Cyber Security Brief (December 2022)

January 3, 2023 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 271 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement**, in Europe and in the US, there were developments in the use of post-quantum cryptography, with authorities testing such technologies or pushing for their use. Japan issued a new national security strategy, which includes the option for offensive cyber operations. US legislators discussed circumstances for banning foreign social media companies. Greece banned commercial spyware. Law enforcement operations targeted miscellaneous cybercrime activities such as identity theft, voice phishing, carding, money laundering, call centres defraud, and SIM swapping.
- On the **cyberespionage** front in Europe, the Cloud Atlas threat actor has narrowed significantly its targeting, with a clear focus on Russia, Belarus, and conflicted areas in Ukraine and Moldova. Globally, researchers published their assessments of Chinese threat actors[1] targeting human rights activists and telecom companies, Iranian threat actors[1] focusing on journalists and activists and a North Korean adversary[1] exploiting a zero-day vulnerability against South Korean users.
- Relating to **cybercrime**, ransomware continues to be a prime area of activity. In Europe, adversaries targeted entities in the healthcare, transportation, education, media, energy, and administration sectors. The top four most active ransomware operations were Play, BlackBasta, Lockbit and Vice Society; the top four most targeted sectors were technology, education, construction & engineering, and automotive. On the global level, a major ransomware operation has switched to a new custom encryptor, while another has introduced a new extortion tactic (cloning a victim's website to leak stolen data). The Lockbit operation apologised for targeting a hospital.
- Regarding **data exposure and leaks**, a number of data disclosures or breaches impacted some high-profile organisations in the IT (password management), social media, healthcare, transportation, law enforcement, banking, and professional services sectors.
- In the area of **information operations**, Meta revealed that since 2017 it had taken down 200 covert influence operations across 42 different languages.

- On the **hacktivism** front, the main activity in Europe and Russia was linked to Russia's war in Ukraine. The activity was linked to DDoS or other attacks in at least 14 European countries. In particular, there was a claim of DDoS attacks against the websites of the ministries of defence in 9 countries.
- We have included several significant vulnerabilities and associated advisories, reported in December 2022.

Europe

Cyber policy and law enforcement

France announces training program for hospital staff to guard against cyberattacks *Capacity*
The French Ministers of Health, Digital Transition, and the Interior issued a joint statement announcing future efforts to prevent cyberattacks against hospitals. The French government plans to invest 1 billion euros to strengthen cybersecurity programs in the healthcare sector and launch a cyber preparedness training program for all the highest priority healthcare providers, to be completed by May 2023. Additionally, the government has assembled a task force to create a cybersecurity plan within the 2023–2027 digital health roadmap; the plan is to be drafted by March 2023.

France announces use of post-quantum cryptography for diplomatic message *Capacity*
On December 1, the French Embassy in the US released a public statement claiming that the Embassy had sent its first encrypted diplomatic message to Paris using a new generation of so-called post-quantum cryptography, aimed at resisting the decryption capabilities of a quantum computer.

Switzerland seeks mandatory reporting of cyber incidents impacting critical infrastructure *Legislation*
Switzerland's Federal Council requested Parliament to amend the Information Security Act (ISA) to ensure that reporting cyber incidents targeting critical infrastructure is mandatory. This proposal seeks to create a legal basis to report such incidents and to define duties for the National Cyber Security Centre (NCSC).

Greece bans commercial spyware *Legislation*
The Greek government passed legislation, on December 9, to ban the use, sale, or distribution of commercial spyware, offered by private sector offensive actors (PSOAs). The new law comes after allegations that threat actors had used such software to spy on political figures.

Law enforcement takes control of domains used in DDoS attacks *Seizure*
Europol announced, on December 15, that a joint law enforcement international operation had taken control of about 50 sites that were offering DDoS-for-hire services to threat actors. The operation called Power Off, involved law enforcement from the US, the UK, the Netherlands, Poland, and Germany.
Analyst note: It is unlikely that these seizures will have any impact to self-proclaimed hacktivist groups as they usually depend on members' efforts rather than paid services.

Four men arrested for identity theft *Arrests*
Authorities in the UK and Sweden arrested four men suspected of hacking into US networks to steal employee data for identity theft.

