Cyber Brief (April 2024)

May 2, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 263 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, in a recommendation the European Commission encourages Member States to adopt a unified approach to transition to quantum cryptography-safe digital infrastructure. Globally, the US and Japan announced partnerships in AI research. US authorities published an advisory on securing election infrastructure against foreign influence operations and charged four Iranian nationals for involvement in cyber intrusions.
- On the **cyberespionage** front, there was reporting of activity by allegedly Russian, Chinese and North Korean threat actors. Additionally, Apple alerted iPhone users across 92 countries about potential targeting of a spyware by private sector offensive actors.
- Relating to **cybercrime**, in Europe, the most active operators were Lockbit3, Blackbasta, Akira, Bianlian, and Hunters while the most targeted sectors were technology, healthcare, manufacturing, retail, and construction.
- Regarding **disruptive** activity, a hospital in France experienced a cyberattack, disrupting operations and leading to cancellations of non-urgent procedures. Additionally, reportedly Russia-linked Sandworm and Muddling Meerkat have targeted France's energy infrastructure and manipulated China's Great Firewall's DNS responses, respectively. Czechia accused Russia of attempting to sabotage European railways.
- About **information operations**, reportedly Russian and Chinese disinformation campaigns are heavily targeting European and US elections, with Russia spreading propaganda through social media and fake websites, while China attempts to influence US elections through covert accounts posing as Trump supporters. Additionally, AI chatbots have inadvertently contributed to misinformation about the EU elections.
- As regards **data exposure and leaks**, a series of significant breaches affected companies in the technology and telecommunication sectors revealing customer information and affecting service integrity.

Europe

Cyber policy and law enforcement

European Commission publishes Recommendation on Postquantum Cryptography
On April 11, the European Commission released a Recommendation on Postquantum Cryptography, encouraging Member States to adopt a unified approach during the EU's shift to postquantum cryptography. This aims to safeguard the security of the EU's digital systems. The Recommendation advocates for a coordinated transition to quantum-safe digital infrastructure across Europe, fostering consistency among Member States and promoting cross-border interoperability of systems and services. `policy` `technology`

UK bans weak default passwords in IoT
From April 29 onwards, a UK ban enters into effect which forbids manufacturers from using weak default passwords in internet and network-connected consumer devices sold in the UK. The law applies to smart consumer goods. `policy`

Belgium investigating EU legislators accused of receiving payments for spreading pro-Russia propaganda
On April 12, Belgian authorities announced that the country's federal prosecutor is investigating EU legislators accused of accepting payments to promote pro-Russia propaganda. Belgian Prime Minister De Croo emphasised Belgium's responsibility to protect the integrity of EU citizens' voting rights, as the seat of EU institutions. The number of legislators facing prosecution is unspecified, but reports from Czech media suggest involvement from Germany, France, Poland, Belgium, the Netherlands, and Hungary. `investigation`

International investigation disrupts phishing-as-a-service platform LabHost
Between April 14 and 17, law enforcement agencies from 19 countries including Europol, dismantled LabHost, a phishing platform. Seventy locations were raided, resulting in 37 arrests worldwide. LabHost, offering phishing tools and services for a fee, hosted over 40.000 domains and had 10.000 users. `take down`

Stop Akira ransomware advisory by CISA, EC3, NCSC-NL and the FBI
On April 18, the FBI, CISA, EC3, and NCSC-NL jointly released a report on Akira ransomware, detailing its tactics, techniques, and indicators of compromise based on investigations up to February 2024. Since March 2023, Akira has targeted businesses and critical infrastructure worldwide, evolving to attack Linux systems and using variants like Megazord. It has affected over 250 organisations, earning around 38 million euros worth of ransom in cryptocurrency. `advisory`

Cyberespionage

Russia-linked Sandworm targeted Eastern Europe with new backdoor since mid-2022
On April 17, WithSecure security researchers uncovered a backdoor named Kapeka, which has been deployed against targets in Eastern Europe since mid 2022, exhibiting features that allow both initial exploitation and persistent access. The overlaps in the technical footprints of Kapeka, GreyEnergy, and Prestige ransomware suggest its integration into the arsenal of the Russia-linked threat actor Sandworm. `russian threat actor`

