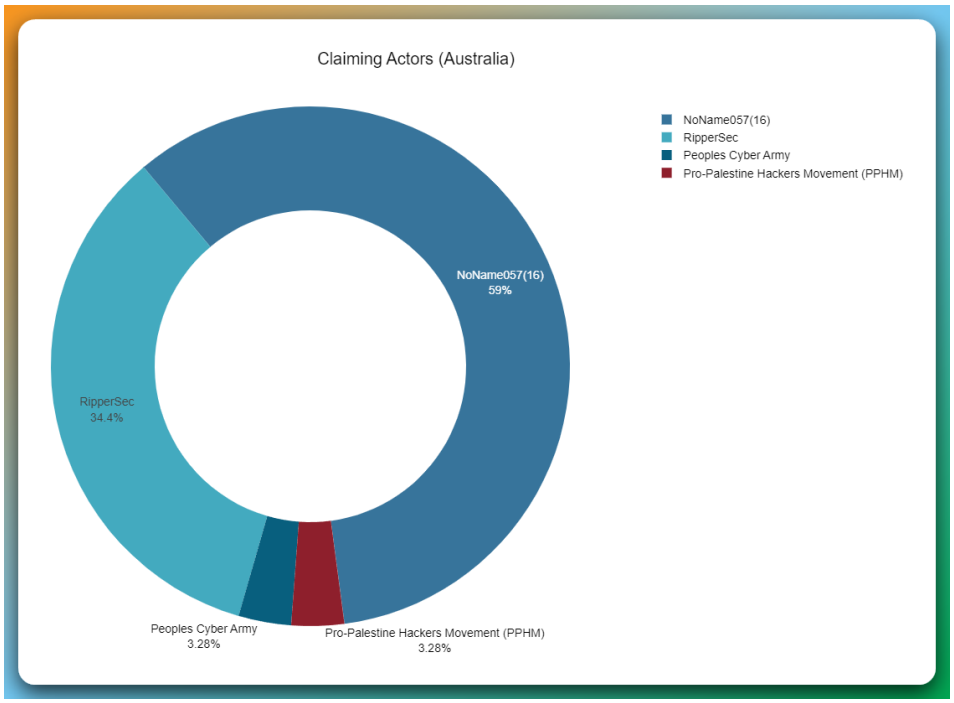

Figure 2: Hacktivists claiming DDoS attacks against Australian organizations in November 2024 [source: Radware]

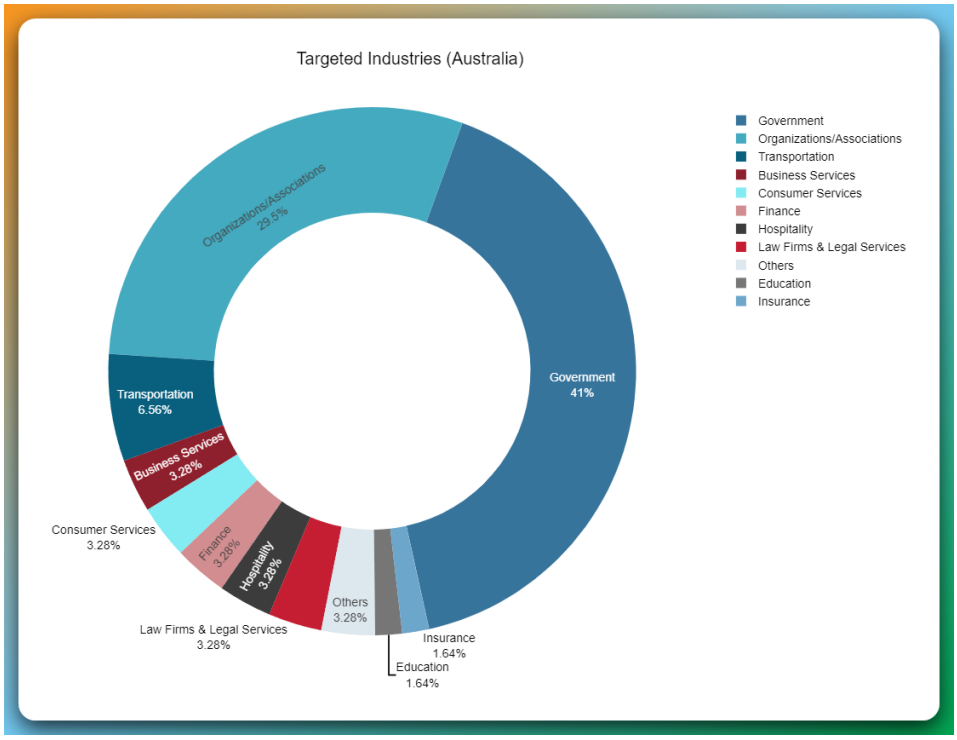

Figure 3: Australian industries targeted by hacktivist DDoS attacks in November 2024 [source: Radware]