Police arrest 55 members of Black Panthers gang *Arrests*
The Spanish National Police arrested 55 members of the Black Panthers cybercrime group, including one of the organisation's leaders based in Barcelona. The gang was operating four specialised activity cells dedicated to social engineering, vishing (voice phishing), phishing, and carding.

European operation leads to 2.400 money mule arrests *Arrests*
The eighth European Money Mule Action (EMMA8) operation resulted in the arrest of more than 2.400 individuals connected to money laundering. EMMA8 was facilitated through a joint effort executed by 25 countries and supported by Europol, Eurojust, Interpol, and the European Banking Federation (EBF). The operation ran from mid-September 2022 to the end of November 2022 and identified 8.755 money mules and 222 money mule recruiters. Authorities arrested 2.469 money mules globally.

Ukraine shuts down fraudulent call centre *Arrests*
A group of imposters operating out of a Ukrainian call centre defrauded thousands of victims while pretending to be IT security employees at their banks. They contacted the victims, claimed that attackers had accessed their bank accounts, and requested financial information claiming it was needed to prevent fraud but, instead, emptied their bank accounts.

Cyberespionage

Cloud Atlas targets entities in Russia and Belarus amid the ongoing war in Ukraine *Unattributed threat actor*
On December 9, CheckPoint cybersecurity firm published an analysis of tools, tactics, techniques and procedures (TTPs), and victimology of Cloud Atlas cyberespionage threat actor in the last year. Since its discovery in 2014, Cloud Atlas has launched multiple, highly targeted attacks on critical infrastructure across geographical zones and political conflicts. In 2022 the scope of the threat actor's activities has narrowed significantly, with a clear focus on Russia, Belarus and conflicted areas in Ukraine and Moldova.

Cybercrime

Ransomware

French hospital targeted by cyberattack *Healthcare*
On December 3, a French hospital in Versailles was the victim of a cyberattack. At the time of the attack, all the computers on the hospital's network were blocked and most of the screens displayed a ransom note from the attackers. By December 20, the hospital was capable of operating at 60% of normal capacity.

French ambulance company suffers ransomware *Healthcare*
On December 7, a French company offering ambulance services suffered a ransomware incident. The incident reportedly caused a loss in patient phone numbers.

Lockbit hits Port of Lisbon *Transportation*
The Lockbit ransomware operation claimed a cyberattack, hitting the Port of Lisbon Administration (APL), the third-largest port in Portugal, on December 25. According to a company statement shared with local media outlets, the cyberattack did not impact the port's operations.

ViceSociety hits Portuguese universities *Education*
The group behind the ViceSociety ransomware put information on their data leak site (DLS), on December 15, about an attack they had performed on the consortium of Portuguese universities Universidad Catolica Portuguesa. The group additionally claimed to have exfiltrated data from the victim.

French university reportedly suffered a cyberattack *Education*
On December 18, the ransomware group ViceSociety claimed responsibility for a cyberattack on the Paris Institute of Technology.

Ransomware hits the newspaper The Guardian *News media*
The newspaper The Guardian reported, on December 21, that a security incident had hit its IT systems, believed to be a ransomware attack. Although the company said online publishing continued to operate, the incident affected parts of the IT infrastructure, and staff was told to work from home.

Play Ransomware added Czech victims to their list *Energy Local administration*
On December 6, the Play Ransomware group added several organisations and companies to its list of victims, three of which are European. Among the claims two Czech entities: “Skoda Praha”, an energy company and Husinec, a municipality.

Antwerp’s city services disrupted after hackers attack services provider *Local administration*
On December 5, a cyberattack affected the digital services of the city of Antwerp, Belgium. The threat actors disrupted Antwerp’s services after breaching the servers of Digipolis, the city’s digital partner that provides administrative software. The group behind the Play ransomware claimed responsibility for the incident on their DLS and said they had exfiltrated 557 GB of data, including personal information, which they threatened to release publicly.

Polish city suffers ransomware *Local administration*
On December 5, the IT infrastructure of the city of Radom, Poland reportedly suffered a ransomware attack.

French department reportedly suffers cyberattack *Local administration*
On December 16, reports emerged that the French department of Oise suffered a cyberattack. The department’s website was inaccessible during the timeframe of the supposed attack.

