10 years CERT-EU

Cyber Brief (July 2024)

August 1, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 252 open source reports for this Cyber Security Brief[1].
- **Cyber policy and law enforcement** efforts in Europe have included the French police's removal of PlugX malware from infected systems, Germany's ban on Chinese telecommunications components, the European Commission's finding against Meta's ad model, international coordination on APT40 and Cobalt Strike, arrests linked to ransomware and hacktivist groups, a joint AI competition statement by US and European agencies. On the global level, the UN's Radio Regulations Board demands Russia stop interfering with other countries' satellite networks, a Thai NGO files a complaint about government use of Pegasus spyware, Iran experiences internet crackdowns as the Raisi administration ended, and China proposes national internet IDs to enhance online identity verification.
- **Cyberespionage** activities in Europe highlight cyberattacks by China-linked groups like APT17 and APT41 targeting Italian government agencies, global sectors, and a German cartography agency, while a new group, TAG-100, targets EU countries, and a German MEP falls victim to mobile spyware from Israeli company Candiru.
- On the **cybercrime** front, reports revealed phishing campaigns targeting SMBs in Europe, a malicious GitHub network, a 75 million US dollars ransomware payment by a Fortune 50 company, SMS-stealing via Telegram bots, APT45 expanding North Korean operations, and extensive FIN7 campaigns worldwide. In Europe, the most active ransomware operations were Ransomhub, Akira, Cactus, Madliberator, and Spacebears, while the most targeted sectors were manufacturing, construction & engineering, healthcare, technology, and legal & professional services.
- As regards **information operations**, new reports show that before the June 2024 European Parliament elections, coordinated networks spread disinformation on social media in France, Germany, and Italy, with 50.000 accounts identified as spreading disinformation, many of which were created after Russia's invasion of Ukraine. Similar disinformation efforts were observed in the UK election and the upcoming US election, with Russian and Iranian campaigns exploiting social media platforms to spread false narratives, sow division, and undermine trust in democratic processes.

- In **data exposure and leaks** incidents, nearly 10 billion passwords were leaked in the RockYou2024 breach, alongside other significant breaches at OpenAI and AT&T, exposing internal data and customer call logs.
- On the **hacktivism** front, pro-Russia hacktivist groups claimed responsibility for DDoS attacks on French entities during the country's snap elections, with similar attacks also targeting organisations related to the 2024 Paris Olympics and a NATO portal breach by SiegedSec, while pro-Ukraine hacktivists leaked e-mails allegedly from a top Russian official.
- Notable **disruptive** incidents included a faulty CrowdStrike update causing a global outage that affected 8.5 million machines, a DDoS cyberattack on Microsoft Azure disrupting services for 10 hours, and a Ukrainian cyberattack targeting Russia's banking system, impacting major financial institutions.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in July 2024.

Europe

Cyber policy and law enforcement

French police push PlugX malware self-destruct payload to clean PCs
On July 18, an operation by the French police, Europol, and cybersecurity firm Sekoia pushed a "disinfection solution" to automatically remove PlugX malware from infected devices in France. This operation targets 3.000 infected systems and involves notifying victims about the clean-up process while urging caution when using USB drives in public places, as the malware spreads via infected USB flash drives. `clean-up`

Germany moves to ban Chinese companies from the country's telecommunications networks
On July 11, Germany joined other EU countries in banning Chinese companies from the country’s telecommunications networks by removing Huawei components from the country’s 5G networks by 2026, as well as Huawei and ZTE components from the nation’s 5G access and transport networks by 2029. `ban` `china`

Kosovo bans TikTok on government IT
On June 28, Kosovo banned TikTok in state institutions, citing vulnerability concerns. Deputy Minister for Internal Affairs stated the ban aims to protect the state institutions of Kosovo against cyber threats. The ban affects all public institutions that own and manage state communication networks, and public officials will be required to remove TikTok. `ban`

European Commission finds Meta's Pay of Consent ad model fails the DMA
On July 1, the European Commission confirmed that it had informed Meta of its preliminary findings that its “pay or consent” advertising model fails to comply with the Digital Markets Act (DMA). In the Commission's preliminary view, this binary choice forces users to consent to the combination of their personal data and fails to provide them a less personalised but equivalent version of Meta's social networks. `regulation`

