Cyber Security Brief (February 2023)

March 1, 2023 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 254 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement**, CERT-EU and ENISA have issued an alert on threat actors that pose a significant and ongoing threat to the European Union. The European Commission, as well as the US and Canadian governments announced a ban of TiTok from, respectively, corporate and government devices. The UK and US authorities are sanctioning cybercrime actors when they cannot directly arrest them, Japan is moving forward with its cybersecurity posture, Russia considers exempting hackers from prosecution, and Türkiye temporarily suspended Twitter to prevent the spread of anti-government sentiment.
- On the **cyberespionage** front, the most important development has been the leak of chip manufacturing data from the Duch ASML to China. Lazarus, an allegedly North Korean threat actor, targeted European research, while several groups attacked entities in South America, the Middle East and Asia.
- Relating to **cybercrime**, we continue to see ransomware activity both in Europe and elsewhere. In Europe, the three most active ransomware operations have been Lockbit, AlphV and BlackBasta. In the education and transportation sectors were especially targeted while the three most targeted countries were the UK, France and Italy. In other types of cybercrime, organisations in the US and Germany were targeted over a long period by the threat actor TA866, researchers detected a fake website resembling that of the Banque de France, AWS was targeted, and the GoDaddy web-hosting provider was breached.
- Regarding **data exposure and leaks**, notable cases were those of a UK hospital, three telecommunication companies (including one in Russia, that revealed signs of state surveillance), two social media platforms (including Reddit), as well as two video gaming companies (including Nintendo).
- Regarding **information operations**, researchers revealed that Iran was responsible for an influence operation on the French publication Charlie Hebdo and that an Israeli organisation was involved in disinformation operations targeting elections and politicians in Africa.
- On the **hacktivism** front, the most notable case has been that of Anonymous Sudan targeting several Swedish entities over a number of days. We also saw several DDoS attacks related to

self-claimed pro-Russia hacktivist groups against the websites of entities in Poland, Slovakia, Sweden, Germany, Latvia, Austria, Lithuania, France, Italy, as well as NATO offices. In the rest of the world, an Iranian hacktivist group disrupted the transmission of the broadcasting of the speech of Iran's President and a supposed anti-Russia hacktivist group released documents linked to Wagner group.

- Regarding **disruptive** operations, the Police site at a German region became unavailable after a DDoS and Cloudflare reported seeing the biggest DDoS attack to date.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in February 2023.

Europe

Cyber policy and law enforcement

CERT-EU and ENISA alerted on sustained activity by particular threat actors *Warning*
On February 15, The European Union Agency for Cybersecurity (ENISA) and the CERT of all the EU institutions, bodies, and agencies (CERT-EU) jointly published a report to alert on sustained activity by particular threat actors. The malicious cyber activities of the presented threat actors pose a significant and ongoing threat to the European Union. Recent operations pursued by these actors focused mainly on information theft, primarily via establishing persistent footholds within the network infrastructure of organisations of strategic relevance.

European Commission bans TikTok from corporate devices *Ban*
In a press release published on February 23, the European Commission announced that, "to increase its cybersecurity, the Commission's Corporate Management Board has decided to suspend the use of the TikTok application on its corporate devices and on personal devices enrolled in the Commission mobile device service."

Police hacked Exclu 'secure' message platform to spy on criminals *Dismantlement*
The Dutch police announced on February 3 that they dismantled the Exclu encrypted communications platform after hacking into the service to monitor the activity of criminal organisations. The operation consisted of two separate investigations starting in September 2020 and April 2022. Eurojust, Europol, and the police forces in Italy, Sweden, France, and Germany assisted in the law enforcement operations. Forty-two persons have been arrested.

Europol dismantles cybercrime group *Dismantlement*
Europol dismantled a Franco-Israeli group that employed business email compromise attacks to divert payments from organisations to bank accounts under the threat actor's control.