Other cybercrime

A scam syndicate targeting French-speaking Europe for years *Fake investment scheme*
According to the cybersecurity firm Group-IB, an investment scam ring codenamed CryptosLabs has been fooling users in France, Belgium, and Luxembourg into voluntarily transferring money to fraudsters since at least 2018. CryptosLabs is a well-organised illicit business that has a hierarchy of kingpins, sales agents, developers, and call-centre operators that, according to Group-IB’s rough estimates, could have collectively earned as much as 480 million euro since the operation’s launch.

Portuguese medical emergency institute experienced unspecified cyberattack *Healthcare*
On December 15, the Instituto Nacional de Emergência Médica in Portugal announced that it experienced a cyberattack. The organisation announced that security protocols had been activated and the National Centre for Cybersecurity and the judicial police notified. The organisation also states that there was no impact on critical systems or on pre-hospital emergency medical activity. Moreover, there is no evidence that the hospital’s databases have been compromised.

German engineering company suffers incident *Engineering*
On December 21, German industrial engineering company ThyssenKrupp AG announced that its Materials Services division and headquarters suffered a cyber incident believed to have come from an organised crime group.

Hacktivism

NoName057(16) DDoS on defence ministries

Greece, Czech Republic, Croatia, Luxembourg, Hungary, Northern Macedonia, Slovenia, Slovakia

On December 8, the pro-Russia hacktivist group Noname057(16) claimed to have launched a DDoS attack on the websites of the ministries of defence of Greece, the Czech Republic, and Croatia. Then, on December 9, the group claimed responsibility for multiple DDoS attacks targeting the websites of the ministries of defence of Luxembourg, Hungary, Northern Macedonia, Slovenia, Slovakia, the website of the European Defence Agency.

NoName057(16) DDoS on Austria

Austria

On December 12, Noname057 claimed to have launched DDoS attacks against the official websites of the Austrian Constitutional Court and the Austrian armed forces. These websites were unavailable during a few hours.

NoName057(16) DDoS on Italy

Italy

On December 15, Noname057(16) launched a DDoS attack campaign against several e-learning portals of the Italian Ministry of Defence used by defence personnel and the military. On December 3, the group had claimed to have launched a DDoS attack against the country's Ministry of Agriculture, Food and Forestry Policy.

NoName057(16) DDoS on UK

UK

In late December, the pro-Russia hacktivist group NoName057(16) claimed DDoS attacks against the career portal of BAE, a British security and aerospace company.

Anonymous Russia disrupts Spotify

Sweden

On December 8, the pro-Russian hacktivist group Anonymous Russia claimed a DDoS attack against Spotify, a major Sweden-based global audio streaming service; the company acknowledged some accessibility issues. Pro-Russia hacktivist group Killnet praised Anonymous Russia for the attack, citing users' reports of disruptions as evidence of the attack's impact and posting a graph displaying that social media mentions of disruptions had increased as a result of the attack. Killnet subsequently posted a message demanding the company make a Bitcoin payment to restore the service.

Anonymous Russia DDoS on Finland

Finland

On December 12, Anonymous Russia claimed to have launched a DDoS attack against Finland's official websites, including the ones of the central bank, the Alandsbanken bank, the Saastopankki bank, and the Fellow bank.

Pro-Russia hacktivists target Spain *Spain*
On December 23, the pro-Russian hacktivist group From Russia With Love claimed to have carried out a destructive attack on an unnamed Spanish company.

Disruption and hijacking

Helsinki public transport disrupted *Transportation*
A DDoS attack against the digital transport services of the Helsinki region, on December 14, resulted in disruptions in some of the services. The administrators disabled parts of the site in order to ensure continued operations in the face of the attack.

Data exposure and leaks

Belgian merchant bank experienced data leak *Banking*
The Belgian bank Degroof Petercam experienced a data leak resulting in the exposure of data of hundreds of its clients. According to a bank spokesperson, the breach only impacted professional Stock Options Plan (SOP) accounts, which, however, contained personal data.

DDoSecrets leaks data from Cyprus-based firms *Professional services*
The Data leak platform Distributed Denial of Secrets (DDoSecrets) published approximately 325.000 files and 72.000 emails from Cyprus-based firms MeritServus and MeritKapital that were allegedly stolen by a threat actor calling themselves FREAKY. The two firms provide corporate registration, asset management, holding-company services, and golden visa and administration services.

