10 years CERT-EU

# Cyber Security Brief (May 2023)

*June 1, 2023 - Version: 1.1*

## TLP:CLEAR

*Disclosure is not limited.*

*TLP:CLEAR information may be distributed freely.*

## Executive summary

- We analysed 250 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement**, The European Commission highlighted the lack of pirate site blocking, the European Parliament added provisions to the AI Act on disclosure of copyrighted materials, and Meta (Facebook) received a record fine over user data protection. In the rest of the world, NATO and Japan plan to expand cooperation countering cyber threats, the US and South Korea imposed sanctions on North Korea for cyber activities, and there was a reveal of Chinese authorities access to TikTok data.
- On the **cyberespionage** front, The UK and the "Five Eyes" disclosed information on a Russian/ FSB implant, a supposedly Chinese threat actor was compromising routers to target European foreign affairs entities, and the likely North Korean Kimsuky group expanded its targeting scope to the US, Europe, and Asia. In the US, a supposedly Chinese group has been targeting critical infrastructure.
- Relating to **cybercrime**, security researchers revealed links between the Russian government and a cybercrime actor, there were attacks on a water supply company in Italy and a German arms manufacturer. In Europe, the top 5 most active ransomware operations have been Lockbit, Blackbasta, Play, Royal, and Trigona; the top 5 most targeted sectors have been legal & professional services, manufacturing, technology, construction & engineering, and financial services. In the rest of the world, the cybercrime group FIN7 returned to operations.
- In Europe there were **data exposure and leaks** in the telecommunications sector, in an education platform, and a health-related company.
- On the **hacktivism** front, the most significant event was DDoS attacks on the Swedish Parliament, claimed by a Russia-affiliated group.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in May 2023.

# Europe

## Cyber policy and law enforcement

**The EU urges for copyright protection enforcement via site blocking**

*Regulation*

The European Commission released, on May 17, its biannual report on the protection and enforcement of intellectual property rights in third countries, highlighting the lack of pirate site blocking as a key issue. Countries like China, Indonesia, and Brazil are listed as priority concerns. The report emphasises the effectiveness of site-blocking in curbing online piracy and urges countries to make progress in this area.

**European Parliament proposes new copyright regulations under AI Act**

*Regulation*

The European Parliament has added new provisions to the Artificial Intelligence (AI) Act that require companies to disclose if generative AI models were developed using copyrighted materials, in an effort to protect citizens' rights and promote innovation. The AI models will be categorised by risk level, and additional reports suggest that the provisions may enable publishers and content creators to seek profit shares if their work is used within generated AI content.

**Italy lifts ban on generative AI**

*Ban lift*

Italy lifted its temporary ban on OpenAI's generative AI model ChatGPT following an announcement issued by the country's data-protection authority.

**Meta fined for inadequate protection of user data**

*Fine*

Meta (Facebook), was fined 1,2 billion euro, on May 22, and was instructed to halt the transfer of user data to the US. The Irish Data Protection Commission found that Meta violated rules regarding data transfers from Europe to the US by relying on contractual clauses that failed to adequately safeguard users' rights and freedoms, despite a previous court ruling on the matter.

**Spanish national police arrest individuals linked to major cybercrime group**

*Arrests*

Spain's National Police have arrested 40 individuals, including two hackers, linked to the organised crime group, Trinitarians, for alleged offences including bank fraud, identity theft, and money laundering. Utilising phishing and smishing techniques, the group is believed to have scammed over 300.000 victims, resulting in losses exceeding 700.000 euros.

**Europol seizes DDoS-for-hire domains**

*Site seizure*

On May 8, Europol and the US Department of Justice announced the seizure of 13 domains linked to DDoS-for-hire platforms.

## Cyberespionage

**Five Eyes share information on Russian Snake implant**

*Russian threat actor*

On May 9, UK NCSC and other Five Eyes members shared analysis and hunting information for the Snake implant. They associated the use of Snake to Center 16 of Russia's Federal Security Service (FSB).

