DREAMLAB TECHNOLOGIES

CYBER INSIGHTS

Research updates and insights from Dreamlab Technologies

In this issue:

Cyberattack on UK hospitals lead to online data breach

On 20 June 2024, a group of cybercriminals disclosed confidential data obtained from a ransomware attack on Synnovis, a joint venture providing pathology lab services for several hospitals run by the National Health Service (NHS), UK (NHS England, 2024). The data released on the darknet site of Qilin, the cybercriminal group behind the attack, likely linked to Russia, included almost 400GB of sensitive information that comprised of patient names, dates of birth, NHS numbers, and blood test descriptions (BBC, 2024).

The ransomware attack that took place on 3 June 2024, severely impacted hospitals in London, disrupting operations and postponing several surgeries and outpatient appointments (NHS England, 2024a). Some services like blood tests were redirected to other providers, while a helpline was established to address inquiries from patients and healthcare staff during the emergency. The NHS and Synnovis are actively collaborating with the National Cyber Security Centre and the National Crime Agency to verify the contents and authenticity of the published data following the ransomware attack. The criminal investigation, however, is expected to extend for weeks as per the NHS announcement, amidst concerns over the rising prevalence and disruptive impact of ransomware attacks on critical infrastructure worldwide. The specific ransom amount demanded by Qilin however remains undisclosed, but publication of data by the hacker group indicates that Synnovis did not meet the ransom demands, a move advisable by global law enforcement agencies.

US imposes sanctions on Kaspersky executives amid ban on software sale

The U.S. government on 21 June 2024, in a press release by the Department of the Treasury's Office of Foreign Assets Control (OFAC) announced sanctions against 12 executives and senior leaders of Kaspersky Lab, a Russia-based cybersecurity firm, to ensure security of the cyber domain and safeguard U.S. citizens from cyberattacks (USDT, 2024). The sanctions came a day after the U.S. government announced a 'first of its kind' ban on the sale of Kaspersky software, citing concerns over national security and user privacy (BIS, 2024).

The sanctions will restrict the executives from starting new ventures and prohibit US citizens from transacting with them in funds, goods or services, among other restrictions (USDT, 2024). The ban on the sale of Kaspersky software in the US was imposed following investigations that revealed concerns over Russia's cyber capabilities and its potential influence on Kaspersky's activities (BIS, 2024). Kaspersky however denied these accusations, intending to contest the ban arguing that the decision was based on the 'present geopolitical climate' rather than an assessment of the integrity of its products (Reuters, 2024). The US government announced that software updates of Kaspersky would be available to existing customers until 29 September 2024, to allow them to find alternative cybersecurity solutions, post which their antivirus protection would become outdated and hence ineffective.

EU targets Apple under new digital markets law, threatens significant penalties

European Union regulators have accused Apple of violating the Digital Markets Act (DMA) by restricting app developers from directing users to cheaper alternatives outside its App Store (EC, 2024). Apple thus likely becomes the first major tech firm accused of violating the DMA, the new legislation by the European Commission aimed at ensuring fair competition in the digital market and preventing tech giants from monopolising it (EC, 2024a).

Earlier in March 2024, the U.S. Justice Department filed an antitrust lawsuit against Apple for monopolising the smartphone market over its management of cloud-based applications and alternative payment systems within iPhone apps (US DOJ, 2024). The European Commission is currently investigating Apple's new 'core technology fee', a fee charged for third-party app downloads, which critics allege could hinder competition and stifle innovation. In response, Apple clarified to have made significant changes in its platform, allowing users to use third-party app stores and have reduced fees in the EU to comply with the DMA guidelines (AP, 2024). A final decision on the issue is expected by March 2025 by the Commission that could potentially lead to fines up to 10% of Apple's global revenue. Apple is already facing a €2 billion fine related to unfair competition in music streaming. Apple however stated that it will 'continue to listen and engage' with the commission.

Australian regulator initiates legal action against Medibank over data breach

The Australian Information Commissioner on 24 June 2024, announced legal action in the Federal Court against Medibank, a major health insurance company in Australia, in relation to a data breach from its October 2022 cyberattack (OAIC, 2024). Medibank was held accountable for neglecting its responsibilities under the Privacy Act 1988, that resulted in the exposure of sensitive personal information belonging to approximately 9.7 million Australians.

The breached data included names, dates of birth, Medicare numbers, and other sensitive medical information, which was reportedly exposed on the dark web, posing serious risks of identity fraud and emotional distress for affected individuals. Earlier in January 2024, sanctions were imposed by the Australian government on Aleksandr Ermakov, the Russian hacker responsible for the Medibank cyberattack, in accordance with the '2023-2030 Australian Cyber Security Strategy', following collaborative efforts by the Australian Signals Directorate, Australian Federal Police, and international partners to disrupt cybercriminal operations (Australian Government, 2024). The legal action against Medibank was initiated after an OAIC investigation and could lead to significant penalties reaching trillions of dollars, reflecting the seriousness of the alleged privacy violation.