Pro-Russian Attack Motivations

The motivations for NoName057(16) and its allies, including the Cyber Army of Russia Reborn, to target Australia last month are rooted in Australia's direct military and logistical support for Ukraine. The Australian government's decision to provide Ukraine with 14 military boats, valued at over $9 million, as part of a larger aid package was a key trigger for the attack campaign. According to the Telegraph Agency of the USSR (TASS), this aid, confirmed by Australian Defense Minister Richard Marles, aims to bolster Ukraine's maritime security and enhance its coast guard capabilities in the ongoing conflict with Russia. From the perspective of these pro-Russian groups, this decision aligns Australia with what they perceive as a hostile Western agenda, supporting Ukraine against Russian interests.

The attack campaign reflects the broader geopolitical motivations of pro-Russian hacktivist groups. These actors view military aid to Ukraine as a direct challenge to Russia's strategic objectives and an extension of NATO-aligned policies. By providing advanced military equipment, Australia is seen as escalating its involvement in the conflict, moving from a neutral or supportive humanitarian stance to active participation in strengthening Ukraine's defense capabilities. This shift solidified Australia as a legitimate target in the eyes of NoName057(16) and its allies.

The campaign was not limited to digital disruption. Z-Pentest, another group aligned with the pro-Russian effort, claimed responsibility for breaches of operational technology systems within

Australia. They alleged access to a sewage pumping station in Melbourne, potentially endangering public health, and interference with cooling systems at a fruit and vegetable warehouse in Sydney, threatening food supply chains. Such claims, whether entirely factual or exaggerated for effect, serve dual purposes:

- Psychological Impact: These attacks aim to sow fear and uncertainty among Australian citizens and businesses.
- Propaganda Value: By publicizing these claims, the groups bolster their image as powerful and capable actors while amplifying their geopolitical message.

Pro-Russian hacktivist groups often seek to undermine and retaliate against nations supporting Ukraine to send a broader message of deterrence and to create public and governmental pressure within those nations. The attacks on Australian infrastructure were designed to highlight vulnerabilities and disrupt daily life as a form of symbolic punishment. By targeting critical infrastructure, the groups aim to draw attention to the "cost" of supporting Ukraine and create a narrative of Australian leadership prioritizing foreign conflict over domestic security.

The participation of allied groups such as the Cyber Army of Russia Reborn and Z-Pentest further underscores the coordinated and multifaceted nature of the pro-Russian hacktivist community. These groups amplify the reach and intensity of campaigns, targeting both high-profile and smaller-scale systems to showcase a broad spectrum of capabilities. This strategy creates a perception of widespread vulnerability while leveraging the publicity generated to reinforce their political narrative.

