10 years CERT-EU

Cyber Security Brief (September 2022)

October 3, 2022 - Version: 0.1

TLP:WHITE

Disclosure is not limited.

TLP:WHITE information may be distributed freely.

Executive summary

- We analysed 389 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement**, in the Balkans, Kosovo and Albania responded to recent state-sponsored attacks by cutting diplomatic ties or establishing new cyber defence capacities. Ukraine warned of possible Russian cyber attacks on critical and energy infrastructure and arrested individuals accused of selling personal data of Ukrainian and European citizens to the Russian government.
- On the **cyberespionage** front, researchers detected activity in Europe by at least two Russian state-sponsored groups. On the global level, a campaign targeted military contractors and likely North Korean activity aimed at a messaging system and the diplomatic sector.
- Relating to **cybercrime**, ransomware attacks continue to target organisations in all businesses. In Europe, the 3 most active ransomware operations in September have been Lockbit, Sparta and AlphV. There were victims in critical sectors like energy, transportation, healthcare, and defence. Ransomware groups also targeted a number of public administrations and two universities.
- In Europe, researchers uncovered a Russia-based **information operation** which is replicating various European media organisations to distribute content with themes denigrating Ukraine and likely fake polls claiming anti-Russia sanctions were causing rising costs of living for Europeans.
- As regards **digital censorship**, the Iranian government disrupted internet services in the country and restricted access to social media. Governments of both Azerbaijan and Armenia put restrictions on TikTok.
- On the **hacktivism** front, the Anonymous collective launched the campaign #OpIran (DDoS attacks, data breaches, and data wipes) against the Iranian government, in support of ongoing anti-government protests. In Russia, there was an intensification of hacktivist attacks following the decree of mobilisation.
- Regarding **disruptive** operations, Kosovo faced a number of attacks targeting its government and critical infrastructure.
- With relation to **data exposure**, in Europe, data leaks affected a number organisations in the financial, IT, defence, healthcare and social media sectors.

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

Europe

Cyber policy and law enforcement

Albania attributed cyber attacks to Iran

Attribution

The Albanian Prime Minister announced on September 7, that the country would cut diplomatic ties with Iran after Albania, suffered attacks on July 15 (see Cyber Brief CB-22-08) reportedly linked to Iran. The attacks combined ransomware with a wiper and caused disruption of government systems. The US Department of Treasury announced sanctions against the Iranian Ministry of Intelligence. On September 9, another similar attack against Albania took place and affecte computer systems used by Albanian state police. NATO sent a senior-level delegation to Albania on September 21, to help with the consequences of the cyber attack.

Analyst note*: After the disruptive attacks in Montenegro, Kosovo, Bosnia-Herzegovina, Albania is the fourth Balkan country in a few weeks facing large-scale disruptive cyber attacks targeting government systems and critical infrastructure. In two cases, the targeted country has reportedly attributed the attacks to a foreign state (Russia in Montrenegro and Iran in Albania).*

Kosovo established a cybersecurity agency

Capacity

After a number of cyber incidents affecting state organisations (see chapter “Disruption and hijacking” below), the government of Kosovo is taking legislative steps to establish a State Authority for Cyber Security.

Ukraine warned of upcoming Russian cyber attacks on critical and energy infrastructure

Warning

CERT-UA issued a warning that the Russian government is preparing cyber attacks against Ukraineʼs critical infrastructure and DDoS attacks against allies.

EU Cyber Resilience Act in the approval process

Legislation

On September 15, the European Commission introduced a proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act. The aim is to bolster cybersecurity rules to ensure more secure hardware and software products.

Romania launched a legislative project to prohibit Russian cybersecurity products

Legislation

On September 14, Romania launched a legislative project on cybersecurity. The draft legislation under discussion prohibits the purchase and use by Romanian public institutions of antivirus products and services from Russian entities. The measure attempts to address the possible abuse of such products by Russian authorities.

Google Analytics deemed unlawful by Danish Data Protection Agency

Data protection

The Danish Data Protection Agency concluded, in a guidance document of September 21, that the use of Google Analytics is unlawful, due to its non-conformity with GDPR. Data protection authorities in Austria, France, and Italy have issued similar decisions in 2022.

