Cyber Security Brief (April 2023)

May 3, 2023 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 223 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement**, the EU and US have imposed sanctions on Iran for surveillance and censorship activities, NATO banned TikTok on work devices citing security issues, while the UK has penalised the platform for breaching data protection laws. Europol has shut down a hub for stolen account credentials. In the rest of the world, the Indian Army is enhancing cyber operations, the Russian FSB accused the US and NATO of launching cyberattacks on its infrastructure, and Australia banned TikTok on federal devices.
- On the **cyberespionage** front, the supposedly Iranian APT group Charming Kitten reportedly targeted critical infrastructure in Europe, the US, Middle East, and India. A private sector offensive actor (PSOA), the Israel-based QuaDream, announced it is shutting down. Supposedly North Korean threat actor Labyrinth Chollima managed to compromise a software-phone application in a supply chain attack. In the rest of the world, a Chinese shopping app can spy on its users, the APT group Evasive Panda was found spying on Chinese and other users and the risks of using public USB charging ports were underlined by the US FBI.
- Relating to **cybercrime**, in Europe, based on information from data leak sites (DLS), the five most active ransomware operations have been Play, Lockbit, Bianlian, AlphV, and Royal. The most targeted sectors have been manufacturing, construction & engineering, agriculture, healthcare, and transportation, while the most affected countries have been Germany, France, Italy, and the UK. In Europe, a ransomware group claimed they were DDosed by Spanish police. In the rest of the world, a Taiwanese hardware manufacturer suffered an attack, Telegram was mentioned as a marketplace for phishing bots, and malicious Google Ads caused big monetary losses.
- There were significant **data exposure and leaks** in the aviation, transport, legal, IT, and automotive sectors. A Russian company supporting Russian government cyber operations suffered a data leak.
- On the **hacktivism** front, Killnet targeted the website of the European Organisation for the Safety of Air Navigation (Eurocontrol), and conducted politically motivated defacements. They furthermore made the uncorroborated claim of becoming a private company.

- Related to artificial intelligence, the European Data Protection Board created a ChatGPT task force.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in April 2023.

Europe

Cyber policy and law enforcement

EU, US sanction Iran over surveillance activity *Sanctions*
The Council of the European Union (EU-GSC) expanded its targeted sanctions against Iran, designating eight Iranians and a telecommunications provider, Ariantel, responsible for enforcing censorship and contributing to the telecommunications surveillance architecture in Iran. In parallel, the US Treasury Department also imposed sanctions on several senior Iranian military and law enforcement officials, as well as the new secretary of Iran's Supreme Council of Cyberspace, responsible for enforcing censorship in the country.

NATO bans TikTok on work devices *Ban*
The North Atlantic Treaty Organisation (NATO) banned the use of TikTok on work devices due to cybersecurity concerns. In any case, even prior to the ban, NATO-provided device users could not easily access the TikTok app due to internal technology restrictions.

UK fines TikTok *Fine*
The UK Information Commissioner's Office (ICO) fined TikTok 15,9 million US dollar for violating UK data-protection laws by allowing 1,4 million children under 13 years of age to use the platform without parental consent.

Europol seizes Genesis market domains *Seizure*
On April 5, Europol reported that an unprecedented law enforcement operation involving 17 countries had resulted in the takedown of Genesis Market. Genesis Market is one of the most dangerous marketplaces selling stolen account credentials to hackers worldwide. As a result of an action day on 4 April, this illegal service was shut down and its infrastructure seized.

Indictment of Russian national for acquiring US technology *Indictment*
After being arrested in Estonia in the end of March, Andrey Shevlyakov was indicted with 18 counts by the US Department of Justice (DOJ) for buying US electronics and software for Russian defence contractors and government agencies over a period of 10 years.

Massive online investment fraud ring shut down *Arrest*
Europol and Eurojust announced the arrest, on April 13, of five individuals connected to an online investment fraud ring that scammed at least 33.000 victims out of approximately 89 million euro. The operation used web and social media ads to entice victims into making small initial investments, promising large returns.

The leader of supposed pro-Russia hacktivist group arrested in Belarus *Arrest*
Belarusian authorities reportedly arrested the leader and other members of Anonymous Russia, a supposed pro-Russia hacktivist group.

