10 years CERT-EU

Cyber brief (June 2022)

July 1, 2022 - Version: 1.1

TLP:WHITE

Executive summary

- In the month of June 2022, CERT-EU analysed 259 open source reports for this monthly Cyber Brief.
- On the **cyberespionage** front, 7 significant campaigns targeted Europe. Globally open source reports mentioned campaigns reportedly originated in Russia, China, Iran and Lebanon. For these activities, APT groups were using spear-phishing, zero-day exploitation (in internet facing assets) and custom malware. The targeted sectors have included telecoms, finance, government, transportation, energy, and high-ranking military officials. Notably, activity by private sector offensive actors (PSOAs) proliferates.
- The most significant **cybercrime** threat remains ransomware. Important victims included, on the global level, the electronics company Foxconn, and in Europe, education facilities in Italy and in the UK, a German energy supplier, an Austrian hospital, and a municipality in Italy. According to open sources and data leak sites (DLS) information reviewed by CERT-EU, in June, the 3 most active ransomware operations in Europe have been Lockbit, Blackbasta, and Vice Society.
- **Information operations** mostly suggested false stories in relation to Russia's war on Ukraine. We also discuss an operation targeting the private sector which discredits strategic mining operations.
- **Hacktivists** operating either against or in support of Ukraine have been making constant claims of breaches and leaks. The Russia-affiliated actor Killnet has been announcing DDoS attacks against several European countries, which had only limited effects, Belarusian hacktivists leaked phone wiretaps of foreign embassies in Belarus, radio and TV broadcasts were hijacked in Ukraine and Russia, and there were several claims of defacements, mainly hitting Russia. Outside of Europe we discuss a Malaysian hacktivist group.
- With relation to **data exposure**, we discussed an incident involving AMD a chip manufacturer.
- We selected vulnerabilities and advisories deemed significant which were publicly reported during the month of June.

Europe

Cyber policy and law enforcement

European Parliament's committee hears NSO Group
In a hearing held before the European Parliament's committee looking into the use of spyware in Europe, the Israeli spyware firm NSO Group confirmed that at least five EU countries have used its software. The firm also reported that it had terminated at least one contract with an EU member country following abuse of its Pegasus surveillance software.

Hearing, PSOA

Germany issues arrest warrant for a GRU hacker
German federal prosecutors issued an arrest warrant for the Russian hacker Nikolaj Kozachek (aka "blabla1234565" and "kazak") who is accused of having carried out a cyberespionage attack against the NATO think tank Joint Air Power Competence Center in Germany in April 2017.

Arrest, Russian threat actor

Telegram reportedly fulfilled a German police data request
Der Spiegel claims that Telegram handed over user data to German police after Germany's Federal Criminal Police Office requested data belonging to users accused of terrorist activity and child abuse. Telegram denies turning the data over to German authorities and asserted that "to this day, we have disclosed 0 bytes of user data to third parties, including governments."

Data request, Privacy

Latvia increases transparency for the use of cryptocurrency
On June 8, the Latvian government announced approval of an amendment proposal to a Law on the Prevention of Money Laundering and Terrorist Financing. The amendment details requirements for customer identification and a ban on opening anonymous accounts. The relevance of the proposals is strengthened by today's geopolitical environment as it also ensures that no attempt is made to circumvent Western sanctions on Russia by using cryptographic assets.

Legislation, Cryptocurrency

Flubot mobile spyware takedown
An international law enforcement operation involving 11 countries has resulted in the takedown of Flubot, one of the fastest-spreading mobile malware to date. FluBot has been spreading aggressively through SMS, stealing passwords, online banking details and other sensitive information from infected smartphones across the world.

Takedown, Mobile spyware

Russian botnet RSOCKS disrupted
An international law enforcement operation involving agencies from Germany, the Netherlands, the UK and the US disrupted the infrastructure of a Russian botnet known as RSOCKS. It covered millions of compromised computers, Android smartphones, and IoT (Internet of Things) devices around the world.