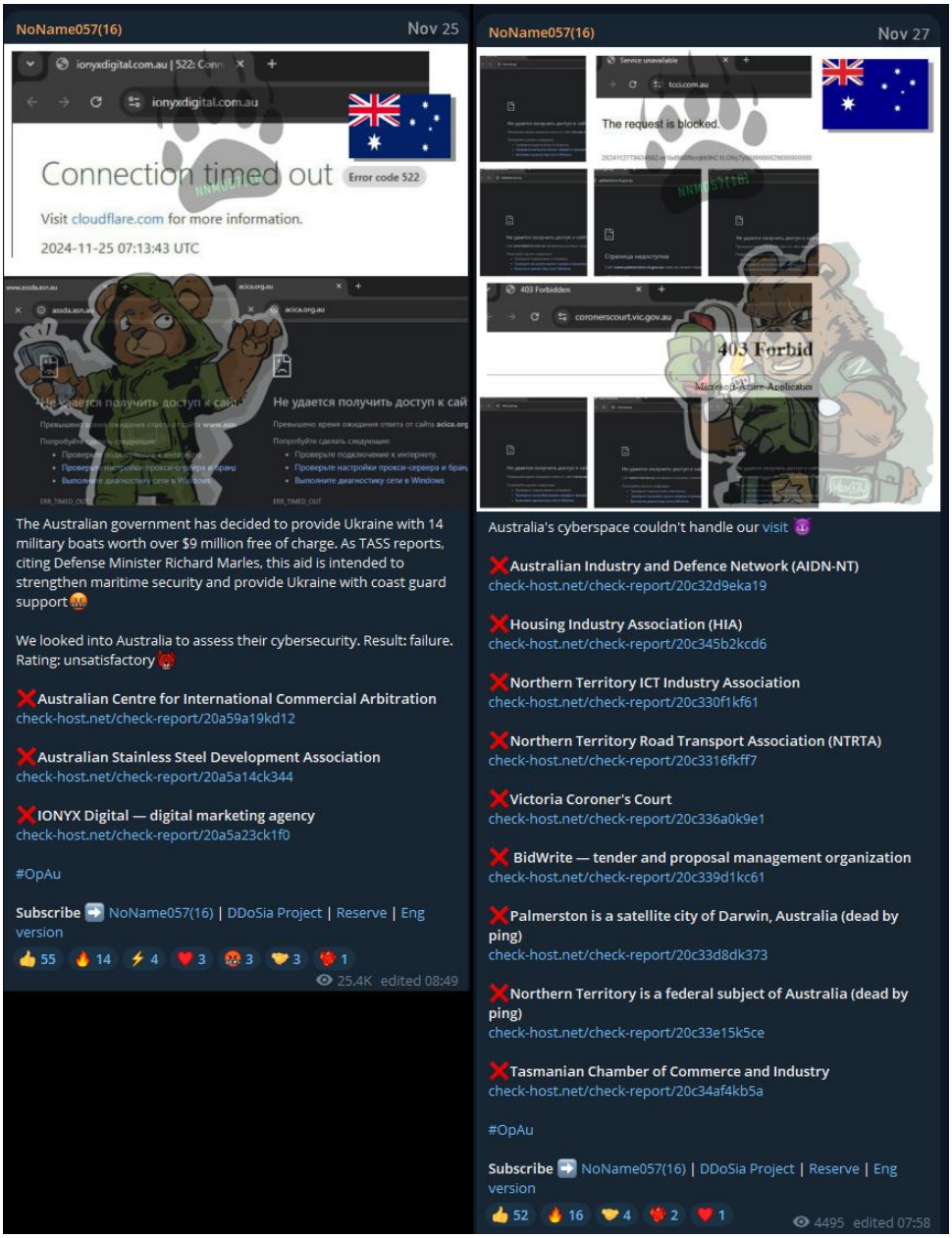

Figure 4: Attack motivations and claims posted by NoName057(16) [source: Telegram]

