10 years CERT-EU

Cyber Security Brief (November 2022)

December 1, 2022 - Version: 1.0

TLP:WHITE

Disclosure is not limited.

TLP:WHITE information may be distributed freely.

Executive summary

- We analysed 241 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement** in Europe, the European Parliament adopted new legislation to strengthen EU-wide cyber resilience, while the Digital Services Act entered into force. Law enforcement operations in several European countries resulted in arrests of cybercriminals. Data protection authorities fined enterprises in various sectors (social networks, messaging, electricity distribution) not respecting the GDPR. At a global level, Turkey imposed temporary restrictions on social media, and the US decided to ban electronic equipment manufactured by Huawei, ZTE, Hytera, Hikvision, and Dahua over national security concerns.
- On the **cyberespionage** front in Europe, a report revealed new Lazarus activity targeting European entities, while researchers analysed a commercial spyware developed by a Spain-based vendor. In the rest of the world open sources reported on three campaigns by China-linked threat actors, a new backdoor used by a North Korean threat actor against selected targets, a Vietnam-linked campaign and an Android spyware linked to Iran. Researchers scrutinised applications of the COP27 and the FIFA World Cup and found they are overly intrusive.
- Relating to **cybercrime**, ransomware continues to be a prime area of activity. In Europe, several attacks targeted local administrations (municipalities, regions), educational institutions, and healthcare facilities. There was a non-confirmed attack on a defence/technology company. Based on information from data leak sites (DLS), in Europe the top 4 most active ransomware have been Lockbit, LV, Black Basta and Vice society, while manufacturing, healthcare, technology and automotive have been the 4 most targeted sectors. Regarding other cybercrime operations, Emotet re-emerged, targeting organisations and individuals in European countries. In the rest of the world, an interesting trend was the use of social media platforms to spread malware.
- Regarding **data exposure and leaks**, a number of data disclosures or breaches impacted a number of high-profile organisations in the IT, cloud, social networks, telecommunications, healthcare, and transportation sectors.

- Regarding **information operations**, there were efforts to influence the US midterm elections and the flooding of Twitter while protests in China took place.
- On the **hacktivism** front, the main activity in Europe and Russia was linked to Russia's war in Ukraine. These resulted in DDoS or other attacks on several European countries. Elsewhere we observed claims made by a pro-Iran hacktivist.
- Regarding **disruptive** operations, in Europe there was the disruption of train operations in Denmark, while in the rest of the world, North Korea experienced inaccessibility to the internet and Microsoft warned of risks from obsolete software in industrial control systems.
- We included several significant vulnerabilities and associated advisories, reported in November 2022.

Europe

Cyber policy and law enforcement

European Parliament rapporteur presents first version of spyware report

Parliamentary investigation

On November 8, Sophie In 't Veld, a Member of the European Parliament and rapporteur for the Inquiry Committee investigating Pegasus and equivalent spyware, presented a first version of their results. The committee can vote on its final findings in 2023.

European Parliament adopts new legislation to strengthen EU-wide cyber resilience

Legislation

On November 10, the European Parliament adopted legislation requiring EU countries to meet stricter supervisory and enforcement measures and harmonise their sanctions. The legislation, already agreed between EP and the Council in May, will set tighter cybersecurity obligations for risk management, reporting, and information sharing. The requirements, among other provisions, cover incident response, supply chain security, encryption and vulnerability disclosure.

The Digital Services Act (DSA) comes into effect

Legislation

On November 16, the Digital Services Act (DSA) — a new legislation established by the EU applicable to all digital services that "connect consumers to goods, services, or content" — went into effect. While media reports suggest this policy is designed to combat online hate speech, disinformation, and data piracy, the EU states the specific objectives of DSA include:

- Maintaining a safe online environment.
- Improving conditions for innovative cross-border digital services.
- Empowering users and protecting their fundamental rights.
- Establishing an effective supervision of digital services and cooperation between authorities.

