Cyber Security Brief (December 2023)

January 4, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 227 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, the EU adopted a Regulation to enhance cybersecurity across its institutions, while the Cyber Resilience Act sets EU-wide cybersecurity standards, and the European Commission initiated formal proceedings against company X under the Digital Services Act. Globally, Star Blizzard cyberattacks were linked to Russia's FSB and there were law enforcement and judicial actions against cybercriminals.
- On the **cyberespionage** front, at least two Russia-linked threat actors and one North Korean threat actors have been active in Europe. In other regions there was reporting of activity by three Iran linked threat actors.
- Relating to **cybercrime**, a ransomware attack on December 24 disrupted emergency services at three German hospitals. In Europe, for December, the top most active ransomware operations have been Lockbit, 8Base, Cactus, Play, BlackBasta, and Akira; the most targeted sectors have been manufacturing, construction and engineering, legal and professional services, retail, technology, and energy and utilities.
- There were **disruptive** attacks in the telecommunications, healthcare, water supply, energy, and legislative sectors.
- As regards **data exposure and leaks** two genetic testing companies and a parking operator suffered significant breaches.
- On the **hacktivism** front, significant attacks were noticed in Israel and Russia.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in December 2023.

Europe

Cyber policy and law enforcement

Cybersecurity at the EU institutions, bodies, offices and agencies *Legislation*
On December 18, the EU officially adopted Regulation (EU, Euratom) 2023/2841, which lays down measures for a high common level of cybersecurity at the institutions, bodies, offices, and agencies of the Union. This regulation aims to enhance the overall cybersecurity framework across EU entities.

Cyber Resilience Act coming closer *Legislation*
On November 30, the European Council and European Parliament negotiators agreed on the Cyber Resilience Act, which sets EU-wide cybersecurity standards for digital products, covers all connected devices, and increases transparency for consumers while holding manufacturers accountable for compliance.

Commission opens formal proceedings against X under the Digital Services Act *Regulation*
On December 19, the European Commission launched formal proceedings to investigate whether the company X (formerly Twitter) breached the Digital Services Act (DSA) in areas linked to risk management, content moderation, advertising transparency, and data access for researchers. The proceedings will focus on several areas including effectiveness in combating information manipulation.

US, UK attribute Star Blizzard to FSB Center 18 *Attribution, Sanctions*
On December 7, the governments of the US, the UK, Canada, Australia, and New Zealand identified Star Blizzard (a.k.a. Callisto) as the work of Center 18 within the Russian Federal Security Service (FSB). The UK government concluded that this threat actor aimed to interfere in UK politics and democracy by using stolen materials for information operations. The UK and US also imposed sanctions on two Russian nationals for their involvement in Star Blizzard's intrusions from 2015 to 2022.

Kelvin cybercrime group arrest *Arrests*
On December 10, The Spanish police reported that they arrested one of the alleged leaders of the Kelvin Security hacking group, which is reportedly responsible for 300 cyberattacks against organisations in 90 countries since 2020.

French police arrest suspected Hive ransomware accomplice *Arrests*
On December 13, the French national police issued a statement that they had arrested an individual for being associated to the Hive ransomware cybercrime activities.

Albanian authorities dismantled a cybercrime gang *Arrests*
Law enforcement in Albania has dismantled a major criminal gang in Kortsa, known for perpetrating an extensive online fraud operation targeting about 5.000 Greek citizens. The gang, led by individuals from Tirana and Kortsa, employed malware to gain access to victims' bank accounts, illegally transferring 3.000 to 5.000 euros per account.

Lapsus$: GTA 6 hacker handed indefinite hospital order *Sentence*
An 18-year-old hacker, Arion Kurtaj, who was part of the international hacking group Lapsus$, has been sentenced to an indefinite hospital order due to his involvement in cyberattacks on tech giants, including Uber, Nvidia, and Rockstar Games, costing nearly 10 million euros. Doctors deemed Kurtaj unfit to stand trial due to his severe autism, and he will remain in a secure hospital for life unless doctors determine he is no longer a threat to the public.

Cyberespionage

Sellafield nuclear site hacked by groups linked to Russia and China *Chinese threat actor*, *Russian threat actor*
The Guardian reported on December 4 that Russian and Chinese hackers had breached the UK's Sellafield nuclear site in 2015. The malware may not have been fully removed, and authorities are criticised for not disclosing the breaches and other cybersecurity issues. The UK government disputed the claims of a successful cyberattack by state actors, citing lack of evidence.