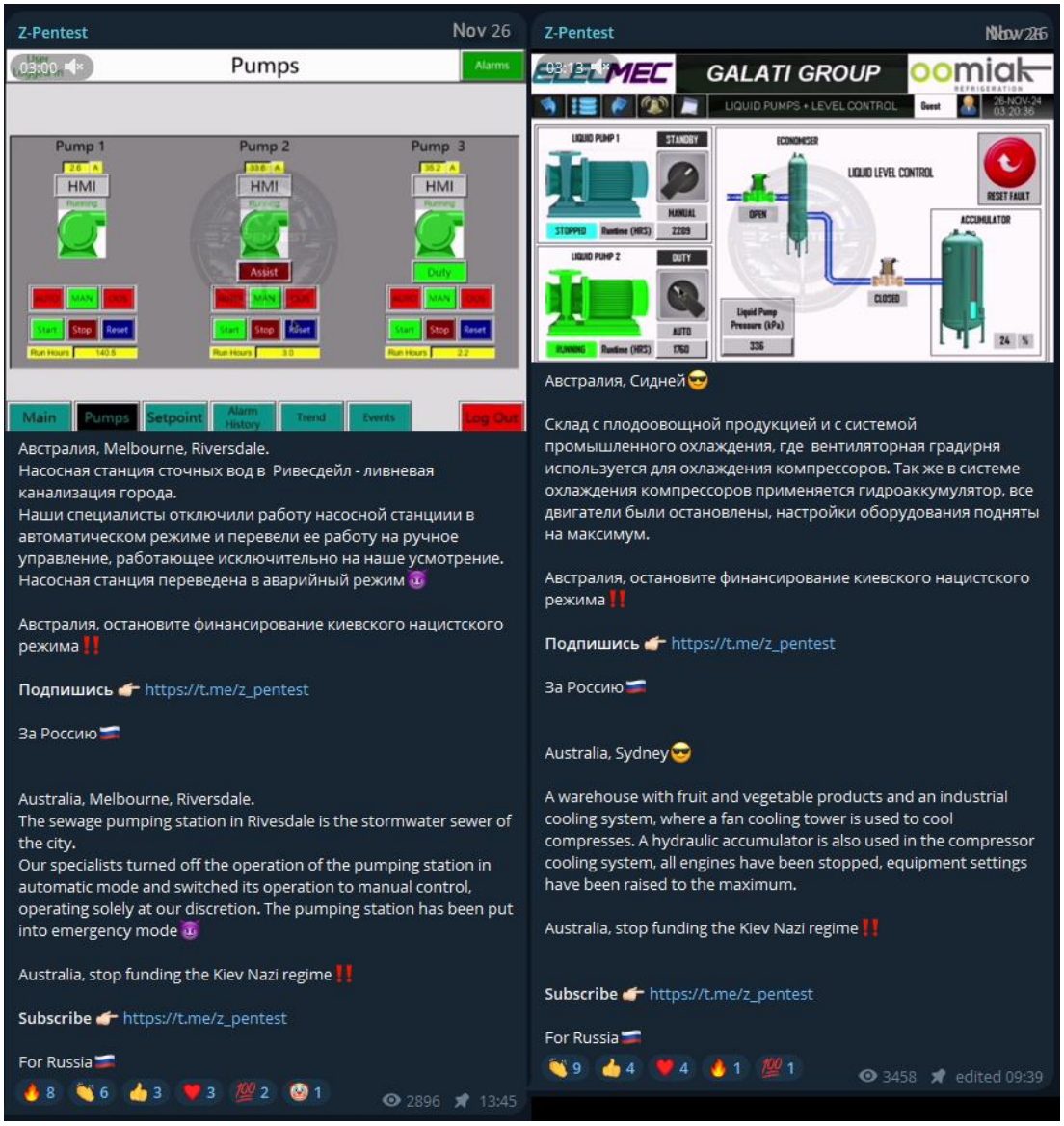

Figure 5: Z-Pentest claiming responsibility for breaches of operational technology systems [source: Telegram]