Discord fined in France over privacy protection

GDPR, Sanction

France's data protection authority CNIL sanctioned the messaging platform Discord with an 800.000 euro fine for failing to adhere to the EU's privacy rules (GDPR). The CNIL said it had identified several breaches of the general data protection regulation (GDPR).

EDF electricity provider fined in France over privacy protection

GDPR, Sanction

French data protection authority CNIL also fined electricity provider Électricité de France (EDF) 600.000 euro for violating the GDP by storing and hashing some 25.800 accounts with an MD5 algorithm that was deemed “cryptographically broken” in December 2008 due to the risk of “collision attacks.”

Meta faces imminent GDPR penalties

GDPR, Sanction

Facebook, Instagram, and WhatsApp are about to face penalties under the EU’s GDPR within the next months. The first penalty in the pipeline is for a massive Facebook data leak in 2021, which saw 533 million records, including phone numbers, user IDs, full names, and birthdates appear online.

UK Government scanning all internet-connected devices in the UK

Vulnerability scanning

The UK’s NCSC announced that it is building a data-driven view of the vulnerabilities in the UK by scanning all internet-connected devices in the UK. This directly supports the UK Government Cyber Security Strategy and is expected to help them better understand the vulnerability and security situation in the UK. It is also hoped to establish the security posture on a day-to-day basis and respond to shocks (like a widely exploited zero-day vulnerability).

Spanish police takes down a network of piracy streaming sites

Takedown

The Spanish police and Europol reportedly conducted a joint operation that led to the takedown of a network of sites streaming pirated content. According to a police announcement, the network had unlawfully distributed audiovisual content from 2.600 TV channels as well as 23.000 films and shows to approximately 500.000 users

Europol arrests Lockbit cybercriminal

Arrest

Europol announced the arrest of a Russian national linked to LockBit ransomware attacks, targeting critical infrastructure organisations and high-profile companies worldwide.

Two Estonian citizens arrested in cryptocurrency fraud and money-laundering scheme

Arrest

Authorities in Estonia arrested two Estonian men, Sergei Potapenko and Ivan Turõgin, for their alleged involvement in a cryptocurrency-mining and money-laundering scheme. The two men allegedly defrauded hundreds of thousands of victims of approximately 575 million dollar. The men are accused of selling cryptocurrency-mining equipment from their service HashFlare.

Ukrainian cybercriminals arrested

Arrest

Ukraine’s cyber police and Europol identified and arrested five key members of an international investment fraud ring estimated to have caused losses of over 200 million euro per year.

Cybercrime group member arrested in Switzerland, to be extradited to the US

Arrest

Swiss law enforcement arrested an alleged member of cybercrime group JabberZeus Crew and agreed to an extradition to the US. The group reportedly stole in total 70 million dollar from US citizens and businesses between 2009 and 2012.

Spanish police dismantle cybercrime group

Seizure

Spanish police dismantled a cybercrime organisation that used fake investment sites to defraud over EUR 12,3 million from 300 victims across Europe.

Cyberespionage

DTrack detected in European organisations
Security researchers have reported that Lazarus, a North Korea-linked threat actor, used a new version of the DTrack backdoor to target organisations in Europe.

North Korean threat actor

Commercial spyware from Spain-based vendor Variston
On November 30, Google Threat Analysis Group (TAG) released a technical analysis on an exploitation framework, named Heliconia, with likely ties to Variston IT, a company in Barcelona, Spain that claims to be a provider of custom security solutions. Their Heliconia framework exploits n-day vulnerabilities in Chrome, Firefox and Microsoft Defender and provides all the tools necessary to deploy a payload to a target device.

PSOA

Cybercrime

Ransomware

French municipality suffers attack
A cyber attack, probably ransomware, hit the French city of Brunoy, according to an announcement by the municipality, on October 31. The authorities had to disconnect IT systems in order to block the spread of the malware. Basic services continued to operate.

Local administration

French departmental council suffers cyberattack
On November 8, the departmental council of Seine et Marne in France announced that its IT infrastructure was unusable and blocked. Despite the intervention of a crisis unit, the department announced that it would not be able to resume normal activity for at least 6 weeks. IT staff shut down the servers that were attacked to prevent further damage. Departmental staff were unable to receive or send emails or access their internal files, which hindered the administration in providing social services to citizens.

