Cyber Brief (August 2024)

September 4, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 249 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, in Europe, the CEO of Telegram was temporarily detained in France, Switzerland joined two European cybersecurity initiatives, and a joint law enforcement operation led to the seizure of Dispossessor ransomware servers. Proton VPN allowed users to camouflage their VPN apps as weather apps to avoid detection by authoritarian regimes. Elsewhere, China introduced a national internet ID and Shanghai Spacecom launched the G60 satellite a competitor for Starlink. A US resident admitted to operating as a Chinese agent in a US telecommunications company, and the US government offered a reward for information about Iranian threat actor Cyber Av3ngers.
- On the **cyberespionage** front, Russia-linked Coldriver targeted Russian opposition figures in exile as well as Western civil society, and APT29 targeted Mongolian governmental websites. The UK realised that components of its nuclear submarine software were partially designed in Russia and Belarus, highlighting the supply-chain risk to UK national security. Iran-linked Peach Sandstorm targeted satellite and governmental entities in the US and UAE, while Iran-linked APT42 targeted US and Israeli influential figures with phishing.
- Relating to **cybercrime**, in Europe, the most active ransomware operations were Ransomhub, Blacksuit, Bianlian, Lynxblog, and Play, while the most targeted sectors were technology, manufacturing, healthcare, construction & engineering, and legal & professional services.
- As regards **data exposure**, data allegedly belonging to 3,2 million Belgian WhasApp users was put up for sale on an underground forum. Amid the US election, a reportedly Iran-linked hack-and-leak revealed data from the Trump Presidential election campaign.
- On the **information operation** front, several sources report of ongoing Iranian efforts to influence the upcoming US elections and warn of upcoming efforts to increase their reach.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in August 2024.

Europe

Cyber policy and law enforcement

Telegram CEO Pavel Durov detained in France on criminal charges
On August 24, Pavel Durov, CEO of Telegram, was detained in Paris on accusations of failing to cooperate with a law enforcement investigation into the criminal misuse of Telegram. This arrest triggered hacktivist groups to launch attacks against French entities and the European Court of Human Rights. `social media and messaging`

Switzerland to join two EU security cooperation projects
On August 21, Switzerland announced its decision to join two EU security initiatives, Military Mobility and Cyber Ranges Federation, under the PESCO framework. This move, which aligns with Swiss neutrality, aims to enhance defence capabilities by simplifying cross-border military operations and improving cyber defence cooperation. Additionally, Switzerland will join the European Cyber Security Organisation (ECSO) to gain access to expert networks and technological developments. `switzerland`

Individual behind Reveton and Ransom Cartel RaaS arrested
On August 9, an international operation, led by the UK National Crime Agency, resulted in the arrest and extradition of an individual believed to have been involved in creating and distributing ransomware such as Reveton and Ransom Cartel, as well as exploit kits such as Angler.

Dispossessor ransomware group's operations seized by joint operation
On August 12, a joint law enforcement action involving the UK's National Crime Agency, the Bamberg Public Prosecutor's Office, the Bavarian State Criminal Police Office and the US FBI led to the seizure of the servers of the Dispossessor ransomware operation. The ransomware group has been active since August 2023. The group primarily targeted small to mid-sized businesses globally, including in Belgium, Croatia, Germany, Poland, and the UK.

Greek investigation finds no state involvement in 2022 Predator spyware scandal
On July 30, the Greek Supreme Court Prosecutor saidthat a probe into how Predator spyware ended up on prominent Greek public figures' phones found that none of the country's state services, including its National Intelligence Service (EYP), were involved in acquiring or deploying the technology. The Supreme Court said the EYP's separate use of spyware between 2020 and 2024 was legal. `psoa`

Proton VPN enhances disguise features
On August 6, Proton VPN updated its Windows and Android apps, introducing a Discreet Icon feature which allows users to camouflage the app icon as a common applications such as a weather or calculator app. This is reportedly aimed at aiding users in authoritarian regimes to avoid detection and prosecution during random device inspections by law enforcement, ensuring safety in environments where VPN use is restricted.

