Cyber Security Brief (August 2022)

September 1, 2022 - Version: 1.0

TLP:WHITE

Disclosure is not limited.

TLP:WHITE information may be distributed freely.

Executive summary

- We analysed 246 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement**, in Europe, France banned a Russian TV broadcasting channel, and Ukraine took down a cybercrime platform. Elsewhere, the US indicted a Russian for spreading disinformation, and offered a bounty for information on Conti associates.
- On the **cyberespionage** front, Chinese groups targeted Ukrainian, Russian, Belarusian, and Australian targets with spear-phishing, and Taiwan and the Philippines with supply-chain attacks. Russian groups targeted NATO countries with spear-phishing. Meta (Facebook) removed operations by state-sponsored groups from its social media platforms. A North Korean threat actor targeted several South Korean entities and an Iranian-origin group targeted Israeli organisations.
- Relating to **cybercrime**, in Europe reports showed that, besides businesses, ransomware targeted the critical infrastructure sector including energy (at least five cases) and healthcare sectors (at least four cases), as well as public administrations in several countries (at least four cases). Notably, the operations of a Danish retailer were disrupted countrywide. The top three ransomware families in Europe were Lockbit (by far the most infections), AlphV, and LV. On the global level, beside ransomware attacks, the cryptocurrency sector was of particular interest to cybercriminals, as well as to North Korea's Lazarus group which showed consistent activity in the sector.
- On the **hacktivism** front, we observed nationalist motivated activity. In Europe, we observed attacks by pro-Russia purported hacktivists against targets in countries opposing Russia's war on Ukraine, while in the rest of the world there were pro-China attacks against Taiwan and a pro-Russia group attacking the US aerospace sector. The targeting focuses on government organisations, especially on those providing services to citizens.
- Regarding **disruptive** operations, Google announced that they responded to the highest volume DDoS attack ever. Montenegro faced disruptive attacks affecting government services and critical infrastructure.
- With relation to **data exposure**, several big IT platforms and services providers, including Twitter, Cisco, the cloud messaging company Twilio, and the Plex media platform, disclosed data breaches which exposed internal or customer data.

- We included several significant vulnerabilities and associated advisories, reported in August 2022.

Europe

Cyber policy and law enforcement

France bans an additional Russian TV broadcasting channel *Ban, Foreign media, Disinformation*

On August 3, the French Audiovisual and Digital Communication Regulatory Authority (Arcom) gave Eutelsat, a French satellite operator, formal notice to cease the European broadcasting of NTV Mir, the international version of the NTV channel. The NTV television group is owned by the Russian gas giant Gazprom. Arcom accuses NTV Mir of remarks inciting hatred or violence. Arcom also sanctions "several serious and baseless allegations, feeding the springs of Russian propaganda" and "disseminated in particular in order to legitimise the war in Ukraine."

Ukraine takes down cybercrime infrastructure hitting crypto fraud victims *Take-down, Cryptocurrency scam*

The National Police of Ukraine announced that they took down a network of call centres used by a cybercrime group to target victims with cryptocurrency scams under the guise of helping them recover their stolen funds. The cybercriminals behind these illegal call centres were also allegedly involved in scamming citizens of Ukraine and EU countries interested in cryptocurrency, securities, gold, and oil investments.

Cyberespionage

Chinese actor targeting Ukraine, Russia, and Belarus *Chinese threat actor, Spear-phishing*

On August 8, Kaspersky reported observing a spear-phishing campaign by the Chinese-origin threat actor TA428. The campaign was detected in January 2022 and targeted the military and industry sectors. The threat actors used highly targeted phishing messages that contained attached MS-Word documents to exploit an older vulnerability. The target countries included Afghanistan.

