CERT-EU

# Cyber Security Brief (January 2023)

*February 1, 2023 - Version: 1.0*

**TLP:CLEAR**

*Disclosure is not limited.*

*TLP:CLEAR information may be distributed freely.*

## Executive summary

- We analysed 248 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement** in Europe, Poland warned of continuous cyberattacks by Russian threat actors, regulators in Ireland and France fined Meta, WhatsApp and TikTok over GDPR violations, and law enforcement agencies participated in the seizure of Hive ransomware infrastructure. On the global level, we noticed the signing of a cooperation agreement between the US and Japan on software security standards and the start of the International Counter Ransomware Task Force. Still on the ransomware front, the US announced they are offering rewards up to 10 million dollars for information linking the Hive ransomware to foreign governments.
- On the **cyberespionage** front, a supposedly Chinese-origin threat actor has been exploiting a zero-day vulnerability in the Fortinet platform. UK agencies warned of increased attacks from Russian, Iranian threat actors. Researchers reported on new activity by supposedly North Korean, Chinese and two non-attributed threat actors.
- Relating to **cybercrime**, ransomware continues to be a prime area of activity. In Europe, we noticed activity by at least 10 ransomware operations. The 4 most active ransomware groups were Lockbit, Play, Vice Society and Royal. Ransomware targeted entities in at least 14 European countries and in 13 different sectors. The most targeted sectors were the automotive, construction & engineering, finance, manufacturing and shipping.
- Regarding **data exposure and leaks**, incidents keep impacting a large variety of sectors. In January, we noticed significant data breaches in the following sectors: IT (code sharing), news media, automotive, aviation, public administration, insurance, social media, healthcare, IT, telecoms, and finance. Some data leaks resulted from cyberattacks while others were due to misconfigured and publicly exposed servers.
- Regarding **information operations**, Google reportedly took down accounts associated with the supposedly Chinese origin influence operation Dragonbridge, on YouTube, Blogger, and AdSense.
- On the **hacktivism** front, the main activities in Europe and Russia were linked to Russia's war in Ukraine. These resulted in DDoS or other attacks on several European countries (Poland,

Denmark, the Czech Republic, Estonia, Germany, Portugal, Spain, the Netherlands, and Norway).

- Regarding **disruptive** operations, the Ukrainian national computer emergency response team (CERT-UA) reported a series of wiper attacks targeting the country's national news agency (Ukrinform). They attributed the attacks to the Russia-nexus Sandworm threat actor.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories, related to Microsoft Windows, Git, VMware, ManageEngine, and QNAP NAS, reported in January 2023.

# Europe

# Cyber policy and law enforcement

**Poland warns of attacks by Russia** *Warning*

The Polish government issued a report on December 30, 2022, about continuous cyberattacks by Russian threat actors since the beginning of the Russian invasion against Ukraine. The report cites as targets of these attacks both the public administration domain and private companies, as well as the media sector and citizens. The report specifically links these activities to pro-Russia hacking groups. Additionally, it mentions the GhostWriter campaign as a method of spreading disinformation.

**Greece to mandate compensation for e-fraud** *Legislation*

Greece has put through public consultation new legislation that will mandate banks to compensate victims of e-fraud for any lost amount over 1.000 euros. The new law is cited as compatible with the EU directive 2015/2366 on payment services of the internal market. Banks have countered that the new law will compel them to adopt lower transaction limits and will make transactions slower, as they will have to pass through more safeguards.

**Irish regulator fines Meta** *GDPR, Fine*

The Irish Data Protection Commission (DPC) issued, on January 4, a fine of 390 million euros on the social company Meta for forcing users to agree to personalised advertising. After the introduction of the GDPR the Meta platforms Facebook and Instagram required users to accept personal data processing for targeted advertising, as a prerequisite of continued access.

**WhatsApp fined in Ireland over GDPR violations** *GDPR, Fine*

On January 22, the Irish DPC fined the social media platform WhatsApp 5,5 million euros over GDPR violations. The fine came after complaints that Whatsapp had required user consent for personal data processing as a condition to allow them using the software. The platform was also ordered to make its data processing operations compliant within six months.