French streaming service admitted leak of user data *Streaming services*
The French music streaming service Deezer, which is used worldwide, admitted, on December 7, on a data breach in 2019, via a third party provider. Some stolen data had started appearing in cybercrime forums in November 2022, with claims that the whole leak concerned more than 240 million Deezer users. Some publicised samples showed that the exposed information included personal data.

World

Cyber policy and law enforcement

US encourages federal government to protect against quantum decryption *Capacity*
On December 21, the US President Biden signed the Quantum Computing Cybersecurity Preparedness Act, which encourages federal government agencies to obtain technology that is protected against quantum computing decryption.

Offensive cyber operations in new Japanese cyber strategy *Capacity*
The government of Japan adopted, on December 16, a new national security strategy, which includes the option for offensive cyber operations. The new strategy calls for offensive operations to prevent major cyber incidents but will first require significant legal changes.

US ban of TikTok *Ban*
In late December, the US House of Representatives ordered its staff and lawmakers to delete TikTok from any government-issued mobile devices due to "security issues". At the end of December, some US states had at least partially blocked the app. On December 13, the US legislature had introduced a new bill that, if passed, would ban social media companies, based in, or under the influence of, foreign countries deemed a concern to national security. The concern of lawmakers has been the obligation by companies like TikTok to make data collected available to Chinese authorities.

Nigeria reportedly prepares to legalise cryptocurrencies *Legislation*
Media reports claim that Nigeria is preparing an amendment to 2007 the Investments and Securities Act to legalise the use of digital currencies.

US government warns of food sector targeting *Warning*
The US government issued an advisory warning that threat actors were targeting organisations in the food sector in business email compromise attacks.

US NSA warns of cyberattacks against the energy sector *Warning*
In the US NSA's annual year in review report, the US warned that Russia could conduct cyber operations targeting the global energy sector over the coming months.

SIM card swapper sentenced for cryptocurrency theft *Sentence*
An individual linked to a cybercrime case, Nicholas Truglia, was sentenced to 18 months in prison, on December 1, for his involvement in a fraud scheme that led to the theft of millions from cryptocurrency investor Michael Terpin. The funds were stolen following a January 2018 SIM swap attack that allowed Truglia's co-conspirators to hijack Terpin's phone number and fraudulently transfer roughly 23,8 million dollars in cryptocurrency from his crypto wallet to an online account.

Cybercriminal sentenced to 5 years in prison in Australia *Sentence*
On December 16, the Australian Federal Police announced the sentencing of an individual to five years and six months in prison for her role in a cyber-enabled ID fraud operation worth 3,3 million US dollars.

Cybercriminal sentenced to 10 years for T-Mobile compromise *Sentence*
the US authorities have sentenced the former owner of a T-Mobile retail store to 10 years in prison for a 25 million dollars scheme in which he unlocked and unblocked cellphones by hacking into T-Mobile's internal systems.

Arrests for taxi system hack *Arrests*
Law enforcement in the US arrested two individuals who had cooperated with Russian hackers to hack into the JFK airport taxi dispatch system for profit. The hack allowed taxis which paid a fee to move to the front of the queue.

Cyberespionage

Likely Chinese threat actor breached Amnesty International Canada *Chinese threat actor*
On December 5, Amnesty International Canada revealed it was the target of a sophisticated digital security breach. The organisation first detected the breach on October 5, 2022, when suspicious activity was spotted on Amnesty's IT infrastructure. Forensic experts with cybersecurity firm Secureworks later established that "a threat group sponsored or tasked by the Chinese state" was likely behind the attack.

Cyberespionage targeting a telecommunications firm in the Middle East *Chinese threat actor*
Cybersecurity firm Bitdefender revealed that the supposedly Chinese threat actor BackdoorDiplomacy highly likely carried out a new cyberespionage campaign targeting a telecommunications firm in the Middle East. According to the cybersecurity firm ESET who uncovered the threat actor in June 2021, BackdoorDiplomacy is a cyberespionage threat actor that has been active since at least 2017. BackdoorDiplomacy has in the past targeted ministries of foreign affairs and telecommunication companies in Africa, Europe, the Middle East, and Asia.

