May 8, 2025

Escalating Hacktivist Attacks Amidst India-Pakistan Tensions

Key Insights:

- Following Operation Sindoor, hacktivist DDoS attacks on India intensified, peaking on May 7, 2025, as tensions between India and Pakistan escalated.
- Less than 24 hours after the India-Pakistan escalation, several groups have pledged to act, which could further escalate the situation significantly.
- Politically, socially and religiously motivated hacktivist groups are increasingly coordinating efforts, amplifying their attacks against shared adversaries.
- Hacktivists are using hybrid strategies, leveraging application-layer and volumetric DDoS attacks that complicate defenses.
- Hacktivists on both sides are targeting critical infrastructure using Web DDoS attacks, botnets, data leaks, and defacements, aiming to disrupt services and erode public trust.

Operation Sindoor – India's Largest Cross-border Strike Since 1971

In the early hours of May 7, 2025 (01:05–01:30 IST), India executed "Operation Sindoor," a 25-minute wave of 24 stand-off-precision missile strikes against nine locations it called "terrorist infrastructure" in Pakistan and Pakistan-administered Kashmir (PoK). The action was presented as retaliation for the April 22 massacre of 26 Indian tourists in Pahalgam, Kashmir. While New Delhi claims the raid killed more than 70 militants and avoided civilian areas, Islamabad reports at least 26 civilian deaths, vows "corresponding action," and says five Indian jets were shot down. Heavy artillery exchanges have since erupted along the Line of Control de facto border that divides Kashmir, triggering airspace closures and international calls for restraint.

Amid the soaring tensions, New Delhi has temporarily blocked overseas users from accessing the National Stock Exchange and BSE websites as a "precautionary and protective measure" against anticipated cyberattacks. The decision was made after a joint meeting of exchanges on Tuesday, during which cyberthreats were discussed. Officials say trading itself is unaffected and access is being granted selectively while threats are assessed. No verified intrusions have hit the exchanges, but Indian media report a rise in Pakistan-origin hacking claims while Pakistan's cyber response agency (PKCERT) has warned that hostile actors are exploiting the crisis to target critical infrastructure with misinformation and attacks.

Hacktivist Activity Targeting India in 2025

India has long been a focal point for hacktivist activity, particularly from Southeast Asian religiously driven groups, with a significant concentration of these operations originating in Bangladesh. For years, these threat actors have consistently targeted the nation's infrastructure and institutions. As of January 1, 2025, 100 organizations across India have been targeted by 26 distinct threat groups, resulting in a total of 256 claimed DDoS attacks.

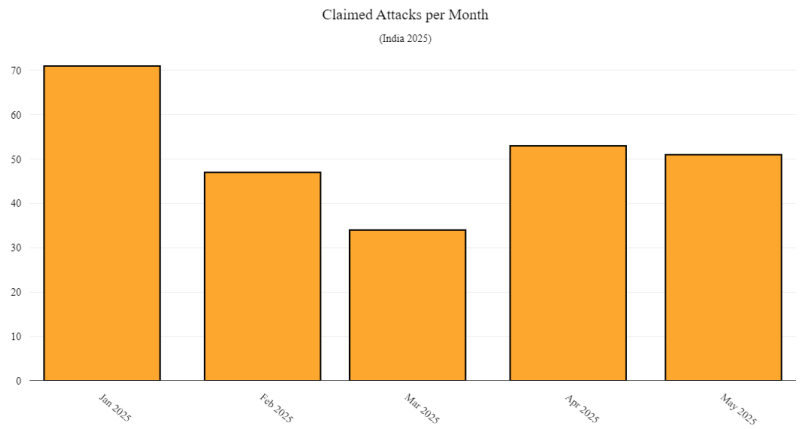

Figure 1: Number of claimed attacks per month targeting India in 2025 (source: Radware)

While the majority of attacks occurred in January, the month of May, with just 7 days having passed at the time of writing, is rapidly becoming the most active month for hacktivists fueled by the ongoing tensions between India and Pakistan.