Russian Callisto group attacking NATO countries *Russian threat actor*

Microsoft issued a report on phishing operations of the Callisto group (aka Reuse Team, SEABORGIUM). The group was observed targeting NATO countries, in particular the US and the UK, with occasional targeting of other countries in the Baltics, the Nordics, and Eastern Europe, as well as Ukraine.
Analyst note: We assess that this activity pose a potential threat to EU institutions, bodies and agencies.

New post-compromise tool used by APT29 *Russian threat actor, Persistence*

Microsoft security researchers discovered a post-compromise capability dubbed MagicWeb, which is used by a threat actor tracked as Nobelium or APT29 to maintain persistent access to compromised environments. Microsoft reports that the group remains highly active, executing multiple campaigns in parallel targeting government organisations, non-governmental organisations (NGOs) and think tanks across Europe, US and Central Asia.
Analyst note: We assess that this activity pose a potential threat to EU institutions, bodies and agencies.

Cybercrime

Ransomware

French hospital suffers ransomware *Ransomware, Health*
A French hospital, Centre Hospitalier Sud Francilien (CHSF), suffered a ransomware attack on August 21. The hospital's computer systems were down, the emergency department operated in a downgraded mode, and staff could no longer fill patient admission forms. For more than 24 hours, caregivers were forced to use paper. Threat actors threatened to leak patient data if the ransom was not paid. Patients requiring urgent care were redirected to other hospitals in the region. In addition, some surgeries were postponed.

French retirement home hit by ransomware *Ransomware, Health*
A French retirement home in Beuzeville was the victim of a ransomware attack on August 24. A crisis unit was set up by a nearby hospital. The ransomware used was reportedly Cryptolocker.

Italian healthcare complex hit by ransomware *Ransomware, Health*
A ransomware attack hit ASL Città di Torino, a health complex, in the Turin area. The affected facilities include the San Giovanni Bosco, Maria Vittoria, Martini and Oftalmico hospitals. The management of the health complex issued a press release listing the services that remain active (First Aid, outpatient visits, hospitalisations, hospital visits and surgical interventions) while the collection of radiological reports could only take place at the Radiology Secretariats.

UK's National Health Service disrupted *Ransomware, Managed services provider, Health*
On August 5, a ransomware attack on Advanced, a British managed services provider, disrupted the National Health Service's emergency services, resulting in their IT system's complete inoperability.

Data of Italian municipalities exposed after attack *Ransomware, Public administration*
A July attack by the RansomHouse ransomware group on several Italian municipalities in the Valdisieve and Valdarno regions resulted in the exfiltration and later, in August, the public exposure of citizens' data, after a ransom demand was not met.

Belgian municipality suffers double extortion *Ransomware, Public administration*
The social services of Maldegem, a municipality in Belgium, suffered a ransomware attack whereby the personal data of citizens leaked. The municipality refused to pay the ransom.

Spanish scientific research council hit by ransomware *Ransomware, Scientific research*
The Spanish Higher Council for Scientific Research (CSIC), a body dependent on the Ministry of Science and Innovation, confirmed they were targeted by a ransomware attack on July 16 and 17. In a public statement, the Ministry indicated that the cyberattack was similar to that suffered by other research centres such as the Max Planck Institute or the US NASA, and that it "comes from Russia".

Ransomware hit energy supplier *Ransomware, Energy*
The AlphV (aka Blackcat) ransomware operation claimed responsibility for a cyberattack against Creos Luxembourg. Creos is a natural gas pipeline and electricity network operator. Creos' owner, Encevo, operates as an energy supplier in five EU countries.

Italian energy company breached *Energy*
The Italian state-owned energy services company GSE suffered a cyber attack and temporarily blocked its website and access portals for security reasons. The company also stated that its gas purchases were guaranteed.
Analyst note: At time of writing, the nature of the attack (ransomware or other) is not known.