**China-linked threat actor compromises routers to target European foreign affairs entities**

*Chinese threat actor*

Check Point revealed that a likely China-linked threat actor named Camaro Dragon compromised TP-Link routers and then weaponised them to target European foreign affairs entities. The TP-Link routers were the so-called SOHO (Small office/home office) routers, typically found in homes. The compromised routers were infected with an implant called Horse Shell which altered their firmware.

**North Korean Kimsuky hacking group expands targeting scope with new version of reconnaissance malware**

*North Korean threat actor*

The likely North Korean Kimsuky hacking group has expanded its targeting scope to government organisations, research centers, universities, and think tanks in the US, Europe, and Asia. They use personalised spearphishing emails containing a link to a malicious password-protected document hosted on Microsoft OneDrive to infect their targets with the ReconShark malware.

## Cybercrime

**Suspected link between cybercriminal group who targeted Ukraine and the Russian government**

*Ukraine*

Security researchers at Blackberry have claimed that the threat actor Void Rabisu, associated with the Cuba ransomware and RomCom backdoor, is in reality a unit of the Russian government attacking Ukrainian military and local governments. This dispels previous attributions, suggesting a deliberate misdirection.

**European water supply company hit by cyberattack**

*Water supply*

The water supply company Alto Calore Servizi SpA was hit by a cyberattack, but water continued to be delivered to customers. The threat actors named the victim on their Medusa data leak site (DLS) and set a deadline of May 10 to leak stolen data unless a 100.000 US dollar ransom was paid.

**BlackBasta breaches German arms manufacturer**

*Defence*

The German arms manufacturer Rheinmetall AG confirmed, on May 23, a BlackBasta ransomware attack on its civilian business, resulting in data theft. The attack was detected on April 14 and, according to the company did not affect its military branch, due to separate IT infrastructure.

**Brasilian group targets Portuguese banks**

*Banking*

The security company Sentinel Labs reported, on May 25, information about a Brazilian hacking group known as Operation Magalenha which has been targeting Portuguese government and financial institutions since 2021. The group employs phishing emails, social engineering, and fake websites, to distribute malware and steal credentials.

**German IT service provider Bitmarck hit by cyberattack**

*IT services provider*

Bitmarck, a German IT service provider, shut down all of its customer and internal systems due to a cyberattack that was discovered over the weekend of April 29-30. Bitmarck claims that patient data stored in the electronic patient file (ePA) was not at risk during the attack.

**Hackers target the website of Italy's ministry of industry**

*Government*

The website of Italy's ministry of industry was targeted by hackers, causing accessibility issues for users.

**ABB confirms ransomware attack and data breach, takes swift action to mitigate impact**

*Technology*

The Swiss tech multinational ABB confirmed that it was targeted by a ransomware attack, resulting in system disruptions and data theft. While the investigation is ongoing, ABB has contained the breach, restored affected services, and implemented additional security measures to prevent future attacks.

# Hacktivism

**Pro-Russia Hacktivist Group claims responsibility for DDoS attack on Swedish Parliament**
The pro-Russia hacktivist group NoName057(16) has claimed responsibility for a DDoS attack on the Swedish Parliament's website and the websites of five other Swedish entities in the transportation, government, and military sectors. The attacks were in response to recent Swedish government actions, including the Nord Stream pipeline explosion investigation, the expulsion of Russian diplomats, and the support package for Ukraine. The Swedish Parliament's website was partially unreachable on May 2 and appeared slow on May 3.

*Russian threat actor*

# Disruption

**DDoS disrupting Greek high school exams**
News sources reported that end-of-year high school exams in Greece were disrupted on May 29 and 30 due to a high volume DDoS attack targeting the country's national academic network (GRNET). There were reports of up to 280.000 connection attempts per second which caused the unavailability of the national repository for exam questions.

*Education*

# Disruption and destruction

**Malware targeting the electrical grid**
Mandiant reported, on May 25, on a new operational technology (OT) malware called CosmicEnergy that targets industrial control systems (ICS) and is designed to cause power disruptions by interacting with IEC 60870-5-104 devices commonly used in electric transmission and distribution operations in Europe, the Middle East, and Asia. CosmicEnergy shares similarities with previous OT malware, highlighting the lowering barriers to developing offensive OT capabilities and the potential threat it poses to electric grid assets.