Cyberespionage

Spearphishing campaign from Russia-linked Coldriver targets Western and Russian civil society
On August 14, CitizenLab reported on an ongoing spearphishing campaign which they associate to Russia-linked Coldriver, targeting Western and Russian civil society. The targets included prominent Russian opposition figures in exile, staff at NGOs in the US and Europe, and media

organisations. All targets share a common focus on Russia, Ukraine, or Belarus. The campaign used personalised social engineering tactics to engage targets. `russia`

Britain's nuclear submarine software linked to Russia and Belarus
On August 2, The Telegraph reported that Britain's nuclear submarines use software which was partially designed with software components from Russia and Belarus, raising significant security concerns about potential vulnerabilities to cyberespionage. This revelation has prompted questions about the oversight of defence contractors. `russia` `defence`

Cybercrime

Novel attack using NGate Android malware targets Czech bank customers
On August 22, ESET researchers reported on a unique cybercrime campaign in Czechia which leveraged NGate Android malware to clone and relay NFC data from victims' payment cards to attackers' devices, enabling unauthorised ATM withdrawals. The malware, active since November 2023, combined phishing, social engineering, and sophisticated malware capabilities without requiring device rooting. `finance`

Destruction

Mobile Guardian suffers destructive attack resulting in data wiped from devices
On August 4, Mobile Guardian, a digital classroom management platform, suffered a security breach. A threat actor gained unauthorised access and remotely wiped data from at least 13.000 student iPads and Chromebooks. The breach affected schools in North America, Europe, and Singapore.

Information operations

Disinformation follows tragic stabbing incident in UK
Following the July 29 Southport stabbing of young children, illegitimate media organisations spread false narratives. Narratives involved false information regarding the attacker's heritage, political status, and religious affiliation, which appears to have contributed to civil unrest in the UK.

China-linked AI-network could be leveraged to conduct harmful activity targeting US and Europe
On August 13, cybersecurity company CyberCX uncovered a network of at least 5.000 AI-operated accounts on X referred to as the Green Cicada Network. According to CyberCX, the network is believed to have been established by an employee of a Chinese AI company which has ties to the People's Liberation Army and Beijing's intelligence services. The network mainly focuses on US political and cultural issues but also amplifies contentious topics in Europe. `china` `united states` `artificial intelligence`

Data exposure and leaks

3,2 million Belgian WhatsApp users exposed in data leak
On August 22, a data leak exposed data allegedly of around 3,2 million Belgian WhatsApp accounts, with the details found for sale on a dark web forum. Users are advised to enable two-factor authentication, be cautious of unknown contacts, and report any suspected fraud to their bank and the police. `social media and messaging`

World

Cyber policy and law enforcement

Interpol recovers 40 million US dollars in BEC scam crackdown
On August 6, Interpol announced that their global stop-payment mechanism facilitated the recovery of over 40 million US dollars from a business e-mail compromise (BEC) scam targeting a Singapore company. BEC scams involve cybercriminals compromising corporate e-mails to reroute payments to their accounts, swiftly dispersing the funds through multiple channels. `business e-mail compromise`

China proposes a national internet ID for its citizens
On July 29, China proposed to implement national cyberspace IDs to protect citizens' personal information and streamline online identity verification. The IDs, proposed by the Ministry of Public Security and the Cyberspace Administration of China, aim to reduce data collection by Internet Service Providers (ISPs). `china`

China's G60 satellite launch
On August 5, China launched the first 18 satellites of the G60 constellation into low-Earth orbit, aiming to provide regional satellite internet coverage by 2025 and global coverage by 2027. This initiative, led by Shanghai Spacecom and backed by the Shanghai government, challenges SpaceX's Starlink in the commercial satellite internet market. `china` `aerospace`

US resident working at a telecommunications company pleads guilty to unregistered foreign agent activities
On August 23, the US Department of Justice reported that a US resident who had worked at a telecommunications company had pleaded guilty to acting as an agent of China without notifying the US Attorney General. According to court documents, the Chinese Ministry of State Security (MSS) uses international cooperative contacts to gather intelligence, including corporate, political, and dissident information abroad. `china` `telecommunications` `united states`

US Department of State offers reward for information on Iranian cybercriminals
On August 7, the US Department of State announced it is offering a reward of up to 10 million US dollars for information leading to the identification of several Iranian nationals suspected of breaching industrial control systems (ICS). The individuals in question are believed to be key figures in the Cyber Av3ngers group, linked to the Cyber Electronic Command of Iran's Islamic Revolutionary Guard Corps (IRGC). `iran` `united states` `reward`

Argentinian federal police arrests Russian for laundering money linked to Lazarus
On August 22, the Argentinian federal police arrested a Russian national in Buenos Aires for laundering cryptocurrency linked to North Korean threat actor Lazarus. The suspect, using complex blockchain networks, processed 100 million US dollars from Lazarus and other threat actors. Authorities, aided by blockchain analysis and Binance, seized 15 million US dollars in cryptocurrency and multiple devices. `north korea`