Takedown, Botnet

Arrest of gang phishing financial assistance to Ukraine - Russia's war on Ukraine
Ukrainian authorities arrested nine members of a criminal group that operated over 400 phishing websites crafted to appear like legitimate EU portals offering financial assistance to Ukrainians. Cybercriminals were using forms on the site to steal visitors' payment card data and online banking account credentials and perform fraudulent, unauthorized transactions like moving funds to accounts under their control.

Arrest, Phishing gang

Cyberespionage

Phone surveillance - Russia’s war on Ukraine

Surveillance, Ukraine

On June 6, the deputy head of Ukraine’s State Special Communications Service stated that phones of Ukrainian officials had been targeted with malware. He elaborated that he and his colleagues were aware of the possibility of zero-click intrusions, but he would not say if they had been targeted by such attacks.

Sandworm phishing Ukrainian organisations - Russia’s war on Ukraine

Phishing, Ukraine

On June 10, CERT-UA reported that media organisations within Ukraine (such as radio stations, newspapers and news agencies) received phishing emails to lure them to download and execute malware such as Crescentlmp and Cobalt Strike Beacon. The threat actors abused CVE-2022-30190 (Follina) and used email addresses which had been acquired in a previous compromise of the Ukrainian government. CERT-UA attributed the activity, with medium confidence, to Sandworm (a Russian threat actor suspected of being part of the GRU).

APT28 Attacks Ukraine - Russia’s war on Ukraine

Malware, Ukraine

On June 20, CERT-UA reported an incident which they attributed to APT28. They reported having identified a malicious document which leads the installation and execution of the CredoMap malware. Metadata suggested that the malicious document was last modified on June 9, proving that was a very recent attack.

Chinese threat actor Gallium targeting finance and government

Chinese threat actor, Telecoms, Finance, Government

According to PaloAltoNetworks, the likely Chinese state-sponsored threat actor GALLIUM (aka Softcell) has deployed a new capability called PingPull in support of its espionage activities. The group is reportedly targeting telecommunications, finance and government organisations across Southeast Asia, Europe and Africa.
Analyst note*: CERT-EU assesses that this activity poses a potential threat to EU institutions, bodies and agencies (EUIBAs).*

Italian private-sector offensive actor’s spyware used in Kazakhstan

PSOA

Researchers at Lookout have uncovered enterprise-grade Android surveillanceware used by the government of Kazakhstan within its borders. The spyware, which was named “Hermit,” is likely developed by Italian spyware vendor RCS Labs S.p.A and Tykelab Srl, a telecommunications solutions company suspected by researchers to be operating as a front. Lookout researchers assess that Hermit had been used before by Italian authorities in an anti-corruption operation in 2019 and by an unknown actor in northeastern Syria. On June 23, Google’s Threat Analysis Group (TAG) revealed that RCS Labs had received help from some ISPs to infect Android and iOS users in Italy and Kazakhstan.

Germany Green Party hit by cyber attack

Political party

The German Green Party was hit by a cyber attack that affected its IT systems. The attack breached the email accounts belonging to Annalena Baerbock and Robert Habeck, who are ministers in the current government, as well as those of other members of the party. Some messages were forwarded to external servers.
Analyst note*: According to open sources, the objective of the attackers is currently unknown. CERT-EU is categorising the attack under “cyberespionage” due to the attackers reportedly stealing emails from victims.*

New APT group targeting Microsoft Exchange servers

APT group

According to Kaspersky’s Global Research & Analysis Team (GReAT), an APT group dubbed ToddyCat had been targeting Microsoft Exchange servers throughout Asia and Europe for more than a year, since at least December 2020. Researchers have also found a previously unknown passive backdoor they named Samurai and a new piece of trojan malware, dubbed Ninja Trojan.
Analyst note*: CERT-EU assesses that this activity poses a potential threat to EU institutions, bodies and agencies (EUIBAs).*