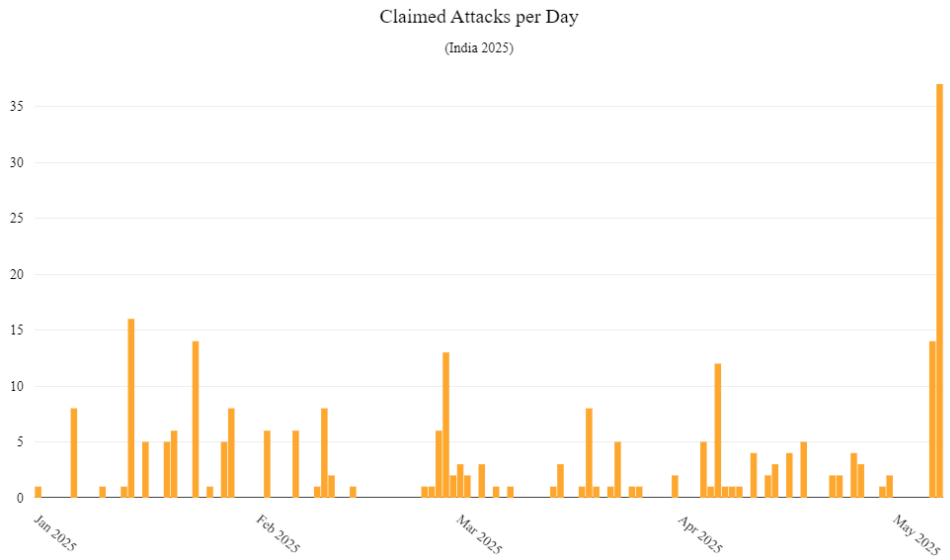

Figure 2: Number of claimed attacks per day targeting India in 2025 (source: Radware)

RipperSec, responsible for over 30% of all DDoS claims, was the most active threat group, followed by AnonSec (16.8%), Keymous+ (10.2%), Sylhet Gang (9%), and Mr Hamza (4.7%), each of which claimed more than 10 attacks in 2025. Other prominent hacktivist groups targeting India include Anonymous VNLBN, Bangladesh Civilian Force, SPIDER-X, RuskiNet, Arabian Ghosts, AnonPioneers, Rabbit Cyber Team, Red Wolf Cyber, Nation of Saviors and several others.

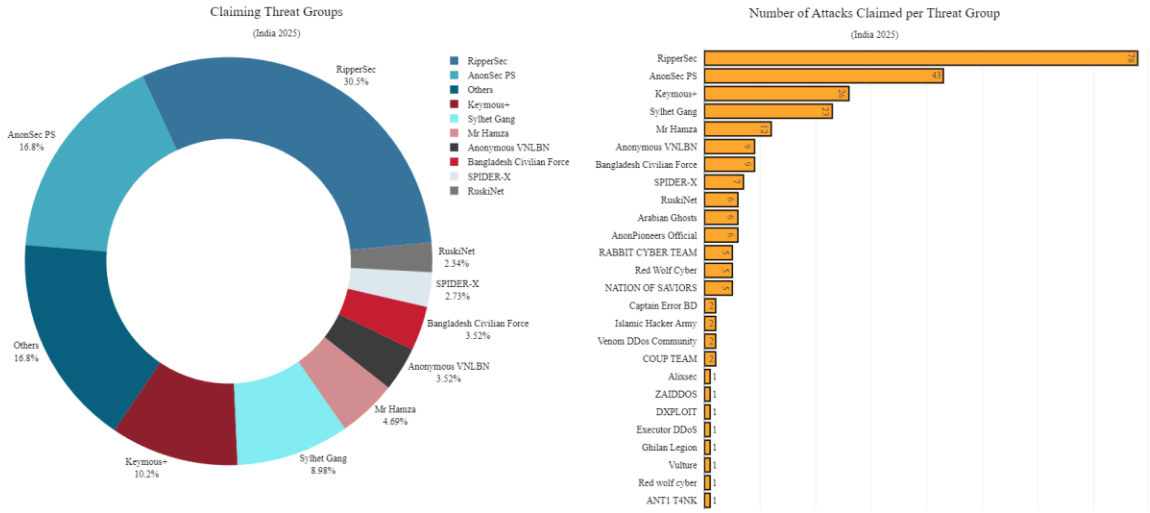

Figure 3: Threat groups targeting India in 2025 (source: Radware)

Over half of all claimed DDoS attacks were directed at government institutions. The most frequently targeted sectors included education (8.3%), finance (7.4%), manufacturing (6.5%) and telecom (6.5%).