Cybercrime

Cybercrime group CoralRaider continues to target entities globally

On April 23, Cisco Talos reported that the cybercrime group CoralRaider is using a content delivery network cache to distribute the malware LummaC2, Rhadamanthys, and Cryptbot to entities worldwide, including Germany and Poland. These info stealers, aimed at harvesting credentials, financial data, and social media accounts, are sourced from malware-as-a-service platforms on underground forums. `content delivery network`

The cybercrime group TA547 targeted German entities with updated tools and techniques

On April 10, Proofpoint reported on the cybercrime group TA547 launching a novel e-mail attack on German organisations, using Rhadamanthys malware. The campaign features e-mails mimicking the German retailer Metro concerning invoices and employs a PowerShell script likely generated by advanced AI tools such as ChatGPT or Gemini. `malware`

Disruption

Hospital Simone Veil in Cannes targeted by cyberattack

On April 16, the Hospital Simone Veil in Cannes, France suffered a cyberattack, disrupting its operations and forcing a return to manual record-keeping. Essential departments were still functioning, but non-urgent procedures were cancelled, and consultations rescheduled. `health`

Russia-linked threat actor Sandworm linked to claim of supposed hydroelectric dam hack in France

According to an article by Le Monde published on April 17, in March, the Russia-linked threat actor Sandworm targeted a hydroelectric dam in France. The telegram channel CyberArmyofRussia_Reborn posted a video showcasing that the attack targeted the hydroelectric dam in Courlon-sur-Yonne. However the video turned out to be fabricated and the target was a mill in Courlandon. `russian threat actor` `energy`

Czech Transport Minister accuses Russia of trying to sabotage European railways

On April 5, the Czech Transport Minister accused Russia of actively trying to sabotage European railways. He said that since the beginning of the war, threat actors had made “thousands of attempts to weaken our (railway) systems,” namely through breaching the signalling systems. `russian threat actor` `transport`

Information operations

Russian disinformation targets France and threatens EU elections

On April 22, the French Minister for Europe, Jean-Noël Barrot, warned that Russian propaganda disseminated via social media and fake websites heavily targeted France with the aim of distorting the outcomes of the upcoming EU parliamentary elections. He cited, for example, a fake French Ministry of Defence website claiming that 200.000 French people were being called up to fight in Ukraine. `russian threat actor` `election`

German Federal Ministry of Interior working against hybrid threats ahead of EU elections

On March 27, the German Federal Ministry of Interior published an article detailing how they’re tackling hybrid threats, disinformation campaigns, and their assessment of the situation in the run-up to the 2024 EU elections. They are namely increasing the resilience of the state and society through public awareness of the issue of disinformation. They are also focusing on cooperation between the federal, state and local levels, within the EU and with partner countries. `election`

Popular AI chatbots provide unintentional misinformation on EU elections
On April 11, a study from Democracy Reporting International showed that Europe's most popular AI chatbots, including Google's Gemini, OpenAI's ChatGPT 3.5 and 4.0, and Microsoft's Copilot, provided misinformation to users inquiring about the upcoming European elections. Examples of misinformation included incorrect election dates and voting rules or false claims regarding the movements and activities of the European Parliament election observation mission. `election` `artificial intelligence`

Unknown threat actor breached a Czech newspaper outlet and published fake articles
On April 23, the Czech News Agency disclosed that an unknown threat actor breached its newspaper outlet České Noviny and posted fake articles. The security breach affected the website's publishing system, but the main news service distributed by Czech News Agency to its clients remained unaffected. `news agency`

Hacktivism

Two hacktivist groups claim to have jointly hacked and leaked French Ministry data
On April 21, the hacktivist groups GroupLapsus and Gloriamists made unproven claims to have jointly breached a French ministry via a cross-site scripting attack. The day after, the hacktivist groups leaked five percent of the allegedly stolen data and advertised access to the entire database for sale. `public administration`

World

Cyber policy and law enforcement

AI research partnerships between the US and Japan
On April 10, the US announced two partnerships with Japan on AI research. These collaborations, backed by 110 million US dollars from companies like Nvidia and Amazon, aim to advance AI ethically and technologically. Each partnership, involving universities like University of Washington and Carnegie Mellon, focuses on different AI themes. `cooperation` `artificial intelligence`

