Cyber Security Brief (March 2023)

April 3, 2023 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 317 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, in Europe, countries are taking action against TikTok on government devices, while law enforcement agencies target cybercriminal activities, with actions such as seizing Netwire RAT assets and arresting DoppelPaymer ransomware suspects. Additionally, new agencies are being established, like the UK's National Protective Security Agency, to counter cyber threats from countries like China. Outside Europe, Russia has banned foreign messaging apps in government organisations, advised officials against using iPhones due to security concerns, acquired a platform to identify anonymous Telegram users. Also in Russia leaked documents have exposed some of the country's cyberwarfare programmes. The US has released a new national cybersecurity strategy focusing on collaboration and shifting defence burden toward private vendors.
- On the **cyberespionage** front, in Europe, several threat actors of supposedly Chinese, Iranian, Russian, and North Korean origin were involved in activities targeting various European countries, organisations, and individuals. The attacks involved, among other techniques, custom malware, social engineering, and spearphishing and were linked to geopolitical goals and current conflicts. New activities attributed to private-sector offensive actors (PSOA) were also discovered.
- Relating to **cybercrime**, in Europe, based on information from data leak sites (DLS), the four most active ransomware operations have been Lockbit, Clop, Royal, and Vice Society. The most targeted sectors have been manufacturing, technology, construction and engineering, and retail, while the most affected countries have been Germany, the UK, Spain, France, and Italy.
- In Europe there were **data exposure and leaks** in the defence, banking, aerospace, hospitality, and retail sectors.
- On the **hacktivism** front, self-claimed pro-Russian groups NoName057(16) and Cyber Army of Russia conducted DDoS attacks on several websites associated with the Western military.
- Related to artificial intelligence, Europol warned of potential criminal use cases of ChatGPT, while a malicious version of the ChatGPT extension for Chrome was detected stealing Facebook session cookies, and Microsoft launched an AI-powered security analysis tool called Security

Copilot. Additionally, Italy's privacy regulator ordered a temporary ban on ChatGPT, citing privacy violations and blocking the processing of Italian users' data until OpenAI complies with the GDPR.

- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in March 2023.

Europe

Cyber policy and law enforcement

European Parliament decided on "kill switch" for smart contracts *Smart contracts*
The European Parliament has voted in favour of adding a "kill switch" to electronic smart contracts, which will allow the contract to be interrupted or stopped preventing accidental executions. The smart contracts must also have strict access control mechanisms. Smart contracts are typically used on platforms such as Ethereum for automatic execution of transactions based on predetermined conditions without intermediaries.

Norway accuses Iran of cyber actions in the country *Denunciation*
The Norwegian Police Security Service accused Iran, in the end of February, of intelligence activities targeting Iranian activists and dissidents in the country. The activities reported included intelligence gathering and surveillance.

TikTok faces bans and restrictions on government devices across European countries *Ban, Warning*
The UK, Denmark, Czech Republic, the Netherlands, Norway, Scotland, and France have taken action against TikTok and other apps on government devices due to security and data privacy concerns. While the UK, Denmark, and France have banned TikTok from government phones, the Czech Republic, the Netherlands, and Norway issued warnings against its use on devices with access to secure systems, and Scotland's Parliament members were encouraged to remove it. France went further by banning all recreational apps, including social media, gaming, streaming, and dating apps, on work phones for their civil servants.

Italian privacy regulator orders temporary ban on ChatGPT over privacy concerns *Ban*
Italy's privacy regulator ordered a temporary ban on ChatGPT, developed by OpenAI, for alleged privacy violations and blocked the processing of Italian users' data until the company respects GDPR.

Moldova bans Russian state-owned media outlet for disinformation *Ban*
Moldova's Security and Intelligence Service (SIS) has banned five online media outlets for spreading false information affecting the country's national security. The outlets are all divisions of the Russian state-owned Sputnik and offer news coverage in English, Russian, and Romanian.

