DREAMLAB TECHNOLOGIES

Cyber Insights

Research updates and insights from Dreamlab Technologies

In this issue:

Florida and other water utilities in the US hit by cyberattack

A regulatory agency in Florida that works closely with utilities on water supply issues, confirmed that it responded to a cyberattack in the first week of December 2023 after identifying 'suspicious activity' in its digital environment and that specific measures were implemented. A ransomware gang on 1 December 2023 claimed the attack, providing samples of what it had stolen without mentioning the total amount of data stolen (Greig J., 2023). The attack happened after an alert notice from the Cybersecurity and Infrastructure Security Agency (CISA) on 28 November 2023 regarding its response to the exploitation of Unitronics programmable logic controllers (PLCs), a specific tool used by various organisations in the water sector for the treatment and distribution of water (CISA, 2023).

Another attack on a water utility in Pennsylvania reported on 26 November 2023, was also linked to Unitronics PLCs (WaterISAC, 2023). A water utility in North Texas reported a similar cybersecurity incident just a day after, but there is no mention of its linkage with Unitronics PLCs by officials (Greig J., 2023). The authorities however clarified that there was no known risk to the drinking water or water supply. According to a CISA advisory, a hacker group by the name 'CyberAv3ngers' allegedly connected to Iran, is behind the attacks (CISA, 2023). The kind of devices that were attacked was mostly due to their public exposure to the internet because of the remote nature of their control and monitoring operations.

Japan and ASEAN collaborate on cybersecurity and AI

Japan and the Association of Southeast Asian Nations (ASEAN) in a collaborative initiative to deepen their relationship, have strengthened their commitment towards digital cooperation, by enhancing cybersecurity and Artificial Intelligence (AI) initiatives based on draft plans. The two sides adopted a joint vision statement in Tokyo, during the commemorative summit for the 50th year of ASEAN-Japan friendship and cooperation, on 17 December 2023. The statement focuses on three broad objectives- partnership across generations, co-creation of the economy and society of the future, and peace and stability, supported by an implementation plan (ASEAN, 2023).

The plan proposes to support ASEAN's efforts on AI governance and ethics for responsible use of innovative AI technologies. It aims to promote membership of ASEAN member states in the Global Partnership on Artificial Intelligence (GPAI) to further inclusivity. A special focus has been given on ASEAN MSMEs to enable their participation in the digital economy. Support to digital startups especially in the fields of AI and Robotics among others, and to promote Japanese investment and business matching for digital startups, are among other goals to enhance digital transformation in the region (ASEAN, 2023).

Trafficking fuelled cyber fraud, a globalised crime: Interpol

Interpol in its first operation specifically targeting the 'human-trafficking fuelled cyber fraud' phenomenon, revealed further insights on 8 December 2023 on the crime trend, which has increasingly become globalised, expanding beyond its origins in Southeast Asia to as far as Latin America. The operation called 'Operation Storm Makers II' (Interpol, 2023) with a participation of law enforcement from around 27 countries, carried out inspections at hundreds of trafficking and smuggling hotspots across Asia and other regions that led to arrests of criminals responsible for human trafficking, passport forgery, telecommunications fraud, torture and sexual exploitation among other crimes.

These hotspots were regularly used to traffic victims, who were often lured through fake job offers, to cyber scam centres. They are often forced to commit online fraud on an 'industrial scale', while enduring severe physical abuse. Some of the fraud schemes include fake cryptocurrency investments, work-from-home job offers, lottery and online gambling scams. Several human trafficking victims were rescued in the operation, leading to opening of more investigations, many of which are ongoing.

Source: growthbusiness.co.uk

UK and allies call out Russia for attempted cyber interference in politics

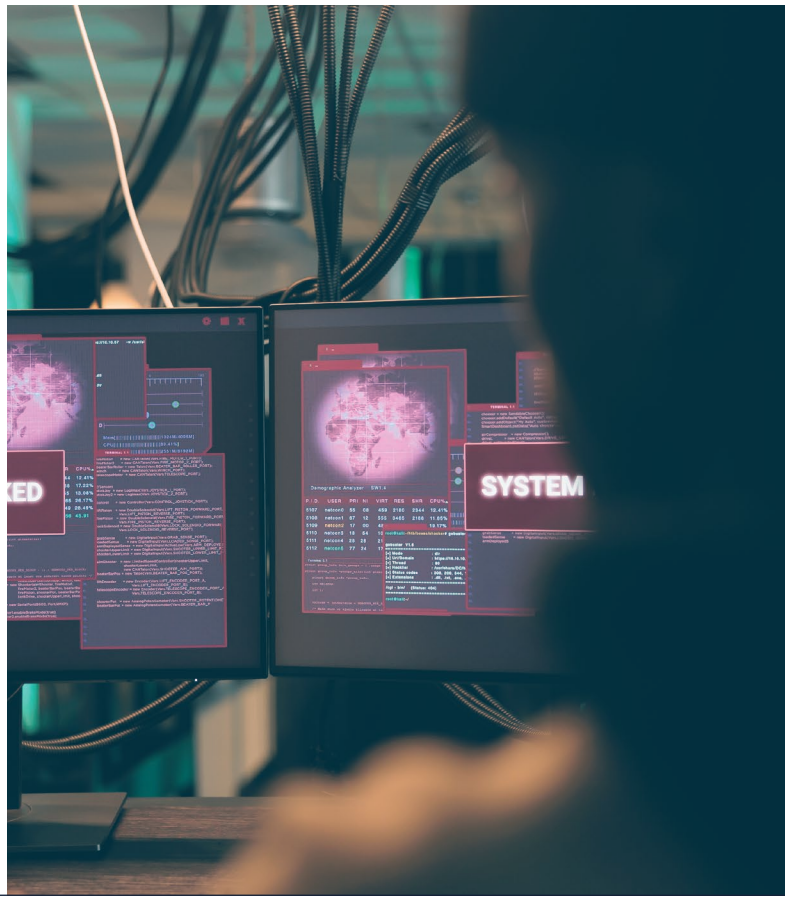
The UK government on 7 December 2023 exposed a series of cyber espionage operations believed to have been linked with Russia's Intelligence Services, targeting the UK (Gov.UK, 2023). 'Star Blizzard', a hacker group also known as 'Callisto Group', most likely subordinate to a unit within the Russian Federal Security Service (FSB) as per UK's National Cyber Security Centre (NCSC) (Gov.UK, 2023), has been using malicious cyber operations targeting parliamentarians, universities, journalists, public sector as well as non-government organisations, the key participants in the UK democracy.