Hacker of Finnish psychotherapy centre arrested *Arrest*
The French police has arrested a Swedish hacker suspected of being part of an extortion scheme targeting a Finnish psychotherapy practice and its patients. He was accused of participating in the hacking of the Vastaamo psychotherapy centre, in October 2020.

Joint Spanish US operation against scammers *Arrest*
The Spanish police cooperated with US authorities in an operation that led, on February 13, to the arrest of nine individuals accused of participating in a cybercrime organisation committing financial fraud. Their activities had resulted in the loss of more than 5 million dollars, mainly in the US.

Dutch police arrest cybercriminals *Arrest*

On February 23, the Dutch police announced that it had arrested three individuals for alleged involvement in cybercrime. The Police's cybercrime team started the investigation in March 2021 in response to a declaration of data theft and threat to a large Dutch company. The group is allegedly responsible for extorting cryptocurrency worth 2,5 million euros from small and large organisations in multiple countries.

US and UK sanction TrickBot operation members *Sanction*

The US Department of the Treasury and UK authorities issued sanctions, on February 9, against nine Russians for their alleged participation in the Trickbot cybercrime group. TrickBot malware was used to support attacks by the Conti and Ryuk ransomware operations. According to authorities, the members of the group have ties with the Russian intelligence services. The Trickbot ransomware targeted in the past hospitals, companies and the US government.

Norwegian police seizes assets from cybercrime heist *Seizing*

Norwegian police have seized 60 million Kroner worth of cryptocurrency. The cryptocurrency was stolen by the North Korean group Lazarus, in 2022 from Axie Infinity's Ronin Bridge.

Cyberespionage

Lazarus stole research data in two-month-long breach in 2022 *North Korean threat actor*

According to Finland-based security firm WithSecure, the likely North Korean threat actor Lazarus executed a new cyberespionage campaign dubbed No Pineapple. This operation lasted between August and November 2022, targeting organisations in medical research, healthcare, chemical engineering, energy, defence, and a leading research university. The threat actors stole 100 GB of data from the victim without causing any destruction.

Chip equipment manufacturer reports stolen data *Chinese threat actor*

The Dutch chip equipment manufacturing company ASML, which is considered in the industry to be a critical part of the international computer chip supply chain, reported, on February 15, that an employee in their Chinese offices had stolen information about its technology. Although the company characterised the data stolen "non-critical", it had to report theft to US and Dutch authorities as it would mean violations of export controls. Additional details revealed by the press showed that the stolen information came from a system used to manage product development and involved technological information on chip manufacturing.

Cybercrime

Ransomware

Ransomware breach hit Irish university campuses — *Education*

In Ireland, the Munster Technological University (MTU) disclosed a ransomware incident affecting all four campuses in the county of Cork. MTU IT personnel discovered a ransom note embedded in an affected server. According to a university official, MTU has full backups and has not engaged with the ransomware operators. On February 13, the operators of the AlphV ransomware said they had managed to steal 6 GB containing personal information of MTU staff and students.

Harz University offline after cyberattack — *Education*

According to German news sources, dated February 2, the Harz University of Applied Sciences was targeted by a cyberattack. A university spokeswoman said the university shut down all computer systems as a precaution.

Cyberattack on Acea by BlackBasta Ransomware — *Energy*

Acea, an Italian public holding company that provides energy and other services to the city of Rome, suffered a ransomware cyberattack, claimed by the cybercriminal group BlackBasta. Although the company reported it suffered damages from the attack, it also stated that these had no effect on the essential services provided to users.

Italian hospital hit by RansomHouse — *Healthcare*

The ransomware group RansomHouse announced they had attacked the Italian hospital HS Hospital Service SpA, on February 14. They also claimed they had managed to steal 50 GB of the data from the victim's systems.

Cyberattack against the Reunion University Hospital — *Healthcare*

According to a report dated February 8, an attack targeted the main hospital in the French overseas territory of Reunion. The cyberattack was detected early and allowed the University Hospital to take appropriate measures to protect the continuity of operations, the data, and the IT tools.