Biden administration reportedly planning on banning Kaspersky in the US
On April 9, CNN reported that the Biden administration is planning to issue an order prohibiting US companies and citizens from using software developed by a major Russian cybersecurity firm, Kaspersky Lab, due to national security concerns. US government agencies are already banned from using Kaspersky software. `ban`

CISA publishes advisory on securing election infrastructure against foreign influence operations
On April 17, CISA, the FBI, and the US Office of the Director of National Intelligence published guidance on safeguarding election infrastructure against foreign malign influence. The document highlights tactics used to shape US policies and target election systems: AI voice cloning, information operations, used by China, Russia, and Iran are prominent in these efforts. `advisory` `election`

US unseals indictment against four Iranians for IRGC-linked cyberattacks
On April 23, the US Department of Justice unsealed an indictment which charged four Iranian nationals for involvement in cyber intrusions affecting the US private and public sector. According to the indictment, one of the defendants worked for the Electronic Warfare and Cyber Defense Unit of the Islamic Revolutionary Guard Corps (IRGC). `indictment`

Chrome Security launches postquantum protection

On April 25, Chrome Security confirmed that it had launched hybrid postquantum TLS Key exchange protection in Chrome 124. Chrome reports that the postquantum protection aims to protect users' traffic from the so-called store now decrypt later attacks, in which a future quantum computer could decrypt encrypted traffic recorded today. Quantum computing poses a significant threat to cybersecurity, challenging traditional encryption methods and demanding innovative solutions. `policy` `quantum computing`

Cyberespionage

Multiple China-linked threat actors exploiting Ivanti vulnerabilities

On April 4, Mandiant disclosed multiple China-linked threat actors exploiting three security vulnerabilities affecting Ivanti appliances. These actors, including groups tracked by Mandiant under designations such as UNC5221, UNC5266, UNC5291, UNC5325, UNC5330, and UNC5337, have been engaged in exploiting these vulnerabilities. Additionally, a Chinese hacking group named UNC3886 has also been linked to these exploits. `chinese threat actor`

CISA urges agencies to mitigate risks of Microsoft hack

On April 2, CISA issued an emergency directive instructing US federal agencies to respond to risks from the breach of multiple Microsoft corporate e-mail accounts by Russia-linked APT29. The directive mandates agencies to investigate affected e-mails, reset compromised credentials, and secure privileged Microsoft Azure accounts. CISA highlights that the group utilises stolen information, including authentication details, to access customer systems. `russian threat actor`

North Korea continues its fake job lure campaign

On April 18, Avast cybersecurity researchers reported that North Korea's Lazarus group is using fake job lures to deliver malware Kaolin RAT. While the specific communication platform used for initial access remains unknown, previous campaigns took place through LinkedIn and e-mail. The threat actor reportedly exploited a vulnerability in the default Windows driver appid.sys, to support its attack. `north korean threat actor`

Apple warns potential victims of mercenary mobile spyware attacks

On April 10, Apple alerted iPhone users across 92 countries about targeting with a mercenary spyware aimed at compromising their devices remotely. `psoa`

Threat actor targets human rights in North African activists with novel malware

On April 9, Cisco Talos unveiled a threat actor, dubbed Starry Addax, targeting activists linked to the Sahrawi Arab Democratic Republic by deploying a new mobile malware called FlexStarling and credential-harvesting techniques for Windows users. This malware, posing as a legitimate app from the Sahara Press Service, is designed to steal sensitive information and deliver further malicious components. `psoa`

DinodasRAT malware targets Linux servers in espionage campaign

On March 31, Check Point reported about DinodasRAT malware targeting Linux servers for espionage purposes. The activity is targeting Red Hat and Ubuntu systems since 2022. Security researchers note its persistence tactics, encrypted communication with a command server, and complete control over compromised systems, primarily affecting victims in China, Taiwan, Turkey, and Uzbekistan since October 2023. `unattributed threat actor`

Global cyberespionage campaign exploiting Cisco ASA and FTD firewall products

On April 24, Cisco has reported that since November 2023, a state-sponsored threat actor has exploited zero-day vulnerabilities in its ASA and FTD firewall products to compromise global government networks in a campaign dubbed ArcaneDoor. Despite patching the identified

vulnerabilities, Cisco is still investigating the initial attack methods used by the threat actors, tracked as UAT4356 by Cisco Talos and STORM-1849 by Microsoft. `unattributed threat actor`