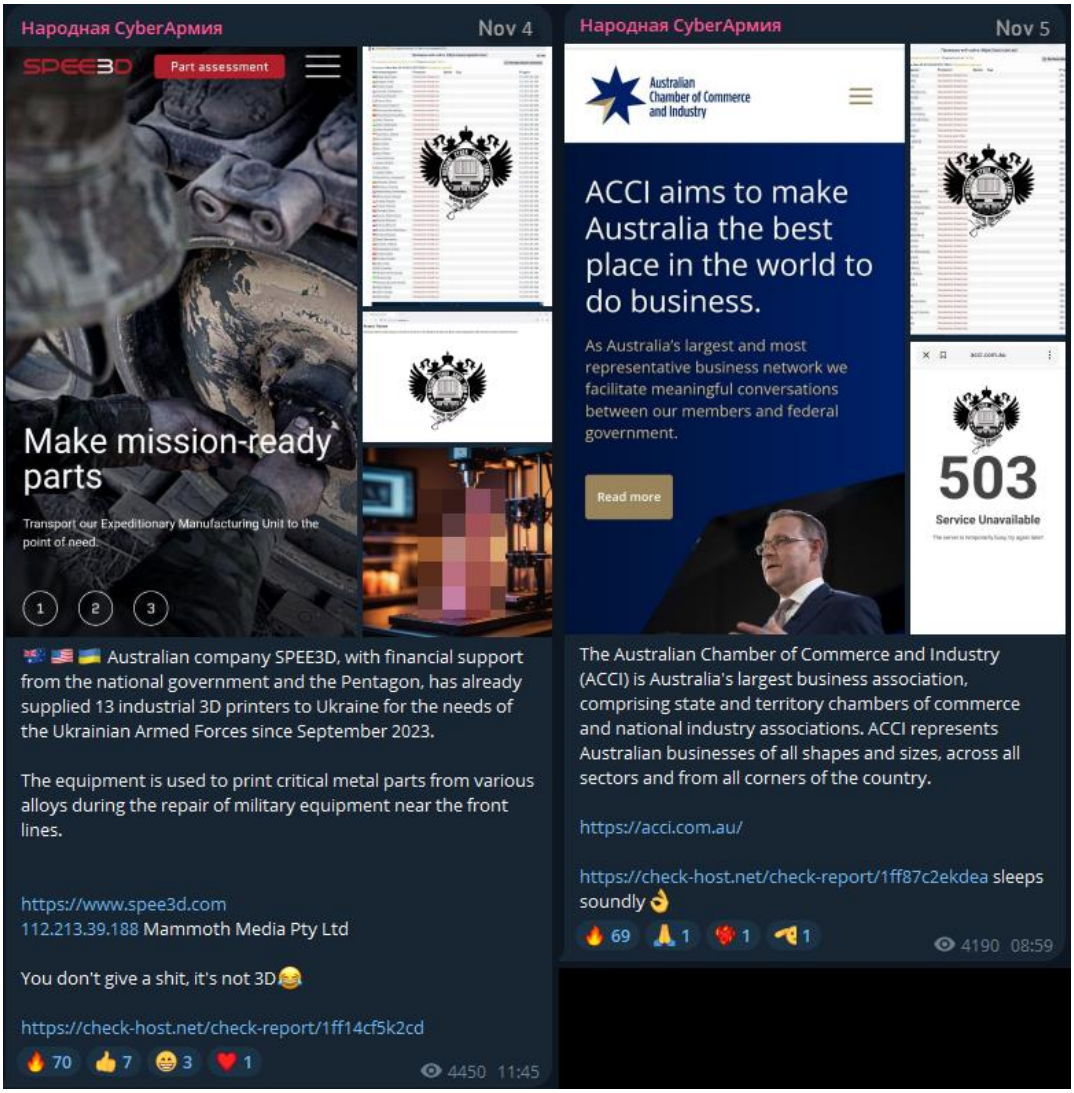

Figure 6: Attack claims posted by Cyber Army of Russia Reborn [source: Telegram]

Pro-Palestinian Attack Motivations

RipperSec's cyberattacks against Australia are primarily driven by their opposition to perceived support for Israel in the ongoing Israel-Palestine conflict. The group explicitly accuses the country of "going too far" in its backing of Israel, which they view as complicit in oppressing Palestine. This ideological alignment with Palestine underscores their stated objective to disrupt and pressure nations until they "open their eyes." For RipperSec, their cyber operations are not only retaliatory but also a symbolic form of activism aimed at drawing global attention to their cause.

The group's rhetoric reflects a larger solidarity with Fighter Blackhat and the Pro-Palestinian Hacker Movement, as they position themselves within a collective effort against Israel and its allies. By aligning with other hacktivist groups, RipperSec amplifies the impact of their actions and portrays their cyberattacks as part of a global resistance. This collaboration highlights their strategic approach, as they leverage the reach and resources of like-minded actors to execute coordinated campaigns and maximize disruption.

RipperSec's campaign is characterized by escalatory and uncompromising language, signaling their intent to create sustained pressure. The declaration of "#OpsAustralia" and "#OpsUkraine" emphasizes the group's plan for a prolonged series of attacks, designed to destabilize and intimidate their targets. Their threats to "destroy" systems highlight the psychological aspect of their campaign, aiming to instill fear among governments, organizations, and citizens of the targeted nations. This rhetoric, combined with their operational focus, demonstrates their belief in cyberattacks as an effective means of political and ideological influence.