Italian social security organisation hit in ransomware attack — *Social security*

The operators of the LockBit 3.0 ransomware claimed on February 14 to have breached the Italian social security organisation cassaragionieri.it. The full extent of the attack could not be confirmed but data leakage and encryption of the organisation's systems were possible.

Data of Belgian town citizens leaked — *Public administration*

News media reported on February 15 that cybercriminals leaked personal data of citizens of the Belgian town of Geraardsbergen. The data had reportedly been stolen in a September 2022 attack by an unspecified ransomware operator.

Lockbit threatens Portuguese water company with double extortion — *Drinking water*

On February 20, reports mentioned that LockBit had compromised Aguas do Porto, a Portuguese municipal water company. Lockbit threatened to release exfiltrated data on March 7. Although the organisation's services were impacted by the cyberattack, water supply and sanitation were not affected.

French defence and space systems maker allegedly breached — *Aerospace*

The Snatch ransomware operation claimed the breach of France-based aerospace company Hemeria Group. The company is a partner of the French Space Agency CNES.

Other cybercrime

Threat actor targets high-value organisations with malware *Germany*
According to Proofpoint, since October 2022 and continuing into January 2023, a financially motivated threat actor tracked as TA866 has targeted organisations mainly in the US and Germany. TA866's attack chain starts with an email containing a malicious attachment or URL and leads to malware that Proofpoint dubbed WasabiSeed and Screenshotter.

Enigma stealer targets cryptocurrency industry with fake jobs *Eastern Europe, Cryptocurrency*
Researchers from Trendmicro reported about an active campaign that uses a fake employment lure to target Eastern Europeans in the cryptocurrency industry. The attackers, suspected of being Russian threat actors, aimed to install an information stealer dubbed Enigma.

Site faking Banque de France *National Bank*
According to news reports, on February 13, cybercriminals had created a fake website resembling that of the Banque de France. The objective of the operation was to steal the credentials of the customers of nine French banking companies.

Hacktivism

Anonymous Sudan DDoS Swedish websites *Sweden*
On February 8, the hacktivist group Anonymous Sudan claimed DDoS attacks against the websites of 22 airports in Sweden. The group announced the attack on their Telegram channel and posted a picture of an aeroplane—engulfed in flames—flying. Text below the image reads: "The Infrastructure of Sweden airports has been down because of their burning of the Quran". On February 10, Anonymous Sudan also claimed DDoS attacks against hospitals in Sweden. The attacks continued on February 14, targeting the aviation, academic, and media sectors. Also, on February 15, the Sweden-based Scandinavian Airlines (SAS) disclosed that the airline had disruptions to its website and mobile app, an incident for which Anonymous Sudan took responsibility. SAS also posted a notice, on February 16, that the cyberattack had caused malfunctions that exposed customer personal data. According to news reports on February 16 Anonymous Sudan claimed to have carried a cyber attack on the Ängelholm-Helsingborg airport in Sweden.

Pro-Russia hacktivists DDoS in Poland *Poland*
On February 4, pro-Russia hacktivist groups, including Usersec, affiliated with the Killnet group, and Mistnet, conducted DDoS attacks against the banking sector in Poland. On February 14, the pro-Russia hacktivist group Noname057(16) announced on Telegram that they had carried out a DDoS attack against the portal of the highest administrative court in Poland. On February 20, the hacker group Anonymous Russia claimed a series of DDoS attacks against airports in Poland.

Pro-Russia hacktivists DDoS in Slovakia *Slovakia*
On February 16, NoName057(16) claimed a DDoS attack against the website of the Ministry of Internal Affairs of the Slovak Republic. The attack followed the recognition by the Parliament of Slovakia of Russia as the "sponsor of terrorism".