Cybercrime

Ransomware likely targeted the United Nations Development Programme
The United Nations Development Programme (UNDP) reported a cyberattack on its Copenhagen facilities on March 27, involving theft of human resources and procurement data. Although the UN agency has not yet attributed the attack to any particular threat group, the 8Base ransomware gang posted a new entry for the UNDP on its dark web data leak site on March 27. `ransomware`

Malvertising campaigns promote fake AI services to distribute password-stealing malware
According to a report by Bitdefender of April 5, threat actors are employing Facebook ads and compromised pages to promote counterfeit AI services like MidJourney, OpenAI's Sora and ChatGPT-5, and DALL-E, aiming to distribute password-stealing malware. The malware targets browser data, extracting stored credentials, cookies, autocomplete entries, and credit card details. This stolen data is either sold on the dark web or utilised in further scams or fraudulent activities. `artificial intelligence`

Exploitation of GitHub comments flaws for malware distribution
On April 19, McAfee released a report on a vulnerability in GitHub being exploited by cybercriminals to spread malware through URLs that mimic those of a legitimate Microsoft repository, thereby enhancing the perceived trustworthiness of the malicious files. This security oversight could potentially be leveraged with any public repository on GitHub, enabling attackers to devise highly credible deceptive tactics. `technology`

Raspberry Robbin spreads in Windows Script Files
On April 10, HP published their findings related to a new variant of the Raspberry Robin worm. Since 2021, Raspberry Robin has been distributed through various means, including USB devices. The malware is now being delivered through Windows Script Files. The scripts are highly obfuscated and use a range of anti-analysis techniques, enabling the malware to evade detection. The malware can be a precursor of ransomware. `malware`

Supply-chain attack in open source library introduces critical vulnerability in Linux systems
A critical vulnerability, CVE-2024-3094, was identified in the XZ Utils library, a file compression utility, on March 29. The flaw stems from a sophisticated backdoor hidden in the binary test files of xz/liblzma versions 5.6.0 and 5.6.1. This backdoor allows for the manipulation of the build process and the injection of malicious code, significantly impacting system security. Many of the major Linux distributions are affected. `supply chain compromise`

Data exposure and leaks

Cisco Duo supplier data breach
On April 1, an incident affected a Cisco Duo telephony supplier that Duo uses to send multifactor authentication messages via SMS and VOIP to its customers. The threat actor downloaded message logs for SMS messages that were sent to certain users between March 1 and March 31. The message logs did not contain any message content but did contain metadata including phone number, and country to which each message was sent. `technology`

CISA discloses Sisense breach
On April 11, CISA warned Sisense customers of a recent security breach reported by the company. Sisense provides business intelligence and analytics services globally, including in the EU. The

exact nature of the breach is unclear, but it likely involves unauthorised access to customer data through compromised credentials. `technology` `critical infrastructure`

Data breach at AT&T affects 51 million customers
On April 10, AT&T informed 51 million former and current customers about a data breach exposing their personal information on a hacking forum. The company has not disclosed how the data was obtained. This relates to a recent leak of AT&T customer data on Breach hacking forums. `telecommunications`

Data breach at global chipmaker Nexperia
On April 12, Nexperia, a subsidiary of Chinese company Wingtech Technology, confirmed a data breach involving unauthorised access to its IT servers in March, potentially involving sensitive information including intellectual property. The Netherlands-based company produces around 100 billion semiconductor components annually, is closely monitoring the situation as the investigation continues. `technology`

Information operations

Covert Chinese accounts pose as American Trump supporters in elections influence campaign
On April 1, the New York Times reported that covert Chinese accounts are posing online as American supporters of former President Donald Trump, spreading conspiracy theories and attacking President Biden ahead of the US election in November. This marks a potential shift in China's influence tactics, resembling Russia's campaign before the 2016 election. `chinese threat actor`

Chinese threat actors developing information operations through AI
On April 5, Microsoft reported about Chinese threat actors (namely Storm-1376) utilising new media and refining AI-generated or AI-enhanced content. In particular, there has been a significant increase in the dissemination of AI-generated content (audio recordings, news anchors and memes), marking the first time Microsoft observed such tactics being used by a nation-state actor. `chinese threat actor` `artificial intelligence`

