DREAMLAB TECHNOLOGIES

CYBER INSIGHTS

Research updates and insights from Dreamlab Technologies

In this issue:

US Federal Judiciary's Electronic Filing System hit by Cyberattack

The U.S. federal judiciary's electronic case filing system was breached in a series of cyberattacks, first determined around early July 2025 (Sakellariadis & Gerstein, 2025), potentially exposing sensitive court data across multiple U.S. states. Authorities, including the Justice Department and district courts, are investigating its scale (US Courts, 2025), with a wide range of threat actors suspected to be behind it. The hack is believed to have affected the judiciary's core management system, which includes the Case Management/Electronic Case Files (CM/ECF) (used by legal professionals to upload and manage case documents) and PACER (for providing limited public access to the same data) (Sakellariadis & Gerstein, 2025), both containing sensitive information like witness details, sealed indictments, and arrest warrants.

While the identities of the cybercriminals remained unclear, both state-sponsored and organised criminal groups are suspected to have stolen sensitive court data across a dozen of districts.

However, the incident likely did not expose highly protected federal witnesses, as their identities are stored on separate Justice Department systems. The Justice Department previously in July 2022, investigated a significant hack of the federal court system, involving three foreign hacking groups, dating back to early 2020 (Sakellariadis & Gerstein, 2025). It remains unclear if the two incidents are related. The federal judiciary has pledged to roll out additional cybersecurity measures (US Courts, 2025) following the breach, to protect its electronic case filing system. It is prioritising collaboration with courts to mitigate the impact on litigants. The incident has raised concerns regarding the outdated federal judiciary systems, with lawmakers stressing the urgent need for infrastructure modernisation to protect the integrity of the legal system.

UK reverses Apple 'Backdoor' Demand after Talks with the US

The UK has reversed its demand for Apple, the iPhone maker, to build a "backdoor" that would have enabled access to encrypted data of U.S. citizens (Singh, 2025) - a request that sparked concerns over potential security vulnerabilities. The announcement was made by US Director of National Intelligence on social media on 18 August 2025, following months of talks between U.S. and UK officials, to ensure that the privacy rights and civil liberties of US citizens are protected. While the UK government did not disclose specifics, it emphasised its commitment towards balancing security and privacy.

The order, linked to the UK's Investigatory Powers Act, could have undermined Apple's commitment to user privacy and security, allowing law enforcement to access tech companies' data secretly, though UK hasn't confirmed the demand (Duffy & Maher, 2025). Apple had firmly opposed the demand, while cyber experts warned that it would compromise global privacy as such access could open the door for cybercriminals and authoritarian governments to exploit the system. While Apple did not comment on the reversed order, the company had already removed its Advanced Data Protection feature for UK users in February 2025, that offered end-to-end encryption for iCloud data (Singh, 2025). U.S. lawmakers had raised concerns that the UK's demand might have violated the CLOUD Act, which prohibits access to citizens' data without proper legal procedures (Singh, 2025).

Southeast Asian Criminal Groups Increasingly Use 'Ghost-tapping' to Launder Funds

Organised criminal groups in Southeast Asia, primarily the Chinese-speaking ones, are increasingly using "ghost-tapping", a sophisticated attack technique to launder their illicit profits (Reddick, 2025). In a report published by Recorded Future's Insikt Group on 14 August 2025 (Insikt Group, 2025), analysts have identified it to be an emerging threat to contactless payment systems as it exploits stolen payment card details linked to mobile wallets. The stolen card details, usually obtained through social engineering, phishing, and mobile malware, are uploaded to a burner phone, which is then used to make in-person purchases of luxury-goods at retail stores unlike traditional card fraud, which relies on online transactions.

The burner phones are typically sold on Telegram channels to criminal syndicates, for e.g., on channels linked to Huione Guarantee, a criminal marketplace (despite being officially shutdown in May 2025), Xinbi Guarantee and Tudou Guarantee, who employ mules to make the purchases of goods, which are later resold. The fraud involves Near Field Communication (NFC) relay technology, which bypasses the need for physical proximity, making it harder for security systems to identify and prevent it. In 2024, several arrests took place in Singapore related to ghost-tapping, including Chinese and Taiwanese nationals (Reddick, 2025), involved in purchasing luxury goods through fraudulent means. The Singapore police earlier in February 2025 had issued warnings (SPF, 2025) regarding risks associated with phishing attacks targeting credit card data and unauthorised transactions using contactless payment methods.