Local administration

German district suffers cyberattack
The German district of Rhein-Pfalz-Kreis disclosed a cyberattack that began on October 24. The incident impacted the district's administrative computer networks, including their ability to make and receive phone calls and emails. The district took steps to restore network access and ensure citizens could still contact the appropriate administrative offices. The Vice Society ransomware operation named the district as a victim on their data leak site (DLS).

Local administration

French region hit by cyberattack
The French region of Guadeloupe disclosed on November 22 that it was the victim of a cyberattack, probably linked to a ransomware operation. The attack resulted in all networks and IT systems being unavailable.

Local administration

Italian municipality suffers ransomware
On November 25, the municipality of Macerata in Italy reportedly suffered a ransomware attack. The group Royal Ransomware claimed responsibility for the attack.

_Local administration

Lockbit claims breach of Thales

Defence & Technology

According to news sources, on November 1, the threat actors behind the Lockbit ransomware claimed on their DLS they had breached the French company Thales Group and stolen sensitive data. The company reported, on November 3, that an internal investigation did not reveal a breach or data exfiltration. Additionally they noted they had not received any ransom note.

ViceSociety lists Spanish clinic as victim

Healthcare

The ransomware operation ViceSociety listed, on November 3, the Spanish clinic Unidad Medica Angloamericana as one of their victims.

Polish healthcare centre suffers ransomware

Healthcare

On November 9, the Polish Brand Health Centre Institute announced that it had suffered a ransomware attack from the LockBit 3.0 threat actor. Apart from the encryption, no data leakage was detected, but if some had indeed been exfiltrated this constitutes loss of personal data entrusted to the Institute.

German university hospital of Detmold confirms cyberattack

Healthcare

On November 22, the University Hospital of Detmold in Germany announced that it had suffered a major breakdown of its computer systems, probably due to a cyberattack. According to the announcement, the failure was caused by a massive external hack.

French company suffers ransomware

Water supply

On November 3, the computer systems of the Office Hydraulique de Corse were hit by a ransomware attack. The attack blocked all network and computer systems and attackers demanded a ransom. According to the office’s press release, the attack affected 33 servers.

French cancer treatment centre suffers ransomware

Healthcare

On November 15, the French Saint-Doulchard oncology centre suffered a ransomware attack. Medical and radiotherapy activities at the centre were suspended from 15 to 18 November due to lack of computer resources. Eventually, chemotherapy treatments were resumed, but not radiotherapy. According to the medical centre, no personal patient data was stolen.

German university suffers ransomware

Education

On November 28, the University of Druisburg-Essen in Germany announced that it had suffered a ransomware attack. Campus communications were interrupted and data has reportedly been exfiltrated.

Spanish regional administration named as victim of cybercrime

Local government

OnNovember 29, Kelvinsecurity, a cybercrime group, added the administration of Castilla la Mancha to its list of victims on a leak forum. They claim to have stolen a GB of data containing personal data such as usernames, passwords and emails.

Other cybercrime

Emotet observed in several European countries

Malware

In early November, a massive Emotet malware campaign targeted organisations and individuals in several European countries. The technique used was to send, via email, a password-protected ZIP attachment containing an XLS file with a malicious macro.

Access broker offering supposed access to Deutsche Bank

Banking

On November 11, reports emerged that a cybercrime group was offering for sale supposed access to Deutsche Bank. The attacker claimed to have access to about 21.000 machines on the bank’s network. He also claimed that he stole 16 TB of data.

Spanish tax agency used as a lure to phish citizens

Citizens

On November 28, reports emerged that a cybercrime group impersonated the Spanish tax agency Agencia Tributaria to lure targets into disclosing personal data. The group sent a fraudulent SMS to victims asking them to fill in a form in order to get a refund for which they were supposedly entitled.