Clop breaches UK water supplier *Ransomware, Critical infrastructure*
On August 15, South Staffordshire PLC, a UK water supplier, revealed that it suffered a cyber attack which resulted in the disruption of its IT systems. In parallel a cybercriminal group claimed responsibility on their data leak site (DLS) and announced that they had supposedly managed to breach the industrial control systems (ICS) of the victim. The attackers also claimed that they had not encrypted compromised systems but instead exfiltrated data. After not receiving the demanded ransom, they started publishing the supposed stolen data on the DLS.

Greek natural gas system operator attacked *Ransomware, Critical infrastructure*
On August 20, DESFA, the Greek national natural gas system operator, announced having suffered a cyber attack on part of its IT infrastructure by cybercriminals who tried to gain illegal access to their data. The company confirmed that some of its systems became unavailable and that there was a potential data leak. The operation of the national gas system was not impacted. According to news reports, data from the DESFA breach leaked on August 19 by the Ragnar Locker ransomware operation, who claimed responsibility for the attack.

Ransomware forces retailer in Denmark to stop operations *Ransomware, Retail*
Retail points of 7Eleven in Denmark ceased operations on August 8 due to a ransomware attack.

Portugese airline suffers ransomware attack *Ransomware Civil aviation*
Portuguese airline TAP was the target of a Ragnar Locker ransomware on August 25, but said that flight safety was not affected. It is unclear whether attackers had access to customer data.

Telecom firm suffers ransomware *Ransomware, Telecom*
Altice, a telecom company was the victim of a cyber attack by the Hive ransomware group. On its data leak site, the group claims to have carried out an attack on August 9, supposedly allowing it to steal data from the company.

German semiconductor manufacturer breached *Ransomware, Technology*
Semikron, a German semiconductor manufacturer, disclosed a cyber incident that led to portions of the company's IT systems and files being encrypted. The company says that a "professional hacker group" claims to have obtained data from the company's systems, but the extent of the data leak remains unknown and under investigation.

Other cybercrime

German organisation hit by cyber attack *Breach, Commerce coalition*
The Association of German Chambers of Industry and Commerce (DIHK) was targeted by a cyber attack. The organisation decided to shut down all of its IT systems and switch off digital services, telephones, and email servers, as a precaution and a way to give IT teams time to develop a solution and build up defence. DIHK is a coalition of 79 chambers representing companies within the German state, with over three million members comprising businesses ranging from small shops to large enterprises in the country.

Data theft extortion targeting MBDA — *Extortion, Defence contractor*

A group calling itself Andrastea claimed to have stolen 60 GB of data from MBDA, a France-based company, through a vulnerability in their network infrastructure. According to Adrastea, the stolen data includes information associated with employees working on military projects, commercial activities, correspondence with other firms, and contract agreements. The group also says it wants to sell the data and discuss the price in chat. MBDA confirmed they are the subject of a blackmail attempt and that the hackers started disseminated the information after the company refused to pay the requested ransom. MDBA claimed that the stolen data were acquired from an external hard drive and that there has been no compromise of corporate networks.

Moldova government servers breached — *Breach, Government*

The Moldovan government announced that the email servers of the country's President had been breached on August 10. it is unclear how long the email servers remained compromised and if any data leaked.

Polish remote water meter reading company breached — *Critical infrastructure*

Isra Polska, a company that manages remote water meter reading suffered a breach on August 11. According to the company's statement, its IT systems were shutdown but no additional information became known.

Dutch municipalities attacked — *Public administration*

Five municipalities in the Netherlands suffered a cyber attack which resulted in IT disruptions. According to the municipalities, no data was stolen.

Banking trojan targeting Spain — *Banking trojan*

On August 18, security researchers reported observing banking trojan Grandoreiro targeting employees of a chemical manufacturer in Spain as well as the automotive sector in Mexico. The attacks started with phishing emails impersonating, in the case of Spain, the Spanish Public Ministry.

Czech crypto company suffers theft — *Cryptocurrency*

General Bytes, A Czech Republic-based company, revealed that its Crypto Application server suffered a cyber attack resulting in the theft of digital currency. The threat actors exploited a zero-day vulnerability. The crypto firm adds that two-way ATMs started to forward coins to the attacker's wallet when customers sent coins to the ATM.