The possible intent behind using the information obtained was to interfere in UK politics and democratic processes, stated the government. Although some of the attacks led to leaking stolen data but attempts to interfere with UK politics and democracy remained unsuccessful. Russia has repeatedly denied claims of its involvement in such activities (Corera G., 2023). 'Spear-phishing 'particularly was used to launch the cyber-attacks. The UK along with the US have sanctioned two members of Star Blizzard for their involvement in the spear-phishing campaigns. The UK NCSC and allies from the US, Canada, Australia, and New Zealand, have issued a cyber security advisory (NCSC, 2023), sharing technical details about the attack tactics and its prevention.

AFP urges Australians to report ransomware attacks to law enforcement

The Australian Federal Police (AFP) has urged Australian victims of ransomware attacks to report ransomware incidents at the earliest, and to seek assistance of law enforcement during the process in an advisory published on 7 December 2023 (AFP, 2023). The advisory followed a recent report published by IBM called 'IBM Security's Cost of a Data Breach Report 2023' which confirmed that victims who reported such incidents to concerned authorities benefitted significant time and saved costs as a result (IBM, 2023).

The report showed that 37% of ransomware victims opted 'not to involve' law enforcement in case of a ransomware breach. As a result, they experienced higher costs (an estimated average cost of about USD 5.11 million) of ransomware breach. However, those who involved law enforcement by reporting the incident experienced much lesser costs of ransomware breach (an estimated USD 4.64 million), a difference of 9.6%. Additionally, those who worked with law enforcement had their attack incident resolved faster in comparison to those who chose not to report the incidents.



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

Corera G. (2023): Russia hacking: 'FSB in years-long cyber attacks on UK', says government. BBC, accessed 5 January 2024, https://www.bbc.com/news/uk-politics-67647548?utm_source=substack&utm_medium=email

Cybersecurity and Infrastructure Security Agency (CISA) (2023): Exploitation of Unitronics PLCs used in Water and Wastewater Systems. CISA, accessed 30 December 2023, https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and- wastewater-systems

Cybersecurity and Infrastructure Security Agency (CISA) (2023): IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities. CISA, accessed 31 December 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

Gov.UK (2023): UK exposes attempted Russian cyber interference in politics and democratic processes. Gov.UK, accessed 5 January 2024, https://www.gov.uk/government/news/uk-exposes-attempted-russian-cyber-interference-in-politics-and-democratic-processes?utm_source=substack&utm_medium=email

Greig J. (2023): Florida water agency latest to confirm cyber incident as feds warn of nation-state attacks. The Record, accessed 30 December 2023, https://therecord.media/florida-water-agency-ransomware-cisa-warning-utilities?&web_view=true

Greig J. (2023): North Texas water utility serving 2 million hit with cyberattack. The Record, accessed 31 December 2023, https://therecord.media/north-texas-water-utility-cyberattack

IBM (2023): IBM Security Cost of a Data Breach Report 2023. IBM, accessed 5 January 2024, https://blogs.microsoft.com/on-the-issues/2023/12/13/cybercrime-cybersecurity-storm-1152-fraudulent-accounts/

Interpol (2023): Interpol operation reveals further insights into ‘globalisation’ of cyber scam centresInterpol, accessed 30 December 2023, https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-operation-reveals-further- insights-into-globalization-of-cyber-scam-centres

National Cyber Security Centre (NCSC) (2023): Russian FSB cyber actor Star Blizzard continues worldwide spear-phishing campaigns. NCSC, accessed 5 January 2023, https://www.ncsc.gov.uk/news/star-blizzard-continues-spear-phishing-campaigns

The Association of Southeast Asian Nations (ASEAN) (2023): Joint Vision Statement On ASEAN-JAPAN Friendship and Cooperation. ASEAN, accessed 29 December 2023, https://asean.org/wp-content/uploads/2023/12/Final-Implementation-Plan-of-the-ASEAN-Japan-Joint-Vision-Statement.pdf

The Association of Southeast Asian Nations (ASEAN) (2023): Implementation Plan of the Joint Vision Statement on ASEAN-Japan Friendship and Cooperation. ASEAN, accessed 29 December 2023, https://asean.org/wp-content/uploads/2023/12/Final-ASEAN-Japan-Joint-Vision-Statement.pdf

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