Hacktivism

DDoS attack on European Parliament website

EU institutions, bodies or agencies

On November 23, a DDoS attack hit the official website of the European Parliament. A few hours earlier, the European Parliament had recognised the Russian Federation as a state sponsor of terrorism. The same day Killnet and Anonymous Russia claimed responsibility for an unspecific attack.

DDoS on foreign policy think tanks and intelligence services

EU countries

On November 4 and 5, Killnet claimed to have conducted cyberattacks against entities in five Eastern European countries including foreign policy think tanks and intelligence services. On November 6, DDoS attacks targeted the websites of the intelligence committees of Estonia, Poland, Romania, Bulgaria, and Moldova. Killnet later claimed responsibility for the DDoS attacks.

DDoS in Poland

EU countries

On November 8, Noname057(16), a supposed pro-Russia hacktivist group, claimed responsibility for a DDoS attack on the login page of the website for the Nenetsky Institute of Experimental Biology of the Polish Academy of Science. It is likely that this attack prevented people working at the institute from logging in for some time. On November 9, a wave of DDoS attacks hit the website of the Polish Institute of Remembrance. The first wave in the morning failed, but a second wave in the evening managed to cause the homepage of the website to be inaccessible for a few hours. On November 16, the pro-Russian hacktivist group KillNet claimed a campaign of DDoS attacks targeting different airports in several cities of the country: Podzna, Lodz, Rzeszow, Gdańsk, Warsaw.

DDoS in Greece

EU countries

On November 12, Killnet claimed to have conducted a cyberattack against a public Power Corporation in Greece. The website of DEH, the Greek public Power Corporation was down for one hour and there were no signs of an intrusion.

DDoS in Spain

EU countries

On November 13, we observed reports that Cyber Army of Russia, a supposed pro-Russia hacktivist group, conducted cyberattacks against Spanish entities. One of the named victims was Leonardo Hispania, a Spanish company in the military sector.

DDoS in Bulgaria

EU countries

On November 13, the website of the Bulgarian Council of Ministers was down following a DDoS attack. A spokesperson for the Bulgarian government stated that the attack probably came from Killnet who claimed responsibility on Telegram.

DDoS in Finland

EU countries

On November 14, the pro-Russia hacktivist entity Cyber Army of Russia Reborn claimed to have conducted a DDoS against the website of the Finnish Army.

DDoS in Estonia

EU countries

On November 19, the services of five Estonian companies started to malfunction due to cyberattacks. The Estonian energy distribution group Eesti was among the victims. The Estonian Information System Authority published a note saying, “It is never possible to say with complete certainty who is behind the attacks, but the available information suggests that it is pro-Kremlin cybercriminals.”

Defacement in Romania *EU countries*

On November 28, Killnet claimed the defacement of a number of Romanian websites. The threat actor disseminated disinformation banners about "Ukrainian crimes in Donbass."

DDoS against UK-based defence manufacturer *UK*

On November 22, Anonymous Russia claimed a DDoS attack against a UK-based defence manufacturer; this company was nearly certainly targeted due to its production of weapons included in UK military aid to Ukraine.

Hacktivists DDoS Kiev hospital website *Ukraine*

On October 31, Phoenix and WeAreClown, two supposed pro-Russia hacktivist groups, claimed to have conducted a DDoS cyberattack against a hospital in Kiev.

Hacktivists leak supposed Ukrainian military data *Ukraine*

On November 1, JokerDNR, a supposed pro-Russia hacktivist group, claimed they had gained access to the Ukrainian Defense Ministry's Delta platform. This platform supposedly integrates intelligence data to provide battlefield monitoring. Following JokerDNR's Telegram post claiming access to the system, Beregini, another supposed pro-Russia hacktivist group released data supposedly coming from the Delta platform. Russian media amplified JokerDNR's claims of having compromised the Delta platform.

DDoS against Ukrainian defence company *Ukraine*

On November 3, NoName057(16), a supposed pro-Russia hacktivist group, claimed to have operated a DDoS attack against Knogsberg Defense and Aerospace. The company produces air defence systems for Ukraine. The impact was temporary unavailability of the company's internal, support, and learning portals.