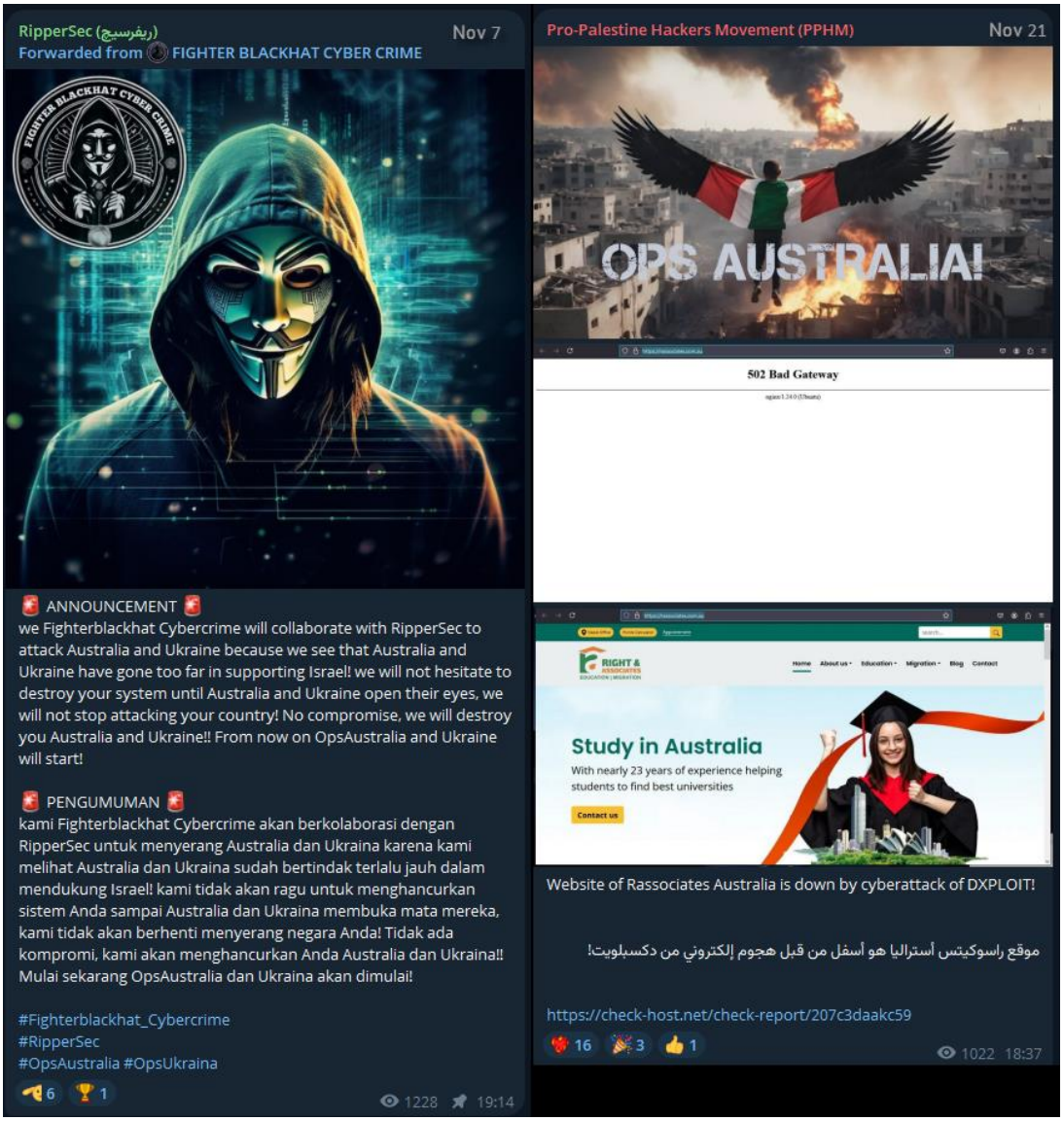

Figure 7: #OpsAustralia announcement and attack claims by RipperSec and the PPHM [source: Telegram]

NoName057(16)

NoName057(16) is a pro-Russian hacktivist group that surfaced shortly after the February 2022 invasion of Ukraine, emerging in direct response to the IT Army of Ukraine's call for volunteers to target Russian entities. This group aligns itself strongly with Russian geopolitical interests, especially regarding the ongoing Ukraine conflict. They manage the DDoSia project, a volunteer-driven and financially incentivized botnet used to launch DDoS attacks against government institutions, critical infrastructure, financial entities, and media outlets in NATO-affiliated nations or any country supporting Ukraine or opposing Russia. To sustain the effectiveness of these volunteer-led attacks, NoName057(16) frequently updates its command-and-control infrastructure. Since February 2022, the group has persistently executed daily DDoS attacks on numerous organizations, making it the most active pro-Russian hacktivist collective since the conflict's onset.

Noname057(16) DDoS Tactics and Techniques

NoName057(16), like many contemporary threat actors, utilizes Layer 7 web DDoS attacks to disrupt their targets' online resources. They rely on a network of volunteers operating their financially incentivized DDosia bot to execute these attacks. What sets NoName057(16) apart is their focused strategy of targeting the backend components of online applications and services.

Before initiating an attack, NoName057(16) conducts thorough reconnaissance on the targeted website to pinpoint the webpages that most critically impact the backend infrastructure, such as search forms and public post forms. They craft specific URLs targeting these high-impact pages and randomize the request data in a way that closely mimics legitimate traffic, making it challenging to distinguish malicious requests from genuine ones.

While their attack volumes typically range in the hundreds of thousands rather than the millions of requests per second (RPS), their precise targeting of backend resources results in a disproportionate impact compared to more generalized Web DDoS attacks. This strategic approach allows NoName057(16) to achieve significant disruption even with relatively moderate attack sizes.