Supposedly Iran-backed threat actor targeting journalists and activists *Iranian threat actor*
On December 5, Human Rights Watch attributed a social engineering and credential phishing campaign to the supposedly Iranian government-linked APT42 (aka TA453, Phosphorous, Charming Kitten) threat actor. The campaign targeted two Human Rights Watch staff members and at least 18 other high-profile activists, journalists, researchers, academics, diplomats, and politicians working on Middle East issues. According to Mandiant, which first identified the hacking group in September 2022, APT42 supports Iran's Islamic Revolutionary Guard Corps intelligence collection efforts and is responsible for more than 30 confirmed operations that have struck non-profit education and government entities since 2015.

Internet Explorer zero day exploited by North Korean actor APT37 *North Korean threat actor*
According to Google's Threat Analysis Group (TAG) the supposedly North Korean threat actor APT37 has been exploiting a zero-day vulnerability (CVE-2022-41128) in the JScript engine of Internet Explorer to target users in South Korea. Google's TAG discovered the zero day in late October 2022.

Cybercrime

Ransomware

Vice Society ransomware gang switches to new custom encryptor *New ransomware strain*
According to researchers from SentibelOne, the Vice Society ransomware operation has switched to using a custom ransomware encryptor that implements a strong, hybrid encryption scheme based on NTRUEncrypt and ChaCha20-Poly1305 algorithms. Vice Society likely sourced this new strain, named PolyVice, from a cybercrime supplier who provides similar tools to other ransomware groups.

New ransomware strains emerging from leaked Conti's source code *New ransomware strain*
Researchers from cybersecurity firm Cyble spotted multiple ransomware strains created based on previously circulated ransomware source code. For example, threat actors have developed new ransomware families, such as Putin Team, ScareCrow, BlueSky Meow, etc., from the leaked source code of the Conti ransomware.

Ransomware gang cloned victim's website to leak stolen data *New extortion tactic*
According to Bleeping Computer, the BlackCat/ALPHV ransomware operation has introduced a new extortion tactic. In at least one case, the threat actors created a replica of a victim's site to publish stolen data on it.

Clop ransomware using Truebot services *Malware collaboration*
Cisco Talos reported, on December 8, on their findings about the Truebot malware. Threat actors used Truebot to drop the Grace malware, which in turn engaged in data theft and the installation of the Clop ransomware. Overall, the researchers pointed to an increase in the number of Truebot infections.

Microsoft-signed drivers used in ransomware attacks *Abuse of trust*
Microsoft disclosed, on December 13, that threat actors were maliciously using some drivers certified by Microsoft's Windows Hardware Developer Program. The use of the drivers was part of post-exploitation activity, after attackers had gained administrative privileges on compromised systems. Microsoft revoked the developer accounts whose profiles were linked to the drivers. Threat actors were using the drivers in cybercrime activities, including ransomware attacks.

Lockbit apologises for hospital attack *Healthcare*
The LockBit ransomware group released a free decryptor for the Toronto-based Hospital for Sick Children (SickKids), saying one of its members violated rules by attacking the healthcare organisation. On December 18, the hospital had suffered a ransomware attack that had impacted internal and corporate systems, hospital phone lines, and its website.

New ransomware group targets US healthcare sector *Healthcare*
On December 8, the US Department of Health and Human Services issued a warning for the country's healthcare organisations regarding ongoing attacks from a relatively new ransomware operation, the Royal group.

Colombian energy provider suffers ransomware *Energy*
On December 12, Empresas Públicas de Medellín, a Colombian energy provider, reportedly suffered a BlackCat/ALPHV ransomware attack. The attack reportedly disrupted the organisation's operations and online services.

Rackspace hit by ransomware *Cloud services*
The cloud service provider Rackspace reported, on December 6, that operation disruptions that took place on December 2, were due to a ransomware attack. The type of ransomware was not revealed. The company also stated they were expecting losses of at least 30 million dollars in their Hosted Exchange business. Furthermore, in an additional statement, on December 8, the company warned its customers that data exfiltrated in the ransomware incident could be used in phishing attacks against them.