US and European agencies release Joint Statement to ensure fair AI competition
On July 23, antitrust agencies from the US, UK, and EU issued a joint statement affirming their commitment to ensure fair competition in the generative AI market to protect businesses and consumers while fostering economic growth and innovation. The agencies will use their respective laws to identify key AI competition risks, promote fair dealing, interoperability, and ample product choices, and highlight potential data and security risks associated with AI models. `artificial intelligence`

Seven countries coordinate public attribution of APT40 to the Chinese Ministry of State Security
On July 8 and 9, Germany, the UK, the US, Japan, South Korea, Canada and New Zealand all publicly attributed APT40, a cyberespionage actor, to the Chinese Ministry of State Security (MSS). The coordinated public attribution statements emphasised that APT40's attacks have primarily targeted private and governmental entities in Australia. The statements detailed APT40's use of complex obfuscation networks made up of SOHO routers and exploitation of public-facing vulnerabilities. `attribution` `china`

ECB review uncovers banks' cyber attack resilience gaps
On July 26, the European Central Bank (ECB) reported that its first review of banks' ability to withstand cyber attacks found deficiencies in their crisis management and resilience, highlighting the need for improved responses to breaches. While the stress test focused on banks' responses rather than prevention capabilities, it revealed the importance of enhancing operational resilience and highlighted that some banks have already taken steps to address identified shortcomings. `resilience` `finance`

Europol contributes to international law enforcement operation targeting Cobalt Strike
On July 3, Europol announced that it had contributed to a global operation to combat the criminal misuse of Cobalt Strike. Older, unlicensed versions of the Cobalt Strike red teaming tool were targeted between June 24 and 28 in what is now known as Operation Morpheus. This investigation was led by the UK National Crime Agency and involved law enforcement authorities from Australia, Canada, Germany, the Netherlands, Poland and the United States. `take down`

Individual allegedly linked to Scattered Spider and AlphV ransomware arrested in the UK
On July 19, UK authorities arrested a 17-year-old male for Blackmail and Computer Misuse Act offences, allegedly connected to the hacking group Scattered Spider, with links to Alphv ransomware attacks on US entities. The individual, who has been released on bail, had several digital devices seized for forensic examination, while earlier in 2024, other individuals connected to Scattered Spider were also arrested in the US and Spain. `arrest`

Spanish police arrests three members of a Russia-linked hacktivist group
On July 20, the Spanish police arrested three individuals linked to the Russia-linked hacktivist group NoName0517(16). The group recently conducted DDoS campaigns against EU countries, including Spain. Spanish websites were listed on DDoSia after the arrests. `arrest` `russia`

Operation Jackal III brings down organised crime groups in several countries including Portugal and Switzerland
On July 16, Interpol announced Operation Jackal III, targeting West African crime groups like Black Axe. Conducted from April 10 to July 3 across 21 countries on five continents, including European nations Portugal and Switzerland, the operation focused on online financial fraud. It resulted in 300 arrests, identifying over 400 suspects, blocking 720+ bank accounts, and seizing 3 million US dollars in assets. `arrest`

Cyberespionage

China-linked APT17 targets Italian government agencies and companies
On July 9, Italian cybersecurity firm TG Soft reported on two targeted cyberattacks that were carried out on Italian companies and government entities by a China-linked threat actor on June 24 and July 2. These attacks utilised a variant of the Rat 9002 malware in diskless mode and are linked to the APT17 group, also known as DeputyDog. `china`

China-linked APT41 targets multiple global sectors in sustained campaign
On July 18, Google / Mandiant reported that APT41 has been targeting and successfully

compromising organisations in the shipping, logistics, media, technology, and automotive sectors across countries such as Italy, Spain, Taiwan, Thailand, Turkey, and the UK since 2023. APT41 used a combination of ANTSWORD and BLUEBEAM web shells, DUSTPAN, and BEACON backdoor for C2 communication, along with tools like SQLULDR2 and PINEGROVE to exfiltrate sensitive data to Microsoft OneDrive. `china` `technology` `automotive`