Cyber Army of Russia Reborn (CARR)

The People's Cyber Army, better known as the Cyber Army of Russia Reborn (CARR), is a pro-Russian hacktivist group known for conducting cyber operations against critical infrastructure in Ukraine, the United States, and Europe. Since 2022, CARR has been responsible for a series of DDoS attacks and other malicious activities targeting sectors such as water supply, hydroelectric, wastewater, and energy facilities. In July 2024, the U.S. Department of the Treasury sanctioned two key members of CARR: Yuliya Vladimirovna Pankratova, identified as the group's leader, and Denis Olegovich Degtyarenko, a primary hacker. These sanctions were imposed due to their

involvement in cyber operations against U.S. critical infrastructure. CARR's activities have been characterized by unsophisticated yet disruptive attacks, often leveraging DDoS techniques to overwhelm targeted systems. The group has claimed responsibility for compromising industrial control systems of multiple U.S. and European critical infrastructure targets, posing significant risks to public safety and security. CARR may have affiliations with Russian military intelligence units, such as the GRU's Sandworm team known for executing some of the most disruptive cyberattacks in history. However, definitive evidence linking CARR directly to state-sponsored entities remains a subject of ongoing investigation.

CARR DDoS Tactics and Techniques

CARR primarily conducts DDoS attacks that flood target servers with excessive traffic, aiming to overwhelm systems and disrupt services. These network-level volumetric attacks are generally low in complexity but can cause significant service interruptions.

Z-Pentest

Z-Pentest is a Russian-speaking threat group, likely connected to the Cyber Army of Russia and known for targeting critical infrastructure in various countries. Their activities have included attacks on water treatment facilities in the United States and grain storage facilities in South Korea.

The group's claims often involve manipulating control systems to cause disruptions, such as causing water tanks to overflow or interfering with grain loading equipment. The group's actions align with pro-Russian hacktivist objectives, aiming to create nuisance effects and potentially pose physical threats against insecure operational technology environments.

RipperSec

RipperSec is a pro-Palestinian, pro-Muslim hacktivist group based in Malaysia, active since June 2023. The group has amassed over 5,000 members on its Telegram channel, where it coordinates cyberattacks such as data breaches, website defacements, and Distributed Denial-of-Service (DDoS) attacks. Their primary targets include government and educational websites, as well as organizations perceived to support Israel.

Between January and August 2024, RipperSec claimed responsibility for 196 DDoS attacks, with a significant portion directed at Israel. Other targeted countries include India, the United States, the United Kingdom, and Thailand. The group's attack strategy relies heavily on community involvement, leveraging a network of volunteers and allied hacktivist groups to conduct coordinated cyber campaigns.

RipperSec DDoS Tactics and Techniques

RipperSec's attack activity includes data breaches, defacements and DDoS attacks—anything that creates chaos, attracts attention and causes disruption that's typical for a hacktivist group.

RipperSec employs sophisticated Layer 7 DDoS attack techniques through its proprietary MegaMedusa tool. Created by a member of the group, MegaMedusa is a publicly available Web DDoS tool written in JavaScript and designed for use with the Node.js runtime environment. Node.js enhances the tool's efficiency by enabling asynchronous, non-blocking input/output operations, allowing it to handle a large volume of simultaneous network requests. This cross-platform capability ensures the tool is easily deployable on various operating systems, including Windows, macOS, and Linux, making it accessible to a wide range of attackers.

MegaMedusa is user-friendly, requiring minimal technical expertise to install and operate. The tool's GitHub repository provides a straightforward installation script that allows users to set up the tool within minutes on Linux-based systems or virtual private servers. Once operational, users can customize attack parameters, such as simultaneous threads, request rate (RPS), and attack duration. MegaMedusa also supports proxy distribution, enabling attackers to diversify traffic sources and obfuscate the origin of requests by randomly selecting proxies from a predefined list. This scalability and accessibility make it a preferred tool for executing high-impact Web DDoS attacks.

The strength of MegaMedusa lies in its advanced randomization techniques, which make detection and mitigation challenging. It randomizes various aspects of web requests, including headers, query parameters, cookies, and IP addresses. For instance, it rotates User-Agent strings to mimic requests from different devices and browsers, alters request methods (GET, POST, HEAD), and modifies TLS/SSL configurations for unique handshakes. These techniques ensure that each request appears unique, evading standard detection mechanisms like Web Application Firewalls (WAFs). Additionally, proxy randomization and IP spoofing enhance the tool's ability to simulate a geographically distributed attack.