Dutch police target RaidForums members, promote white hat careers *Warning*
Dutch Police are contacting former RaidForums members, urging them to cease illegal cyber activities and delete stolen data, while reminding them that anonymity is not guaranteed. Through the GameChangers programme, they aim to deter young individuals from cybercrime and direct them towards white hat careers.

Cyberespionage

Polish government makes a public statement about Russian cyberespionage campaign *Russian threat actor*
On April 13, a public statement from the Polish Military Counterintelligence Service and the CERT Polska team (CERT.PL) reported on a widespread espionage campaign linked to Russian intelligence services. According to the statement the campaign aimed at collecting information from foreign ministries and diplomatic entities. Most of the identified targets of the campaign are located in NATO member states, the EU and, to a lesser extent, Africa. Many elements of the observed campaign – the infrastructure, the techniques used and the tools - overlap, in part or in full, with activity linked to APT29.

Iran's IRGC using new piece of malware *Iranian threat actor*
The Iranian state-sponsored APT group Charming Kitten (aka APT35/APT42, Mint Sandstorm) was reported, on April 26, to be targeting critical infrastructure in Europe, the US, the Middle East, and India with a new, highly customised piece of malware named BellaCiao. The group is associated with the Islamic Revolutionary Guard Corps, and active since 2014. On April 18, Microsoft Threat Intelligence also reported that the same threat actor had targeted critical infrastructure in the US. Recent cyberattacks attributed to IRGC threat actors suggest they have adopted a more aggressive and confrontational approach, with the quick weaponisation of publicly disclosed PoCs.

Israeli PSOA shutting down *PSOA*
On April 11, Microsoft researchers linked the threat group DEV-0196 to an Israel-based private sector offensive actor (PSOA) called QuaDream. QuaDream reportedly sells a mobile device surveilance platform called REIGN to governments for law enforcement purposes. Following reports by Citizen Lab which identified civil society victims in North America, Central Asia, Southeast Asia, Europe, and the Middle East the company announced, on April 16, it is shutting down.

Trojanised 3CX installers deliver malware in supply-chain attack *North Korean threat actor*
Several IT security companies discovered that 3CXDesktopApp, a software-phone application, included malicious code after a supply chain attack. A search for the malicious code on internet databases revealed the existence of the trojanised 3CXDesktopApp package in several EU countries. The 3CX compromise was attributed by many security vendors to the North Korea-affiliated threat actor Labyrinth Chollima, a subgroup of the Lazarus threat actor.

Cybercrime

Ransomware

Ransomware group claims retaliation by Spanish police for hospital attack *Healthcare*
The ransomware group RansomHouse claimed to have been the victim of a DDoS attack by the Spanish police, in retaliation for their computer attack on the Hospital Clinic in Barcelona, Spain. As a result, the group claimed that they would release another portion of the data stolen from the clinic, which contained information on patients with infectious diseases.

Attacks on Italian hospitals *Healthcare*
The IT systems of several hospitals and medical practices in Lombardy, Italy were affected almost certainly from a cyber attack that took place on April 21-22. Information on the number of patients being treated, became unavailable and hospitals could no longer access medical records online, working only with paper. Ambulance transfers to emergency rooms were also stopped. The organisations affected were operating under the same healthcare company. A number of other companies, in the same region were also affected by cyber attacks, around the same period. Multimedica, one of the affected hospitals, also in Lombardy, was hit a second time, on April 25, resulting in the suspension of outpatient services, emergency rooms, and the retrieval of medical reports.

German hospital attacked *Healthcare*
According to a report, on April 25, the German Hochsauerland Clinic suffered a computer attack that was immediately recognised and stopped using automated security systems. All web applications were disabled and the computer system was disconnected from the internet for security reasons. The report stated that communication systems and medical IT systems had not been affected and continued to function normally.

Lille City Council breached *Local administration*
According to a public report released in April, Lille City Council suffered a cyber attack on March 1, disrupting its services, and technical teams were quickly mobilised to protect data. Three weeks later, the Royal hacker group claimed responsibility and published almost 305 GB of stolen data, including bank details of municipal employees and elected representatives.