Ukraine arrested individuals for selling European data subjects’ personal data to a Russian actor

Arrest

On September 28, we observed reports that the Ukrainian police arrested individuals who are accused of having sold personal data of Ukrainian and European citizens to the Russian government. The individuals reportedly sold the personal data of 30 million people on the dark net and received payments via YuMoney, Qiwi and WebMoney.

Dutch police arrested man for laundering millions in stolen crypto *Arrest*

The Dutch police arrested a 39-year-old man on suspicions of laundering tens of millions of euros worth of cryptocurrency stolen in phishing attacks. The police released the suspect on September 8, and the police continues its investigation.

German police carries out raids on suspected internet fraudsters *Arrest*

Germany's federal criminal police carried out raids on the homes of three individuals suspected of orchestrating large-scale phishing campaigns that defrauded internet users of EUR 4 000 000.

WT1SHOP seized *Seizure*

US law enforcement seized WT1SHOP, a Portugal-located forum and payment mechanism, for selling and purchasing stolen personal data. As of December 2021, records showed that the website supported approximately 106 273 users and 94 transactions.

Cyberespionage

Gamaredon targeted Ukrainian organisations *Russian threat actor*

Russian hackers have been targeting Ukrainian entities with previously unseen info-stealing malware during a new espionage campaign that is still active. Security researchers at Cisco Talos attribute the campaign to Gamaredon, a Russia-linked threat actor.

Analyst note*: Before and since the beginning of Russia's war on Ukraine, Gamaredon has been one of the most active Russian cyberespionage groups active in Ukraine. In a few cases, Gamaredon also targeted entities in the EU. We assess that Gamaredon poses a threat for EU institutions, bodies and agencies.*

APT28 spear-phishing campaign in Europe *Russian threat actor*

According to Cluster25, the Russian APT28 threat actor executed a spear-phishing campaign using a PowerPoint vulnerability to deliver the Graphite malware. The malicious PowerPoint file masqueraded as an Organisation for Economic Co-operation and Development (OECD) guideline. The campaign targeted entities in at least two EU countries.

Analyst note: *For several years, APT28 has been a prolific Russian cyberespionage threat actor, globally. While this adversary has focused on Ukraine in recent months, we assess that this threat actor continues to pose a threat for EU institutions, bodies and agencies.*

Cybercrime

Ransomware

French hospital refuses to pay ransomware *Healthcare*

The Corbeil Essones hospital in the southeast of Paris was severely affected in its capacity to operate, following a Lockbit ransomware infection in August. According to the hospital, it will take several months for work to return to normal. The French Gendarmerie negotiated with the cybercriminals and managed to lower the ransom demand to the equivalent of roughly 1 million US dollar. The hospital announced, however, on September 2 that they would not pay the ransom. In late September, attackers started to release personal data stolen from the hospital on the dark net. This data would relate to the hospital's staff, partners and patients.

AlphV group claims attack on Italian energy company

Energy

The ransomware group AlphV (BlackCat) claimed on their data leak site (DLS) on September 2 that they were behind the attack on the state-owned energy firm responsible for running Italy's electricity market, Gestore dei Servizi Energitici, which took place in August.

Energy company Eni hit in attack

Energy

The Italian energy company Eni disclosed, on September 1, that it suffered a cyber attack, claiming it experienced a minor impact. The ransomware group AlphaV claimed responsibility on their DLS, on September 2.

Portugal airline company breached

Transportation

After it had attacked the Portuguese airline TAP, in August, the cybercrime group behind the RagnarLocker ransomware released customer data on the dark web. In the last in a series of releases, the groups exposed company documents on September 21. Attackers claim to have exposed data of about 1,5 million TAP customers. Politicians, including Portuguese President Marcelo Rebelo de Sousa, were among those whose personal data leaked.

Italian municipality victim of Lockbit

Local administration

The municipality of Gorizia, Italy reportedly suffered a ransomware attack according to the DLS of the Lockbit 3.0 ransomware, on September 5. News media reported that more than 50 GB of data was stolen in the breach, allegedly being data of municipal agencies. The municipality reportedly suffered the ransomware attack between 27 and 28 August 2022.

