DREAMLAB TECHNOLOGIES

CYBER INSIGHTS

Research updates and insights from Dreamlab Technologies

In this issue:

Change Healthcare cyberattack impacts 100 million, causing massive data breach in the US

On 24 October 2024, the U.S. Department of Health and Human Services (HHS) updated details in its breach portal from the February 2024 Change Healthcare data breach, that indicates a compromise of personal health information of at least 100 million individuals (HHS OCR, 2024), making it one of the largest healthcare data breaches in the history of the US. The UnitedHealth Group (UHG), a health care provider which owns Change Healthcare, a health tech company, has been notifying affected individuals since late July 2024.

The data breach from the February 2024 ransomware attack on Change Healthcare led to exposing of sensitve information of individuals like names, addresses, social security numbers, health records including diagnoses, medications, insurance and other details (Change Healthcare, 2024).

The notorious BlackCat ransomware gang is believed to be responsible for the attack, which caused significant disruptions across U.S. healthcare services since the attack (Reuters, 2024). According to reports, systems were accessed by cybercriminals using stolen credentials, and lack of multi-factor authentication (MFA) allowed them to deploy ransomware. The breach was temporarily contained by Change Healthcare by disconnecting affected systems and notifying law enforcement. Following the incident, HHS launched a webpage addressing FAQs (HHS, 2024) related to Health Insurance Portability and Accountability Act (HIPAA) whose Privacy, Security, and Breach Notification Rules require healthcare entities to protect patient data and notify affected individuals in case of a breach.

ITU-WTSA 2024 concludes in India, setting new benchmarks in global technology standards

The World Telecommunication Standardization Assembly (WTSA-24), the governing conference for the International Telecommunication Union's (ITU) standardisation efforts was held in India from 15 to 24 October 2024 (ITU, 2024). Leading up to the conference, the ITU's Global Standards Symposium (GSS-24) and World Standards Day celebrations focused on innovation and standards for sustainable AI, virtual environments and smart cities.

The conference assessed and revised the existing guidelines, and agreed eight new WTSA resolutions (ITU, 2024a) that emphasised support for developing countries by directing the ITU to prioritise – responsible, safe, and inclusive AI through the 'AI for Good' platform; trusted and interoperable metaverse applications; sustainable digital transformation across industries; technical specifications for digital public infrastructure; communication technologies for vehicle-to-everything, intelligent transport systems and automated driving; mobile caller-location data for emergency communications; training the next generation of ITU standards experts; and continual adaptation to new policy objectives and market demand. The first International AI Standards Summit was also held, which concluded with the launch of the 'AI for Good Impact India' initiating a series of regional events on 'AI for Good'.

Ireland introduces Online Safety Code for video-sharing platforms to curb harmful content

Ireland's media and internet regulator, Coimisiún na Meán, in October 2024 introduced an Online Safety Code applying to video-sharing platforms based in Ireland (Coimisiún na Meán, 2024), including TikTok, YouTube, Instagram, and Facebook Reels. The Code is set to take effect from next month, mandating platforms to prohibit the uploading and sharing of harmful content like promotion of self-harm, cyberbullying, incitement to violence or hatred, criminal content such as child sex abuse material, terrorism, etc., and holding the platforms accountable for user safety.

The Online Safety Code complements the EU's Digital Services Act (DSA), by targeting harmful content that may not necessarily be illegal but poses significant risks. The code is divided into two parts- Part A providing the legislative framework and general platform obligations, while Part B outlining specific requirements under the directive, including measures to ensure the protection of children and the public. The code mandates age verification, content rating systems, parental controls to protect minors for platforms hosting harmful content, and addresses risks from behavioural targeted advertising. Under the directive, the video-sharing platforms are required to enforce content bans and act on user reports, by providing user-friendly methods to report harmful content.

AFP seizes $9.3 million in cryptocurrency linked to alleged ‘Ghost’ app mastermind

The Australian Federal Police (AFP) in an ongoing operation named ‘Operation Kraken’, arrested a 32-year-old Australia-based man, allegedly the mastermind behind ‘Ghost’, an encrypted messaging app, and later in October 2024, successfully restrained $9.3 million in cryptocurrency linked to him (AFP, 2024). Ghost was specifically designed for criminal activities including providing specialised smartphones to criminals to allow them to communicate securely using the app.

