DREAMLAB TECHNOLOGIES

CYBER INSIGHTS

Research updates and insights from Dreamlab Technologies

In this issue:

Apple warns global users of spyware; BlackBerry notes LightSpy in South Asia

In a threat notification released on April 10, 2024, Apple alerted iPhone users in around 90 countries, warning them of mercenary spyware attacks, and provided them access to emergency assistance. The threat notification, however, did not disclose the identities of the attackers or the geographical regions associated with the attacks (Apple, 2024). Apple mentioned that the threat notifications were designed to inform users who were individually targeted likely because of ‘who they are or what they do’ highlighting it to be a very serious issue.

Mercenary spyware attacks are complex and exceptionally costly cybercriminal activities, often hard to detect and prevent, that target devices of specific individuals like activists, journalists, politicians and diplomats.

Apple has also issued guidance for all users that includes best cybersecurity practices like updating to the latest software, protecting the devices with a passcode, use of two-factor authentication, strong passwords for Apple ID, installation of apps from the App Store and more. Further, it suggested enabling the ‘lockdown mode’ (Apple, 2023) on Apple devices for additional protection. A day after the notification was issued, Blackberry reported the resurgence of LightSpy, a spyware capable of file theft from messenger applications, audio recording, data harvesting and other sophisticated attacks on the victim’s device, linking it with the threat notification from Apple (BlackBerry, 2024). Reportedly, the attackers behind the LightSpy campaign have their active servers in China, Singapore, and Russia and focus on targets in Southern Asia.

CISA announces new release of Malware Next-Gen analysis system

The Cybersecurity and Infrastructure Security Agency (CISA) on April 10, 2024, announced the new release of 'Malware Next-Gen', a malware analysis system that will allow organisations to submit samples of malware and get them analysed (CISA, 2024). The malware analysis system automates the analysis of newly identified malware and provides crucial intelligence for cyber defence efforts. The automated malware analysis support is exclusively provided to US citizens and the CISA aims to further enhance threat detection and response capabilities, thus bolstering the overall national cybersecurity.

The CISA has encouraged all organisations, security professionals, and individuals to register and submit suspected malware for analysis. Users in the US can access the analysis platform by a one-time registration through a 'login.gov' account while others can submit malware through the 'Anonymous submission' method (CISA, 2024a). However, using the latter method will not allow access to the results of malware analysis. Moreover, the CISA warns of unauthorised access or misuse of the system, which can lead to penalties, and strictly prohibits processing classified information on the system. 'Malware Next-Gen' has already helped users identify more than 200 suspicious files and URLs out of the ones that were submitted for analysis; the analyses results are available in PDF and STIX 2.1 formats.

EU Data Protection Body opposes 'consent or pay' model of large online platforms

The European Data Protection Board in an opinion published on April 17, 2024, opposed the 'consent or pay' model of large online platforms, stating its non-compliance with EU data privacy rules. The business model gives users a choice between allowing processing of data to enjoy free services or paying for the services. The board emphasised the need for more free options or 'equivalent alternatives' beyond just paid services and consent to allow the processing of personal data for behavioural advertising purposes (EDPB, 2024).

The EDPB stated that simply obtaining consent from users does not ensure compliance with Article 5 of General Data Protection Rules (GDPR) that include provisions like purpose limitation, data minimisation and fairness (EDPB, 2024a). The underlying issue, as the board notes, is that through the business model the 'fundamental right to data protection' is being transformed into a feature that individuals must pay for to enjoy. Earlier in November 2023, Meta introduced the 'pay or consent' model, following which the European Consumer Organisation (BEUC, 2024) and the non-profit digital rights organisation NOYB filed separate complaints (noyb, 2023) against Meta on grounds of breaching consumers' fundamental rights and illegal processing of data.

Russia-backed Sandworm elevated to APT44, posing a major threat to Ukraine

Mandiant, the cybersecurity firm and subsidiary of Google, on April 17, 2024, released a report titled 'APT44: Unearthing Sandworm', revealing how Sandworm, the notorious cyber threat group has advanced in its operations to reach the Advanced Persistent Threat (APT) level and continues to pose a major threat to Ukraine (Mandiant, 2024).The APT level involves advanced attack techniques used to target victims over extended periods of time.