Pro-Russia hacktivists DDoS in Sweden *Sweden*
On February 6, the pro-Russia hacktivist group Killnet launched a series of DDoS attacks against the official website of the Swedish Financial Supervisory Authority which is the governmental authority for financial regulations. On February 8, Noname057(16) claimed DDoS attacks against the website of the Swedish company System Bolaget which is an alcohol retailer. On February 9, Noname057(16) claimed DDoS attacks against the main website of the Swedish Research Institute.

Killnet targets German airports with a large DDoS attack *Germany*
On February 16, Killnet reportedly managed to disable the information system of the German airline Lufthansa. The group claimed their actions were in retaliation for the supply of Leopard tanks to Ukraine. All flights and landings at Frankfurt airport were reportedly suspended, and the flight schedule to Munich was also affected, causing numerous delays and manual check-in.

Pro-Russia hacktivists DDoS in Latvia *Latvia*
On February 4, pro-Russia hacktivist groups, including Usersec, affiliated with the Killnet group, and Mistnet, conducted DDoS attacks against the banking sector in Latvia. On February 14, Noname057(16) announced on Telegram that they had carried out a DDoS attack against the website of the Latvian National Defence Academy.

Pro-Russia hacktivists DDoS in Austria *Austria*
On February 8, Noname057(16) claimed DDoS attacks against the website of the Austrian Ministry of Labour and Economy. The attacks were claimed to be in retaliation for the Austrian government opposing Russian and Belarusian participation in the 2024 Olympics.

Pro-Russia hacktivists DDoS Lithuanian airports *Lithuania*
On February 12, Noname057(16) launched a campaign of DDoS attacks against airports in Lithuania.

Pro-Russia hacktivists DDoS in France, Italy and Germany *France*, *Germany*, *Italy*
On February 21, NoName057(16) claimed DDoS attacks against France, Germany, and Italy. The victims were reportedly mainly organisations in the defence sector.

Killnet DDoS NATO websites *NATO*
On February 12-13, the pro-Russia hacktivist entity Killnet and affiliates claimed DDoS attacks against at least 15 public-facing websites and subdomains belonging to NATO. On February 12, the alliance acknowledged some of its sites were “experiencing availability issues” and stated that classified networks were not attacked.

Information operations

Iran responsible for Charlie Hebdo attacks *Media*, *Iranian threat actor*
On February 3, Microsoft attributed a recent influence operation targeting the French satirical magazine Charlie Hebdo to an Iranian nation-state actor. In early January, an online group calling itself Holy Souls, which Microsoft identifies as Neptunium, claimed they had obtained personal information of more than 200.000 Charlie Hebdo customers after “gain[ing] access to a database”. This information, obtained by the Iranian actor, could put the magazine’s subscribers at risk of online or physical targeting by extremist organisations.

Disruption and hijacking

DDoS for hire used in hacktivist attacks *DDoS-as-a-Service*
According to news reports, on February 2, a newly created platform that sells DDoS attack services to threat actors was used in January Russian-linked hacktivist attacks against healthcare institutions in Europe and the US. The DDoS-as-a-Service (DDoSaaS) platform is called ‘Passion’ and is active since January 2023.
***Analyst note**: This is a departure from the typical practice of self-proclaimed hacktivist groups, who usually depend on members’ efforts rather than paid services.*

German regional police site disrupted *DDoS, Police*
According to news reports, on February 1, the website of the Baden-Württemberg police, in Germany was unreachable, due to a cyber attack, likely a DDoS. There was no immediate claim of the attack by any hacktivist group or other threat actors.

Data exposure and leaks

Personal data exposed by NHS hospital in Liverpool *Healthcare*
A UK National Health Service (NHS) hospital in Liverpool revealed that sensitive payroll information belonging to roughly 14.000 employees was exposed after a spreadsheet containing the information was distributed to hundreds of NHS managers and some 24 external accounts.

German spa company database has been leaked *Healthcare*
According to a report dated February 26, the cybercriminals claim to have put the database of the German spa company online. The data is said to be contained in an SQL file of approximately 20 GB and contains user IDs, e-mail addresses and locations.