While MegaMedusa incorporates rudimentary CAPTCHA bypass features and claims to evade several security vendors' protections, its effectiveness is limited against modern security solutions. It does not include advanced CAPTCHA-solving capabilities, relying instead on randomized tokens and headers. However, there is evidence suggesting that RipperSec's core members utilize more sophisticated, private versions of MegaMedusa that may include enhanced bypass techniques and other capabilities not present in the publicly available version. This differentiation indicates that RipperSec's internal operations likely involve more advanced tools tailored for higher-impact attacks.

Pro-Palestine Hackers Movement (PPHM)

The Pro-Palestine Hackers Movement (PPHM) is a pro-Palestinian hacktivist group that has claimed responsibility for cyberattacks against entities associated with Israel and its allies. Their

operations include defacing websites, launching Distributed Denial-of-Service (DDoS) attacks, and leaking sensitive data.

PPHM's actions are part of a broader trend of pro-Palestinian cyber activities, where various groups engage in defacements and disruptive attacks amid geopolitical conflicts. These groups often coordinate to amplify their impact, targeting government and media websites, and sometimes extending their operations to entities in allied nations.

Recommendations

Network-based DDoS protection solutions are ineffective at detecting and mitigating Layer 7 DDoS attacks due to their inability to decrypt attack traffic and inspect Layer 7 headers in detail. As a result, these attacks often bypass traditional network defenses. Similarly, while on-premises or cloud-based web application firewalls (WAFs) are effective against standard web-based threats, they fall short in defending against modern Web DDoS attacks for several reasons:

1. Scale: The volume of Layer 7 attacks, measured in requests per second (RPS), has reached unprecedented levels. In the past year, multiple third-party reports disclosed attacks exceeding millions of RPS. The sheer scale of these attacks overwhelms the capacity of traditional on-premises solutions.
2. Attack Sophistication: These attacks mimic legitimate traffic, constantly randomizing requests to evade detection. Without predefined signatures or rule-based mechanisms to identify malicious behavior, traditional defenses are ineffective. Detecting and mitigating such traffic requires behavioral-based algorithms with self-learning and auto-tuning capabilities.
3. Morphing Attacks: Modern Layer 7 threats are dynamic, frequently evolving, and sustaining changes over extended periods. Standard WAF solutions lack the adaptability to respond in real time to these rapidly shifting attack patterns, leaving organizations vulnerable.
4. Human Factor: The complexity of these attacks demands skilled security teams to maintain effective protection. Limited resources, personnel, and budgets often hinder self-managed teams from addressing 24/7 attack campaigns. Additionally, on-premises tools rely on manual rule definitions, which are insufficient for the pace and sophistication of these threats.

Radware Web DDoS Protection addresses these challenges with advanced behavioral-based algorithms capable of identifying and mitigating unknown malicious requests at scale in real time. Unlike volumetric approaches that fail to distinguish legitimate traffic surges from malicious activity, Radware’s solution accurately identifies and blocks malicious traffic while ensuring legitimate users are not impacted.

The system provides comprehensive protection against a wide range of Layer 7 DDoS threats, including sophisticated, randomized attacks, newly developed tools, and high-scale Web DDoS

campaigns. Radware's adaptive technology continuously analyzes threats and their variants, dynamically responding to evolving attack patterns without generating false positives. By automating the detection and mitigation process, Radware ensures robust, real-time protection tailored to the complexity and scale of modern Layer 7 DDoS attacks.

References and more information

NoName057(16)

- What's in a NoName? Researchers see a lone-wolf DDoS group
- Intel insiders go undercover revealing fresh details into NoName hacktivist operations
- NoName057(16) DDosia Project
- Pro-Russian Hacktivists Target Organizations in Austria With DDoS Attack Campaign
- Pro-Russian Hacktivists Target Organizations in Taiwan With DDoS Attack Campaign
- NoName pro-Russian hackers arrested in Spain, group vows retaliation/

Cyber Army of Russia Reborn (CARR)

- US sanctions two members of Russian 'Cyber Army' hacktivist group
- Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities
- Sanctioning Members of the Cyber Army of Russia Reborn
- Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn

Z-Pentest

- Russian group's hack of Texas water system underscores critical OT cyber threats
- South Korean facilities attacked by Russian hackers over plan to track North's troops
- Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

RipperSec

- MegaMedusa, RipperSec's Public Web DDoS Attack Tool

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.