UK agency for countering Chinese cyber activities *Cyber agency*
The UK domestic intelligence service, MI5, will direct the establishment of a new agency tasked to counter Chinese cyber activities. The agency, called the National Protective Security Agency (NPSA) is only one part of the UK government's updated security strategy, known as the "Integrated Review." The NPSA will provide cyber security training and advice to the private and public sector, will be working with the police in support of anti-terrorism actions, and will collaborate with other UK cyber security organisations.

Police operation seizes Netwire RAT assets *Arrests*
European law enforcement agencies, in cooperation with Europol, the US FBI, and Australian police managed to seize the hosting servers of the Netwire RAT and make one arrest in Croatia. Netwire was marketed as a legitimate "remote administration" tool but in fact it was used by cybercriminals to remotely control breached systems.

Doppelpaymer ransomware operation hit by law enforcement *Arrests*
In a combined operation, on February 28, law enforcement agencies from Germany and Ukraine, with support from Europol, the Dutch Police, and the US FBI, arrested suspected core members of the DoppelPaymer ransomware operation.

Ukrainian security service uncovers Pro-Russia bot farm *Takedown*
The Security Service of Ukraine (SBU) has uncovered and eliminated a bot farm using more than 2.000 bots promoting Russian interests. The bots were used to spread disinformation in the Russia-Ukraine war, promoting stories to discredit Ukraine's military and political leadership, and urging Ukrainians to avoid mobilisation. The SBU claimed that Russian security services were the primary customers of the bot farm.

UK law enforcement operation to identify DDoS actors *Law enforcement*
According to news reports on March 24, the UK's National Crime Agency (NCA) created multiple fake DDoS-for-hire websites to identify cybercriminals seeking to use these platforms to attack organisations. Thousands of users accessed the NCA's fake sites. The data collected will be shared with international law enforcement, and users based in the UK will be contacted by the NCA, while those abroad will have their data passed to corresponding law enforcement agencies.

Cyberespionage

Mustang Panda spying on European entities *Chinese threat actor*
The security company ESET released, on March 2, a report on observed activity by the threat actor Mustang Panda (a.k.a. Earth Peta, Temp.Hex, TA416, RedDelta). The activity started in January 2023 and took place all over Europe as well as in several places in Asia-Pacific. The campaign used a new custom backdoor named MQsTTang. In a distinct report released on March 23, TrendMicro analysed how Mustang Panda has been actively changing its tools and techniques to bypass security solutions.

Member of Parliament in Belgium victim of likely Chinese cyber attack *Chinese threat actor*
The Centre for Cyber Security Belgium (CCB) revealed that in January 2021, Belgian MP Samuel Cogolati was the target of a spearphishing attack. The attack followed Cogolati writing a resolution on the "crimes against humanity" faced by Uyghur Muslims in China. According to media sources, the CCB has attributed the attack to the China-linked APT31 threat actor.

Iranian threat group targeting women activists *Iranian threat actor*
The security company Secureworks Counter Threat Unit reported on March 9 that Iranian threat actors were targeting women involved in political affairs and human rights in the Middle East, in a social engineering campaign. The attackers were pretending to be from the US think tank The Atlantic Council. The activity was linked to the hacking group Charming Kitten (a.k.a. APT35, Phosphorus, TA453).

Winter Vivern global cyberespionage activity — *Russian or Belarus threat actor*

SentinelOne published a report on the activity of a threat actor they track as Winter Vivern. The threat actor has, since 2021, targeted governments in Poland, Lithuania, Italy, Slovakia, Ukraine, India, and the Vatican. The group has also focused on private businesses, including telecommunications organisations that support Ukraine in the ongoing war. SentinelOne assesses that Winter Vivern's activities are closely aligned with global objectives that support the interests of Russian and Belarusian governments.

TA473 cyberespionage activities in Europe and in the US — *Russian or Belarus threat actor*

Proofpoint reported cyberespionage-related activities by a threat actor codenamed TA473, including previously unreported targeting of US elected officials and exploitation of an unpatched Zimbra vulnerability to access emails of European government entities. TA473's activities align with Russian and Belarusian geopolitical goals related to the Russia-Ukraine War, as confirmed by SentinelOne analysis.

