DREAMLAB TECHNOLOGIES

CYBER INSIGHTS

Research updates and insights from Dreamlab Technologies

In this issue:

CISA warns of Cleo Zero-Day vulnerability being exploited in ransomware attacks

The Cybersecurity and Infrastructure Security Agency (CISA) on 13 December 2024, issued a critical warning about an actively exploited vulnerability affecting file-sharing products from the software company Cleo (CISA, 2024). The vulnerability, 'CVE-2024-50623', affected three products, Cleo Harmony, VLTrader and LexiCom, allowing attackers to upload malicious files and potentially execute remote code with escalated privileges. CISA added the vulnerability to its 'Known Exploited Vulnerabilities (KEV) catalog', urging organisations to urgently patch it or discontinue use of the products.

Cleo released a patch earlier in December 2024 (Cleo, 2024); however, the flaw was not fully resolved and threat actors continued to exploit it (Huntress, 2024) affecting businesses across industries including consumer products, food and shipping.

Cleo has been working with cyber security experts to investigate the issue and has notified customers regarding instructions on how to mitigate the risk, including blocking specific IP addresses involved in the exploitation. The issue highlights an increase in the targeting of file transfer tools in data theft campaigns. Earlier on 4 December 2024, CISA had added another vulnerability, 'CVE-2024-51378', to the 'KEV catalog' (CISA, 2024), stating that ransomware gangs were actively exploiting it, and had urged immediate action to prevent any data breach. The vulnerability was discovered in CyberPanel, an open-source web hosting control panel typically used by organisations for web hosting, email management, etc., which could be exploited to bypass authentication and execute arbitrary commands, making it extremely dangerous.

EU imposes first-ever sanctions over Russian hybrid threats and destabilising actions abroad

The European Council on 16 December 2024, sanctioned 16 individuals and three entities linked to Russia's hybrid activities including destabilisation efforts, disinformation campaigns and cyberattacks abroad (EU, 2024). The sanctions are in response to Russia's violation of international law and its disregard for a rules-based global order introduced under a framework set up in October 2024, to address hybrid threats by targeting those engaged in malicious cyber activities, assassinations, espionage, spreading propaganda, foreign information manipulation and interference (FIMI), and other destabilising activities (EC, 2024).

The sanctions target members of Russia's GRU Unit 29155, known for assassinations, bombings and cyberattacks across Europe, officials of the "Doppelganger" disinformation campaign aimed at manipulating information, 'Groupe Panafricain pour le Commerce et l'Investissement', a pro-Russian disinformation network operating mainly in the Central African Republic and Burkina Faso, 'African Initiative', a news agency spreading Russian propaganda in Africa, and other individuals linked to espionage and intelligence operations against Germany and France. The sanctions include travel bans, asset freeze and restrictions on financial interactions within the EU.

Australia passes law banning social media for children under 16

The Australian government has granted an extra two months to the tech sector to finalise plans to restrict children's access to adult content, following the Online Safety Amendment (Social Media Minimum Age) Act 2024 (Australian Government, 2024), passed by the Australian Parliament in December 2024. Under the act, certain social media companies are required to ensure that users are 16 years of age or older, to access their platform, through specific enforcement details which are expected to conclude by 2025.

Bypassing age restrictions will lead to penalties for the service providers and not the users or their parents. The law is a part of the Australian government's boarder strategy to protect Australians online that requires online services like websites, social media, search engines, and apps to develop 'industry codes' to include age-assurance mechanisms for harmful content, such as child sexual exploitation and pro-terror material; and to develop additional initiatives like 'Safety by Design', 'Digital Duty of Care', for proactive safeguarding of users (Australian Government, 2024a). The deadline for developing the codes is February 2025, which is two months from the passage of the law. The law has sparked significant criticism from advocacy groups, citing concerns on the potential impact of the ban on children's rights, which could lead them to the dark web, or even increase isolation, besides other privacy risks like platforms collecting sensitive personal data to verify age.

Interpol's 'Think Twice' warns of cybercrime; 'Operation Serengeti' disrupts networks across Africa

The Interpol on 3 December 2024, launched 'Think Twice', a campaign to warn against cyber and financial crimes targeting vulnerable individuals and organisations across the world. Key highlights of the campaign include short videos with a focus on five key emerging online threats: ransomware attacks, malware, phishing, generative AI scams, and romance baiting, which have significantly grown in recent years (Interpol, 2024). Ransomware and malware attacks have surged by 70% and 30% respectively in the last year, with phishing and romance baiting scams becoming more sophisticated, and criminals exploiting generative AI to create realistic human avatars for manipulation.

