CERT-EU

# Cyber Security Brief (July 2023)

*August 1, 2023 - Version: 1.0*

**TLP:CLEAR**

*Disclosure is not limited.*

*TLP:CLEAR information may be distributed freely.*

## Executive summary

- We analysed 263 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement**, Sweden issued fines for GDPR violations, there were arrests in Europe over cybercrime activities, and the EU Council imposed sanctions for Russian information manipulation activities. In the rest of the world, the US and China accused each other of hacking, the US financial markets regulator adopted new rules for cybersecurity disclosures, the US transportation security administration updated cybersecurity requirements for oil and gas pipeline companies, and South Korea and NATO expanded cooperation in cybersecurity.
- On the **cyberespionage** front, recent cybersecurity events in Europe involve a likely Chinese cyberespionage campaign targeting European ministries and embassies using innovative delivery methods, two additional cyberespionage campaigns by supposedly Chinese groups, a breach on Norway's ICT platform, and the revelation of the Decoy Dog malware toolkit. In the rest of the world, a threefold increase in cyber attacks using infected USB drives was recorded, the likely Chinese APT41 was linked to advanced Android surveillance tools, and Russian Turla hackers targeted the defence industry via Microsoft Exchange servers.
- Relating to **cybercrime**, there was a 33.9 million euros theft from an Estonian crypto-payment provider, a cyber incident affected UK medical records, the likely North Korean Lazarus group was involved in a cryptocurrency theft, and Japan's largest port faced ransomware-related operational disruption. In Europe, for July, the top 5 most active ransomware operations have been Clop, Rhysida, Lockbit, AlphV and Noescape; the most targeted sectors have been manufacturing, technology, construction & engineering, education, and media & entertainment.
- In Europe there were **data exposure and leaks** in the University of Manchester, exposing patients' records, while Deutsche Bank AG had a breach leading to customer data exposure.
- On the **hacktivism** front, the pro-Russia group NoName057 targeted the Bank of Spain, an Iranian DDoS hit Israel, and the pro-Russian DDoSia project saw massive growth.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in July 2023.

# Europe

## Cyber policy and law enforcement

**The EU sanctions Russian entities for information manipulation**

*Sanctions*

The EU Council imposed, on July 28, restrictive measures on seven Russian individuals and five entities, involved in a digital information manipulation campaign called RRN (aka Doppelganger), which aimed to spread propaganda and distort information in support of Russia's war against Ukraine. This move is part of the EU's broader efforts to counter foreign information manipulation and interference, with a total of about 1.800 individuals and entities now subject to asset freezes and other sanctions.

**Swedish authority fines companies for GDPR breaches involving Google Analytics**

*Fine*

The Swedish Authority for Privacy Protection (IMY) has imposed a 12,3 million SEK (1 million euros) fine on two companies for using Google Analytics, which it judged to be in violation of the EU's General Data Protection Regulation (GDPR). The firms were penalised for contravening GDPR Article 46(1), which prohibits the transfer of personal data to regions or organisations without adequate safety measures and legal remediation mechanisms.

**Dutch police arrests cyber scammer**

*Arrest*

On July 24, the Dutch Public Prosecution Service arrested a 21-year-old accused of defrauding online banking customers via phishing pages, netting over 400.000 euros and possessing a list of 1,5 million further potential victims.

## Cyberespionage

**Chinese threat actor targeted European Ministries of Foreign Affairs**

*Chinese threat actor*

Check Point Research identified a Chinese cyberespionage campaign focusing on European ministries of foreign affairs and embassies. The campaign, active since December 2022, is linked to Mustang Panda and employs novel delivery methods, such as HTML smuggling to install a new variant of PlugX, resulting in low detection rates.

**Threat actor Storm-0558 targets Microsoft apps with forged token**

*Chinese threat actor*

On July 11, Microsoft announced it mitigated an attack by a China-based threat actor tracked as Storm-0558. The threat actor reportedly targeted customer e-mails of government agencies in Western Europe and focuses on espionage, data theft, and credential access. The threat actor used forged authentication tokens to access user e-mail using an acquired Microsoft account (MSA) consumer signing key.