German light bulb manufacturer suffers cyberattack — *Malware*

German light bulb manufacturer Vosla GmbH was reportedly hit by a cyberattack. It is likely that these attacks were initiated by phishing emails.

Hacktivism

Killnet targets Italian institutions — *Russian threat actor, DDoS*

On July 30, Italian law enforcement announced that pro-Russia purported hacktivists targeted the websites of various Italian institutions and ministries. Killnet claimed responsibility for the attacks. Among the 50 institutions affected are Italy's Supreme Judicial Council, its customs agency and its ministries of foreign affairs, education and cultural heritage.The Italian embassy in London said on Twitter that the websites of the foreign ministry and all the country's embassies had been affected and were not operational at the moment.

Analyst note: We cannot confirm the accuracy of these claims.

Killnet attacks the Latvian parliament with DDoS *Russian threat actor, DDoS*
On August 11, the Russian-origin hacktivist group Killnet launched a DDoS attack against the Latvian parliament after the vote on a resolution that Russia is a statesponsor of terrorism and attacks civilians in Ukraine. The web services of the parliament became inaccessible that day.

Hackvists target Republic of North Macedonia *Breach*
Hacktivist claimed responsibility for breaching the Republic of North Macedonia's Ministry of Education and Science website.

Disruption and hijacking

Hacking concerns delayed balloting for new UK Prime Minister *Political party*
The UK's Conservative Party delayed selection for the next prime minister over concerns that hackers may alter online ballots after Britain's National Cyber Security Center (NCSC) warned that the system was vnerable to abuse. In response to the concerns, the Conservative Party overhauled online voting, which may result in delays as voters will not receive ballots until August 11.

Montenegro state institutions and critical infrastructure attacked
Government officials in Montenegro declared on August 29 that there were several attacks on the country's critical infrastructure. The attacks were coordinated and manage to cause disruption to services to citizens.

Data exposure and leaks

Exposed server at cards operator leaks data *Exposure, Data leak, Financial services*
According to a report on Twitter, on August 8, an EU-based virtual cards operator had an exposed server, which resulted in the leak of more than 67 million records from countries that included France, Germany, Italy, and Spain, in the period 2014-2022.

Autodoc suffered data leak *Data leak*
A German auto parts store, Autodoc, located in Finland, suffered a data breach, according to a statement sent to its customers. Attackers managed to break into the company's internal communication tool and used it to steal customers' personal data. The attack was quickly stopped, but the company says that data was still stolen. Customers' names, home addresses, phone numbers and email addresses were affected.

UK government lawyers leak officials' data *Data leak, Government*
In a data leak incident, revealed on August 24, UK government lawyers, handling reimbursement claims, published the names of several civil servants. The UK government's legal department has launched an investigation.

World

Cyber policy and law enforcement

US indicts Russian for spreading disinformation *Indictment*
A federal grand jury in the US has indicted Russian national Aleksandr Viktorovich Ionov. The individual was charged with spreading disinformation designed to further Russia's political ambitions and to disrupt US elections.

US introduces law on federal data centre cybersecurity *Legislation*
The US Senate has introduced the Federal Data Center Enhancement Act. The law tasks the Office of Management and Budget with establishing baseline security and resiliency standards for federal data centres.

US offers 10 million US dollars for information on Conti associates *Bounty*
US authorities announced that they are willing to pay 10 million US dollars for information on five members of the Conti ransomware operation. News reports clarify that such monetary rewards are offered for information related to threat actors affecting the national security of the United States.

Cyberespionage

Woody RAT used against Russian entities *Aerospace, Defence*
A newly discovered remote access trojan (RAT) dubbed Woody has been used to target Russian entities by using Office documents leveraging the Follina vulnerability. The threat actor targeted a Russian aerospace and defence entity.