North Korea targets security researchers over LinkedIn — *North Korean threat actor*

On March 9, Mandiant reported that UNC2970A, a threat actor associated with North Korea, is targeting security researchers and media organisations in the US and Europe with fake job offers that lead to the deployment of three malware families. The threat actors use social engineering to convince their targets to engage over WhatsApp, where they drop the malware payload PlankWalk with the goal of establishing a foothold in the target's corporate environment.

New threat actor targeted government and transportation organisations in Ukraine — *Unattributed threat actor*

In October 2022, Kaspersky researchers discovered that government, agriculture, and transportation organisations in Donetsk, Lugansk, and Crimea regions were targeted in cyberattacks involving the PowerMagic backdoor and CommonMagic framework, executed by an unidentified threat actor dubbed Bad Magic APT. These attacks occurred amid the Russo-Ukrainian conflict, with victims compromised through spear-phishing or similar methods.

Polish authorities allegedly use Pegasus — *PSOA*

According to news sources, on March 3, the Polish intelligence services targeted a member of the opposition, the mayor of the Polish city of Sopot with the cyberespionage malware Pegasus. The reports mentioned the Central Anti-Corruption Bureau (CBA) of Poland as the ones accessing the target's mobile device. The phone number of the alleged target of the investigation was found between a list of surveillance targets available to researchers.

US citizen in Greece targeted by cyberespionage tool — *PSOA*

The New York Times reported, on March 20, that an American citizen who worked on Meta's security and trust team, based in Greece, was targeted with the cyberespionage tool Predator by the Greek intelligence service. Reportedly, the wiretap took place for several months in the second part of 2021 and in 2022. Interestingly, the sent infection SMS indicated knowledge of information kept in the state vaccine agency, while the infected URL mimicked that of the vaccination platform.

Cybercrime

Ransomware

Nevada group hackers deploy mass ransomware attack — *Multiple sectors*
According to several researchers, Nevada Group orchestrated one of the widest-ranging ransomware attacks on record. The cyberattacks are targeting cloud servers. Meanwhile, the anonymous hackers have demanded an unusually low ransom fee to release the files. The attack targeted various computer networks, gathering almost 5.000 victims in Europe and the US, including Hungarian and US universities, Italian construction and shipping firms, and German manufacturers.

Hospital in Spain severely disrupted by ransomware attack — *Healthcare*
The Hospital Clinic in Barcelona was the victim of a cyber attack linked to the Ransomhouse ransomware, on March 5. The incident severely impacted both the hospital, where all activities switched to pen and paper, and several primary care centres and research institutes that were co-hosting their IT infrastructure. The Catalonia government announcement mentioned that "the cyberattack occurred in virtualised environments. It was a sophisticated and complex attack that did not involve classic techniques, indicating an evolution by the attacker".

Hackers targeted Municipality of Taggia and claimed 700 GB stolen — *Local administration*
The threat actor RansomHouse has taken credit for a ransomware assault on the Italian town of Taggia. The group alleges to have acquired 700 GB of information, which they threatened to release publicly if their ransom demands are not met.

French city suffers ransomware — *Local administration*
On March 14, media reported that the French City of Mont-Saint-Martin had suffered a cyberattack. Personal data of staff and elected officials suffered unauthorised access.

Hacktivism

French National Assembly website attacked — *Parliament*
France's National Assembly website was temporarily blocked, on March 27, after a DDoS attack claimed by the pro-Russian hacker group NoName057(16). The group said the attack was a response to French policy on Russia's war on Ukraine as well as pension reforms. The group also stated they had also attacked the French Senate's website on the same day, although the latter remained operational.

Attacks on sites associated with Western militaries — *Military*
Between 23–24 March 2023, pro-Russia hacktivist groups NoName and Cyber Army of Russia claimed responsibility for DDoS attacks on at least 17 websites associated with the Western military alliance, Czechia, France, Japan, and Taiwan. The attacks were motivated by these countries' military aid to Ukraine and the anniversary of the alliance's military activity in the former Yugoslavia. The targeted websites experienced various degrees of disruption as a result of the attacks.