Backdoor targeting IIS servers in Europe and other continents

Backdoor

According to Kaspersky, a poorly detected malicious IIS backdoor dubbed “SessionManager” has been leveraged starting late March 2021 against NGOs and government organisations in Africa, South-America, Asia, Europe, Russia and the Middle-East. Kaspersky analysts believe with medium to high confidence that the module has been deployed thanks to previous “ProxyLogon”-type vulnerabilities exploitation on Exchange servers.
***Analyst note**: CERT-EU assesses that this backdoor poses a potential threat to EUIBAs. The exploitation of vulnerable MS Exchanges servers has been a major attack vector in incidents affecting EUIBAs since at least 2021.*

Cybercrime

Palermo municipality disrupted and data stolen

Ransomware, Stolen data, Dark web, Municipal administration

The municipality of Palermo in Italy suffered a ransomware attack which resulted in the shutdown of its IT systems. The impacted systems included the public video surveillance management, the municipal police operations centre, and all of the municipality’s services. Data that was stolen during the incident ended up being sold on the dark web. The cybercrime group Vice Society claimed responsibility for the attack.

UK schools affected

Ransomware, Education

Cybercriminals named two UK schools as victims of Vice Society ransomware. The incident reportedly affected the schools’ IT systems, including their website, phone, and email services.

University of Pisa alledgedly compromised

Ransomware, Education

The University of Pisa in Italy has allegedly been held to ransom for $4,5 million. BlackCat has claimed responsibility for the cyber attack.

German energy supplier hit

Ransomware, Energy companies

The IT systems of Darmstadt-based energy supplier Entega have fallen victim to a cyber attack. Two other public utility companies in Germany, namely Mainzer Stadtwerke and Frankfurt Waste Management and Service Group (FES), have also been victims of cyber attacks. Entega spokesman Michael Ortmanns said on June 12 that the email accounts of around 2.000 employees and the company’s websites were particularly affected. The OT such as critical infrastructure that operates Entega’s electricity, gas and water networks, is reportedly not affected.

Austrian hospital suffered disruption and leak

Ransomware, Healthcare

The Medical University of Innsbruck suffered an incident which disrupted IT services and allegedly a data leak. Vice Society, a ransomware gang, has claimed responsibility.

Evilnum APT targets migration services

APT, Targeted attacks

According to a blogpost, the cybercriminal group Evilnum conducted several targeted attacks against European entities since the beginning of 2022. While the key targets of the Evilnum group have predominantly been in the financial services sector, specifically companies dealing with trading and compliance in the UK and Europe, in March 2022, they were observed targeting an intergovernmental organisation which deals with international migration services.
***Analyst note**: CERT-EU assesses that this activity poses a potential threat to EU institutions, bodies and agencies (EUIBAs).*

Cryptostealing campaign infects visitors of cracked versions of software

Cryptocurrency

A cryptostealing campaign, dubbed FakeCrack, infects users through dubious sites that supposedly offer cracked versions of well-known, widely used software. Most infected users were in France and Brazil.

Pharmaceutical company suffers hack-and-leak

Hack-and-leak

Novartis, a pharmaceutical company, suffered a hack-and-leak by the threat group called Industrial Spy, after efforts to extort them for money. On June 2, the group began selling data that was allegedly stolen from Novartis on their Tor extortion marketplace for $500.000 in bitcoins.

Hacktivism

Lithuania and Norway targeted by pro-Russia hacktivists - Russia's war on Ukraine

DDoS, Lithuania Norway

Between June 21 and 27, several Lithuanian state and private websites were targeted with DDOS attacks, in what Killnet claimed is a retaliation for Lithuania's halting of transit goods towards Kaliningrad, Russia in order to enforce EU sanctions on Russia. Targets reportedly included Lithuania's railways ticketing portal and the website of Ltgrid an electricity grid company. Then on June 29, Killnet targeted a number of websites in Norway. These attacks took place after Norway enacted restrictions for Russia on shipping on the very north.