French municipality's online services are offline following an unspecified cyber attack

Local administration

On September 26, the French municipality of Caen reportedly suffered a cyber attack. Some of the city's online services became unavailable.

Server of the Parliamentary Assembly of Bosnia-Herzegovina suffered a ransomware attack

Parliament

According to a press release, the Parliamentary Assembly of Bosnia and Herzegovina shut down its main server of the parliament due to a ransomware attack from September 9 to 10. The CryptoLocker ransomware operation is reportedly behind this attack.

Czech arms supplier and manufacturer suffered a ransomware attack

Defence

According to the media outlet Ransomwaremap, the cybercrime group Lockbit 3.0 claimed responsibility for a ransomware attack against the Czech security and weapons production company DSS on 16 September. The company has until 23 September to pay the ransom and recover 200 gigabytes of stolen data. According to Lockbit, the data contains arms contracts and customer data of DSS.

Italian university extorted after ransomware incident

University

The Stormous ransomware group attacked Tor Vergata University in Rome. The attackers threatened to reveal personal data of close to 20 000 students if their ransom demands were not met.

Other cybercrime

Threat actors abused French government servers in a phishing campaign

Government

Threat actors reportedly exploited legitimate servers belonging to the French government-operated employment site Pôle Emploi to conduct their phishing campaign. The campaign leveraged legitimate servers, a legitimate sender, and legitimate IP addresses. In the attack chain, the threat actor was responding to legitimate job postings on the employment website with PDFs containing malicious URLs.

French municipality’s public WiFi unavailable

Government

Comminter, a French company, provides public WiFi to the municipalty Tarbes. The public WiFI was unavailable following a cyber attack on Comminter. The nature of the attack is unconfirmed.

French university hit

University

The French Leonardo da Vinci University was the victim of a cyber attack. The attackers gained access to an application server containing personal data such as civil status, contact details, bank information, official and administrative documents and academic data of the enrolled people. Attackers did not encrypt the university’s information. They claimed they only wanted to be paid for exposing a security flaw in the system, which they considered a form of pentesting.

Information operations

Russian influence operation imitating European media

Russian threat actor

Researchers at EU DisinfoLab uncovered a Russia-linked influence operation network that has been operating in Europe since at least May 2022 and is ongoing. The operation, dubbed Doppelganger, replicated various European media organisations to distribute content with themes denigrating Ukraine, including allegations that members of the Ukrainian government were Nazis. Additionally, many false websites distributed videos containing likely fake polls claiming anti-Russia sanctions were causing rising costs of living for Europeans; the polls reportedly had hard-coded results supporting the claim of European hardship stemming from the war in Ukraine.

Hacktivism

Killnet threatening Georgia

Russian threat actor

Killnet a purported pro-Russia hacktivist group, threatened on September 14 that it would target Georgia in its next operation. Georgia has reportedly stated that it wants to open a new military front against Russia with the aim of liberating South Ossetia. Killnet added that, should this happen, Killmilk would personally see to the “genocide” of Georgians around the world.

Killnet wants to become more lethal

Russian threat actor

On September 21, Killnet indicated that in parallel with the Russian government’s mobilisation order, the group would also mobilise to become more lethal and less focused on actions now deemed too soft.

Anonymous Russia targets Germany

Russian threat actor, DDoS

On September 23, Anonymous Russia claimed to have targeted the websites of the German federal criminal police, the German astronomical community and a national museum with DDoS attacks.

Disruption and hijacking

Attacks against Kosovo government and critical infrastructure *DDoS*
In the first half of September, government systems in Kosovo faced DDoS attacks that caused occasional interruption of internet services within government institutions and an occasional lack of access to government services. The attack also targeted Kosovo Telecom and internet services on mobile and landline phones were interrupted.

Balkan media hit by a DDoS attack *DDoS*
The websites of the Balkan Investigative Reporting Network and one of its Greek partners reportedly suffered a DDoS attack by Turkish attackers on Saturday morning, following the publication of an investigation into Turkish businessman Yasam Ayavefe, who was convicted of defrauding online gamblers in his home country in 2017 and arrested in Greece in 2019.

