SECTRA NEWSLETTER — FEBRUARY 2025

Monthly Review

Cybersecurity news from around the world

ARTICLE

Sweden takes action to protect against evolving cyber risks

Read article →

SECTRA

General cybersecurity news

1 Police seize several servers of two major hacker forums

Operation Talent, conducted in late January, was an international effort led by Europol, FBI, and other agencies to dismantle two major hacking forums, Cracked and Nulled. Two suspects were arrested in Valencia, Spain, and authorities seized 17 servers, over 50 devices, and €300,000 in cash and cryptocurrency. Together, the forums had over 10 million users and provided tools for cybercrime, including stolen data, malware, and AI-powered resources for phishing and credential-stuffing attacks. Cracked generated $4 million in revenue and impacted 17 million U.S. victims, while Nulled hosted 43 million ads and made $1 million annually.

Authorities also took down 12 related domains and linked services such as Sellix and StarkRDP. Europol's Joint Cybercrime Action Taskforce (J-CAT), supported by the European Cybercrime Centre (EC3), played a key role. The operation disrupted the platforms' economic networks and highlighted the rise of cybercrime-as-a-service, using seized data for further investigations.

2 Zero-cklick-method – infected without action

Zero-click attacks infect devices with malware without requiring the user to click on a link or open a file. These attacks are dangerous as they occur invisibly, making them hard to detect and prevent. They often target mobile phones, which generally have weaker security than computers. Attackers exploit zero-day vulnerabilities, particularly in email or messaging apps, by sending malicious code that is automatically processed by the app when a message is read.

A well-known example is Pegasus spyware, used by state-sponsored actors to monitor dissidents, activists, and politicians, gaining access to communications, location data, and stored files. To reduce risks, users should update apps and devices regularly, use password-protected apps, and limit the number of installed apps. However, zero-click attacks remain one of the most advanced threats, especially for high-risk users targeted by sophisticated threat actors.

3 Apple bows to UK pressure – weakens iCloud security for its users

According to Reuters, Apple has decided to disable its Advanced Data Protection (ADP) feature for UK users due to increasing government demands under the Investigatory Powers Act. ADP, providing end-to-end encryption for iCloud backups, ensures that even Apple cannot access user data. As of now, UK users can no longer activate ADP, and existing users will eventually need to disable it. This change compromises iCloud backup security, which includes sensitive data like photos and iMessages. Experts warn it exposes UK users to greater risks. Professor Oli Buckley from Loughborough University called it a significant weakening of security and stressed the dangers of encryption backdoors.

While device-stored data is unaffected, this reflects ongoing tensions between governments and tech firms over encrypted communications. Critics, including Signal’s president Meredith Whittaker, argue that weakening encryption endangers privacy and cybersecurity globally. Apple emphasized that previous ADP backups remain encrypted and urged users to update their apps for the best security.

ARTICLE

Swedish Armed Forces adopt the app Signal

How secure is secure enough? As the Swedish Armed Forces adopt Signal for safer communication, global efforts to weaken encryption spark serious concerns. In an era of rising cyber threats and surveillance, the push for backdoors risks undermining privacy, security, and trust in digital tools worldwide.

In an era where digital communication is constantly under threat, the Swedish Armed Forces have taken an important step to strengthen the security of their information transfer. In February, they announced their decision to adopt the encrypted messaging app Signal for open communication via mobile phones. Signal, known for its use of end-to-end encryption, is regarded as one of the most effective methods for protecting information from unauthorized access. The move is aimed at reducing the risk of eavesdropping and manipulation of communication. However, the Armed Forces clarified that only less sensitive information would be handled via the app.

With the rise in cyberthreats and surveillance, establishing robust communication frameworks is essential for safeguarding sensitive data in government and public sectors. Despite the security advantages, end-to-end encrypted solutions like Signal have faced resistance and political efforts to introduce backdoors into their systems. →

Such attempts have been seen in multiple countries, including Sweden, where proposed legislation requiring app operators to store user data could undermine existing security measures. Another example, like we mentioned in the article above, with the UK, where Apple was pressured to retract its most advanced encryption feature for iCloud backups following demands from authorities.

The issue with backdoors is that security can never be selective. A backdoor created for one entity can eventually be exploited by cybercriminals or hostile nation-states. Measures introduced to protect citizens today can be repurposed by other regimes with entirely different agendas tomorrow. Compromising encryption and security is a dangerous precedent – once a backdoor exists, it is nearly impossible to ensure it won't be misused.