Medusa ransomware hit Open University of Cyprus *Education*
The Open University of Cyprus was hit by a cyberattack from the Medusa ransomware group, causing severe disruption to its online operations.

Hacktivism

DDoS against Eurocontrol *Civil Aviation*
The pro-Russia hacking group Killnet targeted the website of the European Organisation for the Safety of Air Navigation (Eurocontrol) in a cyberattack that began on 19 April. The attack caused interruptions to web availability, but had no impact on European aviation, according to a spokesperson for the Eurocontrol. Still, the organisation issued a warning to airlines not to use its online system to file flight plans because of connectivity issues.

Romanian Communist Party website defacement *Political party*
The website of the Romanian Communist Party was defaced, on April 23, by unknown hacktivists who left a message against the Romanian political system and corruption.

Data exposure and leaks

Italian aviation company data leak *Aviation*
According to a report dated April 4, databases of the Italian company Alpi Aviation are currently for sale on a leak site of cyber attackers. The extract provided for sale contains an extract of an assembly tutorial.

Dutch railway exposes data *Transportation*
The Dutch National Railway informed 780.000 passengers of a data breach that occurred at Nebu, one of its software providers, exposing personal information, but not passwords or financial information.

Hyundai suffers unauthorised access to personal data *Transportation*
On April 12, Hyundai disclosed a data breach, which exposed personal data of Italian and French car owners who had booked a test drive, to an undisclosed threat actor.

World

Cyber policy and law enforcement

Indian army enhances cyber operations *Capacity*
The Indian Army is establishing a Command Cyber Operations and Support Wing to bolster security along its borders with China and Pakistan, a decision stemming from the Army Commanders Conference held from April 17 to 21. In addition, the Indian Army is reducing its Technical Entry Scheme training duration from five to four years to boost the cadre of cyber operations officers and is developing new technologies including drones and electronic warfare as part of its modernisation efforts.

Russian FSB accuses US and NATO of allegedly launching cyberattacks on critical infrastructure in Russia *Denounce*
The Federal Security Service of the Russian Federation (FSB) accused the US and NATO of allegedly launching over 5.000 cyberattacks against critical infrastructure in Russia with the use of new types of cyber weapons, originating from Ukrainian territories. FSB claims to have taken timely measures to prevent negative consequences.

Australia bans TikTok in Government *Ban*
Australia banned TikTok from all federal devices due to security concerns.

Telegram banned in Brazil for not disclosing data *Ban*
The messaging app Telegram did not provide all the data on neo-Nazi groups on the platform requested by the Brazilian Federal Police, leading to a court order, on April 27, for telecom companies and app stores to remove the app immediately. The police had requested contact and data information of group members and administrators, which Telegram did not provide. The investigation into neo-Nazi groups was prompted by their alleged involvement in school violence, including the attack on a school in Aracruz that left four dead.

US sentences cybercriminal to four years in prison *Arrest*
On April 27, the US Department of Justice announced that they would sentence an individual to four years and three months in prison for stealing over 712 Bitcoin via Helix, a cryptocurrency mixing service.

Cyberespionage

Pinduoduo shopping app raises security concerns *Chinese tech*
On April 3, CNN reported that Pinduoduo, a Chinese shopping app, with 750 million users a month can bypass users' mobile phone security, monitor other apps' activity, and alter device settings.

Gallium targets South African defence organisation *Chinese threat actor*
On April 26, Palo Alto's Unit 42 reported on malware analysis which revealed the targeting of a South African organisation in the defence sector and a Nepalese organisation in the construction sector by Gallium. Palo Alto assesses that the threat actor is a Chinese advanced persistent threat (APT) group that routinely conducts cyberespionage campaigns.

Cyberespionage using updates of Chinese applications *Chinese threat actor*
ESET Research reported on April 26, that Evasive Panda (also known as Bronze Highland and Daggerfly) has been conducting cyberespionage against individuals in mainland China, Hong Kong, Macao, and Nigeria, with government entities and NGOs being the primary targets. Evasive Panda has been using its own custom malware framework, including the MgBot backdoor, a modular piece of malware. The group, which is reportedly China-associated, has been deploying the MgBot backdoor to Chinese users via legitimate updates from known applications, with the targeted users primarily located in the Gansu, Guangdong, and Jiangsu provinces.