Unspecified attack on power grid *Ukraine*

On November 4, Cyber Army, a supposed pro-Russia hacktivist group, claimed to have conducted a cyberattack against the power grid of the city of Krivoy Rog in Ukraine.

Data concerning Ukrainian aircraft *Ukraine*

On November 8, Phoenix, a supposed pro-Russia hacktivist group, claimed to have acquired data concerning 800 Ukrainian aircraft. The data supposedly included aircraft types, serial numbers, certifications and the assigned bases.

Documents belonging to the Ukrainian government *Ukraine*

On November 9, Xaknet, a supposed pro-Russia hacktivist group, claimed to have attacked and breached Ukrainian government IT systems. The group claimed to have access to a large set of documents which they would supposedly hand over to journalists.

Disruption and hijacking

Danish rail transport suffers cybersecurity incident *Transportation*

Danish train operator DSB disclosed that the widespread standstill of its train network on September 29 stemmed from a cybersecurity incident targeting its IT subcontractor's software-testing environment. According to DSB, the incident prompted the subcontractor to shut down several systems. As a result, an emergency procedure was implemented to ensure the safety of DSB's train operations and left locomotive drivers unable to operate the trains.

Data exposure and leaks

Data from Vodafone Italia exposed via a reseller *Telecoms*

The Italian branch of Vodafone started notifying customers, on November 2, of a subscriber data leak. The incident, which took place in the beginning of September, was due to the breach of a Vodafone reseller. Exposed data included personal and subscriber information but no account passwords or network traffic data.

TikTok employees will access data of European users *Social media*

The social media platform TikTok announced, on November 2, that its employees, including those in China, will be able to access the data of users based in Europe. The company added that it does not collect precise location data from its users.

Government of Moldova shaken by big hack-and-leak operation *Political impact*

A newly registered website called Moldova Leaks has been releasing damaging private exchanges of at least two prominent political figures in Moldova. The leaked Telegram conversations have caused a major political scandal.

Hacker steals data from Belgian Police *Police records*

Ragnar Locker released data from a breach incident affecting the Belgian police. An attacker had managed to breach the police IT systems of the municipality of Zwijndrecht in September, stole data and then tried to extort authorities. The data contained information on investigations as well as personal data of citizens.

Phone numbers of French citizens leaked *Social media*

A cybercrime actor disclosed, on November 25, personal data linked to the WhatsApp profiles of about 487 million WhatsApp users, including the full names and phone numbers of 20 million French users.

World

Cyber policy and law enforcement

US FCC bans Chinese IT equipment *Ban*

On November 25, the US Federal Communications Commission announced it will ban the import of electronic equipment manufactured by Huawei, ZTE, Hytera, Hikvision, and Dahua over concerns that the equipment poses an unacceptable national security threat to the US.

Major social media platform suspended in Turkey after deadly blast *Restrictions*

Following a deadly blast on November 13, in Istanbul, Turkish authorities began restricting access to social media platforms including Instagram, Facebook, Twitter, YouTube and Telegram as a nationwide broadcast ban went into effect.

Australia will now fine firms up to AU$ 50 million for data breaches *Legislation*

The Australian parliament has approved a new data privacy legislation, significantly increasing the maximum penalties to AU$ 50 million for companies and data controllers who suffered large-scale data breaches.

US convicts a cybercrime actor who stole Bitcoins *Sentence*

The US Department of Justice announced the conviction of an individual for stealing 50.000 US dollar worth of Bitcoins from the Silk Road dark net marketplace. The individual pleaded guilty to exploiting a withdrawal processing flaw that allowed him to withdraw many times more Bitcoin than he deposited on the dark web marketplace.

Scammers sentenced to 11 years in the US *Sentence*

US authorities sentenced an Instagram influencer to 11 years in prison for conspiring to launder tens of millions of US dollars through business email compromise scams. The US Department of Justice says that the individual admitted to prosecutors that over 18 months, between 2019 and 2022, he conspired to launder over 300 million US dollars.