APT28 targets European NATO member nations *Russian threat actor*
According to PaltoAltoNetworks, the Russian APT28 group used zero-day exploits in Microsoft Outlook to target European NATO member countries, including a NATO Rapid Deployable Corps. They were exploiting the CVE-2023-23397 vulnerability for about 20 months in three different campaigns, targeting 30 organisations in 14 nations that had strategic significance for Russia.

APT28 targets Ukraine *Russian threat actor*
Ukraine's CERT issued a warning about a new phishing campaign by the Russia-linked APT28 group. In this campaign, the threat actor deployed previously unseen malware on a network within an hour. The attack occurred from December 15 to 25 and involved phishing e-mails that urged recipients to click on a link, claiming to be for an important document.

APT29 exploiting JetBrains TeamCity at large scale *Russian threat actor*
On December 13, Poland, the UK, and the US reported that APT29 was exploiting the vulnerability CVE-2023-42793 since September 2023. They targeted servers hosting JetBrains TeamCity software in a large-scale campaign, affecting organisations in Europe, the US, Asia, and Australia across multiple sectors including energy, medical, finance, and technology.

Lazarus' Blacksmith campaign *North Korean threat actor*
On December 11, Cisco researchers revealed information about the campaign, Operation Blacksmith, by the North Korea-linked Lazarus group. The activity used the Log4Shell vulnerability and the NineRAT malware. It targeted a South American agricultural organisation in March and a European manufacturing entity in September.

Cybercrime

Lockbit ransomware disrupts emergency care at some German hospitals *Healthcare*
A Lockbit ransomware attack on December 24 disrupted emergency services at three German hospitals. While patient treatment continued with some restrictions, emergency care became unavailable, and patients were redirected to other hospitals. Investigations are ongoing to determine the extent of the damage and potential data theft.

Disruption

Disruptive attack on Ukrainian telecommunication company *Telecommunications*
On December 12, Kyivstar, Ukraine's largest telecom provider, suffered a powerful cyberattack, disrupting services for millions of subscribers and affecting air raid alerts in Kyiv. Major Ukrainian banks also reported issues with ATMs and card terminals. Multiple pro-Russian hacktivist groups claimed responsibility for the attack.

Cyberattack disrupts water supply in North Mayo's Drum/Binghamstown area *Water*
In Ireland, a cyberattack disrupted the Industrial Control System at the Group Water Scheme in the Drum/Binghamstown area of Erris. The result was a water outage affecting residents in the area.

Serbian state-run energy company suffered ransomware attack *Energy*
Serbia's government-controlled power utility, Elektroprivreda Srbije, experienced a ransomware attack on December 19. The company requested patience from users of its bill payment portal, as the website's operation was affected by the protective measures.

Cyberattack against the Albanian Parliament *Parliament*
Albania's Parliament experienced a cyberattack on December 25, causing temporary disruptions. The data system remained uncompromised. The attack also targeted a cellphone provider and an air flight company. A group called Homeland Justice is suspected, but their involvement lacks independent confirmation.

Information operations

Russia's AI-Powered Doppelganger influence campaign spreading deceptive news *Russian threat actor*
Russia's Doppelganger influence operation employs AI to create deceptive news articles targeting Ukrainian, American, and German audiences. It aims to spread false information, undermine Ukraine, promote anti-LGBTQ views, and negatively influence perceptions of the US military and Germany. However, according to Recorded Future, it has struggled to gain significant engagement from authentic social media users.

Data exposure and leaks

23andMe faces lawsuits and toughens legal defence amid massive data breach *Genetics*
Genetic testing provider 23andMe faces lawsuits after a data breach in October, making it harder for customers to sue due to changes in its Terms of Use. The breach affected 1 million Ashkenazi Jews and 4,1 million UK individuals.

Data 10.000 individuals stolen in Estonia *Genetics*
Estonian genetic testing company Asper Biogene suffered an illegal data download on December 14. An unknown actor copied genetic test results from 10.000 individuals and 40 healthcare companies, demanding a ransom.

EasyPark Group was hacked, affecting customers in the EU and UK *Parking*
On December 26, EasyPark Group, Europe's largest parking services operator, disclosed a data breach to EU and UK regulators. Hackers stole customer personal data as well as partial credit card numbers.

World

Cyber policy and law enforcement

US imposes sanctions over North Korean spy satellite *Sanctions*
The US, along with South Korea, Japan, and Australia, has sanctioned the North Korean cyberespionage group Kimsuky and eight individuals for aiding sanction evasion. This is in response to North Korea's November spy satellite launch and aims to disrupt financial and weapons-related activities.