> *"Smartphones, designed for flexibility and user-friendliness, are not built for high-security environments"*

While Signal provides high security for messaging and calls, it's important to recognize the limitations of any app. Smartphones, designed for flexibility and user-friendliness, are not built for high-security environments. These devices remain vulnerable to advanced attacks such as signal interception, zero-day exploits, and software or hardware infections. Even with encryption protecting communications, attackers with access to the device itself can bypass security, for example, through spyware installation or extracting information directly from the screen. This underscores the need for solutions that go beyond software-based protections in a world where adversaries possess significant resources and technical expertise. →

To address these challenges, there is a need for sophisticated solutions designed for secure communication. Systems that are quantum-resilient, approved for high-security communication, and equipped with advanced end-to-end encryption can provide robust protection against signal interception and threats from both state and non-state actors. Such solutions ensure a level of security far beyond what consumer-grade smartphones and apps can offer. For organizations with stringent security requirements, it is crucial to rely on specialized communication systems rather than exclusively using tools developed for the consumer market.

The Swedish Armed Forces' choice to adopt Signal is a significant step in meeting today's communication challenges. At the same time, the global push to weaken encryption poses long-term risks to security and privacy. While apps like Signal are an excellent choice for private and professional communication, critical environments demand more robust solutions. In a world where digital security is paramount, compromise is not an option – we must choose systems that protect both today, and the future. ■

ARTICLE

Sweden takes action to protect against evolving cyber risks

MUST reports growing cyber threats to Sweden, including ransomware and outsourcing risks in 2024. They warn that without improved cybersecurity and cooperation, Sweden's societal functions and national security remain at risk.

The Swedish Military Intelligence and Security Service (MUST), in their latest report, highlights Sweden's pressing need to address evolving cyber risks and vulnerabilities, emphasizing stronger national readiness against advanced digital threats. Over the past year, the threat environment has intensified, highlighting the urgent need for enhanced cybersecurity and collaboration among key actors within national defense.

The year began dramatically with a large-scale ransomware attack targeting the Finnish IT provider Tietoevry. The attack, carried out by the Russian ransomware hacker group Akjra, resulted in the payroll systems of 120 Swedish government agencies being disrupted, according to Swedish public service television (SVT). However, the effects of the attack were felt widely, particularly on services used by the general public. This incident not only exposed significant vulnerabilities in digitalization but also revealed how dependent society has become on a functioning digital infrastructure. →

Outsourcing has emerged as a critical issue this year. It involves delegating tasks, such as IT management, to external providers. While it can save money and provide expertise, it also poses risks when sensitive information is involved. MUST emphasizes that operations handling sensitive information are increasingly being outsourced to external actors, creating potential security challenges. To address these risks, it became mandatory in April 2024 for the Swedish Security Service (Säpo) and MUST to review and approve all outsourcing of classified operations, particularly when sensitive data is managed outside government premises. The growing reliance on external providers now demands heightened security focus at every level.

"Sweden's cybersecurity must balance the effective use of technology while minimizing risks"

At the same time, MUST's report underscores the importance of cooperation between Swedish agencies to effectively withstand and address the increasingly complex threats to Sweden's security. MUST, the National Defence Radio Establishment (FRA), and Säpo have expanded their joint initiatives this year to identify and manage threats. A key project has been the National Cyber Security Centre (NCSC), whose activities intensified in 2024 to strengthen Sweden's readiness against cyberattacks. This work is conducted in collaboration with both public and private actors and is crucial for the nation's future security. →

Sweden also remains a target for advanced cyber actors tied to nations such as China, Iran, and Russia. These actors engage in intrusions, espionage, and influence campaigns that threaten Sweden's security. Beyond being a strategic target, Sweden is of particular interest due to its cutting-edge advancements in research and technology.

The report's forward-looking perspective is clear: Sweden's cybersecurity must balance the effective use of technology while minimizing risks. By strengthening collaboration and adhering to rigorous security standards, society can be safeguarded against future threats. MUST also stresses the importance of adopting a strategic approach at the national defense level to meet the challenges presented by increasingly sophisticated threat actors. ■

Key takeaways

1. Operation Talent dismantled Cracked and Nulled forums, disrupting global cybercrime networks.

2. Zero-click attacks invisibly infect phones, exploiting app flaws. Pegasus spyware highlights the threat.

3. Apple disables UK icloud encrpytion, sparking privacy and security concerns due to government demands.

4. Swedish Armed Forces adopt Signal, but encryption limitations and global risks remain concerns.

5. MUST urges stronger cybersecurity as Sweden faces rising risks from ransomware and advanced actors.

www.communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden,
and operates through offices in Sweden, the Netherlands and Finland.

Linkedin

SECTRA