June 16, 2025

Cyber Escalation in Southeast Asia: AnonSecKh Targets Thailand

> **Key Attack Insights:**
>
> - Following the unfortunate passing of a Cambodian soldier after an incident with Thai soldiers on the border between both countries, the number of cyberattacks on Thailand has increased significantly.
> - AnonSecKh (aka ANON-KH, aka Bl4ckCyb3r) is a recent hacktivist group that first claimed an attack on their Telegram channel on March 23, 2025.
> - AnonSecKh leverages proof-of-impact reports to claim distributed denial of service (DDoS) attacks via its Telegram channel(s).
> - AnonSecKh claimed 73 attacks against Thai organizations between May 28 and June 10, 2025.
> - AnonSecKh primarily targets government and large, highly visible, Thai organizations.
> - AnonSecKh's campaign is mainly political driven, and they target countries that have harmed Cambodia.

An incident at the border area between Thailand and Cambodia triggered a hacktivist-led cyber campaign targeting Thai organizations and institutions.

Cyber incidents in the region are not uncommon. In the past, politically motivated Cambodian hacktivist groups, such as ANONSECKH, H3C4KEDZ, and NXBBSEC, have launched attacks in response to rising border tensions or nationalistic disputes.

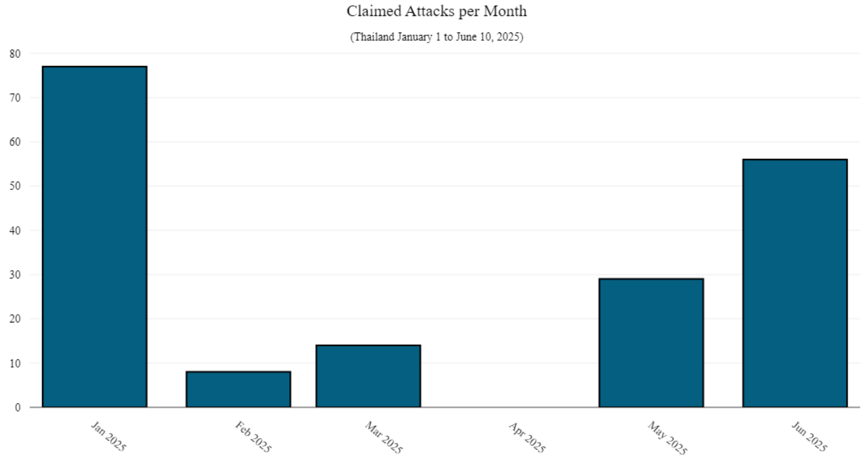
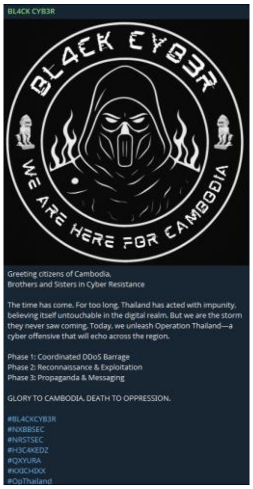


Figure 1: Number of claimed attacks per month targeting Thailand in 2025 (source: Radware)

AnonSecKh (Bl4ckCyb3r)

AnonSecKh, also going by the name of Bl4ckCyb3r on Telegram, first targeted Thailand's official government portals on March 23. By the end of March, they claimed attacks on more Thai government, academic and commercial websites. April was a slow month for the threat group, but by the end of the month, AnonSecKh targeted multiple financial institutes in Vietnam (you can read about the rise of these attacks here).

A turning point occurred on May 28, following the incident with the Cambodian soldier. From that moment, AnonSecKh's activity escalated dramatically.



Greeting citizens of Cambodia.
Brothers and Sisters in Cyber Resistance

The time has come. For too long, Thailand has acted with impunity, believing itself untouchable in the digital realm. But we are the storm they never saw coming. Today, we unleash Operation Thailand—a cyber offensive that will echo across the region.

Phase 1: Coordinated DDoS Barrage
Phase 2: Reconnaissance & Exploitation
Phase 3: Propaganda & Messaging

GLORY TO CAMBODIA. DEATH TO OPPRESSION.

