June 2025

CYBER INSIGHTS

Research updates and insights from Dreamlab Technologies

In this issue:

Global Takedown of Lumma Stealer Networks Linked to Millions of Cyberattacks

LummaC2, a major malware-as-a-service operation was dismantled in the week following 18 May 2025, in a global operation led by the FBI, Microsoft, and other cyber security partners (US DOJ, 2025). The malware, also known as Lumma Stealer, was active since 2022, infecting around 10 million devices, and enabling millions of cyberattacks by stealing usernames, passwords, credit card details, crypto wallets, etc. (Masada, 2025) and targeting individuals, airlines, banks, hospitals, governments and more.

‘Lumma’, was originally developed by a Russia-based hacker also known as “Shamel” (Masada, 2025) that was sold as a malware-as-a-service on Telegram and other platforms, enabling even low-skilled criminals to launch cyberattacks.

It was distributed primarily through phishing, malvertising and fake CAPTCHAs, that could evade common security tools. The operation targeted thousands of domains and cut off links between infected systems and the malware's servers. Despite the seizure of key infrastructure and domains by the U.S. authorities and cyber security partners, officials have warned that the hackers might try to rebuild their networks. However, the disruption of criminal activities successfully imposed both financial and reputational costs on cybercriminals. Authorities have encouraged potential victims to contact the Internet Crime Complaint Center (IC3), while CISA has published a cyber security advisory (CISA, 2025) sharing tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) linked to LummaC2 threat actors, to aid detection and defense efforts.

The Netherlands Passes Law Criminalising Digital Espionage

The Dutch parliament has included a new criminal provision to the Dutch Criminal Code, criminalising a broader range of espionage activities, including digital and diaspora espionage, in the interest of national security and protection of high-value technologies (JenV, 2025). The law reflects growing concerns over non-traditional espionage, including political and economic influence efforts by foreign powers, and represents a broader strategy to enhance national resilience against foreign threats.

Previously, only traditional espionage such as leaking state secrets was criminalised. But under the updated law, effective from 15 May 2025, leaking non-classified sensitive information (business or personal data) to a foreign government, or covertly acting on behalf of a foreign government that could harm Dutch interests, is also a criminal offence. The law also helps counteract espionage activities targeting diaspora communities, including data collection, intimidation, and pressuring individuals to act against critics. Penalties include up to 8 years in prison, or 12 years in severe cases like espionage causing death. Penalties for related crimes like bribery or computer offences may also get harsher when committed on behalf of foreign states.

Coordinated Cyberattacks on Indian Infrastructure Exploit Rising Geopolitical Tensions

Quick Heal Technologies’ Seqrite Labs, an Indian cyber security firm, reported a rise in cyberattacks targeting India's critical sectors between April-May 2025, in a coordinated campaign by Pakistan-linked actors (Seqrite, 2025). The report revealed that parallel cyber campaigns targeted India's defense, healthcare, telecom, and government sectors amid heightened military tensions following the 22 April 2025 Pahalgam terror attack and during ‘Operation Sindoor’, India’s counterterrorism response to it.

The campaign, led by APT36, a known Pakistan-linked cyber espionage group, used spoofed Indian domains, phishing documents, malicious files, etc. to manipulate public perception, spread propaganda, and disrupt security, posing risks to social stability (Seqrite, 2025a). Spear-phishing, malware attacks and data leaks, were conducted by around 35 hacktivist groups, who used hashtags like #OpIndia and #OperationSindoor to claim attacks on Indian systems (msn, 2025). Socially engineered documents (response measures) in relation to “Pahalgam Terror Attack” were used by the hackers to target Indian Government and Defense personnel, involving both credential phishing and deployment of malicious payloads using fake domains impersonating government websites (Seqrite, 2025a). The Indian Computer Emergency Response team (CERT-In) issued ‘high severity’ alerts in May 2025, following a surge in cyber threats (CERT, 2025), urging users to update their systems, including Microsoft tools and follow essential measures to safeguard business operations.

AHRC Privacy Breach Exposes Sensitive Data Online

The Australian Human Rights Commission (AHRC) on 14 May 2025, disclosed a major data breach incident caused by a vulnerability in its website's online form submission system, which led to the exposure of hundreds of confidential documents online (AHRC, 2025). The breach, however, was not caused by a cyberattack, and the AHRC has been working to notify affected individuals, treating it as a high-priority incident.

The breach exposed over 670 documents online between April and May 2025, while about 100 were accessed, including some by search engines like Google and Bing. These documents included attachments submitted via various webforms involving complaints, project feedback, award nominations, and anti-racism initiatives. Some of them contained personal or sensitive information like names, contact information, religion, photographs and much more. Following the incident, the AHRC disabled affected webforms, removed documents from search engines, and reported the breach to relevant authorities. The AHRC has apologised to the victims and pledged to continue investigating the incident while securing its networks and systems. The incident has raised serious concerns over the confidentiality of data through online submissions of personal documents and associated risks to vulnerable individuals.

Meta Wins Nearly $170M in Damages From Israeli Spyware Giant NSO Group

A U.S. federal court on 6 May 2025 ordered the Israeli spyware company NSO Group to pay nearly $170 million in in punitive damages and over $444,000 in compensatory damages to WhatsApp and its parent company Meta (Simons, 2025), due to hacking and breach of contract. The ruling, from a case originally filed in 2019, concluded that NSO exploited a vulnerability in WhatsApp to install its spyware called Pegasus, that enabled unauthorised surveillance of around 1,400 users, including civil society members, diplomats, activists and journalists (Meta, 2025).