Germany accuses China of 2021 cyberattack on cartography agency
On July 31, Germany accused China of a 2021 cyberattack on its federal cartography agency for espionage. The German Interior Minister urged China to stop such actions, highlighting the growing threat. German intelligence linked the attack to Chinese state actors, compromising devices of individuals and companies. `china`

German MEP Daniel Freund targeted by mobile spyware before EU elections
On July 25, German Green MEP Daniel Freund revealed on social media platform X that he was targeted by mobile spyware delivery attempts. The attack occurred on May 27, just two weeks before the EU Parliament Elections. Freund stated that cybersecurity experts identified the spyware as likely originating from the Israeli company Candiru. `psoa`

New likely cyberespionage group TAG-100 targets EU countries
On July 16, Recorded Future reported about a new threat actor they dubbed TAG-100 conducting suspected cyberespionage activities targeting high-profile government, intergovernmental, and private sector organisations worldwide. Victims include The Netherlands and the UK, and reconnaissance activities were likely conducted in France and Italy. The threat actor uses open-source remote access tools and exploits various internet-facing devices for initial access.

Old Microsoft Exchange vulnerabilities exploited by threat actor targeting Georgia
On July 2, the Hunt Research Team, a cybersecurity company, revealed that a server was likely exploiting ProxyLogon and ProxyShell vulnerabilities to gain access and steal sensitive communications. Affected entities were spread across multiple regions and included various sectors, namely in Georgia. Although the server's exposure was brief and its target range limited, the incident underscores a critical issue: threat actors continue exploiting older vulnerabilities and adapting their methods.

Cybercrime

Nine phishing campaigns targeting SMBs in three EU countries
On July 30, ESET reported that, in May 2024, they detected nine ModiLoader phishing campaigns targeting small and medium sized businesses (SMBs) in Poland, Romania, and Italy. These campaigns delivered malware including Remcos, Agent Tesla, and Formbook, using compromised e-mail accounts and servers for distribution and data collection. ModiLoader replaced AceCryptor as the delivery tool.

Disruption

Ukraine’s Main Directorate of Intelligence and pro-Ukraine hacktivist BOTeam conducted offensive cyber activity against Russian and Crimean entities
In late June, Ukrainian media reported that Ukraine’s Main Directorate of Intelligence (HUR) and associated pro-Ukraine hacktivist group BOTeam conducted both joint and separate offensive cyber activity causing disruptions against Russian and Crimean entities. Two of the targeted Russian entities confirmed to have been impacted by the activity. `russia`

Information operations

Disinformation on social media in France, Germany, and Italy before the European Parliament elections
On July 12, The Guardian reported on Dutch researchers who found coordinated networks of accounts spread disinformation on social media in France, Germany, and Italy before the European Parliament elections. The analysis examined 2.3 million posts from 468.000 accounts. It identified 50.000 accounts as disinformation spreaders. Many of these accounts were created after Russia’s invasion of Ukraine but became significantly active just before the elections, rapidly increasing their follower counts. `election`

Disinformation surge in UK election linked to bot accounts
On July 2, Global Witness reported on suspected bot profiles on X distributed over 60.000 posts containing disinformation and hate speech, potentially reaching 150 million views, ahead of the UK general election. These posts included extreme content such as conspiracy theories and various forms of hate speech. The profiles praised Russian President Vladimir Putin, raising concerns about their significant impact on election integrity. `election`

Pro-Russian Facebook pages coordinating disinformation campaign ahead of UK elections
On June 29, ABC News reported on a disinformation campaign involving pro-Russian Facebook pages ahead of the UK elections. Five pages, operated from Nigeria, are spreading Kremlin-aligned propaganda, targeting UK voters with coordinated messages and AI-generated content. These activities aim to sow division and chaos, undermining trust in the media and the electoral process. The Conservative Party expressed serious concerns, recognising it as a deliberate attack on democracy. `election` `russia` `artificial intelligence`