Information operations

Russia-aligned TA499 pursues targets with video call requests *Russian threat actor*
Proofpoint released a new analysis of TA499, (a.k.a. Vovan and Lexus), a Russia-aligned threat actor that has aggressively engaged in email campaigns since at least 2021. The threat actor reportedly attempts to convince high-profile Western government officials to participate in recorded phone or video calls. Proofpoint assesses that the calls are almost certainly a pro-Russia propaganda effort designed to create negative political content about those who have spoken out against Russian President Vladimir Putin and, in the last year, opposed Russia's invasion of Ukraine.

Data exposure and leaks

Claimed data from NATO and other organisations offered for sale *Defence*
A Twitter post, on March 8, claimed that information allegedly belonging to NATO, the Italian Ministry of Defence, the Philippine intelligence, and the MBDA defence company was up for sale at a cybercrime forum. The size of the data file for sale was at 50 GB

Aerospace manufacturer Safran suffers data leak *Aerospace*
According to reports on March 17, the French-based multinational aviation company Safran Group has left misconfigured systems for more than a year, which could have resulted in data leaks of sensitive information. The exposed information included security keys and credentials, which could have allowed attackers to gain access to the company's backend, employee systems, and other servers.

Deutsche Bank data breach *Banking*
On March 15, it was reported that data belonging to Germany's Deutsche Bank had been offered for sale on the dark web. The leaked information included personal data of customers and employees. The bank confirmed the breach and said they would investigate the matter.

Hotel guests information found online *Hospitality*
The personal data of 13.000 customers of the European hotel chain Falkensteiner was found online on an unprotected server. According to March 2 reports, the analysis showed that the data exposure was associated with the hotel's IT provider, Gustaffo.

Italian marketplace customer data leaked *Retail*
According to news reports, on March 2, the customer database of the Italian online marketplace FTDistribution, became available on the cybercriminal forum LeakBasea. The database contained personal data of about 40.000 users of the marketplace.

World

Cyber policy and law enforcement

The US, Turkey and New Zealand take action against TikTok *Ban*
The US House Foreign Affairs Committee has voted to give the President the power to ban TikTok from all US mobile devices and to impose a ban on entities transferring sensitive personal data to China. In addition, Turkey has fined TikTok for failing to protect users' personal data and New Zealand's Parliament has mandated the removal of TikTok from devices with access to their network due to associated risks.

Russia bans foreign messaging apps in government organisations *Ban*
Russia's internet supervision agency Roskomnadzor warned that laws banning the use of many foreign private messaging applications in Russian government and state agencies came into force on March 1. The laws prohibit Russian agencies from using information exchange systems owned by foreign entities. Restrictions extend to companies contracted for state projects.

Russia advises government officials against using iPhone for security concerns *Ban*
Russian presidential administration officials have been advised to stop using iPhones due to security concerns and were given until April 1 to switch to other smartphones. The Kremlin may purchase mobile devices for its employees, and Android OSs, Chinese-made devices, or phones using the Russian Linux-based smartphone operating system, Aurora OS, are recommended as alternatives to iPhones. The Kremlin's updated guidance is reportedly due to iPhones being more vulnerable to hacking and espionage by Western experts compared to other smartphones.

Russian state can identify Telegram users *Surveillance*
The Russian state-owned tech and defence corporation Rostec has reportedly acquired a platform that can reveal the identities of anonymous Telegram users. The tool uses over 700 data points to associate and correlate user information, potentially identifying users. Rostec intends to sell the tool to various departments of the Russian Ministry of Internal Affairs and the country's federal security service. Some experts speculated that the tool may utilise a zero-day vulnerability in Telegram or rely on an insider.

Leaked Documents from NTC Vulkan Expose Russian Cyberwarfare Capabilities and Ties to Intelligence Services *Capacities*
Multiple media outlets and cyber security companies have reported a leak of over 5.000 pages of documents from NTC Vulkan, a Moscow-based contractor, which reveal Russian cyberwarfare capabilities. The leaked information includes the existence of three programmes, Scan-V, Amesit, and Krystal-2B, which are tied to contracts with Russian intelligence services and have been used to support hacking operations, prepare for attacks on infrastructure, and spread disinformation.

