Cyber brief (July 2022)

August 1, 2022 - Version: 1.0

TLP:WHITE

Disclosure is not limited.

TLP:WHITE information may be distributed freely.

Executive summary

- We analysed 232 open source reports for this Cyber Brief.[1]
- Relating to **cyber policy and law enforcement**, the Council of the EU condemned attacks perpetrated by pro-Russia hackers. Public authorities in several EU countries (Germany, Romania, Spain and France) arrested (or issued an arrest warrant for) individuals involved in malicious cyber activities. European countries also banned or considered banning foreign media and technologies suspected of being involved in malicious activities.
- On the **cyberespionage** front, we observed a proliferation of reported activity by private sector offensive actors, the targeting of social media profiles of politicians and a report that the red teaming tool Brute Ratel is being abused by threat actors. In the EU, malicious cyberespionage activities originating in China and North Korea have been reported.
- Relating to **cybercrime**, we observe reported ransomware operations continuously targeting businesses and other organisations such as universities or public administrations. In July, based on open source and data leak sites' information, the top 5 most dangerous ransomware operations in Europe were Lockbit (by far the most active), followed by Hive, Black Basta, Karakurt and Vice Society. US authorities are accusing North Korean hackers of targeting the health sector with ransomware. On a global level, significant supply-chain attacks continue to affect programming language resources used by thousands of downstream applications. A new phishing-as-a-service platform named Robin Banks offers ready-made phishing kits targeting the customers of well-known banks and online services.
- On the **hacktivism** front, most activity related to Russia's war on Ukraine, self-proclaimed pro-Russia hacktivist groups such as Killnet, Xaknet and their affiliates claimed a number of DDoS attacks against the websites of public and private organisations in Ukraine, but also in EU countries such as Poland and Lithuania. Pro-Ukraine groups, such as IT Army of Ukraine and its affiliates, claimed DDoS attacks against hundreds of Russian targets in the governmental, media and telecommunications sectors.
- Regarding **disruptive** operations, Akamai claimed it detected and mitigated the largest DDoS attack ever launched against a European customer. In Sudan, internet services by multiple providers across the country were disrupted while anti-government protests were taking place.

- With relation to **data exposure**, we continue to observe that leaks often occur in conjunction with ransomware and then sold online. Twitter reportedly suffered a leak of phone numbers and email addresses belonging to 5,4 million accounts. Meta and US hospitals are accused of unlawfully collecting sensitive healthcare data about patients for targeted advertising. A threat actor offered what they claim is the personal data of one billion Chinese citizens up for sale.
- We have included several significant vulnerabilities reported in July 2022 and associated advisories.

Europe

Cyber policy and law enforcement

Council of the European Union warned of the escalation risk to cyber attacks *Denunciation, Russian threat actor*
On July 19, the Council of the European Union issued a statement that the increase in malicious cyber activities, such as the DDoS attacks against several EU Member States, claimed by pro-Russian hacker groups creates unacceptable risks of spillover effects, misinterpretation and possible escalation.

The Court of Justice of the EU rejected the appeal of Russia Today France against its broadcast ban *Ban, Foreign media*
The Court of Justice of the European Union dismissed Russian-state media Russia Today France's appeal against its broadcasting ban.

NSO group stated that fourteen EU countries bought Pegasus *Spyware, PSOA*
NSO Group (a private sector offensive actor or PSOA) reportedly claimed to have sold Pegasus spyware to 14 EU governments using export licenses issued by the Israeli government.

German authorities reportedly issued an arrest warrant for a Russian individual whom they accuse of compromising critical infrastructure *Arrest warrant, Critical infrastructure, Russian threat actor*
According to media reports, German authorities issued a non-public arrest warrant for one of the alleged perpetrators of a multi-year cyber operation that targeted, among others, electricity and water supply critical infrastructure. The individual is reportedly accused of being a member of the Russian APT group Dragonfly.