World

Cyber policy and law enforcement

Japan's cybersecurity posture *Capacity building, Cooperation*
On January 31, the Japanese government announced two measures to bolster its cybersecurity posture: the creation of a working group that examines the adoption of offensive cyber operations and the announcement of greater cyber coordination with NATO.

US and Canada ban TikTok from all government-issued devices *Ban*
On February 27, in the US, the White House directed federal agencies to remove TikTok from all government-issued devices within 30 days. The same day, the Canadian government announced a similar ban on TikTok from official electronic devices.

Russian Duma discusses legislation to not punish Russian hackers *Criminal immunity*
According to Russian media reports, in February, the Russian State Duma Committee on Information Policy, Technologies, and Communications began discussing the issue of exempting hacktivists acting in Russian interests from legal liability. While no legislation has been proposed, committee head Alexander Khinshtein stated the exemption could apply to Russian hacktivists working in Russia and also abroad.

Twitter restricted in Türkiye after earthquake *Internet control*
Network data confirmed the restriction of Twitter on multiple internet providers in Türkiye as of February 8 following protests about the handling of the situation after the February 6 earthquake. Although no formal explanation was provided, the incident came as authorities had raised concerns over disinformation online. Twitter disruptions were distinct from those caused by earthquake damage to infrastructure and were implemented by intentional filtering at the ISP level. According to media reports, access to Twitter in Türkiye was restored on February 9.

Iranian nation-state group sanctioned by US *Name and shame*
The US Government said the Iranian Neptunium APT group was responsible for an early January 2023 attack that hit French satirical magazine Charlie Hebdo. Reports also showed that in January 2022, the US FBI linked Neptunium to a "sophisticated influence campaign" that was designed to interfere with the 2020 US presidential election.

US NIST selects lightweight cryptography algorithm for IOT devices *Cryptography*
The US National Institute of Standards and Technology (NIST) selected a group of cryptographic algorithms dubbed Ascon to be its standard for lightweight cryptography in small internet-of-things (IOT) devices such as medical equipment, stress detectors, and keyless fobs.

NY attorney general forces spyware vendor to alert victims *Fine*
The New York attorney general's office has announced a fine of 410.000 dollars for a developer of software for stalking. The convicted individual used 16 companies to illegally promote surveillance tools.

Russian cybercrime actor found guilty in US court *Conviction*
A Russian national was found guilty in a US court for participating in a global cybercrime scheme which stole confidential earnings reports. Knowledge of these reports helped the criminals gain 90 million US dollars.

Russian cybercriminal extradited to US *Extradition*
On February 22, the US Department of Justice announced that a Russian national was extradited to the US for his alleged role in developing, selling, and using the brute-forcing malware program NLBrute.

US indicts four in DeFi Ponzi scheme *Indictment*
A US Federal grand jury in the District of Oregon indicted four Russians who reportedly founded Forsage, a decentralised finance (DeFi) cryptocurrency investment platform. The accused were allegedly running a global Ponzi and pyramid scheme that raised 340 million US dollars.

Cyberespionage

Chinese threat actor targeting South America *Chinese threat actor*
Microsoft reported on February 13 that the China-based cyber espionage actor tracked as DEV-0147 was observed compromising diplomatic targets in South America. This was characterised as a notable expansion in the group's operations, typically seen targeting government agencies and think tanks in Asia and Europe.

Earth Kitsune targeting North Korea *Unattributed threat actor*
On February 17, Trendmicro published details about a new backdoor which they attribute to Earth Kitsune, an APT group. According to Trendmicro, Earth Kitsune has targeted individuals who are interested in North Korea since 2019.

WIP26 a new espionage cluster targeting Middle Eastern telco *Unattributed threat actor*
On February 16, SentinelOne reported that they are tracking WIP26, a new cyberespionage threat cluster which has been targeting telecommunication providers in the Middle East. WIP26 relies on cloud infrastructure such as Microsoft Azure and Dropbox attempting to evade detection by making malicious traffic look legitimate.