Other cybercrime

Fantasy, a wiper deployed through a supply-chain attack against the diamond industry *Supply-chain attack, Wiper*
ESET researchers uncovered a supply-chain attack abusing an Israeli software developer to deploy Fantasy, a new wiper, with victims including the diamond industry. The threat actor built the Fantasy wiper on the foundations of the previously reported Apostle wiper. Fantasy does not attempt to masquerade as ransomware, as Apostle originally did. Instead, it goes right to work wiping data. ESET observed victims were in South Africa, Israel, and Hong Kong. ESET attributes Fantasy to a threat actor named Agrius, a new Iran-aligned group targeting victims in Israel and the United Arab Emirates since 2020.

North Korean hackers stole 1.2 billion dollars in virtual assets *North Korean threat actor, Cryptocurrency*

According to South Korea's National Intelligence Service (NIS), North Korean state-sponsored threat actors have stolen approximately 1,2 billion dollars in cryptocurrency and other digital assets since 2017; more than half of the funds were stolen in 2022 alone. NIS attributes the rise in stolen digital assets to the Democratic People's Republic of North Korea's (DPRK) economic state, after sanctions were imposed by the UN, as well as the country's desire to finance its nuclear program.

Fake cryptocurrency app serving as front for Lazarus malware *North Korean threat actor, Cryptocurrency*

A campaign taking place between June and October 2022 used a new variant of AppleJeus to steal cryptocurrencies. AppleJueus is a cryptocurrency application packaged in a malicious MSI file. The activity is tied to the likely North Korean threat actor Lazarus.

Cryptocurrency investment companies targeted via Telegram *Cryptocurrency*

According to Microsoft, a threat actor tracked as DEV-0139 took advantage of Telegram chat groups to target cryptocurrency investment companies. DEV-0139 joined Telegram groups used to facilitate communication between VIP clients and cryptocurrency exchange platforms and identified their target from among the members.

FIN7 created auto-attack platform to breach Exchange servers *Cybercrime platform Vulnerability exploitation*

The cybercrime threat actor FIN7 uses an automated attack system that exploits Microsoft Exchange and SQL injection vulnerabilities to breach corporate networks, steal data, and select targets for ransomware attacks based on financial size.

Scammers monitoring social media complaints *Scam*

Cyble Research and Intelligence Labs discovered a scam that is targeting citizens in India. The scammers seem to monitor Twitter for user complaint tweets, and when they find a victim's contact information, they will call to initiate the scam.

Android malware infected devices to steal Facebook accounts *Android Facebook credentials*

An Android malware campaign masquerading as reading and education apps has been underway since 2018, attempting to steal Facebook account credentials from infected devices. According to a new report by cybersecurity firm Zimperium, the campaign infected at least 300.000 devices across 71 countries.

Samsung, LG, Mediatek certificates compromised to sign Android malware *Android, Abuse of trust*

Threat actors leveraged multiple platform certificates used by Android OEM device vendors to sign Android apps containing malware. Some of the abused platform certificates belong to Samsung Electronics, LG Electronics, Revoview, and Mediatek.

Information operations

Meta took down covert influence operations *Social media*

On December 15, Meta Platforms stated that since 2017 it has taken down 200 covert influence operations across 42 different languages. Meta said it had also disabled accounts and blocked infrastructure operated by spyware vendors located in China, India, Israel, Russia, and the US. Meta added that networks identified engaging in coordinated and inauthentic behaviour emanated from 68 countries and that at least one disinformation network targeted more than 100 countries. Meta also witnessed a rapid rise in the use of profile pictures created using artificial intelligence techniques in an attempt to pass off rogue accounts as more authentic.

Data exposure and leaks

LastPass password vaults stolen *Password management*
The password management company LastPass revealed, on December 22, that attackers, who had breached their IT systems in November, had also stolen customer vault data. The attackers managed to copy a backup of customer vault data. The company however noted that critical parts of this data were encrypted and should be safe if the customer had followed good password practices.

Twitter links data leak with breach *Social media*
A Twitter vulnerability resulted in a high volume user data leak in the end of 2021. The company disclosed the breach in August 2022. 5,4 million Twitter user data records started circulating online in September and November 2022. Twitter linked, on December 12, the online user data with the 2021 breach.

TikTok employees improperly accessed user data of US journalists *Social media*
Chinese-owned company ByteDance — parent company to social media platform TikTok — fired four TikTok employees for improperly accessing the user data of two US journalists in the summer of 2022. The fired employees were attempting to identify company employees who allegedly shared internal documents with the two journalists.