Russia bans Signal messaging app
On August 9, Interfax, a Russian news agency, reported that Russia's telecommunications watchdog, Roskomnadzor, restricted access to the Signal encrypted messaging service, citing violations of Russian anti-terrorism and anti-extremism laws. The agency stated that the restriction is intended to prevent the use of Signal for terrorist and extremist activities. This action comes after a March 2023 ban that prohibited the use of several foreign private

messaging applications in Russian government and state agencies. `russia` `social media and messaging`

US Justice Department sues TikTok over child privacy violations
On August 2, the US Department of Justice reported that it sued TikTok and its parent company ByteDance, accusing them of violating the Children's Online Privacy Protection Act by collecting personal data from children under 13 without consent. The lawsuit claims TikTok allowed minors to create accounts outside its Kids Mode exposing them to privacy risks and inappropriate content. `social media and messaging`

US indiviual arrested for aiding North Korean IT workers in US job scheme
On August 8, the US Justice Department reported that it had arrested a US national man accused of helping North Korean IT workers secure remote jobs in the US by operating a laptop farm to pose as US-based individuals. The individual is accussed of providing housing for company-supplied laptops, facilitatating identity theft, and laundering payments to North Korean and Chinese accounts, supporting North Korea's nuclear program. He faces multiple charges, potentially leading to 20 years in prison. `united states` `north korea`

Cyberespionage

Discovery of macOS HZ Rat backdoor targeting DingTalk and WeChat messaging apps
In June 2024, Kaspersky reported on a macOS version of the HZ Rat backdoor targeting DingTalk and WeChat users. This variant mirrors the Windows version's functionality but uses shell scripts for payloads. It connects via local IPs, suggesting targeted attacks for lateral movement. Originally detected in November 2022 by DCSO, the backdoor initially targeted Windows systems. `china` `social media and messaging`

China-linked threat actor StormBamboo exploits ISPs to deliver malware via insecure updates
On August 2, Volexity reported that in mid-2023 they detected StormBamboo, a China-linked threat actor, compromise an ISP to poison DNS responses. StormBamboo reporteldy targeted insecure software update mechanisms on macOS and Windows and hijacked update requests to install malware for data exfiltration. `china` `techniques` `ISP`

Iran-linked threat actor Peach Sandstorm targets critical sectors with new Tickler malware
On August 28, Microsoft reported that between April and July, Peach Sandstorm, an Iran-linked threat actor, deployed Tickler malware in the satellite, communications equipment, oil and gas, as well as governmental sectors in the US and the United Arab Emirates. Tickler collects initial network information and uses legitimate Windows binaries to evade detection and establish persistence. `iran` `energy` `technology` `united states` `public administration`

Iran-linked threat actor APT42 targets US and Israeli influential figures
On August 14, Google's Threat Analysis Group reported that APT42, an Iran-linked threat actor, orchestrated phishing campaigns targeting high-profile entities in Israel and the US since the start of 2024, approximately 60% of APT42’s activities focused on influential figures in politics, diplomacy, think tanks, and academia, which align with Iran’s strategic interests. `iran` `united states` `israel` `defence`

APT29 targeted Mongolian governmental websites
Between November 2023 and July 2024, Google’s Threat Analysis Group observed multiple exploit campaigns originating from a watering hole attack on Mongolian governmental websites. These campaigns are reportedly linked to the Russia-linked threat actor APT29 and targeted both iOS and Android users with known vulnerabilities, using exploits similar to those previously deployed by commercial surveillance vendors. `russia`

Hardware backdoors and vulnerabilities in FM11RF08S chip by Chinese manufacturer Shanghai Fudan Microelectronics

On August 16, Quarkslab published a research paper on the security issues of the FM11RF08S chip, a new variant of MIFARE Classic cards manufactured by Shanghai Fudan Microelectronics, which introduced countermeasures against known attacks but contains a hardware backdoor, allowing key compromise without prior knowledge. `supply-chain attack`

Cybercrime

Malvertising campaign on Facebook promotes fake AI editor to deliver password-stealing malware

On August 1, Trend Micro reported on a Facebook malvertising campaign leveraging AI image editing when targeting users with phishing messages. The attackers stole credentials via fake software installs and hijacked pages, then promoted malicious content using the victims' accounts. These activities involved creating fake websites mimicking legitimate AI tools and boosting traffic through paid ads, effectively compromising user data and control over social media pages. `artificial intelligence` `social media and messaging`

Threat actors recover cloud environment credentials from exposed .env files

On August 15, Palo Alto Networks researchers uncovered an extortion campaign that exploited exposed `.env` files containing sensitive credentials in cloud environments. Attackers compromised and extorted multiple organisations by leveraging these files, affecting over 110.000 domains and 7.000 cloud service credentials. They set up infrastructure in AWS environments, used automation for scanning, and ransomed data without encryption, leaving ransom notes in compromised cloud storage containers.