Remote access tool used to spy on Armenia *Unattributed threat actor*
On February 16, researchers at CheckPoint published details about cyberespionage activity targeting Armenia. The identified malware distributed in this campaign is a new version of a backdoor tracked as OxtaRAT, an AutoIt-based tool for remote access and desktop surveillance.

Cybercrime

Ransomware

LockBit ransomware uses new Conti-based encryptor *Encryptor*
According to researchers, the LockBit ransomware operation has again started using encryptors based on other operations. It has switched to an encryptor named LockBit Green which is based on the leaked source code for the now-disbanded Conti ransomware. Since its launch, the LockBit operation has gone through numerous iterations of its encryptor, starting with a custom one and moving to LockBit 3.0 (aka LockBit Black).

ION suffers ransomware attack on derivatives platform *Finance*
ION Markets, a trading technology provider for financial institutions, suffered a LockBit ransomware attack on February 1. The attack impacted overnight trade processing as well as some of the derivatives services.

US satellite broadcast company confirms ransomware attack behind multi-day downtime *Satellite broadcast*
Dish Network, a US-based satellite broadcast provider and TV, confirmed that a ransomware attack was the cause of a multi-day network and service downtime that started on February 24.

ESXi ransomware campaign strikes Florida Supreme Court *Justice*
A spokesperson for the Florida Supreme Court disclosed the institution had suffered an attack by ransomware exploiting the ESXi vulnerability. Infrastructure affected was used to support the Florida state court system. The spokesperson, however, insisted that this was “segregated” from the Supreme Court’s main networks and as such the integrity of the state court system has not been compromised.

Canadian hospital victim of suspected ransomware *Healthcare*
On February 5, Ross Memorial Hospital located in the Canada suffered a cybersecurity incident that disabled critical diagnostic systems and access to medical files. The hospital declared a Code Grey — an emergency code initiated following the loss of a critical operating system.

North Korean threat actors targeting healthcare with ransomware *North Korean threat actor, Healthcare*
The US cybersecurity agencies (CISA, FBI, and NSA) published a joint advisory to highlight techniques, tactics and procedures (TTP) “DPRK cyber actors used to gain access to and conduct ransomware attacks against Healthcare and Public Health (HPH) Sector organisations and other critical infrastructure sector entities”. According to the US agencies, DPRK cyber actors demand ransoms which help to fund other malicious cyber activities.

Other cybercrime

Phishing targeting AWS logins — *Cloud services*
According to Sentinel Labs, a new phishing campaign, targeting Amazon Web Services (AWS) logins, is abusing Google ads to sneak phishing sites into Google Search to steal victims' login credentials.

GoDaddy suffers source code leak — *Web-hosting*
GoDaddy, a web-hosting service, reported that it experienced a data breach following a multi-year attack. Its source code was exfiltrated and malware was installed on its servers following the compromise of its cPanel shared hosting environment.

US citizens lose 8,8 billion US dollars to scams — *Fraud*
On February 23, the US Federal Trade Commission revealed that US citizens lost almost 8,8 billion US dollars to various types of scams in 2022, following a significant surge of over 30% more lost to fraud compared to the previous year.

Hacktivism

Hacktivists claim hack-and-leak of Wagner Group — *Private military contractor*
Bogatyri, a supposed anti-Russia hacktivist group, published 2000 documents allegedly belonging to Wagner Group. Two media outlets and an advocacy group authenticated the documents.

Hacktivists hijack Iranian president's speech — *TV, Radio*
According to news reports, the Iranian hacktivist group Ali's Justice (Edalat-e Ali) disrupted the transmission of the speech of Iran's President over an Iranian State TV channel and a radio station, on February 11. The group aired anti-government messages instead.