**TikTok fined in France** *GDPR, Fine*

France's data protection authority (CNIL) has fined TikTok UK and TikTok Ireland 5.000.000 euros for making it difficult to users of the platform to refuse cookies and for not sufficiently informing them about their purpose.

**Sites of the Hive ransomware seized** *Seizure of assets*

On January 26, an international law enforcement operation involving Europol, the US FBI and the German police succeeded in seizing the Tor payment and data leak sites for the Hive ransomware.

**Europol takedown of cryptocrime call centres**

*Takedown*

On January 9, Europol announced that multiple call centres across Europe controlled by a criminal organisation involved in online investment fraud were taken down. The takedown was the result of a cross-border investigation which started in June 2022. Europol said that the suspects used advertisements on social networks to lure victims to websites covertly operated by the criminals, which offered seemingly exceptional investment opportunities in cryptocurrencies.

**Cryptocurrency exchange executive arrested for money laundering**

*Takedown*

A senior member of Bitzlato, a cryptocurrency exchange platform, was arrested, on January 18. The platform infrastructure was shut down in France for allegedly laundering criminal assets, with six people targeted in Cyprus, Spain, Portugal and the US. The operation was led by French and US authorities, and was strongly supported by Europol.

# Cyberespionage

**Chinese-origin threat actor attacks Fortinet vulnerability**

*Chinese threat actor*

According to security company Mandiant, a reportedly Chinese-origin threat actor exploited a vulnerability of the Fortinet platform (FortiOS SSL-VPN) as a zero day in attacks targeting a European government entity as well as a managed service provider (MSP) located in Africa. Gathered evidence indicates that the attack took place in October 2022, at least two months before the vulnerability was patched.

**UK warns of increased attacks from Russian, Iranian threat actors**

*Russian threat actor, Iranian threat actor*

The UK National Cyber Security Centre repeated that the Russia-based Callisto Group (a.k.a. SEABORGIUM, TA446) and the Iran-based TA453 (a.k.a. APT42, Charming Kitten) threat actors continue to successfully use spearphishing attacks against targeted organisations and individuals in the UK, and other areas of interest, for information gathering activity.

# Cybercrime

## Ransomware

**Romanian hospital discloses ransomware incident**

*Healthcare*

On January 4, Saint Gheorghe Recovery, a Romanian hospital, disclosed a December 2022 ransomware incident. The attack encrypted the hospital's databases and prevented the hospital from receiving payment for services.

**Toulouse clinic suffers ransomware**

*Healthcare*

On January 26, 2023, the Union clinic in Toulouse, France was targeted by a cyberattack which blocked the organisation's servers.

**UK Royal Mail halts overseas shipping due to ransomware**

*Postal services*

On January 11, the UK Royal Mail announced that it was temporarily unable to dispatch items to overseas destinations. News outlets claimed that the interruption was caused by a cyber incident, which reportedly involved the Lockbit ransomware.

**1.000 ships impacted by a ransomware attack**

*Maritime*

Approximately 1.000 ships of 70 maritime operators were affected by a ransomware attack against the Norwegian company DNV, a leading provider of maritime software. The ransomware attack took place on the evening of 7 January and in response, the company shut down the computer servers connected to the ShipManager system operated by the company. The ship systems could, however, still be used offline.

**The Guardian confirms it suffered ransomware in December**

*Media*

On January 11, The Guardian, a UK newspaper, confirmed it was hit by a ransomware attack in December 2022 and that the personal data of UK staff members had been accessed in the incident.

## Other cybercrime

**Raspberry Robin targeting financial institutions**

*Finance*

According to news reports, on January 4, a new version of the Raspberry Robin worm was used to target undisclosed financial institutions in Portugal and Spain. The worm’s initial infection vector continues to be infected USB devices. The new version of the worm allows the collection of more data on victims than before and then loads other malware.

**German financial supervisor issues notice on banking trojan**

*Banking*

On January 9, Germany’s Federal Financial Supervisor Authority (BaFin) released a notice on Godfather, a banking trojan. According to BaFin, the malware targeted approximately 400 banking and cryptocurrency applications. The financial advisor additionally stated that Godfather has displayed phishing pages imitating multiple banking and cryptocurrency applications' websites; the malware also reportedly intercepts multi-factor authentication (MFA) codes.

**DDoS attack against the French Ministry of Economy**

*Public administration*

On January 8, the French Ministry of Economy, in Bercy, reportedly suffered a DDoS attack which caused downtime.

**UK government website abused**

*Public administration*

On January 9, news reports claimed that threat actors abused an open redirect on the official website of the United Kingdom’s Department for the Environment, Food & Rural Affairs to direct visitors to fake OnlyFans sites.

**Council website of Sardinia was down for several days**

*Public administration*

The website of the Regional Council of Sardinia has been inaccessible for several days after being hacked. It seems that this attack was not unexpected after reports of cyber vulnerabilities were presented to the administration, which did not take them into account. The unavailability of the website suggests either a ransomware or a DDoS attack.

**Belgian elderly care centre suffers cyberattack**

*Healthcare*

On January 26, media reported that Curando care group, a Belgian elderly care centre, fell victim to a cyberattack on January 22. The group operates residential care centres and a local service centre.

# Hacktivism

**Anonymous affiliates target Serbia**
*Serbia*

On January 5-6, Anonymous affiliates claimed the disruption of four Serbian government websites as part of the #OpSerbia campaign in response to supposed Serbia's continued ties with Russia throughout Russia's war on Ukraine.

**Pro-Russia hacktivists target Poland**
*Poland*

On January 7, the pro-Russian hacktivist group Noname057(16) claimed responsibility for a DDoS attack on the website of Polish logistics operator PKP CARGO, making the site unavailable for a short period of time.

**Pro-Russia hacktivists target Denmark**
*Denmark*

On January 9-10, NoName057(16) claimed DDoS attacks against six Danish banks' websites and subdomains. Three of the targeted banks acknowledged their sites were experiencing intermittent technical difficulties but did not confirm whether hacktivists had targeted them.
***Analyst note****: The DDoS attacks are likely connected to Denmark's late-December 2022 announcement in which the country stated it would provide in additional military aid for Ukraine.*

**Czech government suffered DDoS coinciding with the presidential election**
*Czech Republic*

The National Cyber and Information Security Agency (NUKIB/NCISA) of the Czech Republic confirmed that several DDoS attacks were disrupting the availability of websites during the presidential election, the first round of which began on the same day.

**Pro-Russia hacktivists target the Czech Republic**
*Czech Republic*

On January 23, NoName057(16) claimed several DDoS attacks against a Czech-based software company. The group stated the attacks were prompted by the company's public disputing of a previous NoName057(16) DDoS attacks and ongoing military aid by the Czech Republic to Ukraine. Since January 19, NoName057(16) claimed DDoS attacks against at least five Czech government and industry targets.

**Pro-Russia hacktivists target Germany**
*Germany*

On January 25, pro-Russia hacktivists claimed DDoS attacks against the websites of at least 36 German public and private sector entities as part of the #GermanyRIP campaign. The campaign had been announced by Killnet on January 24 in retaliation for the German government's planned tank deliveries to Ukraine.

**Pro-Russia hacktivists target Estonia**
*Estonia*

On January 22 and 23, Anonymous Russia and NoName057(16) claimed DDoS attacks against Estonia-based government and private sector entities in retaliation for proposed military aid to Ukraine.

**Pro-Russia hacktivists target healthcare organisations across Europe and the US**
*Europe*

Between January 28 and 30, pro-Russia hacktivists claimed DDoS attacks against at least 140 healthcare entities in the Netherlands, Germany, Portugal, Spain, Finland, Norway, Poland, the UK, as well as the US. This followed Killmilk's (the purported founder and leader of Killnet) January 27 calls for attacks against Western healthcare entities due to the countries' support for Ukraine.

**Turkish hacktivists target Sweden**
*Sweden*

From January 21 to 24, a flurry of claimed activity by Turkish hacktivist groups and personas targeted Swedish public and private sector entities. The activity came after a far-right politician of dual Swedish-Danish nationality burned a Quran at a protest outside the Turkish Embassy in Stockholm, Sweden, on January 21.

# Disruption and hijacking

**New wipers target Ukraine’s news agency Ukrinform**

*News agency*

On January 18 and 27, CERT-UA reported that attackers had targeted Ukraine’s national news agency (Ukrinform) with five different data-wiping malware strains. The attack reportedly took place by mid-January. The list of destructive malware deployed in the attack against Ukrinform included CaddyWiper (Windows), ZeroWipe (Windows), SDelete (Windows), AwfulShred (Linux), and BidSwipe (FreeBSD). CERT-UA suspects that the Russia-linked Sandworm (a.k.a. UAC-0082) is responsible for the attack. On January 25, the security firm ESET had reported about a new wiper named SwiftSlicer targeting Ukraine. ESET researchers attributed this attack to Sandworm. As of time of writing, it is not clear if the two reports relate to the same attack.
*__Analyst note:__: On January 17 and 18 there has been two reports of attacks on Ukrinform: data wiper, attributed to the likely Russia state-sponsored threat actor Sandworm, and a data leak by CyberArmyofRussia_Reborn, a self-claimed pro-Russia hacktivist group. This possibly indicates a form of coordination or even collaboration between the two actors.*

**Disruption of online vote at a French department**

*Online voting*

The platform for the online vote on a flag and anthem for the French overseas department of Martinique had to be taken offline, on January 4, 24 hours after the start of the vote. The reason for the disruption was reported to be a cyberattack.

**French hospitals targeted by cyberattack**

*Healthcare*

On January 25, a cyberattack targeted two hospitals in the French city of Lyon, the Hôpital privé Jean Mermoz and the Hôpital privé de l’est lyonnais in Saint-Priest, forcing them to reduce their activities.

# Data exposure and leaks

**Pro-Russia hacktivists leak data from Ukraine’s news agency Ukrinform**

*News agency*

On January 17, the pro-Russia hacktivist Telegram channel CyberArmyofRussia*Reborn published data allegedly stolen from the state-run national News Agency of Ukraine (Ukrinform). In that channel, the hacktivist actor CyberArmyofRussia*Reborn claimed it had “burned” the victim organisation’s “entire network infrastructure” in an effort to prevent news from populating the website. See also chapter “Disruption and hijacking” above.

**Car companies exposing owners information**

*Automotive*

A security researcher reported, on January 3, about flaws and weaknesses on several car manufacturers’ sites and IT processes that could allow unauthorised operations on the vehicles, their tracking, as well as the exposure of owners’ personal data.

**KLM and Air France notify customers of potential personal data breach**

*Aviation*

On January 6, Air France, KLM and their loyalty program Flying Blue notified specific customers that a potential personal data breach had occurred. Specifically the organisations mentioned that they had detected suspicious behaviour by an unauthorised entity in relation to a customer’s account. Customer names, miles balances, phone numbers and latest transactions may have been compromised.

**French family allowance fund exposes data**

*Public administration*

On January 9, security researchers claimed that a database of the French family allowance fund (CAF) was exposed on the internet due to a human error in the security settings. The personal data of 10.000 users was reportedly exposed.

**Greek social marketplace exposed its database for six months** *Marketplace*

On January 12, news reports claimed that a Greek social marketplace had been exposing a database with user personal data for at least six months. The database included sensitive data such as usernames, full personal names, Facebook IDs, phone numbers and hashed passwords.

**German software provider suffers data leak** *Insurance*

On January 23, media reports suggested that Bitmarck, an IT service provider for German health insurance companies, had suffered a data leak. A cybercrime group reportedly extracted data from the company's Jira project management and databases and put it up for sale. There is no indication that any personal health data was exposed.

**UK sports apparel chain data breach impacts 10 million customers** *Retail*

UK sports apparel chain JD Sports warned of a data breach in which hackers stole online order information for 10 million customers. In data breach notices sent to affected customers, the company warned that the "attack" had exposed customer information for orders placed between November 2018 and October 2020.

# World

## Cyber policy and law enforcement

**Japan and the US to establish MoU on security standards** *Cooperation*

On January 6, US and Japanese officials reportedly met to establish a Memorandum of Understanding to establish similar security standards for government-procured software. According to public reporting, Japan plans to cooperate with the US on developing a Software Bills of Materials (SBOMs) as well as to introduce a Japanese SBOM regulation scheme. SBOMs provide a record of components used when building software products in order for users to track supply chain relationships.

**The International Counter Ransomware Task Force starts operations** *Cooperation*

The International Counter Ransomware Task Force (ICRTF) officially started its operations on January 23. The task force comprises 37 governments, participating on a voluntary basis, organised after a anti-ransomware summit in November 2022. The stated purpose is to disrupt, combat, and defend against ransomware threats through sustained international collaboration.

**US Supreme Court denies NSO Group petition** *PSOA*

The US Supreme Court denied a petition from the Israeli private sector offensive actor (PSOA) NSO Group to dismiss a lawsuit alleging the company exploited the communication app WhatsApp in 2019. NSO Group's April 2022 petition claimed it qualified for foreign sovereign immunity, as it was acting on behalf of a foreign government to investigate terrorist activity when the company exploited WhatsApp.

**Meta's Oversight Board decides to keep strong-worded post** *Censorship*

Meta's Oversight Board overturned Meta's initial decision to remove a Facebook post containing a political slogan that translates to "death to" the Supreme Leader of Iran, Ayatollah Ali Khamenei. The Oversight Board ruled that the slogan "death to Khamenei" is a form of political criticism, akin to saying "down with Khameni". The slogan has been deemed as a part of protected political speech and not a credible threat of violence.

**Nepal obliges ISPs to restrict access to illegal online activities**

*Internet control*

On January 8, the Nepal Telecommunications Authority reportedly ordered internet service providers (ISPs) to prohibit access to websites, apps, or online networks that facilitate the use of illegal online activities. Currently, this order directly affects the use of cryptocurrency and online gambling.

**Ohio and New Jersey ban TikTok on government devices**

*Software ban*

On January 8, Ohio prohibited all state agencies, boards, and commissions from downloading or using any social media application, channel, or platform that is owned by entities located in China, including TikTok. On January 9, New Jersey prohibited the use of software and services deemed high-risk on state-provided or state-managed devices. The list of prohibited software vendors, products, and services provided by the directive included several China-based entities (including ByteDance, the parent company of TikTok) as well as Russia-based Kaspersky Labs.

**US offers up to 10 million dollars for information linking Hive to foreign governments**

*Bounty*

The US Department of State announced on Twitter they are offering up to 10 million dollars for information that would link the Hive ransomware or any other malicious cyber actors targeting US critical infrastructure to a foreign government. This offer comes after a 26 January 2023 announcement that Hive ransomware operations had been successfully disrupted due to a joint effort led by multiple international law enforcement agencies (see chapter Europe / Policy and law enforcement).

## Cyberespionage

**Kimsuky reportedly targets South Korean academic**

*North Korean threat actor*

Security researchers reported identifying three new types of Android malware deployed by the Kimsuky group. The researchers claimed that through an Android trojan, threat actors could browse the Google Drive and Google account of one of the directors of the South Korean Institute of East Asian Studies.

**Ke3chang activity in Iran**

*Chinese threat actor*

Monitoring connections to the malicious Ke3chang's infrastructure, Palo Alto Unit42 observed network activity between Ke3chang's infrastructure and four Iranian governmental organisations, between July and late December 2022. The sustained daily nature of these attempted connections using Ke3chang controlled infrastructure suggests a likely compromise of the Iranian networks. Moreover, these targets also fit historical targeting patterns by the group.

**Saaiwc Group/Dark Pink a reported new APT targets Asia and Europe**

*Unattributed threat actor*

Two industry sources - the Russia-based Group-IB and the China-based Weixin - revealed cyberespionage campaigns executed by a new advanced persistent threat (APT) dubbed Dark Pink or Saaiwc Group. According to Group-IB, the Dark Pink threat actor launched seven successful attacks against high-profile targets between June and December 2022. The threat actor targeted mostly countries in the Asia-Pacific (APAC) region, in the military, government, development, and religious sectors, and one European government ministry.

**Security researchers identify mobile espionage campaign through fake Android app**

*Unattributed threat actor*

ESET security researchers reported on a mobile campaign operated by the StrongPity APT group, which impersonated a legitimate service to distribute an Android backdoor. StrongPity repackaged an official Telegram app to include a variant of the group's backdoor code.

# Cybercrime

## Ransomware

**Microsoft reports on ransomware ecosystem**

*Ransomware ecosystem*

On January 31, Microsoft revealed that, as of end of 2022, they have been tracking more than 50 unique active ransomware families and more 100 threat actors using ransomware in attacks. According to Microsoft, some of the most prominent ransomware payloads in recent campaigns include Lockbit, Black, BlackCat (aka ALPHV), Play, Vice Society, Black Basta, and Royal.

**Australian fire rescue organisation suffers ransomware**

*Critical service*

Fire Rescue Victoria in Australia, disclosed a data breach caused by a December 15 cyberattack that is now claimed by the Vice Society ransomware gang. The incident affected a number of internal servers, including the email system,

## Other cybercrime

**Malware campaign uses fake ads**

*Online advertising*

According to Guardio Labs a new cybercrime technique uses fake web pages of frequently searched brands and uses them to spread malware. The important characteristic of this campaign is the use of the Google Adwords platform so that users who search for the brands are redirected to rogue sites and from there to malicious payload — usually also hiding inside reputable file sharing and code hosting servers.

**Campaign hits banks in French-speaking countries in Africa**

*Finance*

According to Symantec, Bluebottle, a cybercrime group that specialises in targeted attacks against the financial sector, is continuing to mount attacks on banks in Francophone countries in Africa from at least July 2022 to September 2022. The group makes extensive use of the “living off the land” technique, dual-use tools, and commodity malware, with no custom malware deployed.

**US school district cancels classes due to unspecified cyberattack**

*Education*

Des Moines Public Schools, a US school district, cancelled all classes on January 10 after taking networked systems offline in response to a cyberattack, detected on its network on January 9.

**Android TV comes with pre-installed malware in firmware**

*IoT*

A Canadian security researcher discovered that an Android TV box purchased from Amazon was preloaded with persistent, sophisticated malware included in its firmware. The device in question is the T95 Android TV box with an AllWinner T616 processor, widely available through Amazon, AliExpress, and other big e-commerce platforms.

**PayPal accounts breached in large-scale credential stuffing attack**

*Payment*

PayPal is sending out data breach notifications to thousands of users who had their accounts accessed through credential stuffing attacks that exposed some personal data. In credential stuffing attacks hackers attempt to access an account by trying out username and password pairs sourced from data leaks on various websites.

**PoS malware can block contactless payments to steal credit cards**

*Payment*

Researchers found new versions of the Prilex, a point-of-sale (POS) malware, which can block secure, NFC-enabled contactless credit card transactions, forcing consumers to insert credit cards that are then stolen by the malware.

**Cryptocurrency company breach attributed to North Korean actors**

*Cruptocurrency, North Korea*

The US FBI issued a press release, on January 23, in which it attributed the June 2022 breach of the cryptocurrency platform Harmony Bridge, to the North Korean threat actor Lazarus. The breach had resulted in losses amounting to 97 million USD.

**US federal sites breached**

*Government*

The US Cybersecurity and Infrastructure Security Agency (CISA) issued, on January 25, an advisory about the threat to US federal networks by legitimate remote monitoring and management software. Additionally, CISA reported about malicious activities discovered in US federal sites, were linked to a “widespread, financially motivated phishing campaign”. The breaches were performed by portable remote desktop software executables.

## Hacktivism

**Anonymous Cuba defaced University of Havana Department websites**

*Cuba*

On January 1, Anonymous Cuba claimed the defacement of seven University of Havana faculty department websites. The hacktivists published anti-government messages and freedom demands for Cuban political prisoners. Anonymous Cuba claimed they perpetrated the defacement to protest another year of repression and misery due to the Cuban government's policies.

**GhostSec claims data leak at Brazil government**

*Brazil*

On January 10, a social media persona, GhostSec, claimed it had gained access to Brazilian government email accounts and shared 844 Mb of supposedly stolen data. The data reportedly contained identities, passports, government emails and other personal data.

**Sustained DDoS campaign**

*Russia’s war on Ukraine*

SentinelOne reported that NoName057(16), a pro-Russia supposed hacktivist group had been conducting a campaign of DDoS attacks on Ukraine and NATO organisations that began in the early days of the war in Ukraine. Targets have included government organisations and critical infrastructure. NoName057(16) was reportedly responsible for disrupting services across the financial sector in Denmark, in January 2023. Other recent attacks included organisations and businesses across Poland, Lithuania, and others.

**TeamOneFist operation Turn Ruzzia Off**

*Russia*

The pro-Ukraine hacktivist group TeamOneFist conducted the operation Turn Ruzzia Off, against Russia. They reportedly took down 316 Metro and Edge routers across Russia and additionally disabled 944 more.

# Information operations

**Google takes down accounts associated with Dragonbridge**
On January 26, Google's Threat Analysis Group reported that they had taken down 50.000 accounts associated to the Dragonbridge campaign (a.k.a. Spamouflage Dragon) on YouTube, Blogger, and AdSense. The coordinated inauthentic behaviour consisted of a spam influence network, linked to China, which had a presence across multiple platforms.

*Chinese influence operation*

# Data exposure and leaks

**GitHub discloses data breach**
In January, GitHub reported that on December 6, 2022, threat actors breached GitHub's repositories, used for developing GitHub Desktop and Atom, through a compromised Personal Access Token (PAT). The attack resulted in exfiltrating a set of encrypted and password-protected code-signing certificates. GitHub said they had no evidence suggesting the threat actors decrypted the code-signing certificates. However, GitHub revoked the stolen certificates and required users to update to its latest version by February 2.
***Analyst note****: malicious actors can use stolen code-signing certificates to make their malware appear as official GitHub programs.*

*Code signing*

**Twitter user data sold online**
In a continuation of the case of exploitation of a Twitter API vulnerability, which happened in 2021, and had resulted in user data leaked to malicious actors, a set of over 200 million Twitter users email addresses was put for sale online on January 4. A previous sale offer for personal data of 400 million Twitter accounts had prompted an investigation by Ireland's Data Protection Commission, in December 2022.

*Social media*

**Slack code repositories stolen**
Slack issued a security incident notice, on December 31, 2022, in which it said that its private GitHub code repositories were downloaded on December 27, 2022, by an unknown threat actor. Slack mentioned that no downloaded repositories contained customer data, means to access customer data, or the company's primary codebase.
***Analyst note****: We assess that the leaked code may be used to discover currently unknown vulnerabilities. Both cybercriminals and nation-state actors could try to abuse this knowledge to get access to the platform and either steal user data or use it to attack the user base, e.g. by planting malware.*

*Social media*

**A US No Fly list leaked**
On January 19, a security researcher reportedly discovered an unsecured AWS server containing the personal data of individuals who are on a US government Terrorist Screening database and, supposedly, a "No Fly List". The list reportedly contained more than 1,5 million entries and has been shared publicly on a hacking forum.

*Aviation*

**Australian government credentials reportedly exposed**
On January 5, security researchers claimed to have discovered a database containing more than 14 million supposed usernames and passwords. 100.000 credential pairs were reportedly associated with Australian domains, some of which were connected to government accounts. The researchers discovered a user on an underground forum offering to share the database.

*Public administration*

**Healthcare data of 3 million Japanese citizens leaked** *Healthcare*

A Japanese subsidiary of a US healthcare company disclosed a data breach affecting more than 3 million customers' personal data among which health data. The personal data included names and biological sex, as well as information relating to insurance and healthcare coverage. A threat actor gained access to the data through a breach at a contractor

**US Healthcare nonprofit suffers data leak** *Healthcare*

On January 10, a public prosecutor confirmed that Maternal & Family Health Services, a US nonprofit healthcare provider, had suffered a cyber incident from cybercrime actors who accessed the sensitive personal data of 461.070 people.