Russian ICS allegedly hijacked - Russia's war on Ukraine

ICS, Russia

Between May 27 and June 14, four pro-Ukraine hacktivist entities (GhostSec, Squad 303, Miaximus and One Fist) claimed breaches of Russian Industrial Control Systems (ICS) without revealing their specific targets. On June 6, the head of the Russian Foreign Ministry information security division accused the United States of acting under the banner of the hacktivist group IT Army of Ukraine to conduct cyber activities against Russian critical infrastructure.

Defacement of Russian Ministry - Russia's war on Ukraine

Defacement, Russia

On June 5, the website of the Russian Ministry of Construction, Housing, and Utilities was defaced, with pro-Ukraine messages. On June 6, the IT Army of Ukraine claimed responsiblity for the defacement.

Hacktivists broadcast Ukrainian anthem on Russian Radio - Russia's war on Ukraine

Russia, Radio

According to industry reporting, on June 8, hacktivists compromised Russian radio station Kommersant FM and broadcast the Ukrainian national anthem and anti-war songs. Reportedly, the radio station was quickly taken off air. The incident marks the latest attack by likely pro-Ukraine hacktivists against Russian media outlets in response to the invasion of Ukraine.

Hacktivists claim breach of Russian ISP - Russia's war on Ukraine

Russia, Internet Service Provider

On June 9, the pro-Ukraine Hacktivist Anonymous "LulzSecMafia" claimed the breach of UFANet, a Russian internet service provider. The same day, LulzSecMafia published reportedly stolen data from ER-Telecom, a Russian telecommunication company.

Hacktivists force Putin to delay a speech - Russia's war on Ukraine

Russia

Russian President Vladimir Putin was forced to delay a speech at the St. Petersburg International Economic Forum on June 17 after a cyber attack disrupted the site's access-badge management system. The system was hit by a DDOS attack starting on June 16.

Hacktivists leak reported phone wiretaps of foreign embassies in Belarus - Russia's war on Ukraine

Belarus, MFA

The hacktivist group Belarus Cyber Partisans claims to have acquired wiretaps of foreign embassies in Belarus which were reportedly initially collected by the Belarusian government.

Hacktivists claim the takedown of Belarusian governmental websites - Russia’s war on Ukraine
The hacktivist entity YourAnonSpider posted a video on Twitter claiming the takedown of several Belarusian governmental websites. The group claimed it was a retribution for Belarusian governmental support for Russia’s war on Ukraine.

Belarus

Streaming of football game hijacked - Russia’s war on Ukraine
During the World Cup match between Ukraine and Wales, Oll.tv, an Ukrainian online video service, was compromised and the streaming of the match was replaced with other content. The Communications Director of the parent company, SCM, attributed the compromise to Russian hackers.

Ukraine

Hacktivists claim leak of Russian information - Russia’s war on Ukraine
The hacktivist entity Aggressive Griffin — purportedly an offshoot of the pro-Ukraine hacktivist group “Against the West” — claimed to have leaked data from multiple Russian organisations, including the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) and two major Russian companies of the energy sector: Lukoil and Gazprom. The leaked data included email addresses, usernames, and hashed passwords along with other account information.

Data leak, Russia

Killnet calls on cybercrime groups to join operations - Russia’s war on Ukraine
The Hacktivist group Killnet invited groups known for spreading Conti and REvil ransomware to join forces against US, Italian and Polish targets.

Ransomware

Information operations

Anti-Ukraine narratives in Poland - Russia’s war on Ukraine
Researchers identified 27 Polish-language Telegram channels disapproving of Ukrainian refugees in Poland, posting anti-Ukrainian narratives, and favourably depicting Russia's military activity in Ukraine's Donbas region, likely with the objective to negatively impact public opinion about Ukrainian refugees in Poland.

Social media, Poland, Ukraine

Supposed Ukrainian illegal weapons’ sale - Russia’s war on Ukraine
Researchers claim to have uncovered a Russian information operation consisting of a supposed Ukrainian illegal weapons’ sale on the dark web. The researchers claim that these firearms’ sale listings were posted on pro-Russia Telegram channels and on Russian media outlets shortly after publication on the darknet markets.