Hacktivists claim attack on airport — *Aviation, Media, Commerce*
A self-claimed hacktivist group Al-Toufan, or "The Flood" in Arabic, said they took down the websites of Bahrain's international airport, state news agency and chamber of commerce, on February 14, to mark the 12-year anniversary of an Arab Spring uprising in the country.

Information operations

Israeli organisation involved in Africa disinformation — Disinformation
An organisation referred to as Team Jorge, based in Israel, is reportedly involved in manipulating elections and hacking African politicians. This entity offers its clients smear campaigns and disinformation on-demand, ranging from hacking email boxes to spreading rumours through fake news sites and armies of fake profiles on social networks.

Disruption and hijacking

Cloudflare blocks record DDoS attacks *DDoS*
The cloud services provider Cloudflare reported that it had blocked some of the largest (by volume) DDoS attacks to date, between February 11 and 12. The attacks ranged between 50 and 70 million requests per second (rps) with the largest exceeding 71 million rps. According to the company, this was one of the largest reported HTTP DDoS attacks on record, more than 35% higher than the previous reported record of 46M rps in June 2022. The targets of the attacks were cloud computing platforms, cryptocurrency firms, and hosting providers.

Data exposure and leaks

Google Fi data breach let hackers carry out SIM swap attacks *Telecommunications*
Google Fi, Google's US-only telecommunications and mobile internet service, informed customers that personal data was exposed by a data breach at one of its primary network providers. Some customers were warned that information leaked could allow SIM swapping attacks.

Anonymous leaked data from Russian ISP shows state surveillance *Telecommunications*
The anonymous collective leaked 128 GB of data stolen from the Russian Internet Service Provider (ISP) Convex. The stolen documents contain evidence of surveillance activity conducted by the intelligence service FSB. According to the data available, Convex launched a project that aims to spy on Russian citizens by using surveillance equipment. The warrantless surveillance of Russian citizens violates their rights and the country's laws.

Canadian telco suffers potential employee data leak *Telecommunications*
The Canadian Telecommunications company Telus reported that it is investigating a potential personal data breach after a threat actor shared samples online of what appears to be employee data.

Nitendo breached *Gaming*
An unknown individual claimed to have hacked into Nintendo's developer portal, gaining access to more than 50 GB of data that allegedly included back-end code, source code, documents, tools, and more.

Video game maker suffers source code exposure *Gaming*
The video game maker Activision confirmed that it suffered a data breach in December 2022 after one of its employees fell victim to SMS phishing. The organisation confirmed that they responded to an incident on December 4 and that the incident did not expose game source code or player details. The leaked data consists of 19.444 unique records containing personal data of Activision employees.

PeopleConnect confirm data breach affecting 20 million customers *Social media*
PeopleConnect, the owners of the TruthFinder and Instant Checkmate background check services, confirmed they suffered a data breach after hackers leaked a 2019 backup database containing the information of millions of customers.

Reddit breached *Social media*
The social news aggregation platform Reddit disclosed that in a security incident, on February 5, its systems had been breached by unidentified threat actors. The impact of the attack was access to a number of business systems and the leakage of internal documents and code. The company noted that there were no indications that user data had also been accessed.

Misconfigured US military server exposed emails to the internet *Military*
According to media reports on February 20, the US Department of Defense secured a server that due to a misconfiguration had been exposing internal US military emails to the open internet for two weeks. A security researcher identified and reported the exposed server. The US authorities confirmed that the leak was not the result of a breach.

News Corp had state hackers on its network for two years *Media*
The mass media and publishing giant News Corporation (News Corp) disclosed on February 25 that attackers behind a breach disclosed in 2022 had first gained access to its systems two years before, in February 2020. The incident affected multiple news arms of the publishing conglomerate. Earlier, News Corp has associated the attackers with a "foreign government", and mentioned they had exfiltrated some data during the time they had access to its systems.

Significant vulnerabilities

Critical security flaw in Jira Service Management Server and Data Center *Jira*
A critical security flaw has been discovered in Jira Service Management Server and Data Center that can be exploited by an attacker to impersonate another user and gain unauthorised access to instances. The vulnerability is tracked as "CVE-2023-22501" with a CVSS score of 9.4. See CERT-EU's SA 2023-006.

High severity vulnerability in OpenSSL *OpenSSL*
The OpenSSL project team has released a major security update to address 8 vulnerabilities. One vulnerability, tracked as CVE-2023-0286 and rated as High, may allow a remote attacker to read arbitrary memory contents or cause OpenSSL to crash, resulting in a denial of service. See CERT-EU's SA 2023-007.

Vulnerability in OpenSSH *OpenSSH*
The development team of the OpenSSH suite has released the version 9.2 to address several security vulnerabilities, including a memory safety bug in the OpenSSH server ("sshd") tracked as CVE-2023-25136. This vulnerability can be exploited by a remote attacker to execute arbitrary code on the target system. See CERT-EU's SA 2023-008.

Multiple critical vulnerabilities in Microsoft products *Microsoft*
On February 14, Microsoft released its February 2023 Patch Tuesday advisory disclosing 75 vulnerabilities, including 3 exploited zero-day vulnerabilities identified with "CVE-2023-21823", " CVE-2023-21715" and "CVE-2023-23376", which affect respectively Windows Graphics Component, Microsoft Publisher and Windows Common Log File System Driver. Microsoft patched additional three remote code execution Exchange Server flaws (CVE-2023-21706, CVE-2023-21707, and CVE-2023-21529) that are likely to be exploited, but an authentication is required. It is highly recommended patching affected devices. See CERT-EU's SA 2023-009.

Severe vulnerabilities in Citrix Workspace, Virtual Apps and Desktops *Citrix*
On February 14, 2023, Citrix released Security Bulletins regarding severe vulnerabilities affecting its Citrix Workspace, Virtual Apps and Desktops. If exploited, these vulnerabilities could enable attackers to elevate their privileges and take control of the affected system, but they need local access to the target. It is then highly recommended to install the last security updates. See CERT-EU's SA 2023-010.

ClamAV critical vulnerability *ClamAV*
On February 15th, 2023, ClamAV informed about a critical vulnerability in the cross-platform antimalware toolkit. The vulnerability is identified as "CVE-2023-20032" and could lead to remote code execution. See CERT-EU's SA 2023-011.

RCE vulnerabilities in Fortinet products *Fortinet*
On February 16, 2023, Fortinet released advisories regarding critical vulnerabilities in FortiNAC and FortiWeb products that may allow unauthenticated attackers to perform remote arbitrary code or command execution. The first vulnerability identified as "CVE-2022-39952" (CVSS score of 9.8) and is related to the FortiNAC product. FortiNAC is Fortinet's network access control solution that enhances the Security Fabric. It also provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events. The second vulnerability identified as "CVE-2021-42756" (CVSS score of 9.8) and is related to FortiWeb products. FortiWeb is a web application firewall (WAF) that protects web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations. See CERT-EU's SA 2023-012.

Critical SQL injection vulnerabilities in MISP *MISP*
On February 20, 2023, the MISP project team released advisories regarding 2 critical SQL injection vulnerabilities in MISP Threat Intelligence and Sharing Platform. The team decided to follow a silent fix procedure, releasing several updates in November and December 2022, giving enough time to users to update their instances to a safe version. See CERT-EU's SA 2023-013.

Critical vulnerabilities in VMware products *VMware*
On February 21, 2023, VMware released several advisories regarding critical vulnerabilities affecting Carbon Black App Control and VMware vRealize tools. The first vulnerability is identified as "CVE-2023-20858" (CVSSv3 score of 9.1) and impacts several versions of Carbon Black App Control for Windows. The second vulnerability is identified as "CVE-2023-20855" (CVSSv3 score of 8.8) and impacts VMware vRealize tools and VMware Cloud Foundation. See CERT-EU's SA 2023-014.

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.

TLP	Disclosure	Message
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.