**Chinese threat actor targeting industrial organisations in Eastern Europe**

*Chinese threat actor*

The cybersecurity firm Kaspersky, has linked a cyberespionage campaign targeting Eastern European industrial organisations to the China-affiliated group APT31. The group, known for stealing intellectual property, utilised improved variants of the FourteenHi malware to target data on air-gaped systems via infected removable drives. Industrial control systems were, however, not targeted.

**Norwegian government ICT platform breached**

*Unattributed threat actor*

The Norwegian government has reported a breach on its information and communications technology (ICT) platform used by 12 ministries, after the exploitation of a zero-day vulnerability. Although work activities were halted, the Norwegian Security and Service Organisation (DSS) initiated several protective measures, fixed the flaw, and limited remote access. Still, it is speculated that the breach may have resulted in a data leak.

**Decoy Dog, a growing threat**
Security researchers from Infoblox published, on July 25, the discovery of Decoy Dog, a malware toolkit that uses the domain name system (DNS) to communicate. At least three threat actors have been identified using it in a very stealthy and targeted way. They all reacted very quickly to the first article published by the security company and kept developing their capabilities.

*Unattributed threat actor*

## Cybercrime

**CoinsPaid blames Lazarus hackers for crypto theft**
The Estonian crypto-payment service provider CoinsPaid experienced a cyber attack that resulted in the theft of 33,9 million euros worth of cryptocurrency. CoinsPaid is blaming the attack on the North Korean threat actor Lazarus.

*Cryptocurrency*

**Attack on Swedish medical technology provider disrupts municipal British ambulance services**
Swedish healthcare and medical technology provider Ortivus disclosed a cyber incident that took place on July 18, which affected UK customers using their cloud-hosted MobiMed ePR electronic patient record system. The UK National Health Service (NHS) confirmed the intrusion impacted the ambulance services in several parts of the country, preventing access to patient medical histories by ambulance crews.

*Health*

## Hacktivism

**NoName057 group targeted Bank of Spain website with DDOS attack**
The NoName057 group launched attacks towards the website of the Bank of Spain, on July 19. Intelligence sources have provided a list of over 2500 IP addresses associated with the group.

*Russian threat actor*

## Information operations

**Ukrainian crack down on pro-Russian propaganda activity**
The Ukrainian police arrested over 100 individuals suspected of running online propaganda and disinformation campaigns from several Ukrainian cities, seizing numerous pieces of computer equipment, mobile phones, and thousands of SIM cards. These individuals are believed to have used special equipment and software to create thousands of bot accounts on various social networks, spreading illegal content justifying Russia’s invasion, conducting psychological operations, and even leaking personal data of targeted victims.

*Ukraine*

# Data exposure and leaks

**NHS data of over a million patients exposed**

*Health*

A cyber attack targeting the University of Manchester has compromised a dataset containing the information of 1,1 million patients across 200 hospitals, including National Health Service (NHS) numbers and partial post codes. The university alerted health officials, expressing uncertainty about the extent of the breach and whether patient names were also accessed.

**Breach on provider exposes customers of Deutsche Bank**

*Banking*

Deutsche Bank AG disclosed, on July 11 that a breach on one of its providers resulted in exposure of customer data. According to the announcement, the breach happened via the exploitation of the MOVEit platform.

# World

# Cyber policy and law enforcement

**US accuses China of hacking US government agencies**

*Naming and shaming*

On July 12, US national security adviser Jake Sullivan mentioned in an interview that, since May 2023, Chinese state-linked hackers had secretly accessed email accounts at around 25 organisations, including at least two US government agencies, Microsoft, and US officials. The US detected the breach of federal government accounts "fairly rapidly" and managed to prevent further breaches.

**China accuses the US of cyber attack against Wuhan earthquake centre**

*Naming and shaming*

On July 26, the Chinese authorities revealed that an earthquake monitoring centre in central China's Wuhan province suffered a cyberattack from hackers overseas. China's state media claimed the attack was "government-backed" and came from the United States.

**US SEC adopts rules for public companies' breach disclosure**

*Regulation*

The US Securities and Exchange Commission (SEC) adopted new rules to enhance and standardise disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. According to the SEC, the changes are intended to help investors make informed investment decisions based on companies' cybersecurity risks. The adopted changes require companies to disclose "material cybersecurity incidents" within four days of discovery, including the incident's nature, scope, timing, and expected impact.