APT27 targets entities in Taiwan and the Philippines *Supply-chain attack, Chinese threat actor*
Security researchers report that APT27, a Chinese threat actor, compromised the servers of Mimi, a messaging application, in a supply-chain attack, to spread malware. The campaign targeted entities in Taiwan and the Philippines.

APT31 targeting Russian companies *Supply chain attack, Chinese threat actor*
Security researchers report that APT31, a Chinese threat actor, compromised Russian companies by using phishing via legitimate cloud storage platforms. The group used the Yandex.Disk service and Dropbox.

Android malware used by APT groups *Social media, Android*
Meta reports that two APT groups have adopted a new Android malware. The two threat actors convince their targets to install the malware following lengthy interactions on social media.

Meta removes two Asian cyberespionage groups from their social media platforms *Social media*
Meta also reports that it has taken action against two cyberespionage groups, active in Asia. The first, Bitter APT, based in south Asia, targets countries in the South Asia region as well as the UK. The second, APT36, based in Pakistan, targets India, the Middle East and Afghanistan. Both groups were showing low sophistication activity using social engineering, Android malware and a rudimentary iOS app.

RedAlpha APT active in cyberespionage globally — *Human rights organisations, Chinese threat actor*
Security researchers report that RedAlpha APT group, a Chinese threat actor, has engaged in espionage activities since at least 2015. The group targeted humanitarian aid organisations, think tanks, and government organisations globally.

Kimsuky campaign in the Korean peninsula — *North Korean threat actor*
Security researchers report that Kimsuky, a North Korean threat actor, deployed a new cyberespionage campaign, dubbed GoldDragon, against various targets in the Korean peninsula. Among the targets were South Korean government officials, university professors and think tank researchers.

Iran-based Mercury threat actor targets Israeli organisations — *Log4j, Iranian threat actor*
Microsoft reported detecting a threat actor dubbed Mercury leveraging two Log4j vulnerabilities in SysAid applications against organisations in Israel. Microsoft assesses with high confidence that Mercury is affiliated with Iran's Ministry of Intelligence and Security.

TA423 targeting Australia and South China Sea — *Energy, Chinese threat actor*
Proofpoint reports uncovering a cyberespionage campaign which used the ScanBox malware to target entities involved in Australian governmental affairs as well as offshore energy production (wind turbine fleets) in the South China Sea. Proofpoint attributes the campaign to TA423, an espionage-motivated threat actor.

Cybercrime

Ransomware

Fin7 group switching to its own ransomware operation — *Ransomware*
The cybercrime group Fin7 reportedly intends to launch its own ransomware operation. The group previously initiated attacks to facilitate the distribution of malware by other ransomware-as-a-service (RaaS) operations.

Cisco suffers unauthorised access to data — *Ransomware, IT*
Cisco confirmed that the Yanluowang ransomware group had breached its corporate network in late May. The confirmation came after threat actors published data supposedly originating from Cisco and claiming to have exfiltrated 2,8GB of data in total.

Quantum ransomware disrupts a government agency in Dominican Republic — *Ransomware, Government*
The Dominican Republic's Instituto Agrario Dominicano suffered a Quantum ransomware attack which encrypted multiple services and workstations throughout the government agency.

Lockbit attacked security vendor Entrust — *Ransomware, IT Security company*
The operators of the Lockbit RaaS claimed responsibility for the breach of security company Entrust. Later, Lockbit's data leak website suffered a DDoS attack, which Lockbit claims came from Entrust. Lockbit later leaked data supposedly belonging to Entrust on BreachForum, a LockBit 3.0 data leak website.

Other cybercrime

Blockchain platform heist — *Blockchain, Supply-chain attack*

Solana, a US blockchain platform, suffered a cyber attack which reportedly resulted in the draining at least 7700 wallets of cryptocurrency, including Slope, Phantom, Solflare, and Trust Wallet. The value of the stolen crypto assets (including SOL, NFTs, and Solana-based tokens) is valued at 5,2 million US dollars. The platform has not yet determined how the threat actor gained initial access to its system. On Twitter, Solana's cofounder suggested the hack seemed like a supply-chain attack targeting both iOS and Android applications.

