December 2, 2024

Pro-Russian Hacktivists Targeting Canadian Organizations

> **Key Insights:**
>
> - Over the past week, NoName057(16) claimed responsibility for more than 40 cyberattacks targeting Canadian organizations across telecom, transportation, government, and financial sectors.
> - The attacks are largely driven by Canada's support for Ukraine in its conflict with Russia.
> - NoName057(16) specializes in disrupting the backend of online applications by targeting specific high-impact pages, such as search forms and public post forms.
> - They conduct extensive pre-attack analysis to craft URLs that mimic legitimate traffic and bypass traditional defenses.
> - Their attacks, typically in the hundreds of thousands of requests per second (RPS), deliver outsized impact by precisely targeting backend resources.

DDoS Attacks Targeting Canada

Over the past week, NoName057(16) has taken responsibility for conducting more than 40 cyberattacks against telecom, transportation, government, and financial organizations in Canada. On Sunday, December 1, 2024, the group claimed to have carried out twelve attacks.

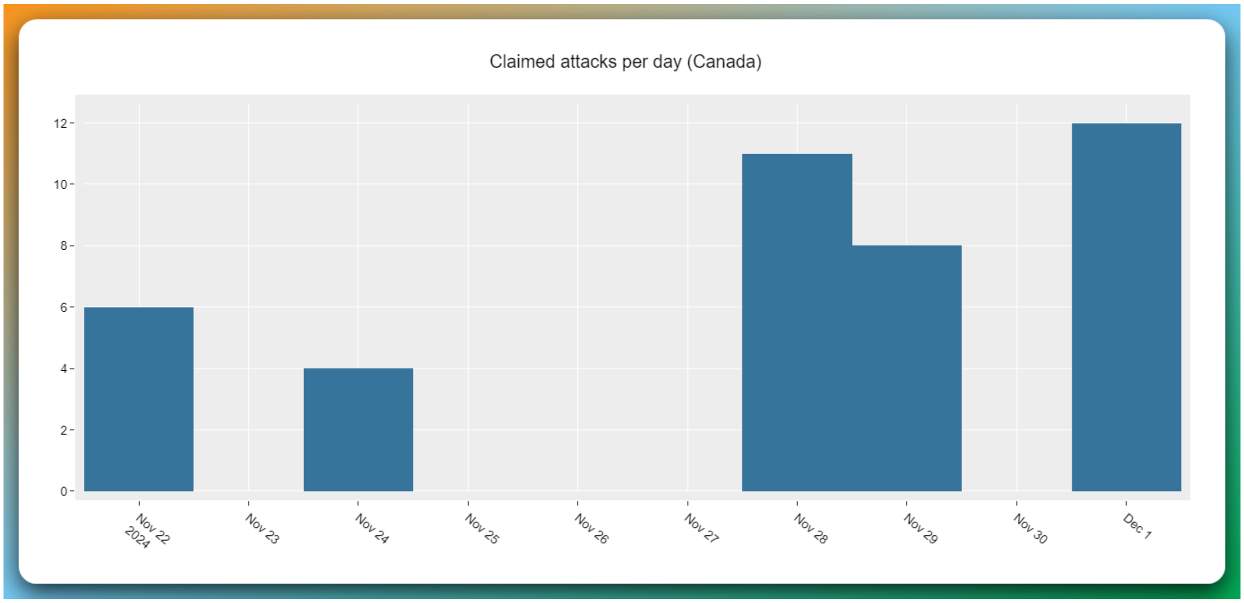
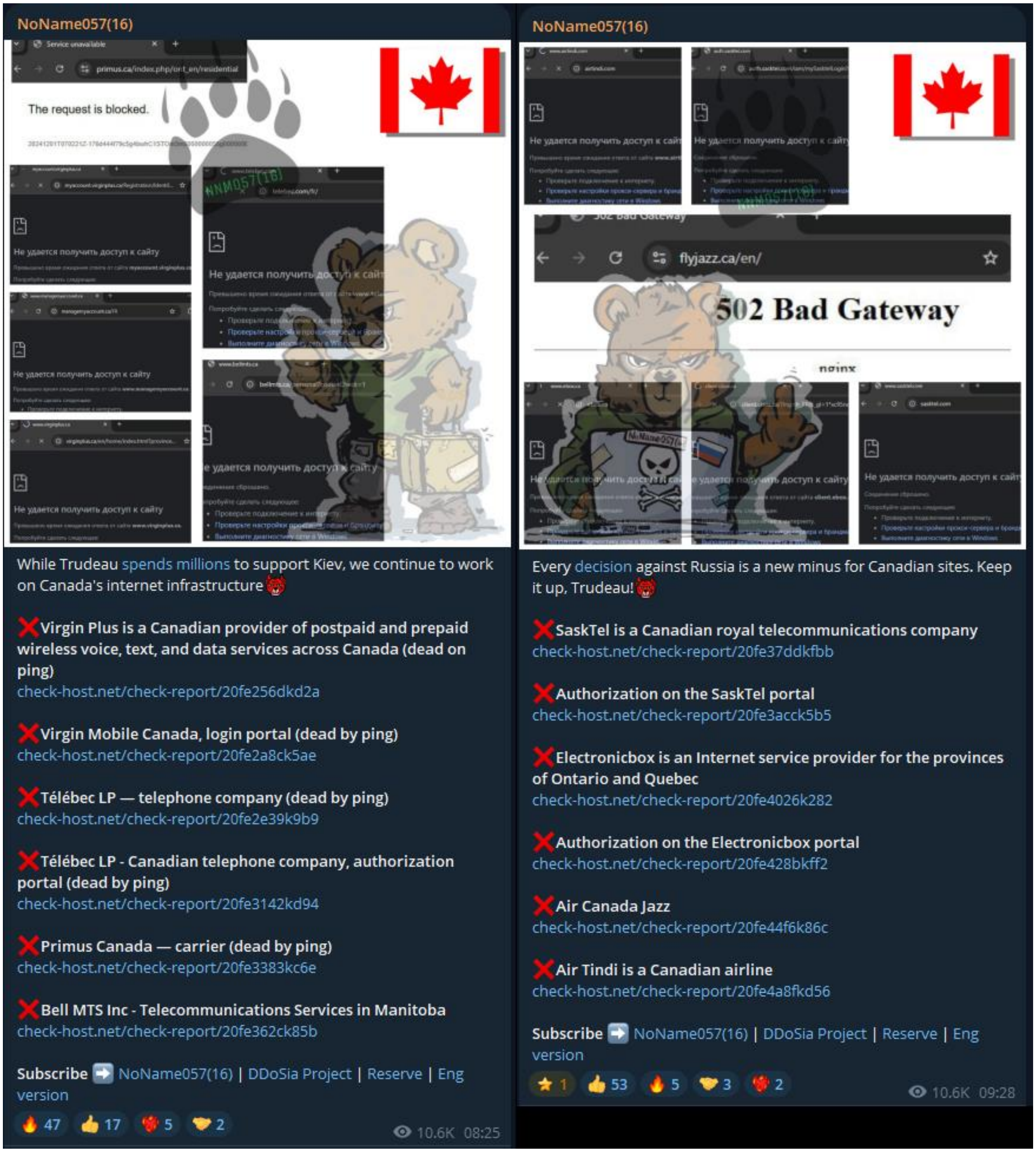


Figure 1: NoName057(16) attack claims per day targeting Canadian organizations [source: Radware]



NoName057(16)

While Trudeau spends millions to support Kiev, we continue to work on Canada's internet infrastructure

❌Virgin Plus is a Canadian provider of postpaid and prepaid wireless voice, text, and data services across Canada (dead on ping)
check-host.net/check-report/20fe256dkd2a

❌Virgin Mobile Canada, login portal (dead by ping)
check-host.net/check-report/20fe2a8ck5ae