Russian clandestine operations intensify in Estonia and Poland
On July 4, the Centre for Security, Diplomacy, and Strategy, a Belgian academic research hub, reported that Russian clandestine operations across Europe, particularly in Estonia and Poland, are intensifying. These operations include cyberattacks, cognitive warfare, and recruitment via social media, aiming to destabilise these countries and influence public perception. Estonia and Poland are actively exposing these Russian activities and enhancing counterintelligence efforts to address the growing threat. `russia`

Project Kylo: Inside Russia's sophisticated disinformation campaign against the West
On July 4, The Insider and Der Spiegel revealed extensive details about "Project Kylo," a disinformation campaign orchestrated by Russia's foreign intelligence agency (SVR). The documents, leaked from the SVR, outline a strategy to manipulate public opinion in the West through various deceptive means, aiming to incite fear, panic, and anti-government sentiments. The campaign focuses on exploiting sensitive issues and leveraging new internet platforms, moving away from older, less effective state-controlled media like RT and Sputnik. `russia`

Hacktivism

Pro-Russia supposed hacktivsts DDoS amid French elections
On June 30, the pro-Russia supposed hacktivist groups Cyber Army of Russia and HackNeT claimed responsibility for DDoS attacks against several French entities. The DDoS attacks coincided with the first round of France’s snap elections that same day. Targeted entities included French political parties as well as two hotel chains. `russia` `political parties`

Russia-linked hacktivists claim DDoS against websites in connection with the Olympics
Between July 26 and 29, multiple pro-Russia hacktivist groups claimed DDoS attacks against French, Israeli, and Ukrainian entities in connection with the 2024 Paris Olympics. The groups

are likely motivated by an alleged “double standard” that allows Israel to participate in the Olympics despite the ongoing Israel-Hamas conflict, while Russia is excluded from the games. `russia`

Hacktivist group SiegedSec claimed to have breached and leaked a NATO portal
On July 7, the hacktivist group SiegedSec claimed to leak data supposedly from NATO's NHQC3S portal, intended only for NATO employees. The breach contains user information and hundreds of documents. The group emerged coincidentally just days before Russia’s invasion of Ukraine and claim that it is the third time that they breached a portal belonging to NATO. `defence`

Pro-Ukraine hacktivist leaks supposed Russian government e-mails
On July 1, The Moloch, a technology journalism project, reported that Cyber Resistance, a pro-Ukraine supposed hacktivist, leaked e-mails supposedly from former Russian president and current Chairman of Russia’s Security Council, Dmitry Medvedev's assistants. The e-mails were leaked on InformNapalm, a Ukrainian outlet, between January and June. The communications reportedly relate to Russia’s nuclear threats, posturing in the Arctic, and Medvedev‘s public appearances. `russia`

World

Cyber policy and law enforcement

UN Radio Regulations Board requests Russia to cease interference in satellite networks of other countries
On July 1, ITU, the International Telecommunication Union, the UN Agency for information and communication technologies, published decisions taken by the Radio Regulations Board (RRB) between June 24 and 28. The RRB requested the Administration of the Russian Federation to immediately cease any deliberate action to cause harmful interference to frequency assignments such as satellite networks of other administrations. `russia`

Thai NGO files complaint over government use of Pegasus spyware; ISOC denies allegations
On July 18, Thailand's Internal Security Operations Command (ISOC) denied using Pegasus spyware against pro-democracy protesters after iLaw's complaint to the parliamentary committee on national security. The complaint, based on Citizen Lab's findings, alleged Pegasus monitored 35 individuals. The committee is investigating, and a civil case against NSO Group is set for witness examination in September 2024. `psoa`

Iran internet crackdown as Raisi administration prepares to leave office
On July 11, Internet Outage Detection and Analysis (IODA), a platform monitoring global internet access quality, reported significant network interruptions in Iran starting on July 10, involving Host Iran and the Telecommunication Company of Iran (TCI). This follows the final days of the Raisi administration, suggesting a last attempt to enforce the severe internet crackdowns characteristic of Raisi's tenure. `iran`

China proposes a "national internet ID" for its citizens
On July 29, China proposed to implement a 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 ISPs. While voluntary, they raise privacy concerns despite potential encryption and safeguards against unauthorised data use, reflecting global issues seen with India's Aadhar and Japan's MyNumber systems. `china`