US charges two Russian suspects for operating pirated eBook website *Indictment*

US authorities charged two Russian nationals with intellectual property crimes linked to Z-Library, an online repository of pirated eBooks. Authorities arrested defendants on November 3 in Argentina at the request of US law enforcement.

US seized 18 web domains used for recruiting money mules *Seizure*

The seized websites claimed to offer jobs as quality control inspectors being requested to ship items from their homes goods using their own credit cards. The victims photographed the packages they received, reshipped them to a different address as instructed, and received 20 US dollar for each processed item.

Interpol seizes cybercriminal assets *Seizure*

An Interpol operation against cybercrime, that was conducted between June 28 to November 23, resulted in the seizure of 130 million US dollar and the arrest of almost a thousand suspects. The operation reportedly resolved more than 1.600 criminal operations.

Taking control of sites supporting cybercrime *Seizure*

The US Department of Justice took control of seven domains that hosted scam websites, on November 24. The criminal activities referred to are romance scams and fake investment platforms for cryptocurrency.

Spoofing site taken offline *Seizure*

An international law enforcement operation, concluded on November 24, succeeded in taking down the cybercrime site iSpoof and making numerous arrests of people involved in its operation. The site was extensively used to fake banks and other financial institutions in support of cybercrime scams.

Interpol announces arrest of 11 involved in cybercrime *Arrest*

Interpol announced that a law enforcement operation targeting cybercrime in Africa resulted in the arrest of 11 individuals, 10 of which are linked to fraud activities 800.000 worth dollar.

Cyberespionage

Emergence of a new China-linked group named Earth Longzhi *Chinese threat actor*

Trend Micro reported on a previously unknown APT, Earth Longzhi which they report has a China-nexus. Earth Longzhi reportedly uses similar techniques, tactics, and procedures as Earth Baku, another China-linked group. Earth Longzhi mainly focuses on organisations in East Asia, Southeast Asia. In Europe, Trend Micro observed them targeting Ukraine.

Global campaign attributed to China-linked Earth Preta *Chinese threat actor*

Trend Micro reported a campaign of spearphishing attacks targeting the government, academic, foundations, and research sectors around the world. They attribute the campaign to a threat actor called Earth Preta which they allege has a Chinese nexus.

New China-linked activity in Southeast Asia

Chinese threat actor

Cybersecurity firm Mandiant reported on a cyberespionage activity that heavily leverages USB devices as an initial infection vector and concentrates on the Philippines. Mandiant tracks this activity as UNC4191. UNC4191 operations have affected a range of public and private sector entities primarily in Southeast Asia and extending to the US, Europe, and Asia-Pacific.

New backdoor called Dophin used by North Korean hackers in highly targeted operations

North Korean threat actor

On November 30, ESET researchers have analysed a previously unreported backdoor, named Dophin, used by the North Korea linked ScarCruft APT threat actor. The backdoor has a wide range of spying capabilities, including monitoring drives and portable devices and exfiltrating files of interest, keylogging and taking screenshots, and stealing credentials from browsers. Its functionality is reserved for selected targets.

APT32 targets digital certificate authority

Vietnamese threat actor

APT32, a Vietnam-linked threat actor, reportedly compromised a digital certificate authority in an Asian country.

Spyware infects Iranian Android devices via malicious VPN app

Unspecified threat actors, Iran

According to Kaspersky researchers, threat actors used SandStrike, a piece of spyware, on Iranian mobile phones. The malware was delivered via a malicious VPN application and targeted Android users. The threat actors focused on Persian-speaking practitioners of the Bahá'í Faith.

COP27 app supposedly too intrusive

Invasive mobile app

News reports claimed that a COP27 mobile phone app was overly intrusive.

The French data protection authority warned of risks associated with applications provided by Qatar for the World Cup

Invasive mobile app

The Commission nationale de l'informatique et des libertés (CNIL), the French data protection authority, advised football fans travelling to Qatar for the world cup to get burner phones or use old phones that have been factory reset. Foreigners are required to download two apps: Hayya, the official world cup app, and Ehteraz, for COVID tracing. In addition, CNIL recommends special care when taking photos, videos as they might infringe the local, strict morality laws.