Swedish Election Authority targeted on the day of the vote *DDoS*
According to officials at the Swedish website val.se, the site faced serious technical problems as a result of DDoS attacks from 10 to 11 September. The head of the authority's secretariat said on 11 September: "There have been three DDoS attacks against val.se".

Akamai stopped new DDoS attack in Europe *DDoS*
A new DDoS attack has broken the previous record that Akamai recorded recently in July. On September 12, these attacks culminated at unprecedented levels when the traffic sent to the target network peaked at 704.8 Mpps, roughly 7% higher than the July attack.

Data exposure and leaks

Lithuanian banking system provider suffered data breach *Finance*
BankingLab, a Lithuanian banking system provider for financial technology (FinTech) companies, disclosed a data breach. According to BankingLab, the threat actor accessed data belonging to several individuals and legal entities. The company also stated threat actors made the stolen data publicly available.

OrangeCyberFR suffered data leak *IT*
OrangeCyberFR, a French company, confirmed the publication of a file containing the personal data of several hundred French customers. Cybercriminals are offering the data for sale on a deep web forum.

Portuguese military reportedly leaked documents *Defence*
Portuguese local news organisation Diario de Noticias, claims that the Armed Forces General Staff agency of Portugal (EMGFA) has suffered a cyber attack that allegedly allowed the theft of classified NATO documents, which are now sold on the dark web. EMGFA is the government agency responsible for the control, planning, and operations of the armed forces of Portugal.

Swedish healthcare data exposed *Healthcare*
A cyber attack on a German medical supplier exposed data from at least 30 healthcare facilities in Sweden, including the Skaraborg Hospital.

Data from a Latvian social media platform put for sale *Social media*
On September 20, a cybercrime group put online information supposedly from the Latvian social media platform ASKfm, up for sale. The seller alleged that the data came from a 2020 breach and claimed the database contained data of 350 million users, with data linked to their use of the social media platform.

World

Cyber policy and law enforcement

US government sanctioned ten Iranians

Sanctions

The US announced sanctions against ten individuals and two entities affiliated with Iran's Islamic Revolutionary Guard Corps for their involvement in ransomware attacks.

US border forces seizing travellers' phone data

Surveillance

A news report, on September 15, claimed that the US Customs and Border Protection agency has conducted warrantless searches of phones and other electronic devices of travellers and has maintained acquired data for up to 15 years. At least 10 000 searches and data seizures have been performed each year and include all types of personal data.

Indonesia gets Data Protection law

Data protection

On September 20, the Indonesian parliament passed a data protection law. The law sets obligations for data managers in the public and private sectors, establishes an oversight body, and specifies fines and punishment for data mishandling.

Censorship, Internet control

Social media restriction in Azerbaijan and Armenia

Social media control

On September 15, the governments of both Azerbaijan and Armenia put restrictions on TikTok. The restrictions were introduced for security reasons and coincided with heightened tensions between both countries.

Internet services disrupted in Iran

Internet disruption
Social media control

According to internet monitoring services, there was a disruption of internet service in Tehran and other parts of Iran on September 16. The disruption coincided with protests against the regime. A disruption also affected internet services in parts of western Iran on the evening of September 19. Authorities restricted social media platforms Instagram and WhatsApp nationally as of September 21. They also shut down mobile networks. See also the "hacktivist" chapter below for more cyber stories related to protests in Iran.

Cyberespionage

Campaign targeting military contractors

Defence

Researchers at Securonix discovered a covert cyberespionage campaign targeting multiple military contractors, including likely a strategic supplier to the F-35 Lightning II fighter aircraft. Attackers used a stager, persistence and obfuscation to hide the malware.

Worok targets Asian governments and companies

Asia

Worok, a cyberespionage group, has reportedly compromised public and private sector targets Asia since at least 2020 using a combination of custom and existing malicious tools.

ShadowPad infections in Asian governments
The espionage malware ShadowPad Remote Access Trojan (RAT), was detected in a range of government and state-owned organisations in some Asian countries since at least early 2021. Intelligence gathering appears to be the main goal.