TrickBot malware developer pleads guilty, faces 35 years in prison *Charge*
A Russian national pleaded guilty to charges related to his involvement in developing and deploying the Trickbot malware, which was used in attacks against hospitals, enterprises, and individuals worldwide. He was arrested in South Korea and extradited to the US in 2021.

International operation against financial crime *Arrest*
A law enforcement operation dubbed HAECHI IV, led by INTERPOL, conducted from July to December 2023, resulted in nearly 3.500 arrests and the seizure of assets worth around 273 million euros across 34 countries. The operation targeted seven types of cyber scams and involved freezing criminal accounts using INTERPOL's Global Rapid Intervention of Payments (I-GRIP) mechanism.

Cyberespionage

Muddywater: Iranian hackers target telecoms in North and East Africa *Iranian threat actor*
Researchers at Symantec have disclosed on December 19 a campaign from November 2023 by Iranian cyberespionage group Muddywater. The group has been targeting organisations in Egypt, Sudan, and Tanzania from the telecommunications sector.

IRGC-affiliated cyber actors target US water systems *Iranian threat actor*
US agencies issued a cybersecurity advisory about Iranian Government-affiliated cyber actors known as CyberAv3ngers. These actors are targeting and compromising programmable logic controllers (PLCs) in sectors like water and wastewater systems by exploiting default credentials and leaving defacement messages.

Iranian national-state actor targets defence industry with FalseFont malware *Iranian threat actor*
On December 21, Microsoft reported that APT33, an Iranian nation-state actor, attempted to distribute a new backdoor named FalseFont to individuals in the defence sector. APT33 has been active since 2013, targeting various sectors in the US, Saudi Arabia, and South Korea. Microsoft has been tracking FalseFont since November 2023.

AeroBlade targeting the US aerospace industry *Unattributed threat actor*
According to Blackberry, AeroBlade, a previously unknown threat actor, has targeted an aerospace organisation in the US in July 2023. Research has found that the group became operational in September 2022, and their goal has been assessed, with medium to high confidence, as commercial cyber espionage.

New toolset used against organisations in the Middle East, Africa, and the US *Unattributed threat actor*
PaloAltoNetworks researchers reported on a series of cyberattacks on organisations in the Middle East, Africa, and the US. While they suspected nation-state involvement based on the nature of the targets and attack methods, they have not identified a specific group.

Cybercrime

North Korean state hackers gather 3 billion US dollars in cryptocurrency theft *North Korea*
According to RecordedFuture, North Korean state hackers, like Kimsuky and Lazarus, have stolen 3 billion US dollars in cryptocurrency since January 2017, accounting for 44% of cryptocurrency theft in this period. This income funds North Korea's military and weapon programs.

Microsoft gets court order to seize Vietnam-based cybercrime domains *Seizure*
On December 7, Microsoft's Digital Crimes Unit seized multiple domains used by a Vietnam-based cybercrime group (Storm-1152) that registered over 750 million fraudulent accounts and made millions of dollars reselling them.

Data exposure and leaks

Leaked API tokens creat significant cyber threat *Technology*
Over 1.500 exposed API tokens on Hugging Face, a data science platform, posed a risk to major organisations like Microsoft, Meta, Google, and VMware. This breach could allow access to accounts of 723 different organisations, potentially leading to manipulation of widely used scientific models, threatening users who rely on them.

Xfinity discloses data breach affecting over 35 million people *Telecommunications*
On December 18, Comcast's Xfinity revealed a data breach that occurred in October, affecting over 35 million individuals. Stolen information included usernames, hashed passwords, and potentially personal and economic data.

Information operations

Fake social media accounts target Taiwan's presidential election *Taiwan*
A report by the security company Graphika revealed an information operation on Facebook, TikTok, and YouTube aimed at influencing Taiwan's presidential election. It involved 800 fake accounts and 13 Facebook pages sharing Chinese-language videos related to Taiwanese politics. The operation supported the pro-China Kuomintang Party and criticised the pro-Taiwan Democratic Progressive Party.

Taiwan claims China fabricated domestic surveillance documents *Taiwan*
In December 2023, Taiwan's Supreme Prosecutor's Office refuted claims of domestic surveillance, asserting that Chinese actors had fabricated relevant documents on an anonymous Facebook account. This was seen as an attempt to sow distrust ahead of the January 2024 presidential election.

Disruption

Israeli group claims disruption of Iranian fuel stations *Energy*
In mid-December, the Israel-linked group Gonjeshk Darand claimed responsibility for a cyberattack on Iranian fuel stations. This group has a history of targeting smart-fuel systems in Iran, recently causing nationwide disruptions.

Fake F5 BIG-IP warning e-mails pushed data wipers *Israel*
In late December, the Israel National Cyber Directorate (INCD) warned of hackers using disguised security updates for F5 BIG-IP devices to deliver data-wiping malware to Israeli organisations. A hacktivist group called "Handala" has claimed responsibility.

Hacktivism

Hacker group claims theft of Israeli medical data *Israel*
The Malek Team hacker group reportedly stole 500 GB of medical data, including 100.000 Israel Defence Force-linked records, from Israel's Ziv Medical Center. The stolen data contains medical diagnoses and medications, raising concerns about security in Israel's healthcare sector.

Ukrainian hackers hit Russian utility company *Russia*
Just one week after the Russia-nexus cyberattack against Ukrainian phone operator Kyivstar, Blackjack, a Ukrainian hacker group, claimed responsibility for an attack against the Russian water utility Rosvodokanal. The activity was likely supported by the Security Service of Ukraine (SBU). Blackjack purportedly targeted more than 6.000 Rosvodokanal computers and deleted over 50 TB of data.

Significant vulnerabilities

Multiple Critical Vulnerabilities in Atlassian Products — *Atlassian*
On December 5, 2023, Atlassian released several security advisories regarding critical vulnerabilities affecting multiple Atlassian products. The exploitation of these vulnerabilities could lead to Remote Code Execution. It is recommended to upgrade to a fixed version as soon as possible. See CERT-EU's SA 2023-094.

Critical Vulnerability in Apache Struts — *Apache Struts*
On December 7, 2023, The Apache Struts group released an update addressing a critical security vulnerability in Apache Struts. This vulnerability could lead, under some circumstances, to remote code execution. It is recommended to upgrade to a not vulnerable version as soon as possible. See CERT-EU's SA 2023-095.

High Severity Vulnerability in WordPress — *WordPress*
On December 6, 2023, WordPress released a new version addressing a vulnerability that, if combined with another vulnerability, could result in remote code execution. While most sites should automatically update to WordPress 6.4.2, it is strongly recommended manually checking WordPress sites to ensure that it is updated. See CERT-EU's SA 2023-096.

Critical Vulnerabilities in Microsoft Products — *Microsoft*
On December 12, 2023, Microsoft released the December 2023 Patch Tuesday which includes security updates for a total of 35 flaws. Among the vulnerabilities, four were rated as critical. It is recommended updating affected products as soon as possible. See CERT-EU's SA 2023-097.

SMTP Smuggling Vulnerability in CISCO Secure Email Gateway — *Cisco Secure Email Gateway*
On December 18, 2023, researchers from SEC Consult released an article about an SMTP Smuggling vulnerability affecting products from several vendors such as Microsoft, GMX or Cisco [1]. While the vulnerability was fixed in GMX and Microsoft products, it is considered as a feature in Cisco Secure Email Gateway and Cisco Secure Email Cloud Gateway, and thus, it was not fixed. It is recommended to change the default configurations of the Cisco Secure Email Cloud Gateway and Cisco Secure Email Gateway. See CERT-EU's SA 2023-098.

Critical Vulnerabilities in Ivanti Avalanche — *Ivanti*
On December 20, 2023, Ivanti has released security updates to fix 13 critical security vulnerabilities in the company's Avalanche enterprise mobile device management (MDM) solution. These vulnerabilities, if exploited, could lead to Remote Code Execution or Denial of Service. The updates also cover 8 medium- and high-severity bugs that attackers could exploit in denial of service, remote code execution, and server-side request forgery (SSRF) attacks. It is strongly recommended updating as soon as possible. See CERT-EU's SA 2023-099.

High Severity Vulnerability in Google Chrome — *Chrome*
On December 20, 2023, Google released an advisory regarding a new high severity vulnerability in its web browser. Google is aware that an exploit for this vulnerability exists in the wild. It is recommended updating as soon as possible. See CERT-EU's SA 2023-100.

All CERT-EU's Security Advisories are available to the public on CERT-EU's website, `https://www.cert.europa.eu/publications/security-advisories#2023`

1.

Conclusions or attributions made in this document merely reflect what publicly available sources report. They do not reflect our stance.

TLP definition

TLP	Disclosure	Message
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER	Limited disclosure, restricted to participants' organisations and their clients.	Recipients may share TLP:AMBER information only with members of their own organisation and it's clients.
AMBER+STRICT	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER+STRICT information only with members of their own organisation.
GREEN	Limited disclosure, restricted to the community.	Subject to standard copyright rules, TLP:GREEN information may be distributed with peers and partner organisations within their sector or community, but not via publicly accessible channels.
CLEAR	Disclosure is not limited.	TLP:CLEAR information may be distributed freely.