Earlier in November 2024, Operation Serengeti, jointly led by Interpol and Afripol and with support from private partners, had resulted in the dismantling of over 134,000 malicious networks and over 1,000 arrests across 19 African countries (Interpol, 2024a), targeting cybercriminal groups responsible for ransomware attacks, business email compromise (BEC), online scams, and digital extortion (all of which are identified as prominent threats in the 'African Cyberthreat Assessment Report 2024'). With such rising threats from cybercrimes, the 'Think Twice' initiative is a right step towards promoting proactive cyber security through measures like verifying unsolicited messages and links before clicking on them, safeguarding personal information, verifying identities and exercising caution in online relationships.

Apple to pay $95 million to settle lawsuit accusing Siri of secretly eavesdropping

Apple has agreed to pay $95 million to settle a lawsuit accusing Siri of secretly eavesdropping on users without their knowledge, violating privacy commitments (Forbes, 2025). According to reports, the proposed settlement filed in federal court on 13 December 2024 is awaiting approval by a U.S. district judge.

The lawsuit, filed five years ago, in 2019, alleges that Siri was activated without the consent of users and some recorded conversations were shared with third parties like advertisers for effective targeting of consumers. Apple, however, stressed on its commitment to privacy by denying any wrongdoing, but settling the lawsuit could avoid further legal costs and reputational damage. The settlement covers consumers in the US who owned Siri-enabled devices from September 2014 to the end of 2023, who could receive up to $20 per device. The settlement terms are subject to review in a court hearing scheduled for 14 February 2025 (AP, 2025). Apple emphasised its ongoing efforts to improve Siri's privacy, including the 2019 changes such as 'opt-in data collection' for analytics, the use of only 'computer-generated transcripts' to improve Siri, among others.

Debopama Bhattacharya
Dreamlab Audit Team
Dreamlab Research Team

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

References

Australian Government (2024): Federal Register of Legislation, Online Safety Amendment (Social Media Minimum Age) Act 2024. Australian Government, accessed 6th January 2025, https://www.legislation.gov.au/C2024A00127/asmade/text

Australian Government (2024a): esaftety Comissioner, Social media age restrictions. Australian Government, accessed 6th January 2025, https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions

Cleo Solution Center (Cleo) (2024): Cleo Product Security Advisory - CVE-2024-50623. Cleo Solution Center, accessed 30th December 2024, https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623

Cybersecurity and Infrastructure Security Agency (CISA) (2024): Known Exploited Vulnerabilities Catalog. Cybersecurity and Infrastructure Security Agency, accessed 26th December 2024, https://www.cisa.gov/known-exploited-vulnerabilities-catalog

European Council (EC) (2024): Russia: New sanctions framework against those responsible for destabilising activities against the EU and its member states. European Council, accessed 3rd January 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/russia-eu-sets-up-new-framework-for-restrictive-measures-against-those-responsible-for-destabilising-activities-against-the-eu-and-its-member-states/

European Union (EU) (2024): Council Decision (CFSP) 2024/3174 of 16 December 2024 amending Decision (CFSP) 2024/2643 concerning restrictive measures in view of Russia's destabilising activities. European Union, accessed 3rd January 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202403174

Forbes (2025): Apple Siri Eavesdropping Payout—Here's Who's Eligible And How To Claim. Forbes, accessed 6th January 2025, https://www.forbes.com/sites/kateoflahertyuk/2025/01/06/apple-siri-eavesdropping-payout-heres-whos-eligible-and-how-to-claim/

Huntress (2024): Threat Advisory: Oh No Cleo! Cleo Software Actively Being Exploited in the Wild. Huntress, accessed 2nd January 2025, https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild

Interpol (2024): INTERPOL campaign warns against cyber and financial crimes. Interpol, accessed 29th December 2024, https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-campaign-warns-against-cyber-and-financial-crimes

Interpol (2024a): Major cybercrime operation nets 1,006 suspects. Interpol, accessed 29th December 2024, https://www.interpol.int/News-and-Events/News/2024/Major-cybercrime-operation-nets-1-006-suspects

The Associated Press (AP) (2025): Apple to pay $95 million to settle lawsuit accusing Siri of eavesdropping. The Associated Press, accessed 6th January 2025, https://apnews.com/article/apple-siri-iphone-lawsuit-settlement-9b8ab3e079ae6962435f38eddb937b39

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