Meta settles 1.4 billion US dollars lawsuit with Texas over unauthorised facial recognition
Meta agreed to pay 1.4 billion US dollars to Texas for using facial recognition on Facebook without users' consent from 2011 to 2019. Despite ending the feature in 2021 and denying any wrongdoing, Meta faced a 2022 lawsuit. This historic settlement underscores Texas' commitment to privacy rights, similar to Meta's 650 million US dollar settlement with Illinois in 2020. `united states`

Kaspersky shuts down operations in the US
On July 15, Kaspersky announced to BleepingComputer that it will completely shut down its operations in the US due to the Biden administration's decisions rendering them "no longer viable". Starting on July 20, 2024, Kaspersky will gradually wind down its US operations and eliminate US-based positions. This decision follows the US Department of Commerce's Final Determination, which prohibits the sales and distribution of Kaspersky products in the US. `united states`

Crackdown on Russian propaganda bot farm
On July 15, a global law enforcement operation led by the US Justice Department dismantled nearly a thousand social media X bots controlled by Russian operatives. These bots, using AI software Meliorator since 2022, spread disinformation to influence global public opinion. The FBI highlighted Meliorator's role in creating deceptive online personas to manipulate perspectives across several countries. `russia` `artificial intelligence`

Meta releases Llama 3.1 as a free and open-source AI model
On July 23, Meta released Llama 3.1 405B, a powerful AI model, for free, marking a significant move against closed AI models like OpenAI's. Though not fully open-source, it allows broad developer usage. Meta faces criticism over potential misuse and the misleading "open-source" label. This release positions Meta strongly in AI development, challenging the business models of other major AI companies. `artificial intelligence`

X begins training Grok AI with users' public posts
On July 25, X started using members' public posts to train its Grok AI chat platform without prior notification. This new default setting can be disabled in the site's privacy settings. Users can opt out by making their accounts private or adjusting the Grok settings under Data sharing and personalisation. The change has been confirmed by X's Safety team and applies to the web version. `artificial intelligence`

Cyberespionage

Chinese hackers deploy new Macma macOS backdoor version
On July 23, Symantec reported that the Chinese hacking group Evasive Panda has been using new versions of the Macma backdoor and Nightdoor Windows malware to conduct cyberespionage, targeting organisations in Taiwan and an American NGO in China. Symantec discovered that Evasive Panda exploited an Apache HTTP server flaw to deliver their modular malware framework, MgBot, showcasing ongoing efforts to enhance their tools and evade detection. `china`

China-linked threat actor exploited Cisco NX-OS zero-day to deploy custom malware
On July 1, Cisco patched a zero-day in NX-OS, exploited during April by the China-linked threat actor Velvet Ant to install malware on Cisco switches. The vulnerability, tracked as CVE-2024-20399, enabled threat actors with admin credentials to execute commands with root access by exploiting insufficient argument validation in CLI commands. `china`

Notorious Chinese threat actor GhostEmperor re-emerges after 2 years
On July 17, Sygnia reported that the covert Chinese hacking group GhostEmperor has resurfaced

after a two-year hiatus with advanced infection chains and sophisticated EDR evasion techniques. Initially discovered by Kaspersky in 2021 for targeting telecommunications and government entities in Southeast Asia, GhostEmperor has now updated its Demodex rootkit, incorporating new obfuscation methods and exploiting vulnerabilities such as ProxyLogon and WMIExec for remote command execution. `china`

JPCERT/CC warns of Kimsuki targeting Japaneses organisations
On July 8, Japan's Computer Emergency Response Team (JPCERT/CC) published a warning regarding DPRK-linked threat actor Kimsuky targeting Japanese organisations. Recent attacks involve malicious ZIP files and CHM malware. Collected information includes keystrokes and user data, aiding further infiltration. `north korea` `japan`

North Korean cyber group targets global industries to advance military and nuclear programs
On July 25, US cybersecurity agencies released an advisory highlighting espionage activities by North Korea’s Reconnaissance General Bureau (RGB) 3rd Bureau, targeting defence, aerospace, nuclear, and engineering sectors to advance the DPRK’s military and nuclear ambitions. The group, known as Andariel, also funds its operations through ransomware attacks on US healthcare entities, exploiting software vulnerabilities, deploying custom malware, and conducting phishing campaigns to gain unauthorised access and exfiltrate sensitive information. `north korea` `military`

CloudSorcerer emerging threat actor targeted Russian government entities
In May 2024, Kaspersky researchers uncovered CloudSorcerer, an APT group exploiting public cloud services to conduct cyberespionage against Russian government entities. This group employs custom malware that integrates legitimate cloud platforms for command and control operations and data storage. Despite similarities to CloudWizard APT's tactics, the distinct malware suggests CloudSorcerer is a new, emerging threat. `russia` `public administration`

India-linked SideWinder threat actor targets ports and maritime facilities in the Mediterranean Sea
On July 25, BlackBerry reported that SideWinder APT targeted ports and maritime facilities in the Mediterranean and Indian Ocean in early 2024 using spearphishing e-mails. The campaign focused on organisations in Pakistan, Egypt, Sri Lanka, Bangladesh, Myanmar, Nepal, and the Maldives, employing tactics like remote template injection, obfuscated JavaScript, and exploiting Microsoft Office vulnerabilities. SideWinder, believed to originate from India, aimed at espionage and intelligence gathering. `india` `transport`

Cybercrime

Malicious network of GitHub accounts distributes links to malicious GitHub repos
On July 24, Check Point reported about a network of GitHub accounts amplifying malicious repositories. The network, dubbed Stargazers Ghost network, lures victims on Discord with links to malicious GitHub repos which have scripts that download and execute payloads from seemingly legitimate websites or sources but instead download malware. The malware being distributed includes Atlantida Stealer, Rhadamanthys, RisePro, Lumma Stealer, and RedLine.

Fortune 50 company pays record 75 million US dollar ransom to Dark Angels ransomware group
On July 30, Zscaler reported that a Fortune 50 company paid a record-breaking 75 million US dollars ransom to the Dark Angels ransomware group. This is the highest known ransomware payment, surpassing CNA's previous record of 40 million US dollars. While the company's identity remains undisclosed, the attack occurred in early 2024, possibly involving pharmaceutical giant Cencora.

SMS-stealing campaign targeting Android devices using Telegram bots
On July 29, Zimperium reported a campaign targeting Android devices using Telegram bots to distribute SMS-stealing malware, capturing OTPs for over 600 services. Zimperium researchers have tracked this since February 2022, finding 107.000 malware samples. The malware, controlled by 13 servers, uses infected devices for authentication and anonymisation. Most victims are in India and Russia.

New cybercrime threat actor CrystalRay targeting over 1500 victims with open-source security tools
On July 11, Sysdig, a cybersecurity company, reported on a new threat actor CRYSTALRAY that targeted over 1500 victims by stealing credentials and deploying cryptominers. Initially identified using the SSH-Snake worm, CRYSTALRAY now employs mass scanning, multiple exploits, and open-source security tools like zmap and nuclei. Targeted vulnerabilities include CVE-2022-44877, CVE-2021-3129, and CVE-2019-18394. The group also monetises stolen credentials and cryptomining, generating revenue from compromised systems.

Fake Google ad for Authenticator distributes malware
On July 30, Malwarebytes researchers reported a threat actor impersonating Google through a fake ad for Google Authenticator, leading users to download malware. The malicious ad redirected to a fraudulent site hosted on GitHub, distributing the DeerStealer malware. Users are advised to avoid clicking on ads and download software from official repositories.