Telegram, Media, Ukraine

Disruption and hijacking

Ukrainian ISP reportedly hijacks Russian internet - Russia’s war on Ukraine
In response to the Russian invasion, a Ukrainian Internet services provider (ISP) reportedly attempted to hijack Russian Internet resources, via BGP hijacking which could redirect traffic to non-intended directions or block transmissions. According to researchers, a significant incident with the use of this technology occurred on March 8, when the Ukrainian internet provider Lurenet made an interception of Russian network traffic. The incident reportedly affected 146 autonomous systems around the world disrupting services on these networks for ten hours.

Internet Service Provider

Slovak Telekom and TMobile CZ reportedly hit by cyber attack
Slovak Telekom was reportedly targeted by a large-scale cyber attack on Sunday, June 26. Internal IT systems were reportedly affected causing the Telekom website and application to malfunction. A similar operator in the Czech Republic (TMobile-CZ) was reportedly affected in a similar fashion.

Telecoms

Data exposure and leaks

Emails leaked in Russia - Russia's war on Ukraine
On June 1, DDOSecrets publised 1,5 million emails reportedly belonging to Vyberi Radio and unearthed by the Anonymous collective. Vyberi Radio is an operator of radio stations throughout Russia.

Radio stations

VPN users data exposed
According to the Cybernews researchers, Romania-based free virtual private network (VPN) provider BeanVPN left some 18,5 GB of connection logs, that included more than 25 million records exposed on the internet and publicly accessible. The logs contained user device and Play Service IDs, connection timestamps, IP addresses, and other information.

VPN

World

Cyber policy and law enforcement

Russian online censorship
Between May 31 and June 2, Russian media regulator Roskomnadzor blocked the official mobile application of the Tor bowser in an app store and confirmed it is planning to block virtual private networks (VPNs) in Russia under the "sovereign internet" law.

Russia, Censorship, VPN

First US Ambassador to cyberspace
Nathaniel Fick has been selected as the first US State Department's inaugural Ambassador-at-Large for Cyberspace and Digital Policy.

US, Ambassador for cyberspace

Anti-privacy measures in India
India issued a new set of rules requiring, among other anti-privacy measures, that VPN providers retain customer logs for at least 180 days. On June 7, the VPN provider Surfshark (which claims to maintain a strong no-logs policy) announced that they'll stop operating servers in India.

India, Data retention, VPN

Singapore charges eight people for a phishing campaign
On June 24, the Singapore District Court charged eight people for suspected participation in a phishing campaign and subsequently laundering the stolen money.

Singapore, Charge

US-Brazil joint operation takes down digital piracy network
Following a joint US-Brazilian investigation dubbed Operation 404.4 focused on preventing digital piracy, 272 websites were taken down and six individuals arrested.

US, Brazil, Takedown, Arrest

Australian court sentenced two for phishing campaign
An Australian court sentenced two individuals for their participation in a financially motivated sms-phishing campaign.

Charge

US law enforcement agencies took down a marketplace with leaked data
US law enforcement, in partnership with Cyprus Police, took offline SSNDOB, an online marketplace that had put on sale stolen names, social security numbers, and dates of birth of approximately 24 million US citizens.

Takedown, Market place

Russia passes bill to fast-track foreign media bans
According to the Moscow Times, Russian lawmakers approved legislation allowing officials to block foreign news outlets in retaliation for clampdowns against Russian state media abroad. The bill gives Russia's Prosecutor General the right to ban foreign outlets without court approval if another government is found carrying out "hostile actions against Russian media abroad."

Russia, Block foreign news

US FCC urges Google, Apple to drop TikTok app
U.S. Federal Communications Commission (FCC) Commissioner Brendan Carr has sent letters to Apple and Google imploring the companies to remove TikTok from their respective app stores based on TikTok's "pattern of conduct and misrepresentation regarding the unfettered access that persons in Beijing have to sensitive U.S. user data," which puts the app "out of compliance" with the companies' app store policies.