Android VPN applications modified to spy on users

Malicious mobile app

An ESET researcher reported on November 24 on findings that attackers had repackaged the SoftVPN and OpenVPN apps for Android to include malicious code with spying functions. The fraudulent apps could exfiltrate personal data and spy on messaging applications.

Cybercrime

Ransomware

East Asian railway administration hit by ransomware

Transportation

A cybercrime group named an East Asian-based railway administration as a victim of LockBit 3.0 ransomware operation. The cybercriminals gave the victim until November 6 to pay the ransom but did not specify how much information was obtained or the demanded ransom.

Ransomware gang threatens to release Australian health data
Healthcare
A ransomware gang that some researchers believe is a relaunch of REvil and others track as BlogXX, has claimed responsibility for a ransomware attack against Australian health insurance provider Medibank Private Limited. On November 9, Medibank warned customers that a ransomware group has started to leak data stolen from its systems. Medibank said in a press release published on November 7, that it would not pay a ransom demand made by the attackers.

Boeing subsidiary disrupted by cyber incident
Airline
Jeppesen, a Boeing-owned navigation and flight planning tool provider, suffered a cyberattack that has resulted in flight interruptions. Media reports allege that Jeppesen suffered a ransomware incident.

US healthcare sector targeted by Venus ransomware
Healthcare
On November 10, the US Department of Health and Human Services warned that Venus ransomware attacks target US healthcare organisations.

Central Bank of Gambia victim of a ransomware attack.
Government, Finance
The Central Bank of Gambia suffered a ransomware attack where the threat actor claimed to have access to 2 TB of data. On November 13, ALPHV, a cybercrime group,announced a cyberattack against the Central Bank of Gambia.

Ransomware operator claims attack on US college
Education
The Vice Society ransomware operation claimed responsibility for a cyberattack on Cincinnati State Technical and Community College, with the threat actors leaking data allegedly stolen during the attack.

Decryptor of the Zeppelin ransomware
Decryptor
Since 2020, security researchers have decrypted files affected by the Zeppelin ransomware, utilising vulnerabilities in its mechanisms. The researchers provided the decryptor to victims without publicising their capability in order to avoid alerting the ransomware group.

Indian health institute suffers ransomware
Health sector
The All India Institute of Medical Sciences (AIIMS) revealed it suffered a ransomware attack on November 23. The cyberattack impacted its server and adversely affected the medical centre's patient care services, appointments, registration, admission, billing, and report generation.

US county suffers Lockbit infection
Local government
On September 6, the US county of Southampton reportedly suffered a ransomware infection by a Lockbit affiliate. The incident caused unauthorised access to personal data including names, social security numbers, driver's license numbers, and addresses.

Other cybercrime

Twitter's verified mark is phishing lure
Social media, Phishing
Following the change of Twitter's policies on users' verified status, cybercrime actors have been sending phishing emails with related lures. The attackers mimicked Twitter's official support forms to deceive users.

Twitter Blue program abuse
Social media
Twitter rolled out its Twitter Blue program for an 8 US dollar monthly fee. Reports emerged that threat actors have started to enrol as verified users.

Wiper disguising as a ransomware
The Azov ransomware is reportedly a data wiper that intentionally destroys victims' data and infects other programs.

Wiper

Cyberattack on the ALMA radio telescope
On November 5, the Atacama Large Millimetre Array (ALMA) observatory suffered a cyberattack which forced it to suspend astronomical observations and the public website. According to a statement on the Atacama website the threat was contained, and specialists were restoring affected systems. The attack did not compromise the ALMA antennas or any scientific data.

Satellite

Cyber associate at Indian Deloitte fired after leading a cybercrime group
WhiteInt, a cybercrime group, was exposed in a sting operation for offering to hack into private email accounts and messages of victims on behalf of investigators working for governments and British lawyers. The group's leader was reportedly an associate director at the Indian Deloitte's cyber unit who was subsequently fired.

