DREAMLAB TECHNOLOGIES

CYBER INSIGHTS

Research updates and insights from Dreamlab Technologies

In this issue:

Major tech companies to combat AI-generated election misinformation

In a welcome move to tackle the rising impact of artificial intelligence (AI)-generated misinformation in elections, major tech firms signed an accord to jointly combat its menace in the 2024 elections worldwide (AI Elections accord, 2024). An estimated 40 countries and more than 4 billion people will soon be involved in the voting process this year, to choose their respective leaders and representatives. Leading companies including Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI, TikTok and X have pledged to work together towards the purpose of the accord.

The accord signed on February 16, 2024, at the Munich Security Conference aims to adopt a voluntary framework involving seven principal goals to prevent, detect, evaluate, identify the origin and create resilience against 'deceptive AI election content' (created through 'publicly accessible, large-scale platforms or open foundational models, or distributed on large-scale social or publishing platforms' of signatories) and thereby respond to and create awareness regarding the same to protect the integrity of elections and public trust in the process. The Cybersecurity and Infrastructure Security Agency (CISA) also in a recent report (CISA, 2024) warned against disinformation using 'generative AI capabilities' in 2024 elections that 'may amplify existing risks to election infrastructure' including cybersecurity threats.

UK, US and EU disrupt the world's most harmful ransomware network

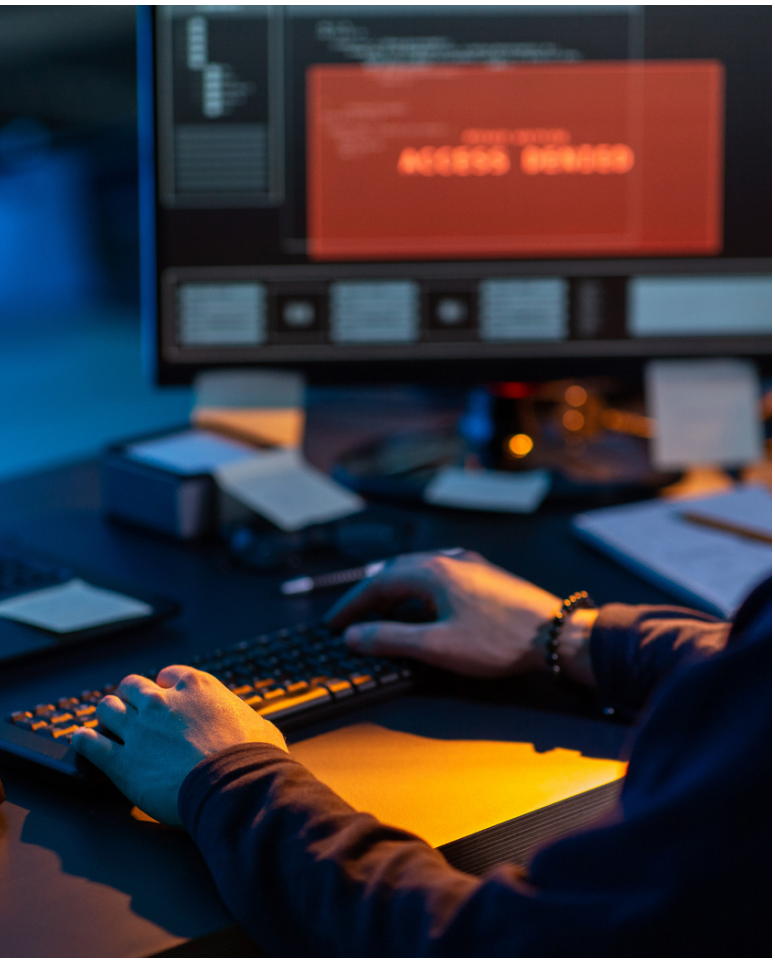
In a coordinated takedown, law enforcement agencies from around 10 countries disrupted the world's most deployed ransomware variant, LockBit, revealing details of the operation on February 20, 2024. The operation led by UK's National Crime Agency (NCA), codenamed 'Operation Cronos' led to disruption of the LockBit ransomware network by infiltrating its servers, obtaining decryption tools, freezing cryptocurrency wallets, arresting members, and imposing sanctions (NCA, 2024).The US has charged a total of five members for the crime so far, including two Russian nationals for their participation in the LockBit conspiracy (US DOJ, 2024).