US, Ban foreign technology

Cyberespionage

Lebanese threat actor reportedly targets Israel
Microsoft reported malicious activity abusing OneDrive, targeting an Israeli organisation, and attributed it to a previously undocumented Lebanon-based threat actor named Polonium.

Lebanese threat actor, Israel

Iranian threat actor reportedly targets US, Middle East, and India
Microsoft reports to have disrupted a spear-phishing operation linked to Bohrium, an Iranian threat actor that targeted a wide range of industry sectors (including tech, transportation, government, and education) in the US, Middle East, and India.

Iranian threat actor, US, Middle East, India

US government warns of Chinese attacks on telecom sector
The US government released an alert stating that Chinese state-sponsored actors have compromised major telecommunications companies and network service providers worldwide to exfiltrate traffic.

Chinese threat actor, Telecoms

Aoqin Dragon, a reportedly Chinese threat actor discovered
SentinelLabs reports to have discovered Aoqin Dragon, a reportedly Chinese threat actor, which has been targeting government, education, and telecommunication organisations in Southeast Asia and Australia since 2013.

Chinese threat actor

Iranian threat actor reportedly targets Middle East with a new backdoor
Zscaler reported a new campaign where the Iranian threat actor Lyceum was utilising a new piece of malware, which targeted companies in the energy and telecommunications sectors in the Middle East. The newly developed malware, a .NET based DNS Backdoor, reportedly copied code from the open source tool "DIG.net".

Iranian threat actor, Energy, Telecoms, Middle East

Spear-phishing towards former, high-ranking, Israeli and US officials
The Israeli company CheckPoint has revealed a spear-phishing operation which it claims was executed by the Iran-affiliated Phosphorous group, which targeted high-level Israeli and US oficials. Targets included former Israeli officials, high-ranking military personnel, academic in research institutions, think tanks, and Israeli citizens. Attackers reportedly took control of executives' existing accounts and created fake identities from stolen accounts to lure their targets into long email conversations.

Iranian threat actor, Israel, US

Chinese threat actor exploits zero-day in Sophos firewalls
Volexity reported on a sophisticated and heavily targeted attack, by multiple Chinese APT groups, leveraging a zero-day exploit to compromise the victim's Sophos firewall. Following the initial breach, the operation launched attacks against the victim's staff. These attacks aimed to further breach cloud-hosted web servers hosting the victim's public-facing websites.

Chinese threat actor, Zero-day, Firewall, Cloud

User data of US TikTok users has reportedly been repeatedly accessed from China
According to leaked audio from more than 80 internal TikTok meetings, China-based employees of ByteDance, TikTok's operator, have repeatedly accessed nonpublic data of TikTok users in the US. The recordings contain statements from nine different TikTok employees indicating that engineers in China had access to US data at least between September 2021 and January 2022.

Social network

Google TAG reports observing Hack-for-hire groups used to exfiltrate data
Google TAG reports it observes Hack-for-hire teams executing attacks rather than selling tools to do so in India, Russia, and the UAE. The groups are reportedly used to exfiltrate data from typically human rights activists, political activists, journalists.

Hack-for-hire

Cybercrime

Foxconn breached by ransomware
Foxconn, an electronics company, was hit by Lockbit ransomware, which impacted one of their factories, in Mexico. The Foxconn CTBG MX factory in Juárez had already been hit by such an attack in December 2020.

Ransomware, Technology

Evil Corp becomes LockBit affiliate
UNC2165, a cybercrime group which overlaps with the infamous Evil Corp gang, has switched to deploying LockBit ransomware on targets' networks. Using LockBit ransomware would allow the cybercrime group to blend in with other affiliates and make attribution more difficult.