Data exposure and leaks

Iranian threats actors' hack-and-leak targets Donald Trump's presidential campaign

On August 10, Donald Trump's presidential campaign announced that they were the victims of a hack-and-leak operation by Iran-linked threat actors. `iran` `united states` `election`

Github authentication tokens found in GitHub Actions artifacts in popular open-source projects

On August 13, Palo Alto Networks reported on leaked GitHub authentication tokens through GitHub Actions artifacts from several popular open-source projects, including those from Google and Microsoft. These leaks, caused by insecure settings and misconfigurations, could allow attackers to access private repositories or inject malicious code. `supply-chain attack`

IntelBroker claims to have breached AMD's internal communications

On August 26, IntelBroker, an anonymous leaker, claimed to sell data from a breach involving AMD's internal communications, allegedly conducted on August 25. AMD is a US semiconductor company, the supposed leak reportedly involved sensitive information from various internal sources, which could affect AMD's operations and security. `technology` `semiconductor`

Information operations

Iran-linked threat actors preparing information operations ahead of US election

On August 9, Microsoft published a report about Iran-linked threat actors laying the groundwork for influence operations targeting US audiences. This activity includes initial cyber reconnaissance and the creation of online personas and websites. In the future, it is expected that Iranian actors will engage in cyberattacks against institutions and candidates while

simultaneously amplifying existing divisive issues within the US, such as racial tensions, economic disparities, and gender-related issues. `iran` `united states` `election`

US government warns of Iranian election influence operations targeting US campaigns.
On August 19, a joint statement from the three US governmental agencies detailed Iranian election influence efforts targeting US campaigns. Iran reportedly seeks to exploit societal tensions and gain access to sensitive election-related information through cyber operations. The agencies report to be actively investigating and collaborating with public and private sector partners to disrupt these foreign interference efforts. `iran` `united states` `election`

OpenAI bans accounts linked to covert Iranian influence operation
In August, OpenAI disrupted an Iranian influence operation, Storm-2035, which used ChatGPT to generate content to manipulate public opinion, mainly on the US presidential election. The operation reportedly had low audience engagement. `iran` `united states` `election` `artificial intelligence`

Disruption

Cyberattack on energy products and service provider Halliburton disrupts operations
On August 21, one of the world's largest providers of services to the energy industry Halliburton experienced a cyberattack which led to unauthorised system access, prompting the company to initiate a cybersecurity response, and shut down some systems. The incident was reported to law enforcement, and efforts are underway to restore and assess the impacted systems. `energy`

DDoS attacks against government internet resources coincide with Ukraine's military incursion into Russia
On August 8, Russian officials reported on DDoS attacks against governmental internet resources in Kursk, Russia, temporarily disrupting internet services in the region. The DDoS attacks coincided with Ukraine's military offensive into the Kursk region, which began on August 6. `russia` `telecommunications` `defence`

Lebanon files UN complaint against alleged Israeli cyber attacks
On August 1, the Lebanon-based newspaper L'Orient reported that Lebanon's Foreign Affairs Ministry filed a complaint with the UN Security Council and the International Telecommunication Union, accusing Israel of cyberattacks that threaten civil aviation and communications safety in Lebanon. The attacks reportedly disrupted GPS accuracy, posing risks to vital Lebanese infrastructure. `telecommunications` `lebanon` `israel`

Significant vulnerabilities

Vulnerabilities in AMD CPUs
On August 9, 2024, AMD disclosed a high-severity vulnerability, CVE-2023-31315 (SinkClose), affecting multiple generations of EPYC, Ryzen, and Threadripper processors. The flaw allows attackers with kernel-level access to gain Ring-2 privileges, potentially installing undetectable malware by modifying System Management Mode (SMM) settings. See CERT-EU's SA 2024-075.