Romanian accused of cybercrime activity extradited to the USA *Extradition, Arrest*
A Romanian citizen was reportedly extradited to the US for facilitating the dissemination the Gozi malware. Additionally, the individual was allegedly involved in distributing the Zeus Trojan and SpyEye Trojan, initiating and carrying out DDoS attacks and disseminating spam. According to the indictment, the Gozi virus infected more than one million computers worldwide, including systems maintained by NASA and IT systems in Germany, Great Britain, Poland, France, Finland, Italy, Turkey and the United States.

Spain arrested suspects who allegedly sabotaged the country's radiation alert system *Arrest*
The Spanish police have arrested two hackers believed to be responsible for cyber attacks on the country's radioactivity alert network, which took place between March and June 2021.

France arrested a reported member of RaidForums — *Arrest*
French authorities have arrested an individual suspected of being a key member of the RaidForums group ShinyHunters. RaidForums was a black hat hacking internet forum active from 2015 until 2022. US prosecutors are requesting the extradition of the individual.

Spain and Romania arrest nine individuals on allegations of cybercrime — *Arrest*, *Scam*
Law enforcement authorities in Spain and Romania arrested three individuals in Spain and six individuals in Romania who are suspected of gaining three million Euro through internet scams including pushing advertisements for used cars.

The Netherlands ban Chrome — *Ban*, *Privacy*
The Ministry of Education in the Netherlands has decided to place a conditional ban on the use of the Chrome OS and Chrome web browser until August 2023 over privacy concerns.

Germany considers banning Chinese technology — *Ban*, *Chinese technology*
Germany is considering banning ZTE and Huawei from its telecommunication networks.

The Italian Data Protection Authority issued a warning to TikTok — *Warning*, *GDPR*, *Chinese technology*
The Italian Data Protection Authority issued a warning to the Chinese-owned TikTok video-sharing app over an alleged breach of the GDPR after TikTok informed users it would be sending targeted advertising without their consent from July 13, 2022 onwards.

UK drafts Online Safety Bill — *Legislation*, *Disinformation*
In its draft Online Safety Bill, the UK government is introducing a new duty of care for online platforms towards their users, requiring them to take action against both illegal and legal but harmful content. It is intended to help curb disinformation, online trolling, illegal pornography and internet fraud.

Maastricht University recovered its ransom — *Seizure*
The University of Maastricht revealed that the Netherlands Public Prosecution Service traced and seized a wallet containing the cryptocurrency paid by the university after a ransomware attack in December 2019.

Ukrainian law enforcement confiscated assets from cryptocurrency brokers — *Seizure*
The Ukrainian Prosecutor General's office confiscated assets belonging to cryptocurrency brokers and handed it to Ukraine's Asset Recovery and Management Agency. The brokers allegedly assisted users from Russia and Russia-occupied territories with cryptocurrency purchases.

Cyberespionage

Politicians reportedly targeted with impersonations on messaging apps — *Messaging app*, *Politicians*
The German government released a warning about targeted attacks against high-ranking politicians. Attackers are reportedly attempting to impersonate their targets on messaging apps such as WhatsApp, Messenger or Telegram in a bid to try and create fake profiles.
***Analyst note**: We consider tactics, techniques and procedures employed by attackers in this campaign to pose a significant threat to EUIBAs, especially individuals occupying high-ranking positions.*

Belgium issued a statement that Chinese hackers attacked its Ministry of Defence *Denunciation, Chinese threat actor*
The Belgian Ministry of Defence issued a statement wherein it accused Chinese threat actors of cyber attacks against the Belgian Ministries of Interior and Defence.

North Korean hackers reportedly attacked EU Member States *North Korean threat actor*
Security researchers reported uncovering a campaign, which they attribute to North Korean hackers, targeting organisations in the Czech Republic, Poland and other European countries. The threat actors reportedly used the Konni malware, a remote access Trojan capable of establishing persistence and performing privilege escalation on the host.

North Korean hackers reportedly used malicious browser extensions *North Korean threat actor*
Security researchers revealed witnessing the abuse of malicious browser extensions and attribute the activity to Kimsuky, a reported North Korean threat actor. The threat actor reportedly stole emails from Google Chrome or Microsoft Edge users reading their webmail.
***Analyst note**: Researchers assess that Kimsuky (aka Thallium, Velvet Chollima, SharpTongue) is a North Korean threat actor known for targeting individuals working for organisations in the US, Europe and South Korea on topics involving North Korea, nuclear issues, weapons systems, and other matters of strategic interest to North Korea.*

Austria-based PSOA *PSOA*
According to Microsoft, DSIRF is an Austria-based PSOA who sells multiple Windows and Adobe 0-day exploits. Microsoft reports that the software was used in limited and targeted attacks against European and Central American customers. The PSOA, which Microsoft tracks as KNOTWEED, reportedly developed malware called Subzero.

A Greek Member of the European Parliament (MEP) was reportedly targeted by mobile spyware *PSOA*
A security audit conducted by the European Parliament reportedly revealed an attempt to plant the Predator spyware, reportedly sold by Cytrox, on a phone belonging to an MEP.
***Analyst note**: We consider mobile spyware, especially those being sold by PSOAs, to be a high risk for EUIBAs.*

Cybercrime

Lockbit ransomware reportedly breached the Italian Revenue Agency *Ransomware, Public administration*
Lockbit group claims to have stolen 78 GB of data from the Italian Revenue Agency

The Spanish National Research Council reportedly suffered a ransomware attack *Ransomware, Public administration*
The Spanish National Research Council (Consejo Superior de Investigaciones Científicas) reportedly suffered a ransomware attack which encrypted some of the information processed by the central headquarters and its centres throughout the country.

German town reportedly suffers ransomware attack *Ransomware, Local administration*
Media reports claimed that the German town of Burladigen suffered a ransomware attack, without clarifying the type of malware strain or suspected threat actor.

La Poste Mobile was reportedly infected with the ransomware LockBit 3.0 *Ransomware, IT*
Media reports suggest that the French mobile postal service fell victim to a LockBit 3.0 ransomware infection around July 3. The organisation announced that its service was unavailable due to IT maintenance.

French energy firm reportedly suffered a by ransomware attack *Ransomware, Energy*
French energy company Idex was reportedly hit by a ransomware attack by a group called Industrial Spy. The group reportedly stole 215.8 GB of data including corporate financial documents and employee passport information.

The Swiss University of Neuchatel reportedly suffered a ransomware attack *Ransomware, Education*
The University of Neuchatel in Switzerland was reportedly hit by a ransomware attack on July 4. The organisation reportedly temporarily blocked access to its servers to protect its IT infrastructure and data.

The University of Wuppertal was reportedly hit by a ransomware *Ransomware, Education*
The University of Wuppertal acknowledged on Twitter that it had been hit with a cyber attack by unknown parties.

Hive ransomware group claims to have compromised a Spanish media organisation *Ransomware, Media*
The Spanish media organisation Castilla-La Mancha reportedly suffered a ransomware attack which rendered its website temporarily inoperable. The Hive group claimed responsibility for the attack on July 13 by publishing the data, reportedly belonging to the media organisation, on the HiveLeak website.

Germany-based construction and engineering company hit by cyber attack *Ransomware, Engineering*
The Knauf Group announced suffering a cyber attack which disrupted its business operations, forcing its global IT team to shut down all IT systems to isolate the incident. The company has been listed on the data leak site of the Black Basta ransomware operation.

Fake investment scams in Europe *Scam*
Media reports claim that a network comprising 10.000 rogue resources targeted European citizens with fake investment schemes. The following countries were reportedly targeted: Belgium, Czech Republic, Germany, Netherlands, Norway, Poland, Portugal, Sweden and the UK.

The British Army's Twitter and YouTube accounts were compromised *Scam*
The UK Ministry of Defence disclosed a breach of the British Army's Twitter and YouTube accounts. The accounts were reportedly compromised by threat actors and abused to spread non-fungible tokens and cryptocurrency scams.

Smishing campaign targeting French users *Smishing*
A vast Roaming Mantis campaign reportedly sent smishing SMSes with a malicious URL to French users. The URL either deployed the MoqHao Android malware, or redirected to an Apple login details credential harvesting page.

Hacktivism

Pro-Russia groups claimed attacks in Ukraine *Russian threat actor, DDoS, Hacking*
Pro-Russia groups such as Xaknet, Killnet and affiliates claimed a number of DDoS attacks against the websites of Ukrainian governmental and private sector targets. Additionally, they claimed the compromise of entities such as the Ukrainian Defence Ministry's Main Intelligence Directorate.

Pro-Russia groups claimed DDoS attacks in the EU *Russian threat actor, DDoS*

Pro-Russia groups such as Killnet and affiliates claimed a number of DDoS attacks against the websites of European public and private sector targets. Targeted countries in Europe include amongst others Poland and Lithuania. The targeted organisations belong to the transportation, energy, electronic, banking, logistics, telecommunications, law enforcement and governmental sectors.

Disruption and hijacking

Large DDoS attack against IT company Akamai *DDoS*

The cybersecurity and cloud service company Akamai revealed that it had blocked a large DDoS attack in Europe. The organisation claims to have been under constant assault, facing dozens of DDoS rounds over the past 30 days. On July 21 and in 14 hours, the DDoS activity peaked at 853.7 Gbps (gigabits per second).

World

Cyber policy and law enforcement

Israel's privacy protection authority seized servers of hacked travel company *Seizure, Israel*

Israel's privacy protection authority seized servers of Gol Tours LTD, which operates travel booking websites, after the owner reportedly failed to cooperate and address a security breach. Media reports allege that Iranian hackers obtained the personal information of over 300.000 Israelis through the security breach.

A former CIA official convicted for espionage *Condemnation, US*

A former CIA programmer has been convicted for espionage. The US Department of Justice said that the individual collected various intelligence-gathering tools to which he had access as a programmer and provided these tools and additional documents to WikiLeaks.

Russia fined Google 21 billion rubles *Fine, Russia*

A court in Moscow has imposed a fine of 21 billion rubles on Google for failing to restrict access to information considered prohibited in the country.

The US Department of Justice seized stolen funds from suspected North Korean hackers *Seizure, North Korean threat actor*

The US Department of Justice seized bitcoins worth nearly 500.000 US dollars from a suspected North Korean threat actor. The threat actor reportedly extorted US healthcare providers with ransomware. US authorities report having returned ransom payments to two hospital groups.

The US State Department increased its bounty for information about North Korean threat actors *Bounty, North Korean threat actor*

The US State Department has increased the reward paid to anyone providing information on any North Korean state-sponsored threat actor's members to 10 million US dollars.

Cyberespionage

New pentest toolkit abused by threat actors to evade defence *Defence evasion tool*

According to Palo Alto Unit 42, a number of threat actors are moving on from Cobalt Strike to the newer Brute Ratel post-exploitation toolkit to evade detection by EDR and antivirus solutions. Brute Ratel Command and Control Center (BRc4) was released in 2020 and was intended for red team penetration testing engagements.
***Analyst note**: Taking the example of Cobalt Strike, Brute Ratel C4 can be expected to become a ubiquitous tool in the threat landscape. We assess that this represents a threat to EUIBAs.*

Journalists infected with Candiru spyware *PSOA*

The Israeli spyware vendor Candiru was found using a zero-day vulnerability in Google Chrome to spy on journalists and other high-interest individuals in the Middle East with the 'DevilsTongue' spyware.

Cybercrime

Software supply-chain attack grabs data from apps and websites *Supply-chain attack*

Security researchers report a software supply-chain attack which targeted more than two dozen Node Package Manager (NPM) modules used by thousands of downstream applications, since approximately December 2021. NPM is a package manager for the JavaScript programming language. The compromised NPM modules have been collectively downloaded more than 27.000 times. The compromised NPM modules reportedly harvested sensitive data from forms embedded in mobile applications and websites.
***Analyst note**: We observe the proliferation of supply-chain attacks affecting programming language packages or libraries.*

Malicious packages steal tokens and bank card data *Supply-chain attack*

Security researchers report observing four suspicious packages each containing obfuscated malicious Python and JavaScript code in NPM repositories. The campaign, called LofyLife, reportedly used the open-source token logger Volt Stealer to steal Discord tokens from infected machines.

Lockbit ransomware gets an update *Ransomware*

The Lockbit group announced the release of an update to its ransomware-as-a-service (RaaS) program called LockBit 3.0. The group also launched a bug bounty program ranging from 1.000 US dollar to 1 million US dollar for flaws in LockBit, the LockBit dedicated leak site, TOX messenger and Tor.

Maui ransomware targets the health sector *Ransomware, North Korean threat actor*

The FBI, CISA and the US Department of the Treasury released a joint advisory reporting that Maui ransomware has been targeting the health sector. Maui ransomware is reportedly used by North Korean state-sponsored threat actors.

H0lyGh0st ransomware targets SMEs *Ransomware, North Korean threat actor*

Microsoft reports that a North Korea-linked group called H0lyGh0st, uses a ransomware payload with the same name for its campaigns and has successfully compromised small-to-medium sized companies in the manufacturing, financial, academic and hospitality sectors since September 2021.

Ransomware targeting internet-exposed QNAP devices *Ransomware, QNAP*

A new ransomware known as Checkmate is targeting internet-exposed QNAP devices with the SMB service enabled and accounts with weak passwords. Attackers are employing a dictionary attack to break accounts with weak passwords.

***Analyst note**: We regularly scan for internet-exposed and vulnerable devices in our constituency and where appropriate we alert them to help reduce the exposed attack surface.*

Cybercrime group 8220 reportedly grew its cloud botnet to more than 30.000 hosts *Cryptomining, Botnet*

8220, a cryptomining group, reportedly exploited Linux and cloud app vulnerabilities to grow its botnet to more than 30,000 infected hosts.

Robin Banks is reported phishing-as-a-service *Phishing-as-a-service*

Security researchers report identifying a new phishing-as-a-service platform named Robin Banks which reportedly offer ready-made phishing kits targeting the customers of well-known banks and online services.

EvilCorp reportedly uses Raspberry Robin *USB worm*

Microsoft reported discovering that a Raspberry Robin Windows worm used to deploy a malware downloader on networks matches EvilCorp's tactics. EvilCorp is a cybercrime group known for deploying ransomware. First spotted in September 2021, the Raspberry Robin Windows worm spread via infected USB devices to other devices.

Disruption and hijacking

Internet disrupted in Sudan amid protests against the military junta *internet service, Sudan*

Security researchers report that internet services by multiple providers across Sudan were disrupted on June 30, 2022. The incident occurred as anti-government protests took place.

Hacktivism

IT Army of Ukraine claimed DDoS attacks against Russian targets *DDoS*

pro-Ukraine groups, such as IT Army of Ukraine and its affiliates, claimed DDoS attacks against hundreds of Russian targets in the governmental, media and telecommunications sectors.

Data exposure and leaks

HackerOne breached by a previous employee *Insider threat, Data breach*

HackerOne, a vulnerability and bug bounty company, reported a security compromise occurring between April 2022 and June 2022. The breach was reportedly perpetrated by a now-terminated employee.

Threat actor offered for sale what it claims is the personal data of one billion Chinese citizens *China, Personal data breach*
ChinaDan, a threat actor offered what they claim is the personal data of one billion Chinese citizens up for sale. The data reportedly leaked from a Shanghai police database.

Data breach affecting Marriott International *Data breach, Hospitality sector*
Marriott International has confirmed that it suffered a data leak after a threat actor managed to trick an employee at a Marriott hotel into allowing the attacker to access that employee's computer, which ultimately allowed the attacker to access Marriott's IT systems.

Twitter reportedly suffered a data leak *Data breach, Twitter*
Twitter reportedly suffered a leak of phone numbers and email addresses belonging to 5,4 million accounts. Devil, a threat actor, offered the reported stolen data for sale.

Meta, US hospitals sued for using healthcare data to target ads *Data breach, Meta*
A class action lawsuit has been filed in the Northern District of California against Meta (Facebook), the UCSF Medical Center, and the Dignity Health Medical Foundation, alleging that the organisations are unlawfully collecting sensitive healthcare data about patients for targeted advertising.

Significant vulnerabilities

Jira Full-Read SSRF Vulnerability *Jira*
On June 29, Atlassian published a security advisory for a high severity security vulnerability in Mobile Plugin for Jira Data Center and Server. The vulnerability allows a remote authenticated user to perform a full read server-side request forgery via a batch endpoint. This vulnerability is tracked as CVE-2022-26135. See CERT-EU SA 2022-047.

Critical Remote Code Execution Vulnerability in GitLab *GitLab*
On June 30, GitLab released new software versions that fix several vulnerabilities, one of which is a critical remote command execution vulnerability identified as CVE-2022-2185 with a CVSS score of 9.9 out of 10. See CERT-EU SA 2022-048.

The Hive Unauthentified API Endpoint Leaking Data *The Hive*
On July 4, StrangeBee published an advisory about a critical vulnerability which could lead to the exposure of sensitive information about current activities in The Hive (creation, modification, deletion of any object). We strongly recommend to update to the latest versions available. See CERT-EU SA 2022-049.

Multiple Critical Vulnerabilities in Microsoft Products *Microsoft*
On July 12, Microsoft released fixes for one actively exploited zero-day vulnerability and 84 flaws. The zero-day vulnerability is tracked as CVE-2022-22047 and concerns a Windows CSRSS elevation of privilege, allowing an attacker to gain system privileges. Out of the 84 other security flows, four of them are classified as critical, as they allow remote code execution. See CERT-EU SA 2022-050.

Cisco Nexus Dashboard Multiple Vulnerabilities *Cisco Nexus*
On July 20, Cisco released a security advisory, which addressed one critical and two high severity vulnerabilities found in Cisco Nexus Dashboard. The vulnerabilities allow an unauthenticated remote attacker to execute arbitrary commands, read or upload container image files, or perform a cross-site request forgery attack. See CERT-EU SA 2022-051.

Critical Vulnerability in Questions for Confluence *Confluence*
On July 20, Atlassian released a security advisory to address a critical vulnerability which affects the Questions for Confluence app. Having the app enabled on Confluence Server or Data Center, creates the Confluence user account “disabledsystemuser”. The account is created with a hardcoded password and added to the “confluence-users” group, which allows viewing and editing all non-restricted pages within Confluence by default. See CERT-EU SA 2022-052.

Oracle Critical Patch Update *Oracle*
On July 19, Oracle released their quarterly Critical Patch Update advisory, a collection of patches which address multiple critical security flaws, affecting several of their products. Many of these vulnerabilities may be remotely exploited without the need for user credentials. It is therefore highly recommended to apply the security patches without delay. See CERT-EU SA 2022-053.

Critical SQL Injection Vulnerability *SQL Injection*
On July 21, SonicWall released security patches for their Analytics On-Prem and GMS products, addressing a critical SQL injection flaw. Immediate update to the patched versions is recommended. See CERT-EU SA 2022-054.

Possible Information Disclosure in MobileIron for Android *MobileIron*
The problem affects Android users using MobileIron and having Use smart send option enabled in Email+ client. When “user A” forwards/replies email to “user B”, “user B” receives a different email body instead of original email. This could lead to information disclosure especially in case of recipients being outside of the sender’s organisation. See CERT-EU SA 2022-055.

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