Social media analytics company suffers personal data breach *Social media*
On December 12, Social Blade, a US-based social media analytics company, suffered a data breach. Purported samples of the data were posted for sale online and contained supposed victims' full names and content. The threat actor claimed to have stolen 5,6 million records of user data. Social Blade confirmed that information compromised in the breach included victims' personal and account data.

Indian COVID-19 vaccination portal leaks *Healthcare*
India's web portal for COVID-19 vaccination, operated by the Ministry of Health and Family Welfare, was reportedly the victim of a breach resulting in the exposure of citizens' personal data.

Uber data leaked via a vendor breach *Transportation*
A breach of an Uber subcontractor providing asset management and tracking services to the company resulted in the leak of Uber employee and company data on December 10. The attack gave access to an AWS backup server used by the Uber contractor Teqtivity. The data was allegedly stolen originally by a member of the cybercriminal group Lapsu$, and then recovered by a third party cybercriminal.

Data theft at the US FBI *Law enforcement*
According to news reports, on December 13, a database originating from the US FBI had been stolen and put up for sale on a cybercrime forum. The database was part of FBI's Infragard program to build partnerships with the private sector and contained the contact details of more than 80.000 people involved in cyber and physical security in critical sectors.

Crypto trading platform 3Commas suffers massive API key leak *Cryptocurrency*
An anonymous Twitter user published, on December 28, a set of about 10.000 API keys that were purportedly obtained from the Canada-based cryptocurrency trading platform, 3Commas. The company acknowledged the API key leak. The Twitter user also announced the intention to publish the API keys.

Significant vulnerabilities

Multiple vulnerabilities in SolarWinds platform — *SolarWinds*
SolarWinds released a patch note for SolarWinds Platform 2022.4 fixing 7 vulnerabilities including 4 highly rated vulnerabilities that could lead to arbitrary commands executed. See CERT-EU's SA 2022-082.

Critical vulnerabilities in NVIDIA GPU display driver — *Nvidia*
NVIDIA released a software security update for its GPU display driver for Windows, containing a fix for a high-severity flaw that threat actors can exploit to perform, among other things, code execution and privilege escalation. See CERT-EU's SA 2022-083.

Critical vulnerability in Visual Studio Code — *Visual Code Studio*
Microsoft published a security advisory about a Remote Code Execution vulnerability in Visual Studio Code. The severity is rated critical as a remote code execution vulnerability exists in VS Code 1.71 and earlier versions for malicious notebooks. These notebooks could use command URIs to execute arbitrary commands, including potentially dangerous commands. See CERT-EU's SA 2022-084.

Type confusion vulnerability in Chrome browser — *Google Chrome*
Google released a new version of its Chrome browser fixing a high-severity flaw, identified by "CVE-2022-4262" that could allow a remote attacker to potentially exploit heap corruption via a crafted HTML page. Google is aware of reports that an exploit for CVE-2022-4262 exists in the wild See CERT-EU's SA 2022-085.

Remote Code Execution Vulnerability in FortiOS SSL-VPN — *Fortinet*
On December 12, 2022, Fortinet released an advisory concerning a heap-based buffer overflow critical vulnerability in FortiOS SSL-VPN that could allow may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests. This vulnerability CVE-2022-42475 has the CVSS score of 9.3. Fortinet is aware of one instance where this vulnerability was exploited in the wild. They do not believe this to be trivial to exploit. However they are advising customers using SSL-VPN to upgrade immediately. See CERT-EU's SA 2022-086.

Critical Vulnerability in Citrix Gateway and Citrix ADC — *Citrix*
On December 13, 2022, Citrix released a Security Bulletin regarding a critical vulnerability CVE-2022-27518 affecting its Citrix Gateway and Citrix ADC products. If exploited, this vulnerability can enable an unauthenticated remote attacker to perform arbitrary code execution on the appliance. According to NSA, the vulnerability is being exploited by APT5 group. APT5 is also known to have exploited Pulse Secure VPN vulnerabilities in 2021. See CERT-EU's SA 2022-087.

All CERT-EU's Security Advisories are available to the public on CERT-EU's website, `https://www.cert.europa.eu/publications/security-advisories#2022`

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.