Crypto tokens being stolen worth 190 million US dollars — *Cryptocurrency*

A token bridge allowing the transfer of digital tokens between Ethereal, Evmos, Moonbeam, Avalanche, and Milkomeda C1 was exploited by threat actors who stole more than 190 million US dollars in crypto tokens.

Fake wallet website pushing malware — *Cryptocurrency*

A security researcher identified a fake website impersonating the official portal of Atomic wallet, a cryptocurrency exchange portal, which distributed copies of the Mars Stealer information-stealing malware.

Lazarus Group targets cryptocurrency employees with social engineering — *Social engineering, Cryptocurrency, North Korean threat actor*

Lazarus Group, a North Korean threat actor, reportedly lured employees of cryptocurrency companies with fake Coinbase job offers in order to compromise them.

Lazarus Group attempted stealing crypto assets — *Phishing, Cryptocurrency, North Korean threat actor*

Lazarus Group attempted to breach the cryptocurrency asset exchange protocol deBridge Finance, aiming to steal funds, through a malicious email campaign.

CISA released a list of the most detected malware strains of 2021 — *Malware*

According to the list, the most prolific malware users of the top malware strains are cyber criminals, who use malware to deliver ransomware or facilitate theft of personal and financial information. The top malware strains observed in 2021 include Agent Tesla, AZORult, Formbook, Ursnif, LokiBot, MOUSEISLAND, NanoCore, Qakbot, Remcos, TrickBot and GootLoader.

US law enforcement warns of residential proxies used in credentials stuffing attacks — *Credential stuffing*

US law enforcement warned that cybercrime groups use residential proxies to conduct large-scale credential stuffing attacks without being tracked, flagged, or blocked.

Malicious PyPl package used to spread minerware — *Supply chain attack, Cryptominer*

Security researchers report that Secretslib, a malicious PyPl package, infected Linux systems with minerware in what appears to be a supply-chain attack. The package downloads a Linux executable which it runs with elevated privileges, to install and execute a Monero miner.

LastPass password management firm breached — *Breach, Password management*

Threat actors reportedly accessed the password management firm LastPass' source code and proprietary technical information. LastPass acknowledged a breach and released a security advisory. A threat actor compromised a developer's account and used it to access the company's development environment.

130 organisations impacted by the Okta phishing campaign *Phishing*
Security researchers reports that a cybercrime group targeted over 130 organisations using a phishing kit codenamed '0ktapus'. The campaign resulted in unauthorised access to 9.931 credentials. The threat actor used the stolen credentials to gain access to corporate networks and systems through VPNs and other remote access devices. The campaign, dubbed 0ktapus, has been underway since at least March 2022.

Cloud messaging company breached *Cloud messaging*
The cloud messaging company Twilio disclosed that it was breached by an unknown actor that targeted it employees with SMS phishing messages. The breach resulted in the unauthorised access of some customer data. Since Twilio provides SMS verification services for other parties, the online messaging platform Signal was also affected. Via Twilio, attackers may have accessed the phone numbers and SMS registration codes of about 1.900 Signal users. Food delivery firm DoorDash disclosed a data breach exposing customer and employee data that is reportedly linked to the Twilio incident.

Email marketing service breached *Email marketing service*
Email marketing service Klaviyo confirmed a data breach compromising the personal data of its subscribers. Threat actors obtained an employee's login credentials through phishing and subsequently used the credentials to access the employee's Klaviyo account and the firm's internal support tools, allowing the threat actor to steal the information of 38 subscribers, all of whom are involved in the cryptocurrency industry.

Email services provider breached *Managed Services Provider*
A breach of the email services provider Mailchimp resulted in the exposure of personal data of the managed services provider DigitalOcean.