**US authorities update security directive for pipeline companies**

*Regulation*

The US Transportation Security Administration (TSA) released the document SD-Pipeline-2021-02D, which updates cybersecurity requirements for oil and natural gas pipeline companies. The companies are now required to annually submit an updated Cybersecurity Assessment Plan to the TSA, and test at least two Cybersecurity Incident Response Plan (CIRP) objectives in annual exercises. The TSA also requires security pipeline security measures of owners and operators to be assessed every three years.

**South Korea and NATO strengthen security collaboration and jointly tackle cyber threats**

*Cooperation*

According to news sources, South Korea and NATO will expand their partnership on global security issues such as the invasion in Ukraine and North Korea's evolving nuclear threats. They have agreed on an expansion of cooperation in 11 areas, including cybersecurity. Cooperation on a global cyber defence training centre and holding an international cyber defence training session are also foreseen.

**Group-IB contests co-founder's conviction**

*Sentence*

According to the cybersecurity company Group-IB, their co-founder, Ilya Sachkov, who was convicted of treason and sentenced to 14 years in prison by a Moscow court, received an "unfair and secretive trial". Due to information disclosure restrictions, the pretext for the conviction may never be known.

## Cyberespionage

**USB-Driven malware attacks**

*Chinese threat actor*

According to the cybersecurity firm Mandiant, the use of infected USB drives has seen a threefold increase as an initial access vector in cyber attacks.Campaigns like SOGU and SNOWYDRIVE have targeted public and private sector entities worldwide. SOGU is attributed to Mustang Panda, while the threat actor UNC4698 employs USB infiltration to distribute the SNOWYDRIVE malware, particularly focusing on Asian oil and gas organisations.

**Threat group APT41 linked to Android spyware**

*Chinese threat actor*

According to the cybersecurity firm Lookout, the Chinese threat group APT41 has been associated with the advanced Android surveillance tools, WyrmSpy and DragonEgg. These tools pose as default Android apps and utilise hidden modules for data collection, including SMS messages, audio recordings, and device location. The link to APT41 was through overlapping Android signing certificates and a company associated with the threat group.

**Russian hackers exploit Microsoft Exchange Servers**

*Russian threat actor*

Hackers associated with the Russian Turla hacking group have launched new attacks targeting the defence industry via Microsoft Exchange servers. They use phishing emails with malicious macros to install a backdoor called DeliveryCheck, which turns the compromised Exchange servers into malware control centres.

**Iran targeting experts in Middle Eastern affairs and nuclear security**

*Iranian threat actor*

According to ProofPoint, the Iran-based threat actor TA453 (aka Charming Kitten) continued to target experts in Middle Eastern affairs and nuclear security. In a mid-May 2023 spearphishing campaign the threat actor used a project called “Iran in the Global Security Context” as a lure.

**North Korean state hackers linked to breach of US software company**

*North Korean threat actor*

The recent breach of the US-based enterprise software company JumpCloud has been attributed to North Korean state-sponsored hackers, specifically the Lazarus Group, by security researchers from SentinelOne and CrowdStrike.

**Around 700.000 TikTok accounts compromised in Turkey**

*Unspecified threat actor*

Around 700.000 TikTok accounts in Turkey were compromised by threat actors, which allowed them to access user private data and take control. This occurred despite TikTok receiving a warning over a year earlier from the UK’s National Cyber Security Centre about a vulnerability in their system’s use of “greyrouting” for SMS messages. Despite understanding the risk, TikTok chose not to implement a costly fix, leading to the largest known compromise of its accounts.

## Cybercrime

**Lazarus group accused of “cyber heist”**

*Cryptocurrency*

According to the blockchain security company Halborn, the North Korean Lazarus group has been implicated in a hack on Alphapo, a cryptocurrency payment provider, which resulted in the theft of nearly 60 million US dollars.

**Ransomware halts operations at Japan’s port of Nagoya**

*Maritime operations*

Japan’s largest port was hit by a cyberattack on July 4, which resulted in an inability to process cargo from around the world. LockBit 3.0, a prolific Russia-based ransomware group, has claimed responsibility for the attack.