New US national cybersecurity strategy has been released *Policy*
Washington's new cybersecurity defence plan focuses on shifting the burden of defending the country's cyberspace toward software vendors and service providers. It also acknowledges the collaboration between public and private sectors and with international allies and partners as essential for securing the nation against cyber threats.

US CISA starts ransomware programme *Ransomware*
In March, US Cybersecurity & Infrastructure Security Agency (CISA) announced the Ransomware Vulnerability Warning Pilot (RVWP) a new pilot programme to help critical infrastructure entities protect their information systems from ransomware attacks. As part of RVWP, CISA will proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks.

US law enforcement arrests cybercriminal *Arrests*

On March 15, Pompompurin, a cybercriminal devoted to breaching companies and selling or leaking stolen data has been arrested. He faces up to five years in prison for allegedly creating and administering a major hacking forum and marketplace called Breached, which sold direct access to over 14 billion compromised records across 888 datasets.

Cyberespionage

Chinese cyberespionage targeting Southeast Asian governments *Chinese threat actor*

The security company Check Point Research issued a report, on March 7, about cyberespionage attacks against Southeast Asian government entities, which they linked to advanced Chinese-backed threat actors. The technical analysis indicates similarity with activity seen since 2021, linked, with medium confidence, to Chinese-origin actors. The report also refers to Soul, a previously unattributed modular malware framework, in use since at least 2017.

China-linked Tick threat actor targets East Asian organisation *Chinese threat actor*

According to cyber security firm ESET, the APT group Tick compromised the internal update servers of an East Asian company that develops data-loss prevention (DLP) software, and used trojanized installers of legitimate tools to deliver malware and execute it on the computers of the company's customers.

Operation Soft Cell: Chinese hackers breach Middle East telecom providers *Chinese threat actor*

Chinese threat actor Gallium has been actively targeting telecommunications providers in the Middle East as part of a long-running espionage campaign dubbed "Operation Soft Cell", using web shells and stealing credentials with tools like Mimikatz. They are continuously maintaining and further developing their espionage malware arsenal, including a customised version of Mimikatz (mim221), with new anti-detection capabilities and leveraging the PingPull backdoor in their attacks.

Iran-linked threat actor impersonates US think tank in cyber attack *Iranian threat actor*

According to the cybersecurity company Secureworks, Iranian state-sponsored actors are continuing to engage in social engineering campaigns targeting researchers by impersonating a US think tank. Notably the targets in this instance were all women who are actively involved in political affairs and human rights in the Middle East region. Secureworks attributed the activity to a hacking group it tracks as Cobalt Illusion (a.k.a APT35, Charming Kitten).

APT group exploited a vulnerability in a tool used by a US Federal agency *Unattributed threat actor*

On March 15, US CISA reported that from November 2022 through early January 2023, a federal civilian executive branch agency suffered a cybersecurity incident. Analysts determined that multiple cyber threat actors, including an APT actor, were able to exploit a vulnerability in Progress Telerik user interface for ASP.

Chinese nuclear sector targeted *Unattributed threat actor*

The cyberespionage hacking group Bitter APT targeted the Chinese nuclear energy industry using phishing emails to infect devices with malware downloaders. Posing as the Embassy of Kyrgyzstan in China, the group sent emails to Chinese nuclear energy companies and academics, urging them to download a malicious attachment. Security company Intezer's analysts discovered the campaign and attributed it to Bitter APT based on tactics, techniques, and procedures consistent with past campaigns by the same threat actor.

TikTok trackers were found in US state government websites *Chinese tech*
According to a review conducted by the Wall Street Journal, TikTok trackers were found to be unknowingly embedded in US state government websites. These trackers are used to collect data from users who visit these websites and could potentially compromise user privacy. The report suggests that such trackers are commonly found on various websites and that they may be difficult to detect.

Chinese IT giant suspected of developing malicious Android applications *Chinese tech*
Android applications signed by China's PDD Holdings exploited a Zero-Day vulnerability (CVE-2023-20963) to access personal data, install malware, and control millions of mobile devices. Though PDD Holdings denies involvement, malicious versions of the Pinduoduo app were distributed through third-party app stores and have since been removed from Google Play Store.