Asia, ShadowPad

North Korean threat actor continued job opportunity phishing
North Korean hackers are reportedly luring targets with fake job opportunities in phishing attacks via WhatsApp. They use trojanised versions of the PuTTY SSH client to deploy backdoors on targets' devices.

North Korean threat actor

North Korea targets MFA of Russia
News reports attributed a recent campaign targeting Russia's Ministry of Foreign Affairs to the North Korean threat actor Kimsuky. The campaign reportedly targeted email accounts of Russian embassies in China and Japan.

North Korean threat actor, Diplomacy

Metador targets MENA region
Security researchers say they have uncovered a previously undetected APT tracked as Metador that has been targeting internet service providers, telecommunications firms, and universities in Middle Eastern and African countries for roughly two years.

Middle East, Africa

APT10 reportedly used steganography to avoid detection
Security researchers report that a threat actor linked to APT10 used steganography to hide their payload in the Microsoft Windows logo to avoid antivirus detection.

Chinese threat actor, Steganography

Cybercrime

Ransomware

Chilean court system suffers ransomware
On August 25, the Chilean judicial system suffered a CryptoLocker ransomware infection which began with a malicious email. On September 27, a spokesperson said that no data was stolen during the incident.

Public administration

US secondary school suffers ransomware attack
Los Angeles Unified, a school district in the US, disclosed that a ransomware attack hit its IT systems. Vice Society claimed responsibility for the attack.

Education

QNAP detects ransomware
On September 3, QNAP Systems Inc, a Taiwan-based company, detected the Deadbolt cybercrime group exploiting a Photo Station vulnerability to encrypt QNAP network access storage systems directly connected to the internet. QNAP released a patched version which mitigates the threat within 12 hours of detecting the vulnerability.

IT

Hotel chain suffers disruptive cyber attack
InterContinental Hotels Group announced that they suffered a disruptive cyber attack after its network was breached.

Hospitality

Emotet serving ransomware variants Quantum and AlphV
Security researchers observed that cybercrime groups are using Emotet to spread the Quantum and AlphV ransomware variants.

Botnet

LockerGoga decryptor released

Decryptor

On September 16, Bitdefender released a free decryptor for the LockerGoga ransomware. A law enforcement operation led to the arrest of LockerGoga in October 2021. As the cybercriminals have stopped using this ransomware, they will not develop new versions of the malware and past victims can use the decryptor.

Other cybercrime

GitHub advisory warned of phishing targeting users' credentials and multi-factor authentication

IT

GitHub warned of threat actors targeting GitHub users with a phishing campaign by impersonating CircleCI to harvest user credentials and two-factor authentication codes. While GitHub itself was not affected, the campaign has impacted many victim organisations. According to GitHub, threat actors often immediately downloaded private repository contents that users have access to.

Hackers breach software vendor for Magento supply-chain attacks

Supply-chain attack

Multiple extensions of FishPig, a vendor of Magento WordPress integration, suffered malware infections. The extension has been downloaded over 200 000 times. The threat actor reportedly had access to FishPig's servers and added malicious code to the vendor's software to gain unauthorised access to websites using the products.

YouTube channel abused to run cryptocurrency scam

Social media

Threat actors reportedly abused a YouTube account called Scuba Jake, and allegedly defrauded his 13 million followers of at 1.01 Bitcoin through a fake bitcoin giveaway.

YouTube abused to spread malware

Self-propagation, Social engineering, Social media

A threat actor has uploaded malicious links on YouTube video content that incorporates these links. The malicious links trigger the download of malware which steal information such as passwords and cryptowallet details. Additionally, the malware uses its victims to self-propagate by uploading malicious videos to new locations.

Healthcare payments stolen

Healthcare

The US Federal Bureau of Investigation (FBI) alerted healthcare payment processors who route payments to bank accounts controlled by threat actors. In 2022, threat actors reportedly stole 4,6 million US dollar from healthcare companies after gaining access to customer accounts and changing payment details.

Uber suffers cyber attack

Transportation, Social engineering

On September 15, reports arose that Uber suffered a cyber attack. A threat actor reportedly gained unauthorised access to the company's vulnerability reports, security software, email dashboard, and Slack server. According to news reports, the threat actors used social engineering methods, including a multi-factor authentication fatigue attack. The company confirmed the breach and reported that they believe the Lapsus$ cybercrime group is behind the attack. On September 23, UK law enforcement arrested a suspect.

TeamTNT hijacking computing resources

Server hijacking, Cryptocurrency

Security researchers reported that TeamTNT, a cybercrime group, attempts to defeat Bitcoin's blockchain encryption. In a campaign called the Kangaroo attack, the group hijacks servers to use them as a computing resource to run an encryption solver.

Cryptocurrency theft *Cryptocurrency*

On September 20, Wintermute, a digital assets trading company, disclosed that after a cyber attack in its Decentralised Finance (DeFi) platform, it lost the equivalent of 162 million US dollar.

Gaming platform abused to spread malware *Supply-chain attack, Gaming*

A threat actor gained unauthorised access to the support system of the gaming company 2K and abused it to spread malware. Specifically, users of the support system started receiving emails, purporting to be replies to their submitted requests, which contained the RedLine information stealing malware.

Game code stolen *Gaming*

A threat actor claimed to have gained unauthorised access to Rockstar Games, a video game company. The actor published videos showing the play development of the game Grand Theft Auto (GTA) 6 and claimed to be in possession of the source code for the game.

Chaos is a Go-based Swiss army knife of malware *Botnet*

Researchers at Black Lotus Labs discovered a new Go-based malware that cybercriminals developed to create botnets. They infected both Windows and Linux machines as well as wide array of software used in devices ranging from home office routers to enterprise servers. Malicious actors can use the botnet for cryptomining and to launch DDoS attacks.

Brute Ratel cracked and shared across the cybercriminal underground *Post-exploitation toolkit*

Researchers found that malicious actors cracked Brute Ratel, a post-exploitation toolkit, and are now sharing the tool for free across Russian-speaking and English-speaking hacking communities. Brute Ratel is similar to other frameworks such as Cobalt Strike. It focuses on evading endpoint detection and response (EDR) and antivirus (AV) tools. Researchers assess that cybercriminals, especially ransomware affiliates, will use this tool in the short-to-medium term.
Analyst note*: We assess that the malicious use of Brute Ratel poses a significant threat to organisations worldwide, including EUIBAs.*

Hacktivism

OpIran by Anonymous targets Iran *Iran*

On September 20, the hacktivist group Anonymous and their affiliates launched the campaign #OpIran. The operation reportedly targeted the Iranian government and coincided with ongoing anti-government protests. The hacktivists claim to have conducted DDoS attacks, data breaches, data wipes, and to have advised Iranian citizens on how to bypass internet restrictions.

Pro-Ukraine hacktivists target Russian mobilisation *Russia*

There was an intensification of hacktivist attacks following the decree of mobilisation in Russia. Several of these attacks were of disruptive nature, aiming at hindering the mobilisation. Notably, a hacktivist entity claims to have compromised a ground-base segment of a Russian satellite communication system.

Disruption and hijacking

Iperva reports observing long DDoS *IT*

On September 20, Imperva, a software company, reported that it observed a significant DDoS attack against one of its customers. The attack took place on June 27 and although it did not exceed previous DDoS incidents in volume, it had the novelty of being particularly persistent, lasting more than four hours.

Data exposure and leaks

Misconfigured server exposed COVID-19 antigen tests of 1,7 million people in India *Healthcare*

A misconfigured Elasticsearch server belonging to an India-based healthcare software provider leaked the personal data of 1,7 million Indian citizens and foreign nationals. Affected individuals include those who took COVID-19 antigen tests using the Covi-Catch kit when traveling to or from India in recent years.

Bad development practices exposed AWS credentials *Mobile applications*

On September 1, Symantec researchers reported that at least 1859 mobile applications (the vast majority of those being iOS applications) were exposing hard-coded Amazon Web Services (AWS) credentials due to bad development practices. Adversaries could use hard-coded AWS credentials to access application databases containing customer records.

