September 2024

DREAMLAB TECHNOLOGIES

CYBER INSIGHTS

Research updates and insights from Dreamlab Technologies

In this issue:

UK aims to build a nationwide evidence base for cyber deception technologies

UK’s leading cyber security authority, the National Cyber Security Centre (NCSC) on 12 August 2024, called on organisations in the country to explore the role of cyber ‘deception’ technologies in creating cyber defense (NCSC, 2024). In a first of its kind conference held in London, the cyber security authority decided to establish a national evidence base on the effectiveness of ‘deception’ technologies, as a part of the ‘Active Cyber Defence 2.0’ initiative which is a comprehensive range of services provided by the NCSC directly, or in partnership with industry and academia to help organisations defend against cyber threats (NCSC, 2024a).

‘Deception’ technologies in the context of cyber security refer to mechanisms or strategies to divert cyber criminals away from an organisation’s true assets through a decoy or trap, alerting organisations of potential attacks and unauthorised activities.

For the policy, legal and executive partners, the NCSC has defined specific deception technologies such as ‘tripwires’ (systems designed to detect unauthorised presence of adversaries), ‘honeypots’ (systems designed to allow adversary interaction to gain intelligence on attack techniques), and ‘breadcrumbs’ (digital artifacts designed to lure attackers). The endeavour involves two primary use cases: firstly, deploying ‘low-interaction’ solutions like digital tripwires and honeytokens (fake IT assets to attract cyber attackers) for all organisations to detect unauthorised access, and secondly, both ‘low-interaction’ and ‘high-interaction’ honeypots to gather threat intelligence, particularly for organisations with mature cyber security capabilities. The goal of creating the evidence base is to collect data on the effectiveness of cyber deception techniques to aid long-term research objectives and enhance cyber security defense mechanisms across the country.

UN finalise draft convention on cybercrime

The UN General Assembly committee established to negotiate a new convention on cybercrime, after three years of negotiations, on 9 August 2024 finalised a draft convention on cybercrime to strengthen international cooperation for combating cybercrimes and to facilitate the exchange of electronic evidence related to serious crimes (UNDOC, 2024). The earlier negotiations could not conclude a draft acceptable by all parties due to disagreements over its scope, and human rights implications. The now finalised draft convention is expected to be adopted later this year and will be the first global legally binding framework on cybercrime, marking a significant milestone in the domain. The United Nations Office on Drugs and Crime (UNODC) will further assist in the implementation and ratification of the convention, once adopted.

The convention aims to promote and strengthen measures to prevent and combat cybercrime through international cooperation, technical assistance and capacity building, particularly for the benefit of developing countries (UNGA, 2024). It seeks to prioritise global criminal justice policies against cybercrime by defining crimes, prosecuting cybercriminals universally, addressing the needs of cybercrime victims, international cooperation in recovering assets from cybercrime. It underscores the importance of all member states to collaborate with NGOs, international organisations, and other stakeholders. The convention highlights the need to uphold human rights, including privacy and data protection as strong safeguards while combating cybercrimes.

US accuses Iran of influencing elections through cyber operations

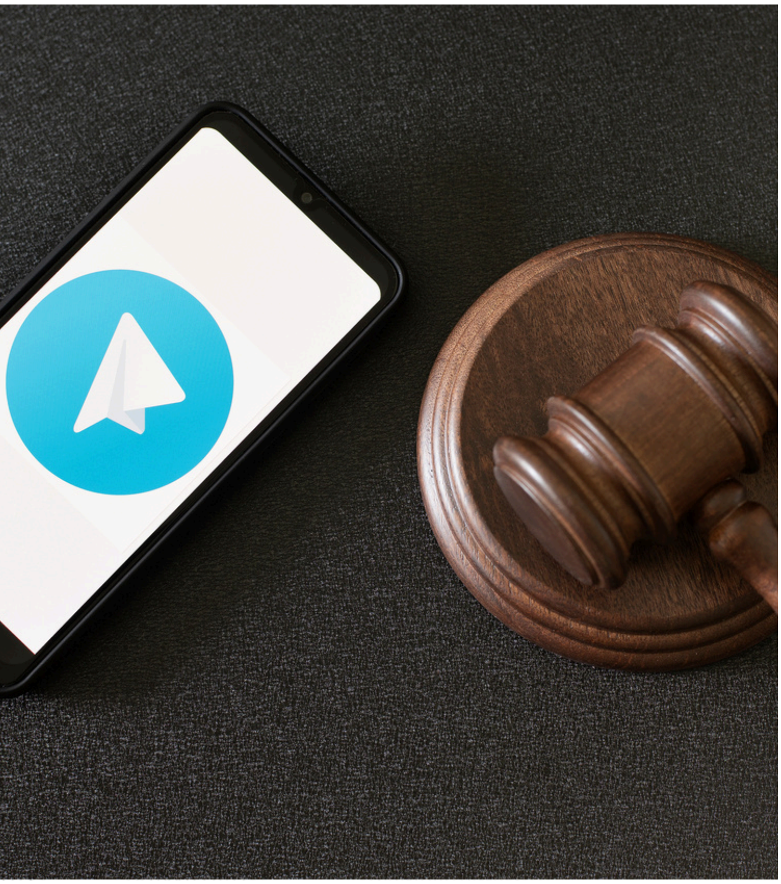
The Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA) in a joint statement on 19 August 2024, revealed efforts by Iran to disrupt U.S. elections through cyber operations, and influence presidential campaigns, including that of former President Trump (ODNI, 2024). Iran, however, has denied the claims; but the US emphasised that the tactics used like social engineering, thefts and disclosures, align with known Iranian methods.