#BL4CKCYB3R
#NXBBSEC
#NRSTSEC
#H3C4KEDZ
#QXYURA
#KXICHDX
#OpThailand

Figure 2: Message from AnonSecKh's Telegram on May 28

Between May 1 and May 27, only 20 attack claims targeting Thailand were observed, but between May 28 and June 10, the number of claimed attacks jumped to a staggering 64 (as seen on Figure 3).

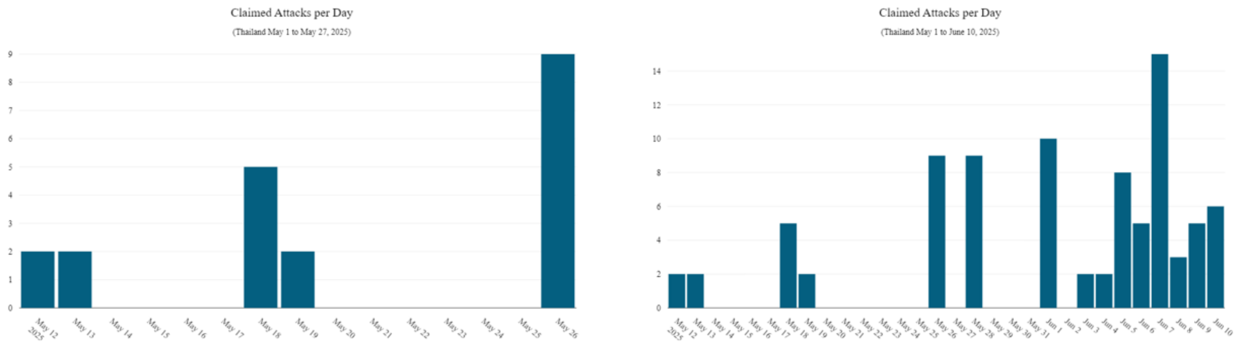


Figure 3: Number of claimed attacks: May 1 – May 27 and May 28th – June 10th (source: Radware)

The attacks between May 28 and June 10 targeted multiple industries, with government websites being the most heavily targeted and representing almost 30% of all attack claims, followed by military (almost 26%), manufacturing (almost 15%) and finance (more than 7%). In early June, there was a brief slowdown with only a few isolated incidents. However, following the strong public statement from the Thai military on June 6, AnonSecKh resumed and scaled up its attacks, continuing its campaign against Thai institutions and showing no intention of slowing down at the time of writing.

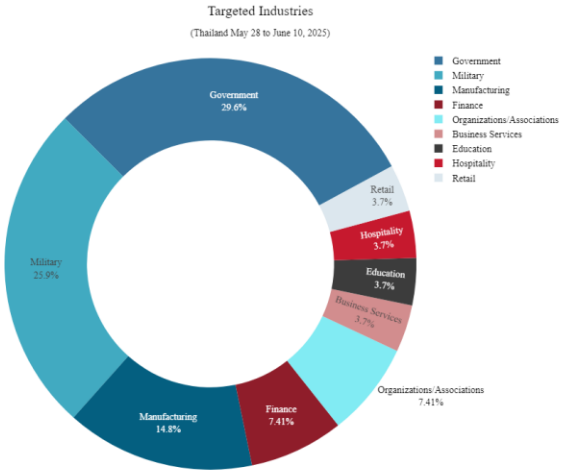


Figure 4: Top verticals impacted May 28 – June 10 (source: Radware)

Reasons for Concern

AnonSecKh's activity highlights several key risks. First, their attacks are tightly linked to political incidents and demonstrate a reactive pattern. This suggests that even isolated or symbolic events can trigger immediate cyber responses.

Second, the group has shown the ability to launch rapid and intense attack waves. The sharp jump in volume following key events reflects a high level of coordination and intent.

Finally, the choice of targets such as government resources, universities and financial institutions raises concerns about potential real-world disruptions. These attacks aren't just aimed at making a statement, they are an attempt at damaging public trust and interfering with essential services.

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**