LockBit cybercriminal gang has been in operation for around 4 years; its ransomware attacks targeted thousands of victims across the world, infecting their systems with malicious software and encrypting them, followed by threats to publish data. The attacks so far have caused losses in billions of euros, dollars and pounds as ransom payments as well as costs of recovery. Lockbit associates used the 'ransomware-as-a-service' (Raas) model, providing other network of hackers with the tools and infrastructure to carry out attacks. Recent reports however show that LockBit ransomware hackers attempted comeback with the gang setting up new site on dark web and releasing a statement on its infiltration (the Guardian, 2024).

NIST releases version 2.0 of its leading Cybersecurity Framework

The US National Institute of Standards and Technology (NIST) on February 26, 2024, released the updated version of its landmark Cybersecurity Framework (CSF 2.0). The earlier versions of the CSF, 1.0 and 1.1 released in 2014 and 2018 respectively were developed as major sources of voluntary cybersecurity guidance for industries crucial to national and economic security. However, after multiyear discussions and public comments on the draft 2.0 version, CSF 2.0 was released, designed to assist a wider audience, from schools and small businesses to local and foreign governments regardless of their current cybersecurity architecture (NIST, 2024).

The updated version CSF 2.0 added the new 'govern' function to its earlier core guidance key functions- identify, protect, detect, respond and recover. Additionally, a new 'CSF 2.0 Reference Tool' (to browse and export details from CSF's core guidance), 'a searchable catalogue of informative references', the Cybersecurity and Privacy Reference Tool (CPRT) (containing a set of NIST guidance documents), 'implementation examples' and 'quick-start guides' have been designed for specific audiences seeking to secure their supply chains. The earlier versions of CSF have been translated to around 13 languages across the world and continue to be popular frameworks for cybersecurity best practices internationally. NIST plans to continue enhancing the CSF as a more resourceful document for a wider set of audience (NIST, 2024a).



North Korean hacker group exploits Windows zero-day vulnerability

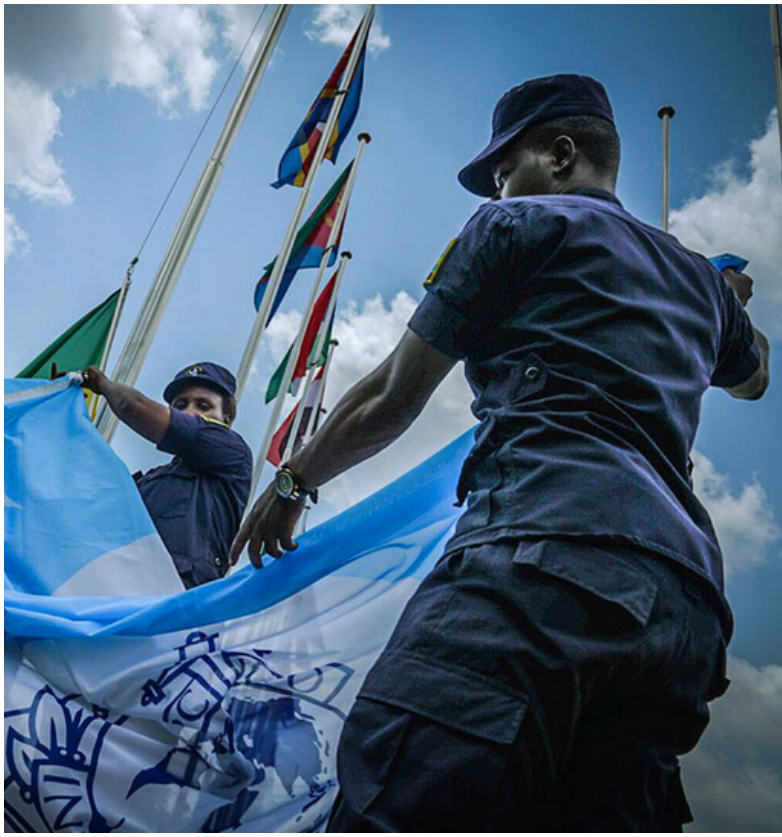
A previously unknown vulnerability in a Windows security feature, was exploited by hackers believed to be a part of the notorious Lazarus group, linked to North Korea, allowing them the highest level of access to specifically targeted systems. Avast, the cybersecurity firm in a report published on February 28, 2024 (Avast, 2024) mentioned that its researchers discovered a zero-day flaw in Microsoft's 'appid.sys' AppLocker driver, which allows users to control the applications allowed to run on a system.The vulnerability tracked as CVE-2024-21338 was later addressed and patched by Microsoft (Microsoft, 2024).