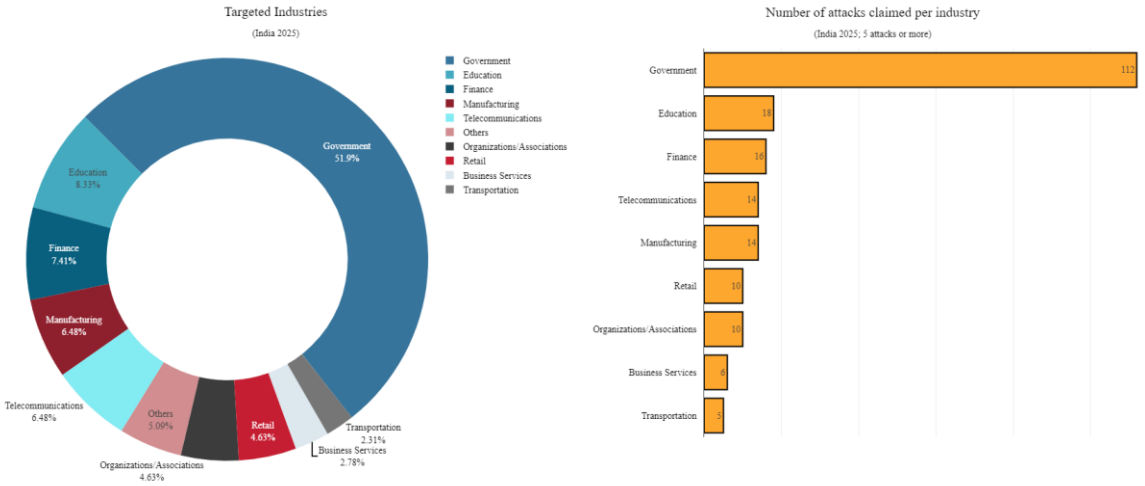

Figure 4: Industries in India targeted in 2025 (source: Radware)

Hacktivist Retaliation Following Operation Sindoor

Following the events of the early morning on May 7, hacktivist DDoS activity targeting India became more frequent and intense. A peak occurred at 4pm UTC (9:30pm IST), with seven claimed DDoS attacks reported per hour.

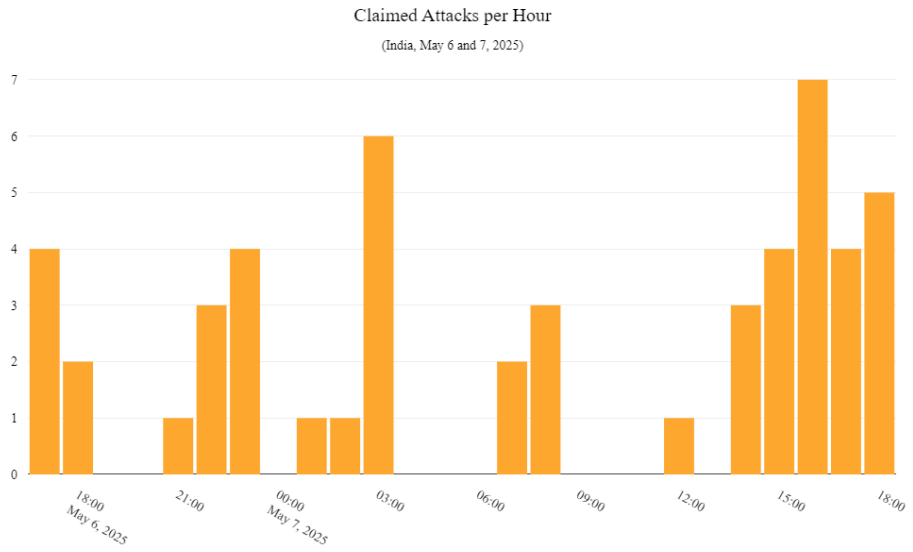

Figure 5: Number of attacks targeting India claimed per hour on May 6 and 7, 2025 (source: Radware)

The most active threat groups included AnonSec, Keymous+, Mr Hamza, Anonymous VNLBN and Arabian Hosts. Additionally, Islamic Hacker Army, Sylhet Gang, Red Wolf Cyber and the Iranian group Vulture also claimed responsibility for DDoS attacks targeting organizations in India.

