November 2023

DREAMLAB TECHNOLOGIES

CYBER INSIGHTS

RESEARCH UPDATES AND INSIGHTS FROM DREAMLAB TECHNOLOGIES

In this issue:

EU likely to be the first region to enact AI legislations

As a part of European Union's (EU) digital strategy, the European Commission is in the final negotiating stages over its artificial intelligence (AI) Act. The first draft regulatory framework was proposed in 2021, which was updated this year and once passed, it will be the world's first legislation on AI. The reason for regulating the AI according to the EU Parliament, is to ensure that AI systems are safe, non-discriminatory, transparent, traceable and environmentally friendly (EP, 2023).

According to the act, AI systems would be classified as 'unacceptable', 'high' and 'limited' risk category according to the risk they pose to users, which in turn will determine the extent of regulations (EP, 2023). The 'unacceptable' risk category would include AI systems that are considered a threat to people and will thus be banned under the regulations. Such systems include real-time and remote biometric identification systems (such as facial recognition) and social scoring (classifying people based on behaviour, socio-economic status or personal characteristics), among others.

The 'high' risk category would include AI systems that negatively affect safety or fundamental rights and will either be assessed before being put on the market (subcategory 1) or have to be registered in an EU database (subcategory 2). Some examples are AI systems used in products like toys, cars, medical devices, etc. falling under the EU's product safety legislation (subcategory 1) and AI systems falling into eight specific areas like management and operation of critical infrastructure, employment, worker management and access to self-employment, among others (subcategory 2). The 'limited' risk category includes AI systems that generate or manipulate image, audio or video content, for instance deepfakes. Such systems should comply with minimal transparency requirements that would allow users to make informed decisions. As for generative AI, certain transparency requirements would have to complied with such as disclosure that the content was generated by AI and disclosure of the data used to train any large language model.

Taiwan, US, Vietnam and Pacific Islands targets of state-sponsored hacking

New research from Symantec published on 10 October, 2023 has revealed that a hacker group under the name “Grayling” is targeting organisations across Taiwan, Vietnam, the U.S. and a government agency located in the Pacific Islands (Symantec, 2023). The attacks took place on several organisations in the manufacturing, IT, and biomedical sectors, with the main goal of espionage rather than financial motives. While researchers in Symantec have not been able to confirm links of the hacker group to a specific country, but they mentioned that heavy targeting of Taiwanese organisations did indicate operations from a region that has “strategic interest” in Taiwan.

According to researchers, custom techniques combined with publicly available tools were used to attack the targets. Havoc, an open-source tool was used that allowed downloading additional payloads, executing commands, manipulating Windows tokens and other activities. Symantec also saw the use of NetSpy, a spyware tool and exploitation of the Windows vulnerability CVE-2019-0803.

New Guidance on Improving Security of Open Source Software (OSS)

A new guidance called “Improving Security of Open Source Software (OSS) in Operational Technology (OT) and Industrial Control Systems (ICS),” was published by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and U.S. Department of the Treasury on 10 October, 2023 (CISA, 2023). It has been developed through the Joint Cyber Defense Collaborative (JCDC) as part of 2023 OSS Planning Agenda, which aims at a more focused collaboration between the government and the private sector to develop and execute cyber defence plans with specific risk reduction. It also aims to promote the secure use of OSS in OT or ICS environments.

The guidance comes in response to concerns related to cybersecurity and safety of critical infrastructure organisations using OT or ICS, due to the potentially far-reaching impacts of incidents and safety implications in connected infrastructure. Even general cyber hygiene practices like updating software routinely, can be challenging for such organisations that use OSS in OT and ICS applications. The guidance is in line with the National Cyber Strategy, the Office of National Cyber Director Open-Source Software Security Initiative (OS3I) and the CISA Open Source Software Security Roadmap (CISA, 2023).

Australia proposes draft legislation to regulate digital payment providers

A draft legislation was released by the Australian Treasury that would provide the Reserve Bank of Australia (RBA) regulatory powers over the digital payment providers in the country (RBA, 2023). The legislations seek to expand the Payment Systems (Regulation) Act of 1998 of Australia to include "new and emerging payments systems" like digital wallets, services like buy now pay later (BNPL) and the New Payments Platform (NPP) that enables customers and businesses to make real-time, data-rich payments, among others (RBA, 2023).

The digital payment systems and mobile wallets which have grown rapidly in recent years are currently outside the scope of Australia's financial regulatory system. The legislation would empower the RBA to monitor digital wallet payments in the same manner as credit card networks and other financial transactions are monitored. Additionally, it would also enable regulators to intervene and address risks (frauds, scams, etc.) if any, posed by any of these payment platforms. Currently, the legislation is under public consultation until 1 November 2023, to seek feedback from important stakeholders and is expected to be introduced in the parliament this year.

Cyberdrill carried out at ITU headquarters by Saudi NCA

The Saudi National Cybersecurity Authority (NCA) held a Cyberdrill at the International Telecommunication Union (ITU) headquarters on 7 October, 2023 in Geneva, Switzerland to raise the level of cyber readiness, and enable the exchange of information and knowledge in the field of cybersecurity (SPA, 2023). The exercise came as a part of Saudi Arabia's initiatives to support cooperation and joint endeavour in the global cyberspace and took place as part of the ITU Learning Labs initiative.

The drill demonstrated a realistic simulation of cyber incidents that enabled participants to comprehend the impact of a cyberattack on a conference and determine the appropriate course of action in order to maintain business continuity. For the purpose, a specialised platform was built, hosted, and operated, with the cooperation of Saudi Information Technology Company (SITE), that helped develop scenarios to simulate the latest methods used in cyber-attacks. Alongside, it also provided strategies to combat cyber threats. The event was attended by the ITU secretary-general, senior directors, and staff of the ITU.

References

- **The Cybersecurity and Infrastructure Security Agency (CISA) (2023):** Improving Security of Open Source Software in Operational Technology and Industrial Control Systems. CISA, accessed 11 October 2023.
- **European Parliament (EP) (2023):** EU AI Act: first regulation on artificial intelligence. European parliament, accessed 13 October 2023.
- **European Parliament (EP) (2023):** Shaping the digital transformation: EU strategy explained. European parliament, accessed 13 October 2023.
- **Reserve Bank of Australia (RBA) (2023):** Payments System Board Annual Report – 2023, At a Glance. RBA, accessed 23 October 2023.
- **Reserve Bank of Australia (RBA) (2023):** Payments System Board Annual Report – 2023. RBA, accessed 24 October 2023.
- **Saudi Press Agency (SPA) (2023):** NCA carries out a cybersecurity drill at International Telecommunication Union headquarters in Switzerland. SPA, accessed 12 October 2023.
- **Symantec (2023):** Grayling: Previously Unseen Threat Actor Targets Multiple Organizations in Taiwan. Symantec Enterprise Blogs/ Threat Intelligence, accessed 12 October 2023.

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.

ISECOM
Board member of the Institute for Security and Open Methodologies.

W3C
Member of the World Wide Web Consortium for security standards.

EUROPEAN UNION
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