❌Télébec LP — telephone company (dead by ping)
check-host.net/check-report/20fe2e39k9b9

❌Télébec LP - Canadian telephone company, authorization portal (dead by ping)
check-host.net/check-report/20fe3142kd94

❌Primus Canada — carrier (dead by ping)
check-host.net/check-report/20fe3383kc6e

❌Bell MTS Inc - Telecommunications Services in Manitoba
check-host.net/check-report/20fe362ck85b

Subscribe ➡️ NoName057(16) | DDoSia Project | Reserve | Eng version

🔥 47 👍 17 5 2 10.6K 08:25

NoName057(16)

Every decision against Russia is a new minus for Canadian sites. Keep it up, Trudeau!

❌SaskTel is a Canadian royal telecommunications company
check-host.net/check-report/20fe37ddkfbb

❌Authorization on the SaskTel portal
check-host.net/check-report/20fe3ack5b5

❌Electronicbox is an Internet service provider for the provinces of Ontario and Quebec
check-host.net/check-report/20fe4026k282

❌Authorization on the Electronicbox portal
check-host.net/check-report/20fe428bkff2

❌Air Canada Jazz
check-host.net/check-report/20fe44f6k86c

❌Air Tindi is a Canadian airline
check-host.net/check-report/20fe4a8fkd56

Subscribe ➡️ NoName057(16) | DDoSia Project | Reserve | Eng version

⭐ 1 👍 53 🔥 5 3 2 10.6K 09:28

Figure 2: Attacks targeting Canada claimed by NoName057(16) on Sunday, December 1, 2024 [source: Telegram]