*Electric grid*

# Data exposure and leaks

**T-Mobile discloses second data breach of 2023, affecting 836 customers**
T-Mobile has suffered a second data breach in 2023, affecting only 836 customers, but exposing highly extensive personal information that may be used for identity theft and phishing attacks. The breach occurred between late February and March 2023, with the company proactively resetting account PINs and offering free credit monitoring and identity theft detection services to impacted customers.

*Telecommunications*

**Brightly warns of breach affecting its educational platform SchoolDude**
Brightly Software, a subsidiary of Siemens, has announced a data breach at its SchoolDude online platform, compromising the personal information and credentials of 600.000 students. SchoolDude, a cloud-based work order management system used worldwide, is one of several SaaS solutions provided by the company.

*Education*

**Leak of Luxotica customer information confirmed** *Retail*

Luxottica, the Italy-based world's largest eyewear company, confirmed, on May 19, that one of its partners had experienced a data breach in 2021, exposing the personal information of 70 million customers. The breached database was recently found available for free on hacking forums. The leaked data contains customer contact details, but Luxottica claims that financial information and login credentials were not compromised.

# World

# Cyber policy and law enforcement

**NATO and Japan to cooperate on cybersecurity** *Partnership*

Media reported that NATO and Japan will expand their cooperation, aiming to sign an Individually Tailored Partnership Programme (ITPP). The two sides reportedly will deepen collaboration in tackling cyber threats, coordinate stances on emerging and disruptive technologies, and exchange notes on fighting disinformation.

**US sanctions on North Korean actors** *Sanctions*

On May 23, US authorities announced sanctions on four entities and one individual involved in illicit IT worker schemes and cyberattacks that aimed to fund North Korea's weapons development programmes. In parallel, the government of South Korea issued sanctions for the same entities. The actions target activities by North Korean IT workers who employ deceptive tactics, such as stolen identities and fake personas, to secure jobs abroad and generate revenue for the country's regime.

**Samsung bans employee use of generative AI tools after sensitive code uploaded to ChatGPT** *Ban*

Samsung Electronics prohibited employees from using generative AI tools like ChatGPT after discovering that sensitive code was uploaded to the platform. The company is concerned that data transmitted to such platforms is stored on external servers, making it difficult to retrieve and delete, and could end up being disclosed to other users, posing a security risk.

**Former employee alleges Chinese Communist Party access to TikTok data in Lawsuit"** *Lawsuit*

A former employee of Bytedance, the parent company of TikTok, has filed a wrongful termination lawsuit alleging the Chinese Communist Party had access to all data, including those held on US servers. He worked for the company between 2017 and 2018 as the head of engineering for US operations. He claimed a special office in the company, known as the Committee monitored Bytedance's activities and influenced content based on the CCP's interests. Bytedance denies the allegations and plans to contest the claims.

**US offers reward for information on Russian hacker** *Bounty*

On May 16, the US Department of State announced that it is offering a 10 million US dollar reward for any information leading to the arrest and conviction of a Russian hacker who is accused of conducting a 2021 ransomware attack that hit the Washington DC Police Department and resulted in the leak of files containing sensitive law enforcement information.

**Russian court sentenses man for DDoS** *Sentence*

On May 18, the press service of the Russian FSB, the Rostov Regional Court sentenced an IT specialist for his involvement in the organisation of DDoS attacks on the information resources of the Russian Ministry of Defence and the website of the Russian president.

# Cyberespionage

**Chinese group targeting US critical infrastructure**

*Chinese threat actor*

A Microsoft report, on May 24, uncovered a Chinese cyberespionage group, Volt Typhoon, reportedly targeting critical infrastructure organisations in the US, including military bases in Guam. Volt Typhoon has been active since mid-2021, using tactics such as exploiting zero-day vulnerabilities, employing living-off-the-land techniques, and leveraging compromised network equipment. According to the report, the objective of Volt Typhoon is to develop capabilities to disrupt communications infrastructure between the US and Asia during future crises, emphasising stealth and maintaining unauthorised access.