Samsung confirmed exposure of customer data *Electronics*

Samsung confirmed a data breach after reports saying that some of its US systems leaked customer data.

US Internal Revenue Service suffered a data leak *Public administration*

The Internal Revenue Service accidentally leaked confidential information for approximately 120 000 taxpayers who filed a form as part of their tax returns.

TikTok clarified that it did not suffer a data leak *Social media*

On September 2, AgainstTheWest, an online persona, created a topic on a hacking forum claiming to have breached both TikTok and WeChat. The actor shared screenshots of a database allegedly belonging to the companies, which they say was accessed on an Alibaba cloud instance containing data for both TikTok and WeChat users. TikTok clarified that the data posted to a hacking forum is unrelated to the company.

Data reportedly belonging to Cisco published *IT*

Yanluowang, a cybercrime group, published data which they allegedly stole from Cisco in August. Cisco reportedly refused to pay the ransom demand.

Revolut breach exposed thousands of clients *Finance*

On September 19, Revolut, a financial services company, disclosed that it had suffered a breach which resulted in the stealing of personal and financial data of more than 50 000 customers, 20 000 of which are based in Europe. The company clarified that user funds had not been accessed.

Data leaked at American Airlines *Transportation*

On September 16, American Airlines disclosed unauthorised access to employee email accounts and personal data of customers.

Australian telecom customer data stolen

Telecommunication

On September 22, Optus, an Australian telecom provider, confirmed that it suffered unauthorised access to its systems and data. The incident resulted in exposure of the personal data of up to nine million Australians to the threat actor. The company clarified that no payment data was exposed.

Auth0, a subsidiary of the authentication service provider, disclosed a data breach

Authentication services

A third-party individual notified the company of being in possession of a copy of certain Auth0 code repositories dating from October 2020 and earlier. Okta, the parent company of Auth0, was already impacted by a January 2022 cyber attack claimed by the Lapsus$ data extortion group.

Significant vulnerabilities

Multiple Critical Vulnerabilities in Microsoft Products

Microsoft

On September 13, Microsoft released its September 2022 Patch Tuesday advisory including fixes for 2 zero-day vulnerabilities identified CVE-2022-37969 and CVE-2022-23960 which affect several Windows system versions. The patch also contains fixes for five critical vulnerabilities affecting Microsoft Dynamics, Windows IKE Extension and Windows TCP/IP. See CERT-EU SA 2022-064.

RCE Vulnerability in Sophos Firewall

Sophos

On September 23, Sophos warned about a critical code injection security vulnerability in the company's Firewall product that is being exploited in the wild. They observed the vulnerability being used to target a small set of specific organisations, primarily in the South Asia region. See CERT-EU SA 2022-065.

Vulnerabilities affecting multiple versions of the BIND 9

BIND

On September 21, the Internet Systems Consortium (ISC) has released security advisories that address vulnerabilities affecting multiple versions of the ISC's Berkeley Internet Name Domain (BIND) 9. A remote attacker could exploit these vulnerabilities to potentially cause denial-of-service conditions. See CERT-EU SA 2022-066.

Critical WhatsApp Vulnerabilities

WhatsApp

WhatsApp has patched two remote code execution vulnerabilities in its September update. These could have allowed an attacker to remotely access a device and execute commands. The vulnerabilities were discovered by WhatsApp internal security team and there are no indications that these have already been exploited. See CERT-EU SA 2022-067.

New Microsoft Exchange Zero-Day Vulnerabilities

MS Exchange

On September 28, security researchers at GTSC described a cyber attack which utilised two zero-day vulnerabilities in Microsoft Exchange that allow an attacker remote code execution. The attackers chained the pair of zero-days to deploy Chinese Chopper web shells on compromised servers for persistence and data theft, as well as move laterally to other systems on the victims' networks. Microsoft identified the vulnerabilities as CVE-2022-41040, a Server-Side Request Forgery (SSRF) vulnerability, and CVE-2022-41082, a remote code execution (RCE) vulnerability when PowerShell is accessible to the attacker. See CERT-EU SA 2022-068.

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.