**Widespread exploitation of bug in WordPress**
Hackers are actively exploiting a critical vulnerability (CVE-2023-28121) in the popular WooCommerce Payments plugin for WordPress. The exploit allows impersonating users, including administrators, and gain complete control over vulnerable WordPress sites.

*Wordpress*

## Disruption

**Water treatment plant attacked by former employee**
A former employee of a water treatment facility in California was indicted, on July 10, for intentionally attempting to sabotage the facility's safety systems by remotely accessing and manipulating critical software tools.

*Critical infrastructure*

**Russian military satellite system compromised by hacktivists**
A major satellite communication system used by the Russian military was disrupted due to a cyberattack. Dozor-Teleport, the system's operator, attempted to mitigate the damage by transferring some users to terrestrial networks, but the network largely remained inoperable. Two different groups, a self-proclaimed hacktivist organisation and a group associated with the Wagner Group, claimed responsibility for the attack, stating they introduced malicious software into the satellite terminals.

*Aerospace*

## Hacktivism

**DDoS attack disables the website of Israel's largest oil refinery**
In the period of July 29-30, the website of Israel's largest oil refinery operator, BAZAN Group, was targeted by a DDoS attack and became inaccessible from most parts of the world. In a Telegram message, the Iranian hacktivist group Cyber Avengers claimed responsibility.

*Energy*

**Pro-Russian crowdsourced DDoS project sees massive growth**
The pro-Russian DDoS project "DDoSia", initiated by the hacktivist group NoName057(16), has experienced a significant 2.400% growth in less than a year, reaching 10.000 active members and 45.000 subscribers on its main Telegram channel. The crowdsourced campaign, which started in the summer of 2022, primarily targets Western organisations.

*DDoS*

**Hacktivist claims unconfirmed NATO hack-and-leak**
SiegedSec, a supposed hacktivist group, posted personal and sensitive data allegedly belonging to an internal NATO IT system. Media reports allege that NATO is investigating the allegations.

*Hack-and-leak*

## Data exposure and leaks

**Average cost of data breach incidents at 4,5 million US dollars**
The latest annual report from IBM revealed that in 2023, businesses witnessed an average cost of 4,45 million US dollars per data breach. This represents a 15% increase from three years past, with 57% of impacted organisations intending to pass these costs to consumers instead of investing in cybersecurity.

*Annual report*

**Maximus reports data breach impacting up to 11 million users**

*Government*

The US government contractor Maximus has reported a significant data breach affecting 8 to 11 million people, due to the MOVEit file transfer application data-theft attacks.

## Significant vulnerabilities

**Path Traversal Vulnerability in Mastodon Media File Handler**

*Mastodon*

A critical security vulnerability has been discovered in Mastodon versions up to 3.5.8/4.0.4/4.1.2. This vulnerability, identified as a path traversal issue, affects the Media File Handler component of Mastodon. Exploitation of this vulnerability could allow an attacker to create or overwrite any file that Mastodon has access to, potentially leading to Denial of Service (DoS) and arbitrary Remote Code Execution (RCE). See CERT-EU’s SA 2023-044.

**Microsoft July 2023 Patch Tuesday**

*Microsoft*

Microsoft has released its July 2023 Patch Tuesday security updates, addressing a total of 130 vulnerabilities, including five that were exploited in the wild as zero-day vulnerabilities. Microsoft has also issued guidance on the malicious use of Microsoft signed drivers. See CERT-EU’s SA 2023-045.

**Access Control Bypass Vulnerability in Adobe ColdFusion**

*Adobe ColdFusion*

Rapid7 discovered an access control bypass vulnerability in Adobe ColdFusion. This vulnerability allows an attacker to bypass access control restrictions by adding an additional forward slash to the requested URL. Adobe has released a fix for this vulnerability on July 11, 2023. See CERT-EU’s SA 2023-046.

**RCE Vulnerability in FortiOS and FortiProxy**

*FortiOS and FortiProxy*

On July 11, 2023, Fortinet released an advisory regarding a critical vulnerability in FortiOS & FortiProxy that may allow remote attackers to execute arbitrary code or command via crafted packets. This vulnerability was identified as “CVE-2023-33308” with CVSS score of 9.8. Due to the level of access and control on the network, we recommend to update as soon as possible. See CERT-EU’s SA 2023-047.

**Critical Vulnerabilities in SonicWall GMS and Analytics**

*SonicWall GMS and Analytics*

On July 12, SonicWall released an Urgent Security Notice regarding a suite of vulnerabilities, among which 4 of them rated as critical, affecting SonicWall GMS and Analytics. CERT-EU recommends upgrading as soon as possible to the latest version. See CERT-EU’s SA 2023-048.

**Critical Vulnerability in Cisco SD-WAN vManage**

*Cisco SD-WAN vManage*

On July 12, 2023, Cisco released an advisory to address a critical vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software. Cisco SD-WAN vManage API is a REST API for controlling, configuring, and monitoring the Cisco devices in an overlay network. The vulnerability could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. It is tracked as “CVE-2023-20214” and has a CVSS score of 9.1. The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability. See CERT-EU’s SA 2023-049.

**Citrix NetScaler Critical Vulnerability**

*Citrix NetScaler*

On July 18, 2023, Citrix released a security bulletin regarding one critical vulnerability and two high severity vulnerabilities affecting Citrix NetScaler Application delivery controllers (ADCs) and Netscaler Gateway. Citrix Netscaler ADC is a purpose-built networking appliance used to improve the performance, security, and resiliency of applications delivered over the web. Citrix NetScaler Gateway consolidates remote access infrastructure to provide single sign-on across all applications whether in a data centre, in a cloud, or if the apps are delivered as SaaS apps. It allows people to access any app, from any device, through a single URL. See CERT-EU's SA 2023-050.

**RCE Vulnerability in "ssh-agent" of OpenSSH**

*"ssh-agent" of OpenSSH*

On July 19, 2023, OpenSSH released an update regarding a vulnerability, identified as "CVE-2023-38408". This vulnerability was discovered by the Qualys Security Advisory team and allows a remote attacker to potentially execute arbitrary commands on vulnerable OpenSSH's forwarded "ssh-agent". "ssh-agent" is a program to hold private keys used for public key authentication. Through the use of environment variables, the agent can be located and automatically used for authentication when logging in to other machines using SSH. See CERT-EU's SA 2023-051.

**RCE Vulnerabilities in Atlassian Products**

*Atlassian*

On July 18, 2023, Atlassian has released its Security Bulletin for July 2023 to address vulnerabilities (RCE) in Confluence Data Center & Server (CVE-2023-22505 and CVE-2023-22508) and Bamboo Data Center (CVE-2023-22506). An attacker can exploit these vulnerabilities to take control of an affected system. See CERT-EU's SA 2023-052.

**Critical Vulnerability in Endpoint Manager Mobile (MobileIron Core)**

*Endpoint Manager Mobile*

On July 24, 2023, US-based IT software company Ivanti disclosed a zero-day authentication bypass vulnerability in its Endpoint Manager Mobile (EPMM) software, previously known as MobileIron Core. The vulnerability tracked as CVE-2023-35078 with as CVSS score of 10 out of 10, is actively exploited and allows unauthorised users to access restricted functionality or resources of the application. Ivanti has released security patches addressing this vulnerability. See CERT-EU's SA 2023-053.

**Privilege Escalation Vulnerabilities in Ubuntu**

*Ubuntu*

On July 24, 2023, Ubuntu issued a fix for two local privilege escalation vulnerabilities, CVE-2023-2640 and CVE-2023-32629, that were discovered in the OverlayFS module of its Linux kernel. See CERT-EU's SA 2023-054.

**High Vulnerability in Endpoint Manager Mobile**

*MobileIron Core*

On July 28, 2023, US-based IT software company Ivanti disclosed a Remote File Write vulnerability in its Endpoint Manager Mobile (EPMM) software, previously known as MobileIron Core. The vulnerability tracked as CVE-2023-35081 with as CVSS score of 7.2 out of 10, is actively exploited and allows an attacker to create, modify, or delete files on a victim's system remotely. Ivanti has released security patches addressing this vulnerability. See CERT-EU's SA 2023-055.

*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. |