Mandiant mentions that the threats are not limited to Ukraine alone. Sandworm has a history of interference in democratic processes, espionage, and in targeting governments and critical infrastructure organisations globally, raising major concerns on the impact of its operations in the 2024 elections worldwide. The report assessed how Sandworm, now classified as APT44, has worked closely with the Russian military, playing a central role in shaping its objectives and supporting Russia's wider national interests. APT44 is infamously known for some of the most disruptive cyberattacks till date such as the attacks on Ukraine's energy grid (2015 and 2016), the NotPetya ransomware outbreak (2017), and several others (Mandiant, 2024). Mandiant has taken various steps to protect customers and the community by enabling safe browsing, threat alerts, victim notifications, and has released the 'APT44-related indicators of compromise' for registered users.

Australian regulators criticise tech titans over defying legal orders

The Australian government has criticised tech companies such as X and Meta for irresponsible handling of content related to the Sydney stabbing incident that took place on April 15, 2024, at a church in Wakeley. In the incident, a priest was attacked and stabbed, and a video of the incident was circulated widely on social media, causing concern among political leaders and legal authorities regarding the potential incitement of further violence. The eSafety Commissioner issued notices to companies seeking removal of the footage from their respective platforms to which some complied (Australian Government, 2024).

However, X Corp. refused the 'global' takedown order, arguing that it violated free speech. Elon Musk, the leader of the company has been fighting a legal battle in the federal court, challenging the authority of national governments to regulate online spaces. The Federal Court had initially granted an interim injunction requiring X to comply with the notice. However, according to the May 13, 2024 court decision, the interim injunction was not extended further (Australian Government, 2024a), granting X a reprieve. The clashes between the two sides however continued, prompting the Australian government to emphasise the importance of 'social responsibility' of the social media (Microsoft, 2024).

Debopama Bhattacharya
Dreamlab Audit Team
Dreamlab Research Team

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

References

Apple (2023): About Lockdown Mode. Apple, accessed 22nd April 2024, https://support.apple.com/en-gb/105120

Apple (2024): About Apple threat notifications and protecting against mercenary spyware. Apple, accessed 22nd April 2024, https://support.apple.com/en-in/102174

Australian Government (2024): Statement on removal of extreme violent content. E safety Commissioner, Australian Government, accessed 29th April 2024, https://www.esafety.gov.au/newsroom/media-releases/statement-on-removal-of-extreme-violent-content

Australian Government (2024a): Statement on Federal Court decision. Australian Government, accessed 22nd May 2024, https://www.esafety.gov.au/newsroom/media-releases/statement-on-federal-court-decision

Bureau Européen des Unions de Consommateurs (BEUC) (2024): How Meta is breaching consumers' fundamental rights. Bureau Européen des Unions de Consommateurs, accessed 22nd April 2024, https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-020_How_Meta_is_breaching_consumers_fundamental_rights.pdf

BlackBerry (2024): BlackBerry blog, LightSpy Returns: Renewed Espionage Campaign Targets Southern Asia, Possibly India. BlackBerry, accessed 23rd April 2024, https://blogs.blackberry.com/en/2024/04/lightspy-returns-renewed-espionage-campaign-targets-southern-asia-possibly-india

The Cybersecurity and Infrastructure Security Agency (CISA) (2024): CISA Announces Malware Next-Gen Analysis. The Cybersecurity and Infrastructure Security Agency, accessed 20th April 2024, https://www.cisa.gov/news-events/news/cisa-announces-malware-next-gen-analysis?ref=news.risky.biz

The Cybersecurity and Infrastructure Security Agency (CISA) (2024a): Malware Next-Generation Analysis. The Cybersecurity and Infrastructure Security Agency, accessed 20th April 2024, https://www.cisa.gov/resources-tools/services/malware-next-generation-analysis?ref=news.risky.biz

European Data Protection Board (EDPB) (2024): Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms. European Data Protection Board, accessed 22nd April 2024, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en

European Data Protection Board (EDPB) (2024a): EDPB: 'Consent or Pay' models should offer real choice. European Data Protection Board, accessed 22nd April 2024, https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_en

Mandiant (2024): APT44: Unearthing Sandworm. Mandiant, accessed 29th April 2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

Microsoft (2024): Elon Musk Slams Australian Government For Saying 'Social License' Is Required Amid Tussle With X: 'Doubt...People Of Australia Agree With Suppressing Their Rights'. Microsoft, accessed 22nd May 2024, https://www.msn.com/en-us/money/news/elon-musk-slams-australian-government-for-saying-social-license-is-required-amid-tussle-with-x-doubtpeople-of-australia-agree-with-suppressing-their-rights/ar-BB1mc0vI

NOYB (2024): noyb files GDPR complaint against Meta over "Pay or Okay". NOYB, accessed 22nd April 2024, https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay

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