According to Avast, the vulnerability allowed hackers to gain kernel-level access, the highest level of access in the operating system which might turn off security tools (like Microsoft Defender), allowing them to exploit known vulnerable drivers, in a technique called BYOVD (Bring Your Own Vulnerable Driver). An updated version of Lazarus' FudModule rootkit, a malware, was used to carry out the attacks. The names of targeted organisations however were not mentioned in the report. The notorious Lazarus hacker group has also been mentioned as one of the threat actors in a February 19, 2024, joint advisory issued by Germany and South Korea's intelligence agencies that warned of ongoing North Korean cyber threat operations targeting the defense sector (BfV and NIS ROK, 2024).

AFRIPOL signs MoU with Group-IB to strengthen cybersecurity across Africa

A Memorandum of Understanding (MoU) to enhance cybersecurity and combat cybercrime was signed between AFRIPOL and Group-IB, a global cybersecurity company headquartered in Singapore on February 20, 2024. The MoU, which was signed at the headquarters of AFRIPOL in Algiers, is aimed at fostering collaboration between the two sides, Group-IB and AFRIPOL to jointly combat cybercrime across Africa (AFRIPOL, 2024).

The cooperation would involve threat intelligence sharing, exchanging insights on cybercrime and cybercriminals, joint investigations and operations against cybercrime in the African region. AFRIPOL, an agency of the African Union (AU) is aimed at enhancing collaboration among police forces of the AU member states to achieve shared objectives like fighting and preventing cross border organised crime, terrorism, as well as cybercrime. Under the partnership, Group-IB will be assisting AFRIPOL with its specialised technical knowledge in reverse engineering, incident management response, and investigations in cyber to combat cyber threats, prevent cyber scams like phishing, etc. and enhance cybersecurity awareness.



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

AFRIPOL (2024): Cooperation AFRIPOL-GROUP IB to enhance cybersecurity across Africa. AFRIPOL, accessed 1st March, 2024, https://afripol.africa-union.org/cooperation-afripol-group-ib-to-enhance-cybersecurity-across-africa/

AI Elections accord (2024): A Tech Accord to Combat Deceptive Use of AI in 2024 Elections. AI Elections accord, accessed 29th February 2024, https://www.aielectionsaccord.com/uploads/2024/02/A-Tech-Accord-to-Combat-Deceptive-Use-of-AI-in-2024-Elections.FINAL_.pdf

Decoded Avast.io (Avast) (2024): Lazarus and the FudModule Rootkit: Beyond BYOVD with an Admin-to-Kernel Zero-Day. Avast, accessed 4th March 2024, https://decoded.avast.io/janvojtesek/lazarus-and-the-fudmodule-rootkit-beyond-byovd-with-an-admin-to-kernel-zero-day/

The Bundesamt für Verfassungsschutz of the Federal Republic of Germany and the National Intelligence Service of the Republic of Korea (BfV and NIS ROK) (2024): Joint Cyber Security Advisory, Warning of North Korean cyber threats targeting the Defense Sector. The Bundesamt für Verfassungsschutz, accessed 5th March 2024,https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?__blob=publicationFile&v=2

The Cybersecurity and Infrastructure Security Agency (CISA) (2024): Risk in focus: Generative A.I. and the 2024 election cycle. The Cybersecurity and Infrastructure Security Agency, accessed 27th February 2024, https://www.cisa.gov/sites/default/files/2024-01/Consolidated_Risk_in_Focus_Gen_AI_ElectionsV2_508c.pdf

Microsoft (2024): Windows Kernel Elevation of Privilege Vulnerability. Microsoft, accessed 5th March 2024, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21338

National crime Agency (NCA) (2024): International investigation disrupts the world's most harmful cyber crime group. National crime Agency, accessed 29th February 2024, https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group?ref=news.risky.biz

The National Institute of Standards and Technology (NIST) (2024): The NIST Cybersecurity Framework (CSF) 2.0. The National Institute of Standards and Technology, accessed 1st March 2024, https://doi.org/10.6028/NIST.CSWP.29

The National Institute of Standards and Technology (NIST) (2024a): NIST Releases Version 2.0 of Landmark Cybersecurity Framework. The National Institute of Standards and Technology, accessed 1st March 2024, https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

The Guardian (2024): Russia-based LockBit ransomware hackers attempt comeback. The Guardian, accessed 29th February 2024, https://www.theguardian.com/technology/2024/feb/26/russian-based-lockbit-ransomware-hackers-attempt-comeback?utm_source=substack&utm_medium=email

US Department of Justice (US DOJ) (2024): U.S. and U.K. Disrupt LockBit Ransomware Variant. US Department of Justice, accessed 29th February 2024, https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant?ref=news.risky.biz

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