US Secretary of State says China is attempting to influence US elections
On April 26, the US Secretary of State said that the US sees evidence of Chinese attempts to influence and arguably interfere with the upcoming US elections, despite an earlier warning to leader Xi Jinping not to do so. `chinese threat actor` `election`

Disruption

China-linked Muddling Meerkat manipulates China's Great Firewall's DNS responses
On April 30, the US-based IT company Infoblox reported on a China-linked threat actor called Muddling Meerkat. This threat actor reportedly conducted a complex multi-year operation in which China's Great Firewall's DNS responses were falsified. The goal of the operation remains opaque, it may be used for future DDoS attacks or for prepositioning. `chinese threat actor`

Significant vulnerabilities

Multiple Vulnerabilities in Ivanti Connect Secure
On April 2, 2024, Ivanti has addressed critical vulnerabilities in its Connect Secure and Policy Secure products, notably CVE-2024-21894, allowing unauthenticated attackers to perform remote code execution (RCE) and denial of service (DoS) attacks. See CERT-EU's SA 2024-033.

Multiple Vulnerabilities in Microsoft Products
On April 9, 2024, Microsoft addressed 150 vulnerabilities in its April 2024 Patch Tuesday update, including 67 remote code execution (RCE) vulnerabilities and 2 zero-days exploited in malware attacks. It is recommended applying updates as soon as possible on affected products. See CERT-EU's SA 2024-034.

Critical Vulnerability in Rust on Windows
On April 9, 2024, the Rust Security Response WG issued a security advisory regarding a critical vulnerability in the Rust programming environment affecting Windows platforms. This flaw allows command injection attacks via crafted batch file executions with untrusted arguments. It is recommended updating as soon as possible, prioritising assets running code (or one of its dependencies) which executes batch files with untrusted arguments. See CERT-EU's SA 2024-035.

Vulnerabilities in Fortinet products
On April 11, 2024, Fortinet released multiple advisories regarding high and critical vulnerabilities affecting FortiOS, FortiProxy, FortiClient Mac and FortiClient Linux. It is recommended upgrading affected software as soon as possible. See CERT-EU's SA 2024-036.

Critical Vulnerability in PAN-OS software
On April 12, 2024, Palo Alto Networks released a security advisory for a critical vulnerability affecting a feature of PAN-OS software. This vulnerability allows an unauthenticated remote attacker to execute arbitrary code as root on the affected device. See CERT-EU's SA 2024-037.

Critical vulnerabilities in Junos OS and Junos OS Evolved
Multiple critical vulnerabilities have been identified in Juniper Networks Junos OS and Junos OS Evolved, primarily related to outdated cURL libraries. These vulnerabilities could allow remote attackers to execute arbitrary code, cause denial of service, or leak sensitive information. It is strongly advised to update affected systems to the latest versions to mitigate these risks. See CERT-EU's SA 2024-038.

Crtitical Putty Client Vulnerability
A critical vulnerability, identified as CVE-2024-31497, affects the PuTTY SSH client. This vulnerability stems from a bias in ECDSA nonce generation when using the NIST P-521 elliptic curve. Attackers can exploit this bias to recover private keys after observing a relatively small number of ECDSA signatures. See CERT-EU's SA 2024-039.

Vulnerabilities in Atlassian Products
On April 16, 2024, Atlassian released a security advisory addressing 7 high vulnerabilities in Bamboo Data Center, Confluence Data Center, Jira Software Data Center, and Jira Service Management Data Center. It is recommended updating as soon as possible prioritising internet facing instances. See CERT-EU's SA 2024-040.

Multiple Vulnerabilities in Ivanti Avalanche MDM
On April 16, 2024, Ivanti disclosed several vulnerabilities in its Avalanche MDM solution, including two critical heap overflow issues allowing unauthenticated remote command execution. It is recommended updating as soon as possible. See CERT-EU's SA 2024-041.

Vulnerability in Cisco Integrated Management Controller
On April 17, 2024, Cisco disclosed vulnerabilities in its Cisco Integrated Management Controller product. It is recommended upgrading affected products as soon as possible. See CERT-EU's SA 2024-042.

Vulnerabilities in Cisco ASA and FTD Software
On April 24, 2024, Cisco disclosed three vulnerabilities in its management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software product. It is recommended upgrading affected products as soon as possible, and checking for possible compromise. See CERT-EU's SA 2024-43.

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

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.