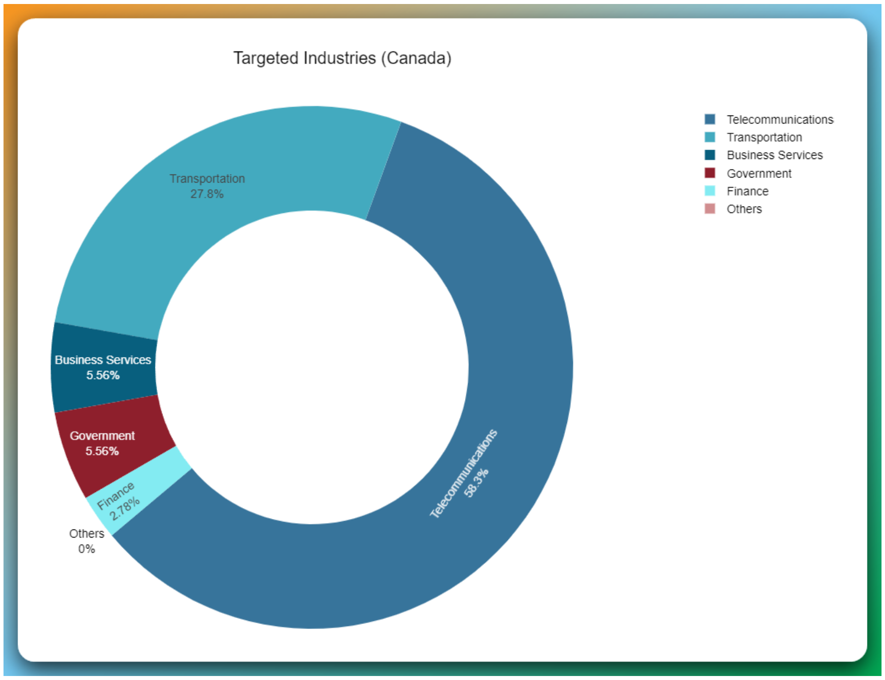


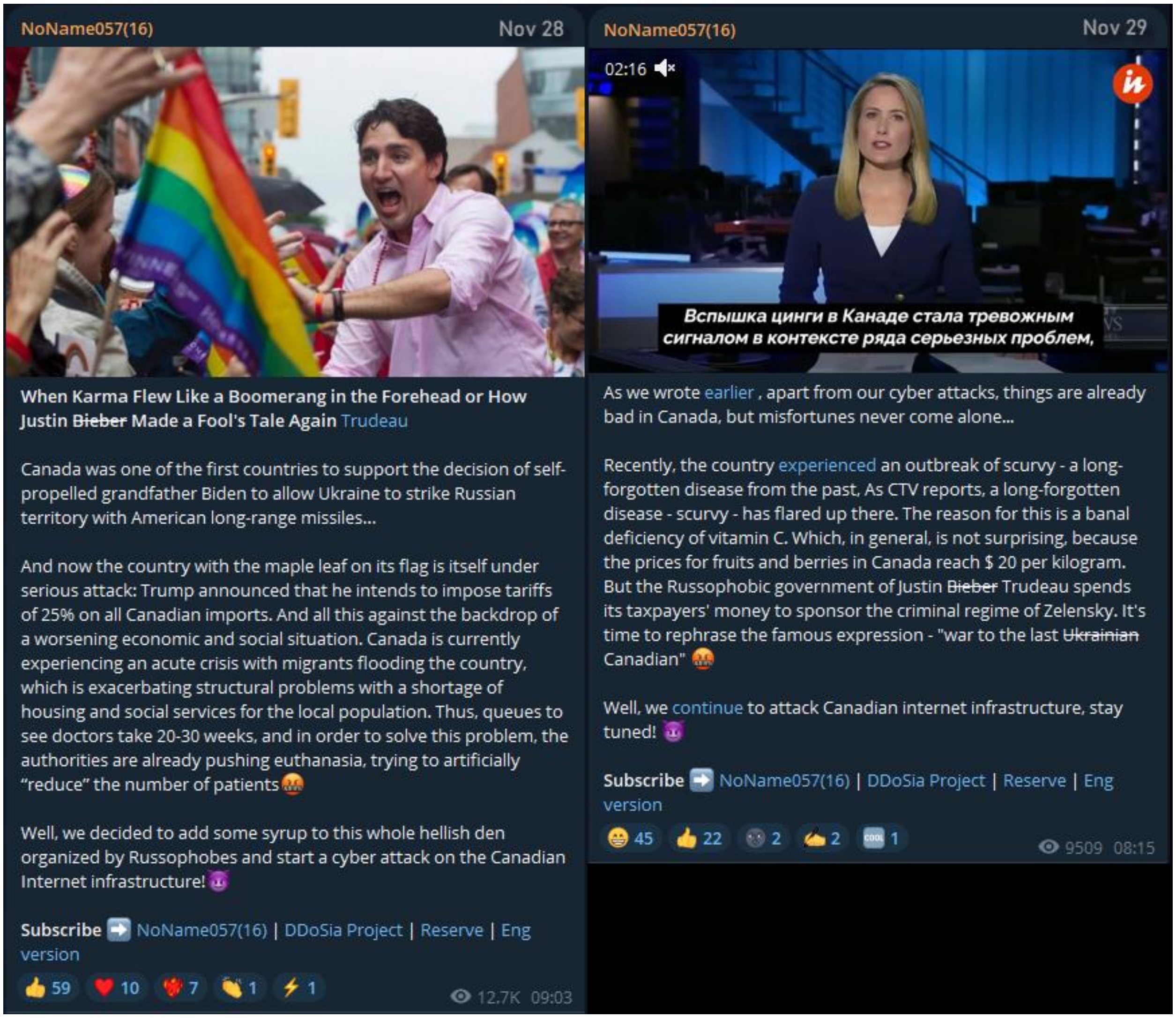
Figure 3: Industries targeted by NoName057(16) between November 22 and December 1, 2024 [source: Radware]

Attack Motivation

NoName057(16)'s cyberattacks on Canadian organizations appear to be motivated by both geopolitical grievances and a desire to exploit domestic vulnerabilities. The group criticizes Canada for its strong support of Ukraine in the ongoing conflict with Russia, particularly its alignment with U.S. policies, which they describe as "Russophobic." They cite Canada's financial and political backing of Ukraine, including decisions made by Prime Minister Justin Trudeau's administration, as key reasons for their campaign. These actions are framed as prioritizing foreign interests over domestic needs, further fueling the group's animosity.