Indonesia's data centre hit by ransomware attack

Indonesia's national data centre suffered a major cyberattack on 20 June 2024, resulting in widespread disruptions to government services including significant delays at Jakarta's main airport (Reuters, 2024a). Reportedly, the attack is among the most severe cyberattacks in Indonesia recently, affecting more than 40 government entities, including critical infrastructure in the country.

The malware behind the ransomware attack was identified as a new version of the notorious Lockbit, infamous for encrypting systems and data, following which hackers demand a hefty ransom in cryptocurrency; reportedly a $8 million in this attack (Reuters, 2024b). The government, however, has refused to pay the amount. The communications ministry of Indonesia confirmed that data recovery efforts successfully restored operations in several agencies and is continuing to fully restore affected services. Cybersecurity analysts remarked that the incident highlighted the persistent threat of ransomware attacks on critical infrastructure worldwide and the urgent need for robust cybersecurity measures in maintaining public trust in digital services.

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 Government (2024): Cyber sanctions in response to Medibank Private cyber attack. Australian Government, Defence, accessed 30th June 2024, https://www.minister.defence.gov.au/media-releases/2024-01-23/cyber-sanction-response-medibank-private-cyber-attack

The Associated Press (AP) (2024): Apple becomes first target of EU's new digital competition rules aimed at big tech. The Associated Press , accessed 2nd July 2024, https://apnews.com/article/apple-european-union-digital-regulation-rules-app-store-07c34a80a5c98d0014e1c669a86af6a4

BBC (2024): Stolen test data and NHS numbers published by hospital hackers. BBC, accessed 2nd July 2024, https://www.bbc.com/news/articles/c9ww90j9dj8o

Bureau of Industry & Security (BIS) (2024): Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers. Bureau of Industry & Security, accessed 23rd June 2024, https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-us-customers

The European Commission (EC) (2024): Commission sends preliminary findings to Apple and opens additional non-compliance investigation against Apple under the Digital Markets Act. The European Commission, accessed 3rd July 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3433

The European Commission (EC) (2024a): The Digital Markets Act. The European Commission, accessed 3rd July 2024, https://digital-markets-act.ec.europa.eu/index_en

NHS England (2024): Synnovis cyber incident. NHS England, accessed 2nd July 2024, https://www.england.nhs.uk/synnovis-cyber-incident/

NHS England (2024a): Update on cyber incident: Clinical impact in south east London – Thursday 27 June. NHS England, accessed 2nd July 2024, https://www.england.nhs.uk/london/2024/06/27/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-27-june/

Office of the Australian Information Commissioner (OAIC) (2024): OAIC takes civil penalty action against Medibank. Australian Government, accessed 30th June 2024, https://www.oaic.gov.au/newsroom/oaic-takes-civil-penalty-action-against-medibank

Reuters (2024): Biden bans US sales of Kaspersky software over Russia ties. Reuters, accessed 27th June 2024, https://www.reuters.com/technology/biden-ban-us-sales-kaspersky-software-over-ties-russia-source-says-2024-06-20/

Reuters (2024a): Cyber attack compromised Indonesia data centre, ransom sought. Reuters, accessed 2nd July 2024, https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/

Reuters (2024b): More than 40 Indonesian agencies hit by cyberattack on data centres. Reuters, accessed 2nd July 2024, https://www.reuters.com/world/asia-pacific/more-than-40-indonesian-agencies-hit-by-cyberattack-data-centres-2024-06-26/

US Department of Justice (US DOJ) (2024): Justice Department Sues Apple for Monopolizing Smartphone Markets. US Department of Justice, accessed 3rd July 2024, https://www.justice.gov/opa/pr/justice-department-sues-apple-monopolizing-smartphone-markets

US Department of the Treasury (USDT) (2024): Treasury Sanctions Kaspersky Lab Leadership in Response to Continued Cybersecurity Risks. U.S. Department of the Treasury, accessed 24th June 2024, https://home.treasury.gov/news/press-releases/jy2420

ISECOM

ISECOM

Member of the World Wide Web Consortium for security standards.

W3C

W3C

Board member of the Institute for Security and Open Methodologies.

UNIÓN EUROPEA

Research partner for EU cyber security research projects.

OWASP

OWASP

Member of the Open Web Application Security Project.

ITU

INTERNATIONAL TELECOMUNICATION UNION

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

FIRST

FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST)

Liaison Member.

swiss made software

SWISS MADE SOFTWARE

Officially certified as a provider of Swiss Made Software solutions.

CYBERSECURITY MADE IN EUROPE

CYBER SECURITY MADE IN EUROPE

Recognition of the quality of our cybersecurity services and products.

Partner CYBER SAFE

PARTNER CYBER SAFE

Audit partner for the label certification process.

nw Fachhochschule Nordwestschweiz

FACHHOCHSCHULE NORDWESTSHWEIZ

Research partner for digital initiatives in Switzerland.

ALSEC

ALSEC

Specialized partner for critical operational technology (OT) infrastructures.

SLINF share & lead

SLINF

Specialized partner of government security solutions.

ccig

GENEVA CHAMBER OF COMMERCE

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

black hat

BLACK HAT

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

swiss cyber security DAYS

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