NullBulge threat actor targets entities focused on AI
On July 16, SentinelLabs published a report about a new threat group called NullBulge. This group targets entities focused on AI and gaming. In July 2024, NullBulge released data allegedly stolen from Disney's internal Slack communications. Their method of attack involves targeting the software supply chain by weaponising code in publicly available repositories on GitHub and Hugging Face. `artificial intelligence`

APT45: North Korea's cyber warfare machine
On July 26, Mandiant reported that APT45, a moderately sophisticated North Korean cyber operator active since 2009, has expanded from espionage to financially motivated operations, including suspected ransomware deployment. Unique among North Korean groups for its focus on critical infrastructure and financial targets, APT45 has continued to evolve its operations, utilising a distinct set of malware tools and aligning closely with the DPRK's shifting geopolitical priorities. `north korea`

FIN7 massive campaigns targeting organisations worldwide
On July 10, cybersecurity company Silent Push reported on extensive FIN7 campaigns which include several hundred active phishing, spoofing, shell, and malware delivery domains and IPs, targeting various organisations. Over 4.000 domains and subdomains, nearly half active recently, are used in these attacks. Prominent global brands like the Louvre Museum, Meta, Reuters, and Microsoft are targeted. FIN7 employs tactics such as spearphishing, malware distribution, and renting infrastructure from Stark Industries Solution. `russia`

Data exposure and leaks

Massive password leak RockYou2024 exposes 10 billion of credentials
On July 4, nearly ten billion unique passwords have been exposed in a leak on a hacking forum, by the user ObamaCare. The compilation, named RockYou2024.txt, contains a mix of old and new breached data, significantly increasing the risk of credential stuffing and brute-force attacks on users who reuse passwords. `passwords`

OpenAI suffered a breach in April 2023 exposing AI design details
On July 20, The Verge reported that a hacker accessed OpenAI's internal messaging systems in April 2023, stealing insights from an employee forum but not penetrating AI development systems. The incident, revealed to employees and the board, was not made public as it involved no customer data and posed no national security threat. The hacker was identified as a private individual unaffiliated with any government. `technology` `artificial intelligence`

AT&T data breach exposes call logs of 109 million customers
On July 12, AT&T reported a data breach affecting 109 million customers, where call and text logs from May 2022 to January 2023 were stolen from its Snowflake account. The breach included phone numbers and interaction counts but no sensitive personal information. After consulting with the FBI, public notification was delayed due to national security concerns. `telecommunications`

Information operations

Iran's covert online operations aim to undermine Trump, US intelligence says
On July 29, the Washington Post reported that US intelligence agencies indicate Iran is conducting covert online influence operations to undermine Donald Trump's presidential campaign, fearing increased tensions if he returns to power. These efforts include using online personas and propaganda to spread disinformation. Tehran’s actions aim to fuel distrust in US political institutions and exacerbate social discord. `iran` `united states` `election`

Russian Doppelganger campaigns spread fake Fox News articles on X ahead of the US Presidential debate
On June 27, NBC News reported that a network of pro-Kremlin accounts on X, known as the Doppelganger campaign, pushed fake Fox News articles in the hours ahead of the US presidential debate on June 27, attempting to spread false narratives including one about former President Donald Trump’s support in the business community. `russia` `united states` `election`

Russia-linked disinformation uses fake news articles which masquerade as Jewish American news outlets
On June 27, The Forward, a Jewish American news outlet, reported that a Russia-linked disinformation campaign had intensified, spreading fake news articles, dummy websites, and AI-generated voice-over videos about the Gaza war, Israeli protests, and international relations. The campaign included fake articles posing as The Forward and Hamodia, which were shared by thousands of bot accounts on X, aiming to spread misinformation. `russia`

Disruption

CrowdStrike update causes global outage, impacting 8,5 million machines
On July 19, a faulty software update from CrowdStrike caused a global IT outage, impacting around 8,5 million machines. The update led to widespread "blue screens of death" on Windows machines, forcing them into a bootloop and rendering them unusable. The issue disrupted major services, grounded flights, and affected emergency services. CrowdStrike worked to deploy a fix, but their stock dropped by 11% by the end of the day. `technology`

Microsoft Azure outage caused by DDoS cyberattack disrupts services for 10 hours
On July 30, Microsoft Azure experienced an outage caused by a DDoS cyberattack that disrupted access to Microsoft 365 products and Azure services for nearly 10 hours. This incident, affecting companies like UK bank NatWest, follows a recent CrowdStrike update issue. Microsoft's DDoS

protection mechanisms inadvertently amplified the attack's impact. Microsoft plans to release a Preliminary Post Incident Review within 72 hours. `technology`