In their rhetoric, NoName057(16) highlights Canada's internal challenges to justify their attacks and amplify their impact. They point to economic struggles, including high costs of basic goods, a shortage of affordable housing, and strained healthcare services. The group emphasizes long wait times for medical care and even accuses the Canadian government of promoting euthanasia as a means to address healthcare inefficiencies. Additionally, they criticize Canada's handling of migration issues, which they claim exacerbate these systemic problems. By referencing these issues, the group positions their actions as a response to a failing government that neglects its citizens.

NoName057(16) seeks to leverage these existing crises to further destabilize Canadian society. Their attacks are framed as symbolic retribution, intended to target both the government and the nation’s identity. The group uses inflammatory language and mockery, such as ridiculing Trudeau and highlighting a resurgence of scurvy, to delegitimize Canada’s leadership and foster public discontent. By combining geopolitical grievances with a focus on Canada’s domestic challenges, the group justifies their cyberattacks as both punishment and a means to exacerbate perceived failures in governance.


02:16
Вспышка цинги в Канаде стала тревожным сигналом в контексте ряда серьезных проблем,

NoName057(16) Nov 28

When Karma Flew Like a Boomerang in the Forehead or How Justin ~~Bieber~~ Made a Fool's Tale Again Trudeau

Canada was one of the first countries to support the decision of self-propelled grandfather Biden to allow Ukraine to strike Russian territory with American long-range missiles...

And now the country with the maple leaf on its flag is itself under serious attack: Trump announced that he intends to impose tariffs of 25% on all Canadian imports. And all this against the backdrop of a worsening economic and social situation. Canada is currently experiencing an acute crisis with migrants flooding the country, which is exacerbating structural problems with a shortage of housing and social services for the local population. Thus, queues to see doctors take 20-30 weeks, and in order to solve this problem, the authorities are already pushing euthanasia, trying to artificially “reduce” the number of patients🤬

Well, we decided to add some syrup to this whole hellish den organized by Russophobes and start a cyber attack on the Canadian Internet infrastructure!😈

Subscribe ➡️ NoName057(16) | DDoSia Project | Reserve | Eng version

👍 59 ❤️ 10 ❤️‍🔥 7 👏 1 ⚡ 1 👁 12.7K 09:03

NoName057(16) Nov 29

As we wrote earlier , apart from our cyber attacks, things are already bad in Canada, but misfortunes never come alone...

Recently, the country experienced an outbreak of scurvy - a long-forgotten disease from the past, As CTV reports, a long-forgotten disease - scurvy - has flared up there. The reason for this is a banal deficiency of vitamin C. Which, in general, is not surprising, because the prices for fruits and berries in Canada reach $ 20 per kilogram. But the Russophobic government of Justin ~~Bieber~~ Trudeau spends its taxpayers' money to sponsor the criminal regime of Zelensky. It's time to rephrase the famous expression - "war to the last ~~Ukrainian~~ Canadian" 🤬

Well, we continue to attack Canadian internet infrastructure, stay tuned! 😈

Subscribe ➡️ NoName057(16) | DDoSia Project | Reserve | Eng version

😁 45 👍 22 🌚 2 ✍️ 2 🆒 1 👁 9509 08:15

Figure 4: Attack motivations posted by NoName057(16) on November 28 and 29, 2024 [source: Telegram]

Who is 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.

More information:

- 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/

Noname057(16) 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.

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.

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.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED “AS IS” WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILBILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER’S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIREC, INCIDENTAL, CONSEQUENTIAL, OR EXAMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY RELATED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. **CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE**