Cyber Security Brief (June 2023)

July 3, 2023 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 312 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement**, in the EU, large online platforms risk fines for not marking deepfakes, the EU's Artificial Intelligence Act bans high-risk AI practices and there were fines for breaching user data access rights. In the rest of the world, the US put a bounty for information on the Clop ransomware.
- On the **cyberespionage** front, a German political party was attacked, the cybercrime group Asylum Ambuscade engaged in cyberespionage, while France and the UK warned about hackers-for-hire targeting law firms. In the rest of the world, Russia alleged there is a US surveillance campaign involving zero-click iPhone exploits and there were concerns over Chinese-origin chips.
- Relating to **cybercrime**, Siemens Energy had a breach and subsequent data exfiltration. In Europe, for June, the top 5 most active ransomware operations have been Play, Lockbit, Darkrace, BlackBasta, and Snatch; the most targeted sectors have been construction & engineering, manufacturing, technology, and transportation. In the rest of the world, US agencies issued an advisory on the Clop ransomware, a 2023 Nokia report pointed at the threat of IoT botnet DDoS and there was new Android malware.
- In Europe there were **data exposure and leaks** in the UK communications regulator.
- On the **hacktivism** front, pro-Russia hacktivist groups targeted with DDoS attacks European ports and European banking institutions, including the European Investment Bank. In the rest of the world, Microsoft's Azure was affected by DDoS, there were indications that Anonymous Sudan may have links with the Russian state, and Türk Hack Team stated they would be cooperating with Anonymous Sudan.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in June 2023.

Europe

Cyber policy and law enforcement

European laws to enforce deepfake labelling and AI-generated content disclosure *Regulation*
Under the Digital Services Act (DSA), large online platforms such as Meta, Twitter, and TikTok are required to clearly mark deepfakes by August 25 or risk hefty multimillion-euro fines. The European Parliament is also advocating for a similar rule encompassing all AI-generated content, including text, under the impending Artificial Intelligence Act, possibly in effect by 2025.

EU Parliament votes on AI *Regulation*
The European Parliament adopted, on June 14, its negotiating position on the Artificial Intelligence (AI) Act, aiming to ensure that AI developed and used in Europe aligns with EU rights and values. The rules include prohibitions on certain high-risk AI practices, such as real-time remote biometric identification, predictive policing systems, and untargeted facial recognition databases, while also promoting innovation and protecting citizens' rights through exemptions, sandboxes, and complaint mechanisms.

European project on important technologies *Research*
The European Commission approved, on June 8, the "Important Project of Common European Interest" (IPCEI) called "ME/CT", which aims to support research, innovation, and industrial deployment of microelectronics and communication technologies across the value chain. Fourteen EU member states will provide up to 8,1 billion euro in public funding and the project will involve 56 companies and 68 projects in areas such as 5G, 6G, autonomous driving, artificial intelligence, and quantum computing.

Spotify fined in Sweden *Fine*
The music streaming service Spotify was fined 5 million euro in Sweden, on June 13, for breaching user data access rights mandated by the EU's GDPR. The fine came more than four years after a complaint was filed by a privacy rights NGO.

International money laundering network dismantled *Arrest*
Authorities in Italy and Spain, supported by Europol and Eurojust, have arrested 33 suspects involved in an international money laundering network. The criminal network, comprised of individuals from various nationalities, utilised a complex system of companies worldwide to launder illicit funds, resulting in the seizure of 18,5 million euros in assets.

International law enforcement operation cracks down DDoS-for-hire *Arrest*
Polish Central Bureau for Combating Cybercrime arrested two suspects linked to a DDoS-for-hire service in operation since 2013. The arrests were part of Operation PowerOFF, an international effort to dismantle platforms that allow users to launch extensive DDoS attacks for a fee.

Cyberespionage

Cyber attack against German SPD party *Russian threat actor*
According to the newspaper Tagesschau, an executive of the German party SPD became the victim of a hacker attack in January 2023, resulting in possible data exposure. Reportedly, there have been concrete indications of a Russian origin of the attack.

Gamaredon active against Ukraine with new tools *Russian threat actor*
Symantec reported, on June 15, that the Russian hacking group Gamaredon was actively targeting Ukraine's military and security intelligence sectors using new infection tactics and a refreshed toolset. Gamaredon recently incorporated USB malware to achieve propagation within infected networks. They have also shown interest in spearphishing attacks on HR departments, indicating their evolving strategies and objectives.

Asylum Ambuscade: crimeware or cyberespionage? *Unknown threat actor*
ESET published a report about Asylum Ambuscade, a cybercrime group that has been performing cyberespionage operations on the side. The report detailed the early 2022 espionage campaign and multiple cybercrime campaigns in 2022 and 2023.

French & UK cybersecurity agencies say hackers-for-hire are targeting law firms *Hackers-for-hire*
According to reports issued by France's ANSSI and Britain's NCSC, hackers are actively targeting law firms in order to steal data that could alter the outcomes of legal cases. ANSSI said "mercenaries with offensive cyber capacities" are increasingly targeting the legal sector. NCSC is seeing hackers-for-hire being engaged "to gain the upper hand in business dealings or legal disputes".

Information operations

Digital information manipulation campaign against France involving Russian actors *Disinformation*
The French authorities reported, on June 13, about a sophisticated disinformation campaign dubbed Doppelgänger or Reliable Recent News (RRN). The year-long operation had produced fake French official websites and media articles, including imitations of major publications. The campaign, believed to be orchestrated by Russian individuals and companies, targeted multiple countries, spreading false narratives supporting Russia and undermining democratic institutions.

Cybercrime

Siemens Energy experiences threat of data leak following ransomware _Energy
On June 27, Clop ransomware listed Siemens Energy as a victim of ransomware and threatened to release its stolen data. Siemens Energy confirmed that they had suffered a global data security incident during a recent Clop ransomware data theft attack which exploited a vulnerability in the MOVEit platform.

Hacktivism

Pro-Russia hacktivists DDoS websites of more than 20 ports *Russian threat actors*
Between June 5 and 8, the pro-Russia hacktivist group NoName057(16) targeted with a DDoS campaign the websites of more than 20 European and international ports and associated services. The ports were in at least nine countries, including Finland, Germany, Greece, Latvia, the Netherlands, Poland, Spain, Sweden, and Canada. The campaign was motivated by the various forms of support that the nine countries' governments had provided for Ukraine.

Pro-Russia hacktivists targets European banking institutions *Russian threat actors*

In mid-June, a group of pro-Russia hacktivists (Killnet, Anonymous Sudan, and REvil) claimed attacks on European banking institutions, listing European Investment Bank (EIB) as one of their victims. EIB confirmed the claims and tweeted that the cyberattack affected the availability of its website.

Ukrainian hacking group disrupts Russian ISP, claims effects to the banking system *Ukrainian threat actors*

A group of Ukrainian hackers called the Cyber.Anarchy.Squad claimed responsibility for a massive attack on Russian telecom provider Infotel JSC, on June 9. The group also claimed to have caused disruption to Russia's banking systems and cutting off access to major banks for online payments. The hackers released evidence of their attack to the ISP. A statement on Infotel's website confirmed that "a massive hacker attack" that had resulted in damages. However, the banking system disruption was not confirmed.

Data exposure and leaks

UK communications regulator breach *Telecommunications*

The UK communications regulator Ofcom disclosed, on June 12, that it had suffered a data breach due to the MOVEit vulnerability. The breach resulted in the leak of some confidential information on the regulated companies, as well as personal data of employees.

World

Cyber policy and law enforcement

US government offers 10 million dollar bounty for information on Clop *Reward*

The US State Department's Rewards for Justice programme is offering a bounty of up to 10 million dollars for information linking the Clop ransomware attacks to a foreign government. The reward is intended for anyone who can provide a tip connecting any cyber actors targeting US critical infrastructure to a foreign government.

US government guidelines on software supply chain security *Supply chain*

The US administration issued on June 9 updated instructions on software supply chain security to government executive departments and agencies. The instructions aim to provide guidance and advice on the issue.

Cyberespionage

Russia alleges US surveillance campaign — *US threat actor*

On June 1, Russia's Federal Security Service (FSB) claimed it had identified an alleged surveillance campaign against Russia-based individuals. The FSB blamed the US government for the campaign but provided no evidence for the attribution. According to the FSB, the campaign delivered a zero-click exploit using backdoor vulnerabilities in iPhones. The same day, the Russian cybersecurity firm Kaspersky Lab published a report describing a surveillance campaign, called Operation Triangulation, impacting company employees; Russian authorities later indicated the two sets of activity were related.

Chinese group exploits VMware ESXi — *Chinese threat actor*

The security company Mandiant reported, on June 13, that a Chinese-sponsored hacking group known as UNC3886 had exploited a zero-day vulnerability in VMware ESXi to deploy backdoors on Windows and Linux virtual machines. The objective was to steal data and escalate privileges to root. The group, targeted the defence, government, telecom, and technology sectors, and demonstrated advanced capabilities and a deep understanding of complex technologies.

Chinese group exploiting Baracuda vulnerability to steal data — *Chinese threat actor*

According to Mandiant, on June 15, a new pro-China hacker group, UNC4841, was linked to data-theft attacks on Barracuda ESG appliances exploiting unpatched instances of the vulnerability CVE-2023-2868. The group remotely executed code on the devices, infecting them with malware and stealing email data, leading Barracude to issue a recommendation to replace compromised devices for complete security.

Concerns over the use of Chinese-origin chips — *Chinese threat actor*

According to Wired, on June 15, encryption chips sold by Hualan Microelectronics, a company linked to the Chinese military, have found their way into Western military and intelligence networks through its subsidiary, Initio. Although no backdoor in the chips has been discovered, their presence raises concerns about potential hidden vulnerabilities that could give China access to sensitive Western information.

APT15 threat actor targets American foreign ministries with new backdoor — *Chinese threat actor*

According to Symantec, the Flea threat actor, also known as APT15 or Nickel, conducted an attack campaign from late 2022 to early 2023 against foreign ministries, primarily in the Americas, leveraging a new backdoor called Backdoor.Graphican. The group also targeted a government finance department in the Americas, a corporation in Central and South America, and a European entity, which notably diverges from their usual pattern of targeting.

Kimsuky social engineering campaign aims to steal credentials — *North Korean threat actor*

On June 6, Sentinel One reported a targeted social engineering campaign against experts in North Korean affairs. The campaign focused on theft of email credentials, delivery of reconnaissance malware, and theft of NK News subscription credentials. Sentinel One assessed with high confidence that the campaign has been orchestrated by the Kimsuky threat actor.

Kimsuky adopts new strategies — *North Korean threat actor*

The cybersecurity company AhnLab identified significant changes in the Kimsuky threat actor strategies. The group, previously known for using document files for malware distribution with a focus on North Korea-related topics, has now shifted to using CHM files and a broader range of subjects for their attacks.

New malware family used by North Korean Andariel threat actor — *North Korean threat actor*

Researchers at Kaspersky discovered a new malware family associated with the likely North Korean threat actor Andariel. Andariel, a part of the notorious Lazarus group, is known for its use of the DTrack malware and Maui ransomware in mid-2022. During the same period, Andariel also actively exploited the Log4j vulnerability.

Cybercrime

Cybercrime group exploits MOVEit vulnerability *Supply-chain attack*

On June 7, The FBI and the US National Security Agency (CISA) issued a joint cybersecurity advisory, with mitigating actions to prevent the Clop ransomware gang exploitation of the CVE-2023-34362 MOVEit vulnerability.

IoT botnets threatening global telecom networks *Telecoms*

The 2023 Nokia Threat Intelligence Report, released on June 9, revealed a significant increase in IoT botnet DDoS attacks targeting telecom networks globally, with a fivefold rise over the past year. These attacks exploit insecure IoT devices, and the report highlighted the growing threat posed by profit-driven hacking collectives, jeopardising critical infrastructure and services. Additionally, the report pointed out the threat of trojans targeting personal banking information on mobile devices.

SpinOk Android malware distributed over 400 million downloads on Google Play Store *Mobile phone malware*

In June 2023, a new Android SDK malware named SpinOk was identified in approximately 190 apps on the Google Play Store, impacting over 400 million downloads. The malware, embedded in applications as a module serving mini-games with daily rewards, can be remotely controlled by a command-and-control server.

Wagner ransomware wants to recruit its victims *Ransomware*

Researchers at Cyble cybersecurity firm reported on a new ransomware named Wagner. This ransomware is a variant of Chaos ransomware. Researchers found that the ransom note dropped by this ransomware, instead of demanding money, urges users to join the PMC Wagner.

Hacktivism

Microsoft Azure affected by DDoS *Russian threat actor*

The Microsoft Azure Portal was down on June 9, highly likely due to a DDoS attack, claimed by the self-claimed hacktivist group Anonymous Sudan, protesting the US's involvement in Sudanese affairs. There were, however, suspicions of Russian involvement too. This attack followed similar disruptions to other Microsoft web portals, including Outlook.com and OneDrive, prompting Microsoft to investigate and take measures to protect customers and stabilise their services.

Investigation revealed that Anonymous Sudan may be affiliated with the Russian state *Russian threat actor*

In March-April, the group Anonymous Sudan conducted DDoS attacks on Australian organisations in the aviation, healthcare and education sectors. CyberCX cybersecurity company investigated several of these attacks and found that Anonymous Sudan is unlikely to be an authentic hacktivist actor, as it claims, and instead may be affiliated with the Russian state.

Anonymous Sudan and the Türk Hack Team to cooperate *Turkish threat actor*

On April 29, Anonymous Sudan and the hacktivist group Türk Hack Team announced that they would be cooperating in cyberattacks.

Significant vulnerabilities

Critical Vulnerability in MOVEit Transfer *MOVEit*
On May 31, 2023, an SQL injection vulnerability has been found in the MOVEit Transfer web application. This critical vulnerability could lead to escalated privileges and potential unauthorised access to the environment. At this time there is no associated CVE or CVS score, but there are already signals of active exploitation in the wild. CERT-EU highly recommends taking immediate action if you are using this product. See CERT-EU's SA 2023-033.

Multiple Vulnerabilities in Splunk Enterprise *Splunk*
On June 6, 2023, Splunk issued security updates to fix several vulnerabilities, 5 of which are being classified as high. These vulnerabilities could lead to privilege escalation, path traversal, local privilege escalation, denial of service or HTTP response splitting. CERT-EU highly recommends updating Splunk as soon as possible to the latest version. See CERT-EU's SA 2023-034.

Type Confusion Flaw in Google Chrome *Chrome*
Google has released a security update to address a zero-day vulnerability in its Chrome web browser, identified as "CVE-2023-3079". The high-severity flaw is a type confusion issue within the V8 JavaScript engine. Google is aware that an exploit for this vulnerability exists in the wild. Users of Google Chrome are strongly advised to update to the latest version to mitigate potential threats. See CERT-EU's SA 2023-035.

Critical Vulnerabilities in VMware Aria Operations for Networks *VMware*
On June 7, 2023, VMware issued multiple security patches to address critical vulnerabilities in VMware Aria Operations for Networks, formerly known as vRealize Network Insight. The vulnerabilities allow attackers to gain remote execution or access to sensitive information. CERT-EU recommends upgrading as soon as possible. See CERT-EU's SA 2023-036.

Critical Vulnerability in FortiOS *FortiOS*
Fortinet has released several versions of FortiOS to patch a critical pre-authentication remote code execution (RCE) vulnerability in its Fortigate SSL VPN devices. The vulnerability, identified as CVE-2023-27997, allows a hostile agent to interfere via the VPN, even if Multi-Factor Authentication (MFA) is activated. See CERT-EU's SA 2023-037 and SA 2023-038.

Microsoft June Patch Tuesday *Microsoft*
Microsoft's June 2023 Patch Tuesday includes security updates for more than 70 flaws, including multiple critical vulnerabilities. See CERT-EU's SA 2023-039.

Multiple Vulnerabilities in VMWare Products *VMware*
On June 22, VMWare released an advisory regarding multiple memory corruption high severity vulnerabilities in VMware vCenter Server. The affected software provides a centralised and extensible platform for managing virtual infrastructure. The vulnerabilities were found in the DCERPC protocol implementation utilised by vCenter Server. The protocol allows for smooth operation across multiple systems by creating a virtual unified computing environment. See CERT-EU's SA 2023-040.

Multiple Vulnerabilities in BIND 9 DNS System *BIND*
On June 22, The Internet Systems Consortium (ISC) has released security advisories that address high severity vulnerabilities affecting multiple versions of the ISC's Berkeley Internet Name Domain (BIND) 9. A remote attacker could exploit these vulnerabilities to potentially cause denial-of-service conditions. See CERT-EU's SA 2023-041.

RCE vulnerability in Fortinet FortiNAC *Fortinet FortiNAC*

On June 23, 2023, Fortinet released one advisory regarding a critical vulnerability in FortiNAC that may allow unauthenticated attackers to perform remote arbitrary code or command execution. This vulnerability was identified as “CVE-2023-33299” with CVSS score of 9.6. FortiNAC is a network access control solution utilised by organisations to manage network access policies and compliance. Due to the level of access and control on the network, we recommend to update as soon as possible. See CERT-EU’s SA 2023-042.

Grafana Authentication Bypass Using Azure AD OAuth *Grafana*

On the 22nd of June, 2023, a critical security vulnerability - CVE-2023-3128 - was identified in Grafana. Grafana was found to be validating Azure Active Directory (AD) accounts based on the email claim. However, on Azure AD, the profile email field is not unique and can be easily altered. This issue can lead to Grafana account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant Azure AD OAuth application. See CERT-EU’s SA 2023-043.

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.