**Earth Longzhi Group launches new campaign targeting organisations in Asia-Pacific Region**

*Chinese threat actor*

Earth Longzhi, a subgroup of APT41, has launched a new campaign targeting organisations in Taiwan, Thailand, the Philippines, and Fiji. This campaign involves abusing a Windows Defender executable, exploiting a vulnerable driver, and using a new technique called stack rumbling to disable security products, and it installs drivers as kernel-level services using Microsoft Remote Procedure Call (RPC) to evade typical API monitoring.

**New APT group GoldenJackal**

*Unattributed threat actor*

Kaspersky reported on May 23 about GoldenJackal, a new APT group that primarily targets government and diplomatic entities in the Middle East and South Asia. The group employs a specific toolset of .NET malware, including JackalControl, JackalSteal, JackalWorm, JackalPerInfo, and JackalScreenWatcher. The group's activities have been ongoing since 2019, and they demonstrate capabilities in espionage, with a focus on stealth and persistence.

**Dark Pink threat actor continues to target government and military organisations**

*Unattributed threat actor*

According to cyber security firm Group-IB, the Dark Pink APT group continues to be very active in 2023, targeting government, military, and education organisations in Indonesia, Brunei, and Vietnam. The threat group has been active since at least mid-2021, primarily targeting entities in the Asia-Pacific region.

**Barracuda discloses zero-day exploitation and data theft in email security gateway appliances**

*Unattributed threat actor*

Barracuda has disclosed that a zero-day vulnerability, CVE-2023-2868, was exploited for at least seven months to backdoor customers' Email Security Gateway (ESG) appliances, enabling data theft. The company promptly issued a security patch, blocked access to compromised devices, and alerted affected customers, urging them to investigate potential intrusions. Multiple previously unknown malware strains were discovered during the investigation.

# Cybercrime

**FIN7 returns to operations**

*Ransomware*

According to Microsoft, the financially motivated cybercriminal group FIN7 (a.k.a. Sangria Tempest ELBRUS) returned to active operations in April 2023 after a period of inactivity. The group was deploying the Clop ransomware in opportunistic attacks.

**New malware steals cookies and hijacks accounts on Meta and other platforms**

*Facebook*

Facebook has detected a new malware named NodeStealer distributed on Meta that allows cybercriminals to steal browser cookies to take over accounts on Meta, Gmail, and Outlook, with Facebook identifying and disrupting the operation only two weeks after the initial deployment. The malware was written in JavaScript and executed through Node.js, and the attacks have been attributed to Vietnamese threat actors.

**A new advanced phishing-as-a-service tool targeted global businesses**

*Phishing-as-a-service*

A new phishing-as-a-service (PaaS) platform called Greatness has been discovered in multiple phishing campaigns, focusing on Microsoft 365 users and featuring advanced capabilities like multi-factor authentication bypass and IP filtering. The service provides highly convincing decoy and login pages, making it particularly effective against business users, with victims largely being companies worldwide primarily in the manufacturing, healthcare, and technology sectors. Greatness leverages a phishing kit and API, enabling even less skilled cybercriminals to perform sophisticated man-in-the-middle attacks to steal authentication credentials or cookies.

## Information operations

**Iranian State-Backed Hackers increase use of information operations to amplify cyberattacks, says Microsoft**

*Iran*

Microsoft's Digital Threats Analysis Center has reported that Iranian state-aligned hackers are increasingly deploying information operations to amplify their cyberattacks and support the regime's agenda in the Middle East and against Western targets. In 2022, researchers linked 24 unique cyber-enabled influence operations to the Iranian government, marking an increase from just seven in 2021, with the operations combining offensive computer network operations with online messaging and amplification.