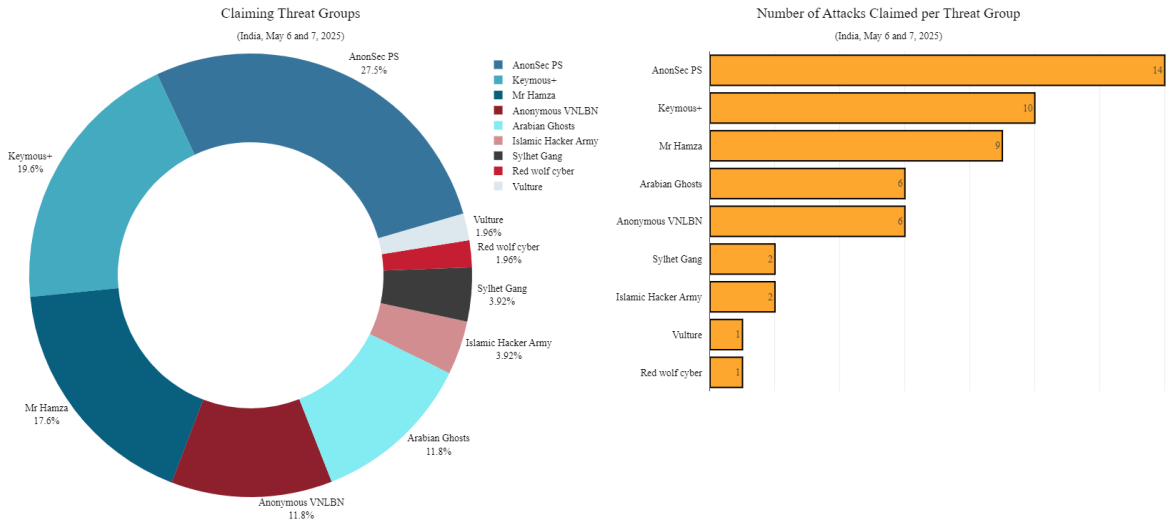

Figure 6: Threat groups claiming attacks targeting India between May 6 and 7 (source: Radware)

Over 75% of the claimed DDoS attacks were directed at government organizations. Along with attacks on finance (8.5%) and telecom (6.4%) sectors, this accounts for 90% of all reported attack activity.

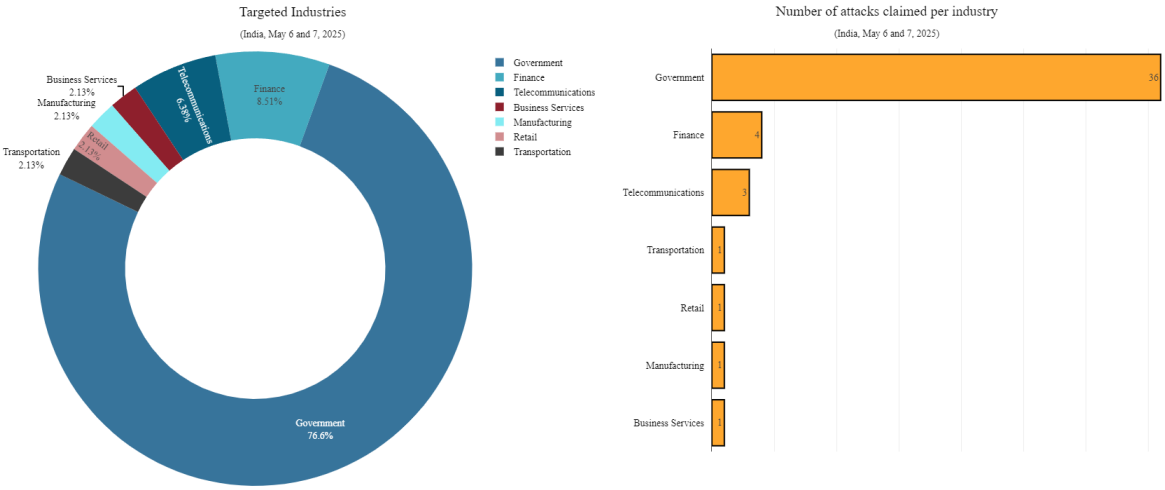

Figure 7: Industries in India targeted by hacktivist DDoS claims between May 6 and 7 (source: Radware)