Google’s Threat Analysis Group (TAG) confirmed the hacking attempts, sharing insights on APT42, an Iranian government-backed threat actor associated with the Islamic Revolutionary Guard Corps (IRGC) that has been targeting high-profile individuals and organisational accounts related to the U.S. presidential elections (Google, 2024). APT42 employs tactics using services like Google, Dropbox, and OneDrive to host malware, and sophisticated and tailored phishing techniques to obtain credentials from email services, security settings of targets and their geographic locations. The FBI has been working actively to track and counteract these foreign interference attempts with public and private sector partners, to enhance security and preserve the integrity of elections.

Australia develops new ‘world leading’ digital infrastructure

Australia is developing a new digital infrastructure called 'Trust Exchange' (TEx) that will allow Australians to verify their identity and credentials with businesses securely without revealing unnecessary personal information or no information at all (MDSS, 2024). The announcement was made on 13 August 2024; TEx is expected to roll out early next year, enabling individuals to use a digital ID wallet system such as ‘myGov’ to provide businesses with ‘confirmation tokens’ instead of documents directly, to verify age, address, etc.

TEx aims to streamline processes from opening bank accounts to renting properties, or even proving age at a pub, simply by using a QR code or a ‘digital handshake’ with the myGov wallet. The technology has garnered support from major companies like Telstra and Google and promises robust privacy and security standards. ‘Confirmation tokens’ received by businesses are based on official information already held by the government, and hence lack any actual data, which in turn can minimise the risk of data breaches. Moreover, TEx offers benefits of ‘consent', ‘choice’, and ‘trust’ to users by ensuring they control the extent of the exposure of personal information to respective third parties. This system is being developed as a distinct project alongside the Australia’s broader Digital ID legislation (Australian Government, 2024) for adoption and expansion of the Australian Government Digital Identity System (AGDIS), also known as myGovID.



Telegram founder faces legal charges; concerns about ‘encryption’ heightened

Pavel Durov, CEO of Telegram, is facing serious legal charges in France, for allegedly providing encrypted messaging services to criminals, suspected complicity in allowing illicit transactions, child abuse material, drug trafficking, fraud, and money laundering (Reuters, 2024). The Russian-born Durov was arrested on 24 August 2024 in France, which sparked tensions between France and Russia, with some in Moscow speculating it to be politically motivated.

Durov has been granted bail under strict conditions, while his lawyer argued that Telegram complies with European laws, and it was ‘absurd’ to hold the CEO responsible for misuse of the platform. Telegram’s encryption process differs from those of other messaging apps like WhatsApp, or Signal, as the one-to-one chats are not encrypted by default except the ‘secret chats’ that need to be manually activated by users. ‘Encryption’ has long remained a controversial topic among governments and tech companies worldwide due to the need for balancing digital privacy with concerns on misuse of the technology. According to a report by Guardian, detailed manuals and video guides on sextortion have been found to be readily accessible on online platforms; a specific 80-page guide was discovered on Telegram that has been linked to over 250 financial transactions (the Guardian, 2024). Telegram however has emphasised its commitment to banning sextortion and monitoring its platform for policy violations.

September 2024

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): Australia’s Digital ID System, Digital ID Act 2024. Australian Government accessed 28th August 2024, https://www.digitalidsystem.gov.au/what-is-digital-id/digital-id-act-2024

Google (2024): Iranian backed group steps up phishing campaigns against Israel, U.S. Google Threat Analysis Group, accessed 30th August 2024, https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/

Ministers for the Department of Social Services (MDSS) (2024): The Hon Bill Shorten MP Media Releases Trust exchange drives secure digital services. Ministers for the Department of Social Services, accessed 29th August 2024, https://ministers.dss.gov.au/media-releases/15621

The National Cyber Security Centre (NCSC) (2024): Building a nation-scale evidence base for cyber deception. The National Cyber Security Centre, accessed 28th August 2024, https://www.ncsc.gov.uk/blog-post/building-a-nation-scale-evidence-base-for-cyber-deception?ref=news.risky.biz

The National Cyber Security Centre (NCSC) (2024a): Introducing Active Cyber Defence 2.0. The National Cyber Security Centre, accessed 28th August 2024, https://www.ncsc.gov.uk/blog-post/introducing-active-cyber-defence-2

Office of the Director of National Intelligence (ODNI) (2024): Joint ODNI, FBI, and CISA Statement on Iranian Election Influence Efforts. Office of the Director of National Intelligence, accessed 30th August 2024, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3981-joint-odni-fbi-and-cisa-statement-on-iranian-election-influence-efforts?utm_source=substack&utm_medium=email

Reuters (2024): Pavel Durov's lawyer says the case against Telegram boss is 'absurd'. Reuters, accessed 29th August 2024, https://www.reuters.com/world/europe/lawyer-telegram-boss-durov-dismisses-allegations-absurd-french-media-reports-2024-08-29/?utm_source=substack&utm_medium=email

The Guardian (2024): Sextortion guides and manuals found on Telegram and YouTube. The Guardian, accessed 30th August 2024, https://www.theguardian.com/uk-news/article/2024/aug/22/video-sextortion-guides-and-manuals-found-on-tiktok-and-youtube?utm_source=substack&utm_medium=email

United Nations Office on Drugs and Crime (UNODC) (2024): United Nations: Member States finalize a new cybercrime convention. United Nations Office on Drugs and Crime, accessed 29th August 2024,
https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html

United Nations General Assembly (UNGA) (2024): Draft United Nations convention against cybercrime. United Nations General Assembly, accessed 29th August 2024, https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/AC.291/L.15&Lang=E

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/

Monbijoustrasse 36
CH-3011 Bern
Tel: +41 31 398 6666
Fax: +41 31 398 6669
contact@dreamlab.net