Cybercrime

Ransomware

Conti-based ransomware 'MeowCorp' gets free decryptor *Decryptor*
Researchers at Kaspersky found a leak of decryption keys for a variant of Conti ransomware on a Russian-speaking forum. The variant was used in attacks against various private and public organisations over the past year by a ransomware group that some researchers track as MeowCorp. Kaspersky added the decryption code and the 258 private keys to its RakhniDecryptor, a tool that can recover files encrypted by more than two dozen ransomware strains.

Disruption of satellite services provider *Satellite services*
The Satellite broadcast provider, also active in TV broadcasting, Dish Network, disclosed, in a filing to the US Securities and Exchange Commission (SEC) that, on March 3, it had fallen victim to a ransomware attack. The incident caused disruptions to its services that lasted several days. The company also mentioned that information had been exfiltrated from its network on February 27.

FBI reveals 860 ransomware attacks against critical infrastructure *Critical infrastructure*
The US FBI revealed in its 2022 Internet Crime Report that ransomware attacks had breached the networks of at least 860 critical infrastructure organisations during that year.

Cl0p ransomware attacks several big companies *Enterprises*
The Cl0p ransomware group listed on its official leak site, on March 17, a total of 60 victim organisations, including the Shell Global in the energy sector, Bombardier Aviation, and several big universities in the US. Many of the samples of the alleged leaked files contained sensitive information from university students and customers and employees of the targeted companies.

Other cybercrime

Emotet botnet reactivated *Emotet*
Starting March 7, the operators of the Emotet botnet resumed their activities, engaging in phishing email campaigns, aiming to spread their malware. According to reports, in the first phase of reactivation, the threat actors were using phishing emails faking invoices.

IcedID malware evolution: discovering 'Forked' and 'Lite' variants *IcedID*

Proofpoint identified three distinct IcedID malware variants, including two new ones called "Forked" and "Lite." The new variants display key differences, such as the removal of banking functionalities, and are linked to different threat actors, with Emotet operators potentially using an IcedID variant with altered functionality.

Stealer attacking Facebook business accounts *Social media*

The security company Morphisec released a report, on March 7, on their findings about an advanced infostealer named "SYS01 stealer". The stealer was tracked since November 2022, targeting critical government infrastructure employees, manufacturing companies, and other industries. It was also used in a campaign targeting Facebook business accounts by using Google ads (malvertising) and fake Facebook profiles. The attack was designed to steal sensitive information, including login data, cookies, and Facebook ad and business account information.

Disruption and hijacking

Akamai blocks record DDoS attack in Asia *DDoS*

The content delivery network (CDN) company Akamai reported, in March that it had blocked the largest recorded DDoS attack in the Asia-Pacific region. The attack, which took place on February 23 reached 900,1 gigabits per second and 158,2 million packets per second. Akamai mentioned that they managed to maintain service to their customer during the attack.

Data exposure and leaks

Threat actor advertises 350 GB of law enforcement data *Public administration*

The US Marshals Service (USMS) says it was hit by a ransomware attack that exposed sensitive law enforcement data, including alleged witness security program information and personal information belonging to the targets of investigations. The agency discovered a "ransomware and data exfiltration event" on February 7, which had affected a system that was not connected to the federal network. The 350 GB of stolen information was posted on an underground forum, on March 15, by a Russian-speaking threat actor.

Data of one million customers of law firm leaked *Law*

On March 1, a North American law firm specialising in traffic offences was hit by the BlackCat ransomware. The threat actors claim to have stolen more than one million pieces of personal data, including scans of driver licences, full names, addresses and credit-card information.

Crime marketplace leaks credit card numbers *Credit cards*

The online credit card marketplace BidenCash leaked more than 2 million credit and debit card numbers in celebration of its one year of operations, in the beginning of March. A sampling of the cards showed that at least some of those had not been used before. The highest number of cards of European origin in the leak came from the UK and Italy. The leaked information also included user personal data exposing victims to phishing and identity theft.