**Fake image causes confusion**

*US*

A fake image was circulated, on May 23, on Twitter by several verified accounts, depicting an explosion near the Pentagon. The fake news caused confusion and a temporary stock market dip. The image, suspected to be generated by artificial intelligence, was accompanied by false claims of an incident. The account responsible was suspended, and prompted local officials to declare that no explosion had occurred near the Pentagon.

## Data exposure and leaks

**Twitter suffers data exposure**

*Social Media*

On May 7, Twitter reportedly informed impacted users of a security incident that caused private tweets sent to Twitter Circles to appear publicly to users outside the groups.

**Toyota data breach exposes customers car-location information for 10 years**

*Automotive industry*

Toyota Motor Corporation revealed a ten-year-long data breach, caused by a cloud environment misconfiguration that divulged the car location data of over two million customers. The breach was identified within the company's Japanese division, with information managed by Toyota Connected Corporation made publicly accessible due to the lapse in security.

# Significant vulnerabilities

**Vulnerability in Wordpress Gravity Forms Plugin**

*Wordpress Gravity Forms Plugin*

On May 30, 2023, an unauthenticated PHP Object Injection vulnerability has been discovered in the Wordpress' Gravity Forms plugin. This vulnerability, identified as CVE-2023-28782 (CVSS score of 8.3), may allow an unauthenticated user to pass ad-hoc serialised strings to a vulnerable "unserialize" call, resulting in an arbitrary PHP object(s) injection into the application scope. This vulnerability could be triggered in a default installation of the Gravity Forms plugin and only needs a form that contains a list field. See CERT-EU's SA 2023-032.

**GitLab - Critical Path Traversal Vulnerability**

*Gitlab*

On May 23, 2023, GitLab released an emergency security update to urgently address a critical severity path traversal flaw - CVE-2023-2825 - with a CVSS v3.1 score of 10.0. This issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) version 16.0.0, with older versions not being affected. The flaw allows an unauthenticated attacker to read arbitrary files on the server when an attachment exists in a public project nested within at least five groups. See CERT-EU's SA 2023-031.

**Sysmon - Local Privilege Escalation Vulnerability**

*Sysmon*

On May 9, 2023, Microsoft disclosed the existence of a Local Privilege Escalation vulnerability in Sysmon. It is identified as CVE-2023-29343 and could allow an attacker to gain SYSTEM privileges with low attack complexity and without any interaction from a user. See CERT-EU's SA 2023-030.

**Critical Privilege Escalation in Wordpress Elementor Plugin**

*Wordpress Elementor Plugin*

A critical security vulnerability (CVSS score: 9.8), tracked as CVE-2023-32243, has been discovered in a popular Wordpress plugin Essential Addons for Elementor. This flaw could allow an attacker to escalate their privileges to that of any user on the WordPress site, as long as they know their username, thus being able to reset the password of the administrator and login on their account. See CERT-EU's SA 2023-029.

**Microsoft May 2023 Patch Tuesday**

*Microsoft*

Microsoft has released its May 2023 Patch Tuesday security updates, addressing a total of 38 vulnerabilities, including three zero-day vulnerabilities, and six Critical vulnerabilities that allow remote code execution. See CERT-EU's SA 2023-028.

**Critical Vulnerability in Wordpress Plugins**

*Wordpress Plugins*

A reflected XSS vulnerability has been discovered in the Advanced Custom Fields (ACF) and Advanced Custom Fields Pro WordPress plugins (versions 6.1.5 and below). This vulnerability allows unauthenticated users to potentially escalate privileges on a WordPress site by tricking a privileged user into visiting a maliciously crafted URL. The issue has been fixed in version 6.1.6, and has been assigned CVE-2023-30777. See CERT-EU's SA 2023-027.

**Critical Vulnerability in a Cisco Product**

*Cisco*

On May 3, 2023, Cisco released an advisory to address a critical vulnerability in the web-based management system of the Cisco SPA112 2-Port Phone Adapters. The vulnerability is tracked as "CVE-2023-20126" and has a CVSS score of 9.8. See CERT-EU's SA 2023-026.

*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 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. |