Risk of Escalation

Throughout 2025, numerous hacktivist groups have targeted organizations in India, the majority of which are based in Bangladesh. Following the events in the early morning of May 7, several groups, including Sylhet Gang, Mysterious Team, and Red Wolf Cyber, have expressed their support for Pakistan and issued threats of attacks targeting India.

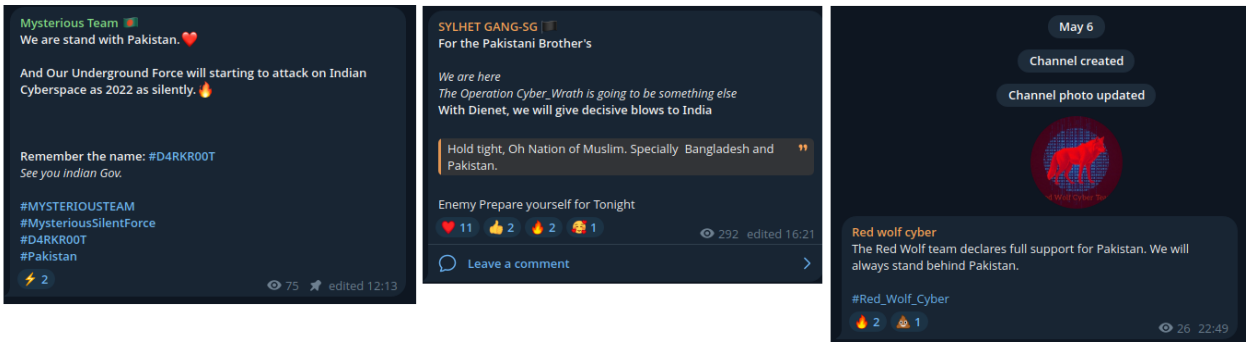

Figure 8: Groups pledging support for Pakistan and threatening India (source: Telegram)

As noted in the Radware 2025 Global Threat Analysis Report, 2024 was a significant turning point for hacktivist alliances, as groups driven by different political, social and religious motivations united in coordinated campaigns to target shared perceived adversaries. In 2025, this trend has

gained momentum, with more hacktivists offering mutual support for each other's actions and campaigns, amplifying their messages and boosting their visibility.