Ransomware

Mandiant denies that there is evidence proving the claim that they were breached with ransomware
LockBit ransomware claimed that they had hacked the network of the cybersecurity firm Mandiant and had stolen data, additionally saying, "All available data will be published!". Mandiant responded that there was no evidence to support these claims.

Ransomware, Cybersecurity

Ransomware actors build site for victims to search for their stolen data
The BlackCat (aka ALPHV) ransomware gang has built a new website on which ransomware and data breach victims can check whether their information had been compromised in a ransomware attack.

Ransomware

BlackCat ransomware targets unpatched Exchange servers
According to Microsoft, affiliates of the BlackCat ransomware are now attacking Microsoft Exchange servers using exploits targeting unpatched vulnerabilities.
***Analyst note**: In significant incidents to which CERT-EU responded in 2021, the most targeted technology was Microsoft's Exchange server, which was compromised in more than half of the attacks. As regards BlackCat, according to information available on DLS, as of mid June, at least 31 organisations in Europe had fallen victims to this piece of ransomware since the beginning of the year.*

Ransomware, Microsoft Exchange

Emotet steals credit card information
Operators of the Emotet malware have updated their techniques and started using the botnet to specifically target credit card information stored in the Chrome web browser.
***Analyst note**: CERT-EU observes that Emotet has been the malware strain with the highest amount of sightings in EU institutions, bodies and agencies (EUIBAs) in June 2022.*

Botnet, Credit card info stealer

Clipminner makes millions with cryptocurrency mining
A cybercriminal operation is making millions in illicit gains from cryptocurrency mining and theft. The latter is implemented with a botnet dubbed Clipminer, which performs clipboard hijacking.

Botnet, Cryptojacking

Facebook users were phished in a large-scale campaign
A phishing operation has tricked Facebook and Messenger users into entering their account credentials and seeing advertisements. The campaign operators used these stolen accounts to send further phishing messages to their friends, generating significant revenue via online advertising commissions. Researchers estimate that in 2021, 2,7 million users had visited one of the phishing portals, with another 8,5 million in 2022.

Social Media, Phishing

1,65 million Elrond stolen from cryptocurrency exchange Maiar
Cryptocurrency exchange (DEX) Maiar was compromised by threat actors who stole 1.65 million Elrond (EGLD) after which the platform was taken offline.

Cryptocurrency

Largest NFT marketplace breached
OpenSea, the largest non-fungible token (NFT) marketplace, with more than 600,000 users and a transaction volume that surpassed $20 billion, disclosed a data breach and warned users of phishing attacks that could target them.

NFT

Lazarus reportedly steals $100 million USD worth of cryptocurrency
According to the blockchain analytics company Elliptic, there are strong indications that North Korea's Lazarus Group is responsible for the theft of nearly $100 million USD worth of cryptocurrency that resulted from the compromise of the Harmony Horizon Bridge.

North Korean threat actor, Cryptocurrency

Information operations

DRAGONBRIDGE influence operations targeting rare earth mining sector
According to Mandiant, a pro-China information operation on social media targeted the rare earth mining industry, a strategically significant sector whose resources are used in defense products. The fake content pushed environmental concerns on social media critical of US, Canadian and Australian mining projects.

Chinese threat actor, Rare earth mining

Hacktivism

Malaysian hacktivists deface Indian government websites
A Malaysia-based hacktivist group called DragonForce Malaysia targeted prominent government websites throughout India, reportedly in response to comments regarding the Prophet Mohammad, which had been made by an Indian politician. The group defaced approximately 70 Indian government websites, including the Indian embassy in Israel, the National Institute of Agriculture Extension Management, and the e-portal of the Indian Council of Agriculture Research.

Defacement, India, Malaysia

Data exposure and leaks

Chip manufacturer AMD sufferes hack-and-leak
AMD, a manufacturer of semiconductors suchs as chips says they are investigating a cyber attack after the RansomHouse gang claimed to have stolen 450 GB of data from the company last year.