Palestinian-associated Arid Viper group employing new malware in cyberespionage attacks *Palestinian threat actor*
Symantec reported that Arid Viper, a supposed Palestine-associated advanced persistent threat group, conducted cyberespionage attacks against organisations in Palestine as well as Israeli citizens using the BarbWire Windows backdoor.

Supposed North Korean group phish US and South Korean targets *North Korean threat actor*
Google's Threat Analysis Group (TAG) reports that Archipelago, a supposed North Korean government-backed advanced persistent threat group targeted academics, government and military personnel, think tanks, policy-makers, and researchers in the US and South Korea.

Android malware infects 60 applications, affecting 100 million downloads *Mobile spyware*
McAfee reported that it detected Goldoson malware in 60 legitimate apps with 100 million downloads. The malware can collect user data and perform ad fraud by clicking ads without consent.

FBI warns against mobile malware spreading through public charging stations *Mobile spyware*
The US FBI warned US consumers against using public USB charging ports. Officials specifically advise avoiding USB ports in airports, malls, and hotels where the risk of hacking is higher.

Cybercrime

MSI attacked by ransomware group demanding 4 million US dollar *IT*
MSI, a Taiwanese hardware manufacturer, suffered a ransomware attack. A threat actor claimed to have exfiltrated 1,5 TB of data and demanded 4 million US dollar.

Amazon bans sale of Flipper Zero portable pen-testing tool *Ban*
Amazon has banned the sale of the Flipper Zero portable multi-tool for penetration testing after tagging it as a card-skimming device. The device is a compact and programmable penetration testing tool that can experiment with and debug various digital and hardware devices using various protocols.

Telegram used by phishing bot creators for marketing and recruitment *Phishing*
Kaspersky reports that Telegram is a marketplace for phishing bots to recruit unpaid helpers and market products. While Telegram has been used for cybercriminal activities for years, it appears that it has become a popular platform for phishing in recent times.

Minecraft copycat games on Google Play infected with adware *Video game*
38 Minecraft imitation games on Google Play contained HiddenAds adware, which discreetly loaded ads in the background to produce income for its operators. The games were downloaded by about 35 million Android users.

Malicious Google Ads cause 4 million US dollar losses for DeFi crypto users *Crypto currencies*
Threat actors used Google Ads to impersonate legitimate DeFi crypto protocols, causing around 3.000 users to lose over 4 million US dollar. The malicious ads used various methods to avoid detection during the review process.

Hacktivism

Killnet makes uncorroborated claim of being a private company *Nationalist hackers*
On April 27, Killnet, a supposed pro-Russia hacktivist group, posted on Telegram that going forward they are a Russian private military hacker company. They added that they would continue working to defend the interests of the Russian Federation but would also take others' work orders.

Disruption and destruction

DDoS attacks shift to breached virtual private servers *DDoS*
Cloudflare reports that in Q1 2023, hypervolumetric DDoS attacks transitioned from using compromised IoT devices to breached virtual private servers (VPS). This new tactic allows threat actors to create high-performance botnets up to 5.000 times stronger than IoT-based botnets, by exploiting vulnerable VPS servers with leaked API credentials or known exploits.

Mercury conducting destructive activity *Destruction*
On April 7, Microsoft Threat Intelligence reported that they detected destructive operations by Mercury, a supposed nation-state actor linked to the Iranian government. The attack targeted both on-premise and cloud environments and masqueraded as a standard ransomware campaign. The unrecoverable actions show destruction and disruption were the ultimate goals of the operation.

Canadian pipeline attacked by supposed pro-Russia hacktivist group *Critical infrastructure*
On April 26, the New York Times reported that leaked US Pentagon documents revealed that a cyberattack by Zarya, a supposed pro-Russia hacktivist, targeted an unnamed Canadian gas pipeline. The attack reportedly took place on February 25, impacted the company's profits but did not result in physical damage. Zarya supposedly has the capability to increase valve pressure, disable alarms, and make emergency shutdowns of the gas distribution station.