Hiden malware in James Webb telescope images *Phishing*
Security researchers uncovered an email phishing campaign dubbed GO#WEBBFUSCATOR in which attackers use space images from the James Webb telescope to spread malware.

Hacktivism

Taiwan's Presidential Office website hit by DDoS attack *DDoS, Taiwan, Chinese threat actor*
Taiwan's Presidential Office confirmed that its website suffered a DDoS attack on August 2, causing the website to be down for 20 minutes. In addition to the attacks on the president's website, experts noted that the websites of the Ministry of National Defence, the Ministry of Foreign Affairs and the country's largest airport, Taiwan Taoyuan International, were also affected.

Defacements in Taiwan *Defacement, Taiwan, Chinese threat actor*
On August 2, supermarkets in Taiwan began reporting that their televisions were hacked and began displaying messages telling US House Speaker Nancy Pelosi to leave Taiwan. Taiwanese media outlets also reported that TV screens at a Taiwan Railways Administration station seemed compromised and displayed a message in simplified Chinese referring to Pelosi in derogatory terms, the message was claimed by a pro-China purported hacktivist.

Pro-Russia purported hacktivist claims supposed attack on Lockheed Martin *Defence sector, US, Russian threat actor*
Pro-Russia purported hacktivist Killmilk, called on other hacktivists to target Lockheed Martin as well as to disseminate personal data of employees of the company. The group leaked supposed credentials of employees which were collected during a previous incident.

Disruption and hijacking

Google reports observing the largest DDoS attack so far *DDoS*
Google reports having observed the largest DDoS attack in history against one of its customers. The attack took place on June 1 and targeted a Google Cloud Armor customer with 46 million requests per second via an HTTPS DDoS attacks. It is reportedly the most powerful Level 7 DDoS attack to date.

Information operations

Meta removes disinformation network *Disinformation, Social media*
Meta reported that it had removed an entity called Cuber Front Z from its social media platforms. The entity ran a low-sophistication inauthentic operation that spread content in favour of Russia in relation to Russia's war on Ukraine.

Pro-Western influence campaign uncovered on social media *Influence operation, Social media*
Graphika and the Stanford internet Observatory investigated an interconnected web of accounts on Twitter, Facebook, Instagram, and five other social media platforms which used deceptive tactics to promote pro-Western narratives in the Middle East and Central Asia.
Analyst note: This is the first observed large-scale takedown of a pro-Western influence operation by a social media platform.

Data exposure and leaks

Twitter user data exposed *Social network*
Twitter revealed that it suffered a data breach due to an unknown threat actor exploiting a zero-day vulnerability. The breach resulted in the scraping of data from 5,4 million user accounts.

Over 80.000 exploitable Hikvision cameras are exposed online *Email service provider*
Security researchers report having discovered over 80.000 Hikvision cameras vulnerable to command injection vulnerability CVE-2021-36260. The vulnerability was addressed by Hikvision via a firmware update in September 2021.

Plex media streaming service acknowledged unauthorised access to data *Media streaming*
The Plex media streaming service informed its users that they should change their passwords following a detection of unauthorised access to a database containing usernames, email addresses and hashed passwords of users.

Russian media streaming platform breached *Media streaming*

A data breach has affected the Russian media streaming platform Start, impacting a reported 7,5 million users. Threat actors managed to steal a 2021 database of which they distributed samples online. The stolen database contains email addresses, phone numbers and usernames.

Massive leak of Chinese citizen information *Physical access control*

According to news reports a massive Chinese database storing faces and vehicle license plates, containing at least 800 million records, had been left exposed on the internet for months, until discovered and removed in August. The data was handled by a tech company managing systems for physical access control and personnel management, which was gathering face recognition and licence plate information.

Significant vulnerabilities

Critical vulnerabilities in Samba. *Samba*

The Samba Team has released security updates to address several vulnerabilities in their product. Exploitation of these vulnerabilities may allow an attacker to cause a DoS condition, data leakage, or even to take control of the whole domain. See CERT-EU SA 2022-056.