Vulnerabilities in OpenVPN
On March 20, 2024, the OpenVPN community project team disclosed several vulnerabilities, CVE-2024-27459, CVE-2024-24974, CVE-2024-27903 and CVE-2024-1305 that could be chained to achieve remote code execution (RCE) and local privilege escalation (LPE). On August 8, 2024, Microsoft released a writeup for those vulnerabilities. See CERT-EU's SA 2024-076.

Vulnerabilities in Microsoft Office
On August 8, 2024, Microsoft disclosed a high-severity vulnerability tracked as CVE-2024-38200 affecting Office 2016 that could expose NTLM hashes to a remote attacker. This security flaw is caused by an information disclosure weakness that enables unauthorised actors to access protected information. See CERT-EU's SA 2024-077.

Ivanti vTM Critical Authentication Bypass Vulnerability
On August 13, 2024, Ivanti disclosed a critical authentication bypass vulnerability, CVE-2024-7593, affecting the Ivanti Virtual Traffic Manager. This flaw allows remote, unauthenticated attackers to bypass authentication and create rogue administrator accounts, posing a significant security risk. The vulnerability is due to an incorrect implementation of the authentication algorithm. See CERT-EU's SA 2024-078.

Critical SAP Authentication Bypass Vulnerability
On August 13, 2024, SAP released a security advisory for a critical authentication bypass vulnerability, CVE-2024-41730, in SAP BusinessObjects Business Intelligence Platform. This flaw allows remote attackers to bypass authentication mechanisms, potentially leading to full system compromise. The vulnerability has a CVSS score of 9.8. See CERT-EU's SA 2024-079.

Multiple Critical Vulnerabilities in Microsoft Products
On August 13, 2024, Microsoft addressed 89 vulnerabilities in its August 2024 Patch Tuesday update, including ten zero-day vulnerabilities. The Patch Tuesday also fixes six critical vulnerabilities. See CERT-EU's SA 2024-080.

SolarWinds Web Help Desk Critical Remote Code Execution Vulnerability
On August 14, 2024, SolarWinds disclosed a critical remote code execution vulnerability, CVE-2024-28986, affecting all versions of their Web Help Desk software. The vulnerability, caused by a Java deserialization flaw, allows attackers to execute arbitrary commands on the affected system. The vulnerability has a CVSS score of 9.8. See CERT-EU's SA 2024-081.

Zabbix Server Critical Arbitrary Code Execution Vulnerability
On August 13, 2024, a critical vulnerability, CVE-2024-22116, was disclosed in Zabbix Server, allowing attackers with restricted administrative permissions to execute arbitrary code. The flaw, identified in the Ping script execution within the Monitoring Hosts section, can compromise the entire infrastructure. The vulnerability carries a CVSS score of 9.9. See CERT-EU's SA 2024-082.

Palo Alto Cortex XSOAR CommonScripts Critical Vulnerability
On August 14, 2024, Palo Alto Networks released a security advisory for a critical command injection vulnerability, CVE-2024-5914, in Cortex XSOAR. This flaw allows unauthenticated attackers to execute arbitrary commands within the context of an integration container, potentially compromising the system. The vulnerability affects the product's CommonScripts Pack and is rated as high severity with a CVSS score of 9.0. See CERT-EU's SA 2024-083.

High Severity Vulnerabilities in F5 Products
On August 14, 2024, F5 released a security advisory addressing nine vulnerabilities in their products. Four of these vulnerabilities have been classified as high severity due to their potential to facilitate session hijacking and DDoS attacks. See CERT-EU's SA 2024-084.

Multiple Vulnerabilities in Moodle
On August 19, 2024, Moodle released a security advisory addressing sixteen vulnerabilities of various severities. See CERT-EU's SA 2024-085.

Chrome ZeroDay Vulnerabilities
A critical zero-day vulnerability, CVE-2024-7971, has been identified and patched in Google Chrome. This marks the ninth such vulnerability discovered in 2024. The flaw, which has been actively exploited in the wild, is rooted in a type confusion issue within Chrome's V8 JavaScript engine. This vulnerability allows attackers to potentially execute arbitrary code on affected

systems. On August 26, Google announced that it patched the tenth zero-day vulnerability in Chrome. This vulnerability is also reported as being exploited. See CERT-EU's SA 2024-088.

Critical Vulnerability in SonicWall SonicOS
On August 23, 2024, SonicWall issued a security advisory regarding a critical access control vulnerability (CVE-2024-40766) in its SonicOS. This flaw could allow attackers to gain unauthorised access to resources or cause the firewall crash. See CERT-EU's SA 2024-089.

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 its 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.