The AFP under the operation conducted raids targeting networks involved in organised crimes that resulted in numerous arrests, seizure of illicit drugs, firearms and weapons, recovery of around $2.67 million in cash and restraining over $11 million in assets (AFP, 2024a). ‘Ghost’ was successfully dismantled in a coordinated global effort with law enforcement from nine countries, supported by Europol, through a specialised infiltration method by modifying software updates, and enabling access to content on devices tied to various criminal activities (AFP, 2024b). A criminal syndicate linked to Ghost was also disrupted under the operation, arresting six men on serious charges including conspiracy to fabricate a dangerous terrorism plot. The operation has highlighted the ongoing challenges posed by evolving encryption technologies, rapidly adopted by organised criminal networks across the world.

Microsoft reports 600M daily cyberattacks, calls for effective deterrence measures

Microsoft, in October 2024 reported handling over 600 million cyberattacks daily, including ransomware, identity theft, phishing, and increasingly sophisticated threats from both cybercriminals and state-sponsored actors (Microsoft, 2024), in its Digital Defense Report 2024, covering trends from July 2023 to June 2024. With the growing challenges against highly skilled and resourced adversaries, Microsoft calls for effective deterrence measures and meaningful consequences for violation of international norms, through joint public and private sector efforts.

Key insights from the Digital Defense Report 2024 indicate a rise in nation-state actors collaborating with cybercriminals, using their tools and tactics for espionage and financial gain. Research showed that their activities were concentrated in regions with active military conflicts such as Israel and Ukraine. Efforts to influence the U.S. elections were seen getting intensified with Russia, Iran, and China using spoofed links for phishing and malware attacks. Microsoft also noted a troubling rise of tech scams by 400% since 2022 and ransomware attempts by 2.75 times year over year, however, with a successful reduction in the number of attacks reaching the encryption stage. While AI is increasingly being used by threat actors to enhance their attacks, it also shows promises in cyber security through automated tasks like impact analysis, enabling faster response to cyberattack and improved defence strategies.

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 Federal Police (AFP) (2024): Operation Kraken: AFP restrains $9.3 million in crypto linked to alleged head of global organised crime app. Australian Federal Police, accessed 24th October, 2024, https://www.afp.gov.au/news-centre/media-release/operation-kraken-afp-restrains-93-million-crypto-linked-alleged-head

Australian Federal Police (AFP) (2024a): Operation Kraken: alleged head of global organised crime app charged with drug and proceeds of crime offences. Australian Federal Police, accessed 24th October, 2024, https://www.afp.gov.au/news-centre/media-release/operation-kraken-alleged-head-global-organised-crime-app-charged-drug-and

Australian Federal Police (AFP) (2024b): AFP Operation Kraken charges alleged head of global organised crime app. Australian Federal Police, accessed 24th October, 2024, https://www.afp.gov.au/news-centre/media-release/afp-operation-kraken-charges-alleged-head-global-organised-crime-app

Change Healthcare (2024): HIPAA WEBSITE SUBSTITUTE NOTICE. Change Healthcare, accessed 25th October 2024, https://www.changehealthcare.com/hipaa-substitute-notice

Coimisiún na Meán (2024): Online Safety Code. Coimisiún na Meán, accessed 30th October 2024, https://www.cnam.ie/wp-content/uploads/2024/10/Coimisiun-na-Mean_Online-Safety-Code.pdf

International Telecommunication Union (ITU) (2024): World Telecommunication Standardization Assembly (WTSA-24) New Delhi, India, 15 – 24 October 2024. International Telecommunication Union, accessed 29th October 2024, https://www.itu.int/wtsa/2024/

International Telecommunication Union (ITU) (2024a): New global agreements on AI, metaverse and sustainability at key ITU standards conference. International Telecommunication Union, accessed 29th October 2024, https://www.itu.int/en/mediacentre/Pages/PR-2024-10-24-WTSA-closing.aspx

Microsoft (2024): Microsoft Digital Defense Report 2024. Microsoft, accessed 31st October 2024, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Reuters (2024): UnitedHealth says 'Blackcat' ransomware group behind hack at tech unit. Reuters, accessed 25th October 2024, https://www.reuters.com/technology/unitedhealth-confirms-blackcat-group-behind-recent-cyber-security-attack-2024-02-29/

U.S. Department of Health and Human Services Office for Civil Rights (HHS OCR) (2024): Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. U.S. Department of Health and Human Services, accessed 25th October 2024, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. Department of Health and Human Services (HHS) (2024): Change Healthcare Cyber security Incident Frequently Asked Questions. U.S. Department of Health and Human Services, accessed 25th October 2024, https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cyber security-incident-frequently-asked-questions/index.html

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