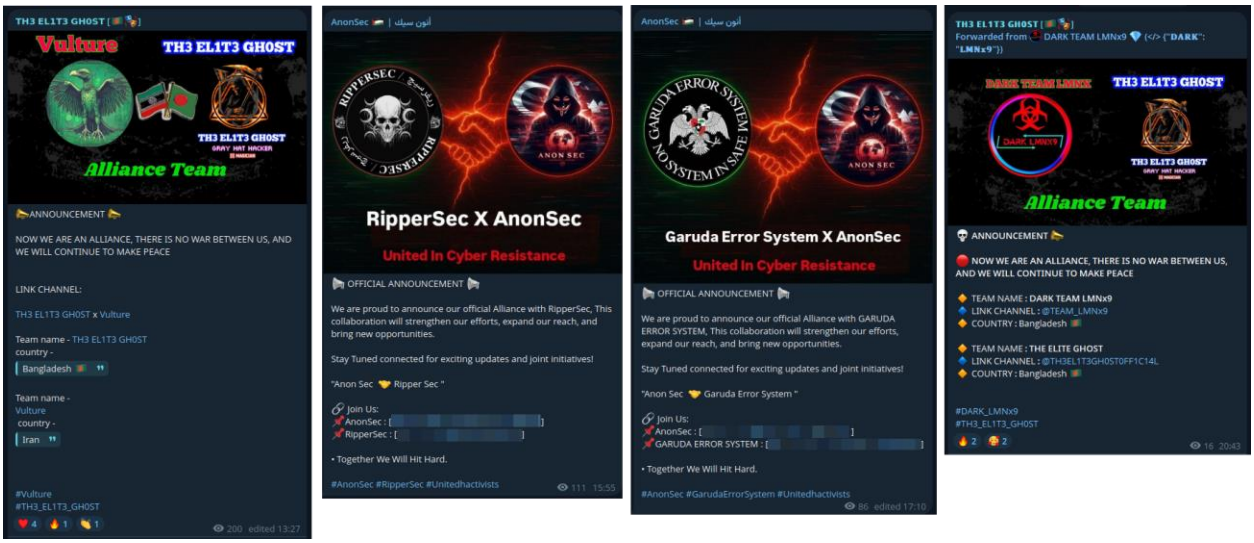

Figure 9: A few of the alliances being forged in the aftermath of Operation Sindoor (source: Telegram)

In the wake of Operation Sindoor, new alliances are emerging among Southeast Asian hacktivists. Some of these alliances even extend to groups traditionally opposed to Israel, such as the Iranian hacktivist group Vulture.

Figure 10: Vulture, an Iranian threat group, announcing they stand with Pakistan (source: Telegram)

Reasons for Concern

As of now, less than 24 hours have passed since the escalation between India and Pakistan, and the situation remains highly volatile. Several prominent politically motivated groups, such as RipperSec and Mysterious Team Pakistan, have publicly pledged to take action but have not yet claimed responsibility for any attacks. Their impending involvement could significantly raise the stakes.

Simultaneously, hacktivist groups supporting India, such as Indian Cyber Force, Cryptojackers of India, Dex4o4 and Ghost Force are expected to intensify their efforts to target Pakistani organizations. This could create a dangerous cycle of retaliation, increasing the risk of further cyberattacks, potentially targeting critical infrastructure on both sides.

Hacktivists frequently deploy application-layer DDoS attacks to target specific server resources, often without generating overwhelming traffic volumes. These attacks are harder to detect and mitigate, as they imitate legitimate user interactions. Common techniques include HTTPS encrypted floods and form POSTs, which overwhelm online services and their backend systems. This can result in significant service disruptions or even complete outages, especially for critical websites like government portals, financial institutions or news outlets.

Volumetric attacks, while generally less sophisticated, are still a common strategy employed by hacktivist groups to overwhelm network infrastructure. These attacks often involve tactics such as direct path UDP floods or reflection and amplification attacks, where the target is flooded with a massive volume of UDP packets. This consumes significant bandwidth and network resources, which can potentially bring down online services or impact connectivity.

Given the increasing sophistication of and orchestration between hacktivist groups, hybrid DDoS attacks that combine multiple techniques can be observed. These attacks could simultaneously target network infrastructure with volumetric methods while also executing application-layer attacks. These strategies complicate detection and mitigation efforts.

Many groups may use publicly available DDoS tools to conduct their attacks. RipperSec members, for example, maintain and share a tool called MegaMedusa. Built using Node.js, MegaMedusa leverages its asynchronous and non-blocking I/O capabilities to manage multiple network connections efficiently, making it suitable for orchestrating extensive DDoS campaigns. The tool is publicly accessible via GitHub, allowing users to install and operate it with minimal technical expertise. Its user-friendly installation process involves executing a few commands, making it accessible even to individuals with limited technical backgrounds. The availability of these tools makes it easier for groups with varying levels of technical expertise to launch impactful attacks.

Hacktivist groups may also utilize botnets – networks of compromised devices, often IoT devices – to launch large-scale DDoS attacks. These botnets can be rented or created through the use of malware, enabling attackers to distribute traffic across a wide range of devices. Some hacktivist groups have evolved from politically and religiously motivated attackers to DDoS-as-a-service providers, offering these services either for a fee or in exchange for advertising on their Telegram channels.

Some hacktivists may also engage in website defacements and claim responsibility for data leaks as part of their strategy to create chaos and erode public trust in institutions. These actions are often intended to undermine the credibility of targeted organizations and spread ideological messages.

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**

©2025 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.