Pegasus, a "zero-click malware", allows covert access to smartphones, enabling users to control microphones and cameras and extract data without user interaction. The NSO Group, however, has repeatedly claimed that Pegasus aids governments in national security efforts, to counter criminal and terrorist activities. It had claimed sovereign immunity earlier, but the courts affirmed that private companies, even if state clients, are not immune from lawsuits over illegal surveillance. The group has already been put in the U.S. Commerce Department's "entity list" for engaging in activities counter to national security interests (Simons, 2025). The latest court ruling marks a major victory for privacy advocates as it sets a precedent for holding spyware makers accountable for aiding unauthorised surveillance activities. Meta now plans to seek a court order to permanently bar NSO from targeting WhatsApp, and release transcripts to expose global spyware abuse, while supporting digital rights groups, and researchers (Meta, 2025).

Debopama Bhattacharya
Dreamlab Audit Team
Dreamlab Research Team

Despite the care taken in the preparation of this newsletter, the authors assume no liability or responsibility, under any circumstances, for the accuracy of the data, information, or guidance provided as well as any typographical errors contained herein.

All the articles and information in this issue were sourced from publicly available sources.

References

Australian Human Rights Commission (AHRC) (2025): Data breach notification. AHRC, accessed 21st May 2025, https://humanrights.gov.au/about/news/data-breach-notification

Cybersecurity and Infrastructure Security Agency (CISA) (2025): Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations. CISA, accessed 26th May 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141b

Indian Computer Emergency Response team (CERT-In) (2025): Latest Security Alert, 10 & 15 May 2025. CERT-In, accessed 20th May 2025, https://www.cert-in.org.in/s2cMainServlet?pageid=PUBWEL01

Masada, S.(2025): Disrupting Lumma Stealer: Microsoft leads global action against favored cybercrime tool. Microsoft, accessed 26th May 2025, https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

Meta (2025): Winning the Fight Against Spyware Merchant NSO. Meta, accessed 19 May 2025, https://about.fb.com/news/2025/05/winning-the-fight-against-spyware-merchant-nso/

Ministry of Justice and Security (JenV) (2025): More forms of espionage to be a criminal offence from 15 May onwards. Government of the Netherlands, accessed 22nd May 2025, https://www.government.nl/ministries/ministry-of-justice-and-security/news/2025/05/15/more-forms-of-espionage-to-be-a-criminal-offence-from-15-may-onwards

msn (2025): Cyber hackers launched 650 attacks on Indian infrastructure between May 7–10: Report. msn, accessed 19 May 2025, https://www.msn.com/en-in/technology/cybersecurity/cyber-hackers-launched-650-attacks-on-indian-infrastructure-between-may-7-10-report/ar-AA1FmshK

Seqrite (2025): Advisory on Heightened Cyber Threat Landscape Amid Geopolitical Tensions. Quick Heal Technologies, accessed 20th May 2025,
https://seqrite.com/documents/en/misc/customer-advisory.pdf?utm_source=deepti&utm_medium=deepti&utm_campaign=customer-advisory

Seqrite (2025a): Advisory: Pahalgam Attack themed decoys used by APT36 to target the Indian Government. Seqrite Blog, accessed 20th May 2025, https://www.seqrite.com/blog/advisory-pahalgam-attack-themed-decoys-used-by-apt36-to-target-the-indian-government/

Simons, M. (2025): Meta wins $168 million in damages from Israeli cyberintel firm in Whatsapp spyware scandal. Courthouse News Service, accessed 19 May 2025, https://www.courthousenews.com/meta-wins-168-million-in-damages-from-israeli-cyberintel-firm-in-whatsapp-spyware-scandal/

US Department of Justice (US DOJ) (2025): Justice Department Seizes Domains Behind Major Information-Stealing Malware Operation. US DOJ, accessed 26th May 2025, https://www.justice.gov/opa/pr/justice-department-seizes-domains-behind-major-information-stealing-malware-operation

ISECOM

Member of the World Wide Web Consortium for security standards.

W3C

Board member of the Institute for Security and Open Methodologies.

UNIÓN EUROPEA

Research partner for EU cyber security research projects.

OWASP

Member of the Open Web Application Security Project.

INTERNATIONAL TELECOMUNICATION UNION

Sector Member of the UN's specialised agency for information and communication technologies.

FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST)

Liaison Member.

SWISS MADE SOFTWARE

Officially certified as a provider of Swiss Made Software solutions.

CYBER SECURITY MADE IN EUROPE

Recognition of the quality of our cybersecurity services and products.

PARTNER CYBER SAFE

Audit partner for the label certification process.

FACHHOCHSCHULE NORDWESTSHWEIZ

Research partner for digital initiatives in Switzerland.

ALSEC

Specialized partner for critical operational technology (OT) infrastructures.

SLINF

Specialized partner of government security solutions.

GENEVA CHAMBER OF COMMERCE

Partner in investigation projects focused on e-commerce security solutions.

BLACK HAT

Member of the Review Committee at Black Hat International Cybersecurity Conference.

SWISS CYBER SECURITY DAYS

Founding Partner of the Swiss Cyber Security Days.

About Dreamlab Technologies

Dreamlab Technologies is a Swiss IT security company with locations on four continents. The combination of the Swiss technical capabilities as well as their international expertise enables Dreamlab to develop, assess and control cybersecurity based on quantifiable and verifiable open-standard technologies. Dreamlab advises organisations and authorities and helps them integrate information security awareness into their management cycle. In addition to its software products CyObs, CySOC and many other solutions, Dreamlab also offers IT security audits and training at all its locations.

Further information: https://dreamlab.net/

DREAMLAB
TECHNOLOGIES

Monbijoustrasse 36
CH-3011 Bern
Tel: +41 31 398 6666
Fax: +41 31 398 6669
contact@dreamlab.net