Hack-and-leak

Significant vulnerabilities

Critical vulnerability in Atlassian Confluence
On June 2, researchers at Volexity revealed that hackers were actively exploiting a new Atlassian Confluence zero-day vulnerability tracked as CVE-2022-26134 to install web shells. Altassian released fixes on June 3. See CERT-EU SA 2022-040.

Atlassian Confluence

Critical vulnerability in Gitlab
On June 1, GitLab released updates fixing several vulnerabilities, one of which could lead to Account Take Over. This critical vulnerability is identified as CVE-2022-1680 with a severity score of 9.9 out of 10. See CERT-EU SA 2022-041.

Gitlab

Critical Vulnerability in Windows NFS
Microsoft issued security fixes for the critical vulnerability CVE-2022-30136 which is a RCE vulnerability in the network file system (NFS). The vulnerability can be exploited by an unauthenticated attacker using a specially crafted call to a NFS service. The vulnerability is not exploitable in NFSV2.0 or NFSV3.0. See CERT-EU SA 2022-042.

Windows

Critical vulnerability in Splunk
Splunk addressed a critical-severity vulnerability - CVE-2022-32158 (severity score of 9.0) - existing in Splunk Enterprise deployment servers prior to version 9.0 that allow clients to leverage the server to deploy forwarder bundles to other clients. Because of this issue, an attacker could compromise an Universal Forwarder endpoint and then abuse it to execute arbitrary code on other endpoints connected to the deployment server. See CERT-EU Guidance 22-003.

Splunk

Critical vulnerabilities in Citrix ADM
Citrix released security updates to address critical vulnerabilities (CVE-2022-27511 and CVE-2022-27512) in Application Delivery Management that could allow an unauthenticated attacker to log in as administrator. All supported versions of Citrix ADM server and Citrix ADM agent are affected. See CERT-EU SA 2022-043.

Critix

NTLM Relay Attack for Windows Domain Takeover *Windows*

A Windows NTLM relay attack has been discovered that uses MS-DFSNM, Microsoft's Distributed File System, which can take over a Windows domain. This service is vulnerable to NTLM relay attacks, which is when threat actors force, or coerce, a domain controller to authenticate against a malicious NTLM relay under an attacker's control. See CERT-EU SA 2022-044.

TheHive and Cortex Active Directory Authentication Bypass *TheHive, Cortex*

StrangeBee published an advisory about a critical vulnerability in the Active Directory (AD) authentication module of TheHive. The vulnerability allows impersonating any account on the platform, including administrators. The exploit is possible if the configured AD is on-premise. If the Active Directory authentication module is not enabled nor configured, or if Azure AD is used, the system is not vulnerable. See CERT-EU SA 2022-045.

Critical PHP flaw exposes QNAP NAS devices to RCE attacks *QNAP NAS*

Certain QNAP NAS products are vulnerable to remote code execution (RCE) when certain conditions are met. The CVE-2019-11043 is reported to affect PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11. See CERT-EU SA 2022-046.

Hardware attack against Apple's M1 chipset *MacOS*

Researchers at the Massachusetts Institute of Technology (MIT) have uncovered a new hardware attack dubbed "PACMAN" which is rooted in pointer authentication codes (PACs). The attack has been demonstrated to work against Apple's M1 processor chipset, and could potentially be exploited by attackers to achieve arbitrary code execution (RCE) on macOS systems.

Bypassing tenant separation in Azure *Azure*

Researchers revealed a critical vulnerability, called SynLapse, in Microsoft Azure Synapse Analytics, also affecting Azure Data Factory. It permitted attackers to bypass tenant separation while including the ability to (1) obtain credentials to other Azure Synapse customer accounts, (2) control their Azure Synapse workspaces, (3) execute code on targeted customer machines inside the Azure Synapse Analytics service, (4) leak customer credentials to data sources external to Azure. Microsoft has now fixed the issue.
Analyst note*: This issue is yet another reminder of the inherent complexity of cloud-based solution and of poor design choices sometimes made by cloud services providers.*

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`

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.

TLP	Disclosure	Message
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.