Acer data offered for sale *IT manufacturing*

The Taiwanese IT equipment manufacturer Acer confirmed, on March 7, that data linked to them, offered for sale at an underground marketplace, was indeed the result of a February 2023 breach. The company denied that any customer data was affected. The data on offer amounted to 160 GB, claimed to be technical information.

Breach at healthcare provider leaks data of the US House of Representatives *Legislative body*

The US FBI was investigating, on March 8, a case of data leak affecting the US House of Representatives. The leak was due to a breach at the healthcare provider for the organisation's members, staff, and their families. The leak included account and personal data.

AT&T customer data leaked *Telecoms*

The US telecom company AT&T put out a notification to about 9 million of its customers, on March 9, that some of their information was leaked to an unknown threat actor. The leak was due to a breach, which happened in January, at one of AT&T's subcontractors, handling marketing. Data exposed had to do with Customer Proprietary Network Information, mainly referring to connection details.

Healthcare platform leaks data *healhtcare*

Cerebral, a healthcare platform sent personal data breach notifications to a reported 3,18 million people who have interacted with its websites, applications, and telehealth services.

Leaked Twitter code on GitHub *Social media*

Twitter's internal source code had become available online for several months before GitHub, where it was posted, complied with legal action to remove it. Twitter also used legal action to force GitHub to provide identifying information about the user that leaked its code and anyone who accessed or distributed it. The potential security risk posed by the leaked code remains unclear, but it could be scrutinised to find vulnerabilities in Twitter's platform.

Fourteen million customers impacted from data breach at Australian company" *Financial sector*

Latitude Financial Services, an Australian loan company, warned customers that their data breach has affected 14 million individuals, different than the initial estimate of 328.000. The breach occurred on March 16, 2023, when a cybercriminal accessed Latitude's customer data by stealing an employee's login and infiltrating two service providers.

Artificial intelligence

ChatGPT-4 amplifies misinformation more than its predecessor *Misinformation*

According to NewsGuard, a journalism and technology tool, ChatGPT-3.5 had been found to generate misinformation 80% of the time when prompted with 100 false narratives. Surprisingly, its successor, ChatGPT-4, had a poorer performance, advancing all 100 false narratives. This indicates a concerning increase in the AI's ability to spread misinformation.

Europol report highlights potential criminal use cases of ChatGPT *Malicious use*
Europol released a report highlighting several potential criminal use cases of ChatGPT. These include the creation of malicious code, the generation of fake news and disinformation, the creation of convincing phishing emails, the production of sophisticated and personalised scams, the development of deepfakes for use in cybercrime and fraud, and the production of highly realistic fake identities and forged documents. The report also noted that ChatGPT could be used to automate criminal activities such as social engineering and phishing attacks, allowing criminals to operate at a scale and efficiency previously impossible. The report concludes that law enforcement agencies must adapt and develop new tools and techniques to keep up with the evolving threat landscape presented by ChatGPT and other large language models.

Malicious ChatGPT Chrome extension hijacked Facebook accounts *Malicious use*
A malicious version of the ChatGPT extension for Chrome has been discovered on the Chrome Web Store, with over 9.000 downloads. The extension, which is promoted through Google Search advertisements, steals Facebook session cookies from users who install it, allowing the attackers to log in to their accounts and gain full access to their profiles.

AI used in a phone scam *Malicious use*
According to news reports, on March 6, an elderly couple in Canada, were scammed out of 21.000 dollars in a phone call allegedly using AI-generated voice. The artificial voice successfully faked the voice of the couple's son, indicating a high degree of sophistication.

Website impersonating OpenAI spreads malware *Malicious use*
A website impersonated OpenAI in order to spread a possible Rust loader disguised as a ChatGPT installer.

Microsoft launches AI-powered Security Copilot to accelerate incident response and threat hunting *Security assistant*
Microsoft has launched Security Copilot, an AI-powered security analysis tool that uses its threat intelligence footprint to help security analysts respond to threats quickly, process signals at machine speed, and assess risk exposure within minutes. It answers security-related questions through a ChatGPT-like interface, continuously learns from interactions, and integrates data and insights from other Microsoft security tools (including Sentinel, Defender, and Intune) to provide custom guidance for each organisation.