Ukrainian intelligence targets Russian banking system with cyber attack
On July 23, a massive cyber attack by the Ukrainian Defense Ministry's Main Intelligence Directorate targeted Russia's banking system, disrupting services at major financial institutions, mobile operators, and internet providers. The attack has severely impacted digital services at banks like Alfa-Bank and Sberbank, and national payment systems, causing widespread complaints from Russian users and acknowledgment from Russia of the politically motivated cyber offensive. `russia`

Significant vulnerabilities

Critical Vulnerability in Juniper Networks Products
On June 27, 2024, Juniper Networks issued an advisory about a critical vulnerability, CVE-2024-2973, affecting Session Smart Router (SSR), Session Smart Conductor, and WAN Assurance Router products. This vulnerability allows an attacker to bypass authentication and gain full control of the device, primarily affecting high-availability redundant configurations. See CERT-EU’s SA 2024-065.

Critical Vulnerability in OpenSSH
On July 1, 2024, a new OpenSSH unauthenticated remote code execution (RCE) vulnerability dubbed regreSSHion was reported, affecting glibc-based Linux systems. This vulnerability, identified as CVE-2024-6387, allows remote attackers to execute arbitrary code as root due to a signal handler race condition in sshd. See CERT-EU’s SA 2024-066.

Multiple Vulnerabilities in Microsoft Products
On July 10, 2024, Microsoft addressed 139 vulnerabilities in its July 2024 Patch Tuesday update, including four zero-day vulnerabilities. Two zero-day vulnerabilities are actively exploited. Additionally, five critical vulnerabilities leading to Remote Code Execution have been patched. See CERT-EU’s SA 2024-067.

Critical Vulnerabilities in GeoServer and GeoTools
On July 2, 2024, several critical vulnerabilities were addressed in GeoServer and GeoTools. These vulnerabilities can result in arbitrary code execution through the unsafe evaluation of user-supplied "XPath" expressions. See CERT-EU’s SA 2024-068.

Vulnerabilities in Citrix Netscaler
On July 9, 2024, Citrix released a security advisory addressing two vulnerabilities in Citrix NetScaler Console, Agent, and SDX (SVM). The vulnerabilities "CVE-2024-6235" and "CVE-2024-6236" can result in sensitive information disclosure and denial of service. See CERT-EU’s SA 2024-069.

Critical Vulnerabilities in Cisco Products
On July 17, 2024, Cisco issued several security advisories addressing critical and high severity vulnerabilities in its products. It is strongly recommended applying update on affected devices as soon as possible, prioritising internet facing and business critical devices. See CERT-EU’s SA 2024-070.

Critical Vulnerabilities in SolarWinds Access Rights Manager
On July 18, 2024, SolarWinds issued an advisory addressing multiple critical vulnerabilities in its Access Rights Manager (ARM) software. These vulnerabilities could lead to remote code execution, arbitrary file deletion and sensitive information leakage. See CERT-EU’s SA 2024-071.

Vulnerabilities in Ivanti EPMM
On July 12, 2024, Ivanti released a security advisory addressing several vulnerabilities in its EPMM solution (formerly known as MobileIron). These vulnerabilities could lead to remote code execution, authentication bypass, and sensitive information leakage. See CERT-EU’s SA 2024-072.

Apache HTTP Server Critical Vulnerabilities
On July 23, 2024, Apache issued an advisory about two critical vulnerabilities in its HTTP Server, CVE-2024-40725 and CVE-2024-40898. These vulnerabilities can lead to HTTP request smuggling and SSL client authentication bypass, potentially resulting in unauthorised access and other malicious activities. See CERT-EU’s SA 2024-073.

RADIUS Vulnerability Impacts Cisco Products
A critical vulnerability, identified as CVE-2024-3596, has been discovered in the RADIUS (Remote Authentication Dial-In User Service) protocol, allowing for man-in-the-middle (MitM) attacks that bypass authentication mechanisms. Dubbed the Blast-RADIUS attack, this vulnerability leverages an MD5 collision attack to forge authentication responses, potentially granting unauthorised access to network resources. In particular multiple CISCO products are impacted by this vulnerability. See CERT-EU’s SA 2024-074.

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.