Interpol and African authorities Dismantle Cybercrime Networks, Recover Millions

Operation Serengeti 2.0, a major operation led by Interpol, coordinated across 18 African countries and the UK, from June to August 2025, resulted in the arrest of 1,209 suspected cybercriminals, and the recovery of nearly 97.4 million USD (Interpol, 2025). The operation, involving countries like Benin, Cameroon, Ghana, Kenya, Nigeria, and South Africa, among others, targeted cybercrimes such as online scams, ransomware, and business email compromise affecting almost 88,000 victims, and dismantled over 11,400 instances of malicious infrastructure.

Other operation highlights include dismantling of 25 cryptocurrency mining centres and confiscating 45 illicit power stations in Angola, which led to the seizure of over 37 million USD worth of equipment. Zambian authorities dismantled a major fraud scheme that defrauded 65,000 victims who lost an estimated 300 million USD, arrested 15, and disrupted a human trafficking network, seizing 372 forged passports. Additionally, a transnational inheritance scam originating in Germany was disrupted in Côte d'Ivoire, in which victims were tricked into paying fees resulting in 1.6 million USD losses. The operation, which follows the success of the first Operation Serengeti, highlighted the rising threat of cybercrimes in Africa, and their growing sophistication including AI-driven fraud.

Australia's Second-largest Internet Provider Hit by Major Cyberattack

A major cyberattack hit iiNet, Australia's second-largest internet provider, on 16 August 2025 that compromised the personal data of hundreds of thousands of customers (Glover, 2025). TPG, iiNet's parent company, confirmed the hack, notifying its customers three days later regarding the approximately 280,000 email addresses, 20,000 phone numbers, and user information like addresses and modem passwords that were potentially accessed by an unknown third party.

The breach affected iiNet's order management system, that is used for creating and tracking broadband connections of customers. The attackers accessed the system by using stolen employee credentials, extracting customer information but reportedly, no sensitive financial or identification information, like details of credit card or driver's license were exposed as those were not stored in the affected system. TPG has implemented measures to remove unauthorised access and is working with cybersecurity experts, as well as coordinating with the Australian Cyber Security Centre, the National Office of Cyber Security, the Office of the Australian Information Commissioner, and other relevant authorities (ABC, 2025). iiNet has apologised to its customers, assuring enhancement in its security measures. Meanwhile, customers have been advised to be cautious of suspicious communications claiming to be from iiNet and contact a dedicated hotline set up in this regard for additional concerns.

Debopama Bhattacharya
Dreamlab Audit Team
Dreamlab Research Team

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

References

ABC (2025): Cyber attack exposes details of thousands of internet provider iiNet's customers. ABC news, accessed 22nd August 2025, https://www.abc.net.au/news/2025-08-19/iinet-reveals-details-accessed-by-cyber-criminal/105671974

Duffy, C. & Maher, L. (2025): UK government walks back controversial Apple 'back door' demand after Trump administration pressure. CNN business, accessed 23rd August 2025, https://edition.cnn.com/2025/08/19/tech/uk-retreats-apple-back-door-vance-gabbard

Glover, A. (2025): At least 280,000 Aussies exposed in major cyberattack. MSN, accessed 22nd August 2025, https://www.msn.com/en-au/technology/cybersecurity/at-least-280-000-aussies-exposed-in-major-cyberattack/ar-AA1KLpmm

Insikt Group (2025): Ghost-Tapping and the Chinese Cybercriminal Retail Fraud Ecosystem. Recorded Future, accessed 23rd August 2025, https://www.recordedfuture.com/research/ghost-tapping-chinese-criminal-ecosystem

Interpol (2025): African authorities dismantle massive cybercrime and fraud networks, recover millions. Interpol, accessed 24th August 2025, https://www.interpol.int/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions

Reddick, J. (2025): Scammers turn to 'ghost-tapping' retail fraud to launder funds. The Record, accessed 23rd August 2025, https://therecord.media/scammers-ghost-tapping-retail-fraud-launder-cash

Sakellariadis, J. & Gerstein, J. (2025): Federal court filing system hit in sweeping hack. Politico, accessed 23rd August 2025, https://www.politico.com/news/2025/08/06/federal-court-filing-system-pacer-hack-00496916

Singapore Police Force (SPF) (2025): Unauthorised Card Transactions Made Using Contactless Payment Methods In Singapore. Government of Singapore, accessed 23rd August 2025, https://www.police.gov.sg/media-room/news/20250217_unauthorised_card_transactions_made_using_contactless_payment_methods_in_singapore

Singh, K. (2025): US spy chief Gabbard says UK agreed to drop 'backdoor' mandate for Apple. Reuters, accessed 23rd August 2025, https://www.reuters.com/sustainability/boards-policy-regulation/us-spy-chief-gabbard-says-uk-agreed-drop-backdoor-mandate-apple-2025-08-19/

US Courts (2025): Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System. The Federal Courts of the United States, accessed 23rd August 2025, https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

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