**NortonLifeLock warns that hackers breached Password Manager accounts** *IT*

In January 2023, NortonLifeLock reported that, on December 12, 2022, they had detected credential stuffing attacks targeting 925.000 NortonLifeLock Password Manager accounts. The company claimed they "had secured" the accounts.

**T-Mobile hacked to steal data** *Telecoms*

T-Mobile disclosed a new data breach, in which a threat actor stole the personal information of 37 million current customer accounts through one of its Application Programming Interfaces (APIs).

**Indian education app suffers data leak** *Education*

A misconfigured server of India's Education Ministry has reportedly exposed the personal data one million Indian teachers and 600.000 students. The application reportedly provided remote access to academic materials throughout the Covid-19 pandemic.

**Investment company leaks information from 820.000 customers** *Finance*

According to news reports, on January 25, a breach at the investment company Zacks, which took place between November 2021 and August 2022, resulted in the leak of personal and other sensitive data of 820.000 customers. The firm said that it had no evidence that financial data had been exposed.

**Self-proclaimed Iranian group leaks data from Saudi Arabian government** *Government*

The self-proclaimed Iran-linked, anti-Israel, and pro-Palestinian group Moses Staff (Cobalt Sapling) has been spotted leaking data stolen from ministries in the Saudi Arabian government, using a newly created persona called Abraham's Ax. According to reports, Moses Staff posted data from 16 campaigns it had conducted as of December 2022. The leaked data was claimed to be collected from Israeli firms and personal data belonging to individuals associated with an Israel Defense Force intelligence unit.

## Significant vulnerabilities

**Zero-day and critical Vulnerabilities in Microsoft Windows** *Microsoft Windows*

On January 10, on their first Patch Tuesday of 2023, Microsoft fixed an actively exploited zero-day Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability and a total of 98 flaws. Eleven of them were classified as critical by Microsoft as they allow remote code execution, bypass security features, or elevate privileges. It is highly recommended applying the fixes as soon as possible.. See CERT-EU's SA 2023-001.

**Multiple critical vulnerabilities in Git** *Git*

During a code audit, X41 discovered several vulnerabilities in the version control system “git”. On January 17, the “git” project resolved the two most critical security vulnerabilities (CVE-2022-23521 and CVE-2022-41903) that could allow the remote execution of arbitrary code. GitHub and GitLab have also issued updates for their products, including the latest version of “git”. A third vulnerability (CVE-2022-41953) affects the Windows version of the “Git GUI” software and could also lead to the execution of arbitrary code. See CERT-EU’s SA 2023-002.

**Critical vulnerability in VMware vRealize Log Insight** *VMware*

On January 24, 2023, VMware released a new security advisory revealing multiple vulnerabilities in VMware vRealize Log Insight. There are two critical vulnerabilities including a directory traversal vulnerability (“CVE-2022-31706”) and a broken access control vulnerability (“CVE-2022-31704”). Both of them have the CVSS score of 9.8 out of 10. It is highly recommended applying the last version.See CERT-EU’s SA 2023-003.

**Critical vulnerability in several ManageEngine products** *ManageEngine*

On January 18, ManageEngine released updates to several ManageEngine OnPremise products. The potentially vulnerable products use outdated versions of the open-source library Apache Santuario (XML Security for Java). Products must have enabled Single-Sign-On (SSO) using the Security Assertion Markup Language (SAML) to be vulnerable. For some products, the SSO must be active, while for others, it is sufficient that SSO was active once. As a result, the vulnerability allows an unauthenticated adversary to execute arbitrary code. Additionally, a Proof-of-Concept exploit is available. See CERT-EU’s SA 2023-004.

**Critical code injection vulnerability in QNAP devices** *QNAP*

On January 30, QNAP published an advisory related to a critical vulnerability, identified as “CVE-2022-27596”, allowing remote attackers to inject malicious code on QNAP NAS devices. See CERT-EU’s SA 2023-005.

*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. |

| TLP | Disclosure | Message |
|---|---|---|
| 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. |