Critical vulnerability in VMware products *VMware*

Multiple critical vulnerabilities were reported by VMware. Exploitation of these vulnerabilities may lead to remote code execution without authentication, on the affected servers. See CERT-EU SA 2022-057.

Critical shell command injection vulnerability in Apache Spark *Apache Spark*

On July 18, Apache Spark released a security bulletin regarding a newly found critical vulnerability within Apache Spark's ACL implementation, tracked as CVE-2022-33891 and with a CVSS score of 8.8 out of 10. The flaw was discovered by a security researcher, with the proof of concept (PoC) exploit already available on GitHub and exploitation attempts in the wild being detected since, at least, July 26. Apache Spark is an open-source, unified engine for large-scale data analytics, which executes data engineering, data science, and machine learning tasks. Additionally, it provides high-level APIs in multiple programming languages. See CERT-EU SA 2022-058.

Critical vulnerabilities in Cisco VPN Routers *Cisco VPN Routers*

On August 3, Cisco released a security advisory and patches regarding several critical vulnerabilities affecting Cisco VPN routers. It is highly recommended to upgrade affected appliances as soon as possible. See CERT-EU SA 2022-059.

Windows vulnerabilities reported in Microsoft advisory *Microsoft*

On August 9, Microsoft released its August 2022 Patch Tuesday advisory including fixes for 2 zero-day vulnerabilities identified as CVE-2022-34713 and CVE-2022-30134, which affect respectively Microsoft Windows Support Diagnostic Tool (MSDT) and Microsoft Exchange Server. The patch also contained fixes for 17 additional critical vulnerabilities affecting Active Directory Domain Services, Azure Batch Node Agent, Microsoft Exchange Server, as well as other services. See CERT-EU SA 2022-060.

Reflected amplification DoS vulnerability in PAN-OS *Palo Alto Firewalls*

On August 10, 2022, PaloAlto released a security advisory regarding a Denial-of-Service (DoS) vulnerability affecting PAN-OS. Exploiting this vulnerability, a network-based attacker would be able to obfuscate its identity and implicate the vulnerable firewall as the source of an attack. While some software updates are not yet available, some mitigation and workarounds are available and should be applied as soon as possible. See CERT-EU SA 2022-061.

Remote Command Execution Vulnerability in Gitlab *Gitlab*
On August 22, GitLab released a security advisory regarding a Remote Command Execution affecting its products. This vulnerability exists in the “import via Github” functionality. Exploiting this vulnerability, allows an authenticated user to achieve remote code execution on the affected server. See CERT-EU SA 2022-062.

Path Traversal Vulnerability in Unrar affects Zimbra software *Zimbra*
In May 2022, security research team from SonarSource discovered a 0-day vulnerability in the “unrar” utility for Linux and Unix systems. This utility is a third party tool used in Zimbra. The exploitation of this vulnerability allows a remote attacker to execute arbitrary code on a vulnerable Zimbra instance without requiring any prior authentication or knowledge about it. Proof of Concepts (POC) are now publicly available as well as a metasploit module.

Remote command execution vulnerability in Gitlab *Gitlab*
On the August 22, 2022, GitLab released a security advisory regarding a remote command execution affecting its products. This vulnerability exists in the “import via Github” functionality. Exploiting this vulnerability, allows an authenticated user to achieve remote code execution on the affected server. See CERT-EU SA 2022-063.

All CERT-EU’s Security Advisories are available to the public on CERT-EU’s website, `https://www.cert.europa.eu/publications/security-advisories#2022`

1. Conclusions or attributions made in this document merely reflect what publicly available sources report. They do not necessarily reflect our stance.

TLP definition

TLP	Disclosure	Message
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER 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.
WHITE	Disclosure is not limited.	TLP:WHITE information may be distributed freely.