Information operations

Leaked Pentagon documents later abused in information operation *Defence*
In April, classified documents belonging to the US Pentagon which had been previously leaked by a US military insider, began circulating in an altered form on social media. The altered documents related to Russia's war on Ukraine. Media organisations reported that this manipulation of previously leaked documents suggests a potential information operation.

Data exposure and leaks

Vulkan files *Government cyber operations*
On March 30, several news outlets published and reported on documents and e-mails associated with NTC Vulkan. NTC Vulkan is a Russian cybersecurity company which according to the leaked documents supported state-sponsored Russian cyber operations.

Kodi confirms data breach affecting 400.000 user records and private messages *IT*
Kodi, a US media player software provider confirmed that an unauthorised actor accessed one of its databases. The threat actor accessed personal data such as sensitive personal data and private messages as well as exfiltrated copies of the database backups.

American Bar Association leaked members' credentials *Legal*
On April 21, news reports claimed that on March 6 the American Bar Association exposed outdated login credentials of 1.466.000 of its members. The credentials reportedly served a legacy IT system that was decommissioned in 2018.

Artificial intelligence

European Data Protection Board creates ChatGPT task force *ChatGPT*
The European Data Protection Board (EDPB) adopted a dispute resolution decision regarding Meta Platforms Ireland Limited's data transfers to the US for its Facebook service, addressing legal questions raised by the Irish Data Protection Authority's draft decision. Separately, the EDPB will launch a dedicated task force on ChatGPT to promote cooperation and exchange information on potential enforcement actions by data protection authorities, following an Italian enforcement action against OpenAI's Chat GPT service.

Significant vulnerabilities

Remote code execution vulnerability in Windows HTTP protocol stack *Microsoft Windows*
On March 14, Microsoft released a security fix for a vulnerability (CVE-2023-23392) in the HTTP/3 protocol stack of Microsoft Windows Server 2022 and Windows 11 systems. This vulnerability allows a remote attacker to execute arbitrary code. Microsoft expects this vulnerability likely to be exploited soon. See CERT-EU's SA 2023-020.

Critical vulnerabilities in SAP products *SAP*
On April 11, SAP released 24 patches for various products, which contain five critical severity fixes that impact SAP Diagnostics Agent, SAP Business Client, SAP NetWeaver Process Integration, SAP BusinessObjects Business Intelligence Platform, and SAP NetWeaver Application Server for ABAP Platform. See CERT-EU's SA 2023-021.

Critical authentication vulnerability in Fortinet product *Fortinet*
On April 11, Fortinet released an advisory regarding a critical vulnerability in FortiPresence on-prem infrastructure server. This vulnerability is identified as CVE-2022-41331 (CVSS score of 9.3) and may allow remote unauthenticated attackers to access the Redis and MongoDB instances. Moreover, Fortinet has also released security updates to address 9 high, and 10 medium severity vulnerabilities in FortiPresence, FortiOS, FortiWeb, and other Fortinet products. See CERT-EU's SA 2023-022.

Remote code execution vulnerability in Microsoft Message Queuing *Microsoft*
On April 11, Microsoft released a security update for a critical vulnerability in Microsoft Message Queuing. This vulnerability is identified as CVE-2023-21554 (CVSS score of 9.8) and could allow unauthenticated attackers to remotely execute arbitrary code. See CERT-EU's SA 2023-023.

Type confusion flaw in Google Chrome *Chrome*
Google has released out-of-band updates to address a vulnerability in its Chrome web browser, identified as CVE-2023-2033. The high-severity flaw is a type confusion issue within the V8 JavaScript engine. Users of Google Chrome, Microsoft Edge, Brave, Opera, and Vivaldi, are strongly advised to update to the latest version to mitigate potential threats. See CERT-EU's SA 2023-024.

Critical vulnerabilities in PaperCut *PaperCut*
On April 20, we released a security advisory concerning two critical vulnerabilities in PaperCut MF/NG, which are actively being exploited in the wild. The vulnerabilities allow unauthenticated remote code execution and information disclosure. PaperCut users are strongly urged to update their software immediately to mitigate these risks. See CERT-EU's SA 2023-025.

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.

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.