Significant vulnerabilities

RCE Vulnerability in Fortinet Products *Fortinet*
On March 7, 2023, Fortinet released an advisory regarding one critical vulnerability in FortiOS and FortiProxy administrative interface. This vulnerability is identified as "CVE-2023-25610" (CVSS score of 9.3) and it may allow remote unauthenticated attackers to execute arbitrary code on the device and/or to perform a DoS on the GUI. Fortinet was not aware of any instance where this vulnerability was exploited in the wild. See CERT-EU's SA 2023-015.

High Vulnerability in Veeam Backup & Replication *Veeam*
On March 8, 2023, Veeam released a new security advisory revealing one high vulnerability in a Veeam Backup & Replication component. This vulnerability is identified by "CVE-2023-27532" (CVSS score of 7.5) and it may allow an attacker to obtain encrypted credentials stored in the configuration database. This may lead to gaining access to the backup infrastructure hosts. It is highly recommended installing the latest version. See CERT-EU's SA 2023-016.

Severe Vulnerabilities in Jenkins Products *Jenkins*
On March 8, 2023, Jenkins released advisories regarding 2 severe security vulnerabilities in Jenkins server and Update Center. These vulnerabilities are identified by "CVE-2023-27898" and "CVE-2023-27905" and could allow an unauthenticated attacker to execute arbitrary code on the victim's Jenkins server, potentially leading to a complete compromise of the Jenkins server. Furthermore, these vulnerabilities could be exploited even if the Jenkins server is not directly reachable by attackers and could also impact self-hosted Jenkins servers. See CERT-EU's SA 2023-017.

Microsoft Outlook Elevation of Privilege Vulnerability *MS Outlook*
On March 14, 2023, Microsoft released a security fix for an elevation of privilege vulnerability ("CVE-2023-23397") in Microsoft Outlook. A specially crafted e-mail can trigger the vulnerability automatically when it is retrieved and processed by the Outlook client. Such an e-mail could lead to exploitation before the e-mail is viewed in the Preview Pane and allows an attacker to steal credential hashes by forcing the targets' devices to authenticate to an attacker-controlled server. The Computer Emergency Response Team for Ukraine (CERT-UA) reported the vulnerability to Microsoft. Based on Microsoft Threat Intelligence, a Russia-based threat actor used it in attacks to target and breach the network of several governments, military, energy, and transportation organisations in Europe between April and December 2022. They used the stolen hashes for lateral movement within the victims' networks and to change Outlook mailbox folder permissions for e-mail exfiltration. Online services such as Microsoft 365 do not support NTLM authentication and are not vulnerable to being attacked by these messages. See CERT-EU's SA 2023-018.

Several Critical Vulnerabilities in SAP Products *SAP*
On March 14, 2023, SAP released 19 patches for various products which contain five critical severity fixes for SAP Business Objects Business Intelligence Platform (CMC) and SAP NetWeaver: Improper Access Control in SAP NetWeaver AS for Java (CVE-2023-23857), Code Injection vulnerability in SAP Business Objects Business Intelligence Platform (CMC) (CVE-2023-25616), OS command execution vulnerability in SAP Business Objects Business Intelligence Platform (Adaptive Job Server) (CVE-2023-25617), Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform (CVE-2023-27269), and Directory Traversal vulnerability in SAP ERP and S4HANA (SAPRSBRO Program) (CVE-2023-27500). Due to the company's high global market share, SAP products are a valuable target for threat actors and criminals. Therefore, CERT-EU recommends applying the issued patches as soon as possible. See CERT-EU's SA 2023-019.

Remote Code Execution vulnerability in Windows HTTP protocol stack *MS Windows*
On March 14, 2023, Microsoft released a security fix for a vulnerability ("CVE-2023-23392") in the HTTP/3 protocol stack of Microsoft Windows Server 2022 and Windows 11 systems. This vulnerability allows a remote attacker to execute arbitrary code. Microsoft expects this vulnerability likely to be exploited soon. See CERT-EU's SA 2023-020.

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

1.

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