Hack-for-hire

Iranian hackers attack US government for profit
News reports, on November 21, followed by a warning by the US CISA, indicated that Iranian hackers launched a campaign against US federal agencies. The threat actors reportedly installed cryptocurrency mining software.

Government, Cryptomining

Android file manager apps infect thousands with Sharkbot malware
The cybersecurity company Bitdefender discovered that software apps downloaded from Google Play were acting as droppers for the SharkBot banking trojan. The apps disguise as file managers and drop the banking trojan shortly after installation, depending on the user's location.

Banking trojan

Cybercrime actors target users of Facebook's Business platform.
Security researchers report on an information stealing operation called Ducktail wherein threat actors target users of Facebook's Business platform. The campaign is financially motivated.

_Advertising _

TikTok trend abused to spread malware
Threat actors are reportedly abusing a TikTok trend to install information stealing malware. The trend is called Invisible Challenge, the information stolen potentially potential cryptocurrency wallets.

Crypto, Social media

Disruption and hijacking

North Korea's internet went down, a cyberattack is suspected
On November 17, a news report claimed that North Korea's internet was down. The report claimed that this outage was the longest since January. The cause is reportedly a cyberattack. Two waves of outages are believed to have interrupted the internet for two and a half hours.

Outage

Warning for an obsolete web server
On November 22, Microsoft warned that a discontinued web server, called Boa, had vulnerable components that attackers could exploit to affect services still using it. The software is used, among other cases, in IoT devices. Exploitation of Boa's vulnerabilities has been cited as the reason for a 2020 attack on an Indian power company.

Obsolete software

Hacktivism

Pro-Iran hacktivist claims attack on Saudi Ministry of Interior
A supposed pro-Iran hacktivist group, Abraham’s Ax, claimed on their website that they gained access to the Saudi Ministry of Interior systems. The group shared supposed proof on their website. It is unclear if the data authentic and whether it belongs to the supposed victim.

Middle East

Pro-Ukraine hacktivist attacks on Russian telecoms
Between October 28 and November 3, the pro-Ukraine hacktivist entity Team OneFist claimed to have conducted Operation Switchblade and Operation Dark Fiber. They claim to have compromised 55 devices such as Cisco and HP switches and routers across Russia. Among the supposed targets were Rostelecom and Kuban-Telecom, two telecom providers.

Russia

Pro-Ukraine hacktivist attacks on Russian investment company
On November 7, Team OneFist claimed to have penetrated the virtual machine server of a Russian company referred to as Energy Union. The company is reportedly dedicated to attracting foreign investment in the Russian energy sector. They claim to have achieved admin rights which they used to brick the system.

Russia

Pro-Ukraine hacktivist attacks on Russian WiFi routers
On November 8, TeamOneFist, claimed to have carried out Operation Wimark. They claim to have destroyed a WiFi router management system in Russia. The system supposedly included 58 commercial WiFi routers in 28 locations including metros and airports. They claim the operation disrupted internet services of the victims.

Russia

Pro-Ukraine hacktivist attacks on Russian payment systems
On November 17, Team OneFist announced Operation Pasłęk. It supposedly targets Russian billing and payment IT systems.

Russia

Information operations

Cartoons form part of information operation ahead of US midterm elections
On November 3, Graphika announced that suspected Russian actors targeted far-right US audiences with politically divisive messaging ahead of the November midterm elections. The information operation reportedly included direct attempts to undermine support for Democratic candidates in Pennsylvania, Georgia, New York, and Ohio. Other narratives promoted by the network supposedly comprise inflammatory messaging about sensitive cultural and political issues, as well as criticism of President Joe Biden. The narratives used a series of political cartoons, which Graphika assesses were likely created by the actors and are almost certainly intended to go viral. Similar cartoons disseminated by this campaign have previously achieved significant levels of engagement from authentic online communities.

Elections

TikTok accused of being tool for influence operations
In November, the director of the US FBI voiced concerns about TikTok. He warned of potential Chinese government abuse of the app to control millions of users’ data or software, and its recommendation algorithm which could be used for influence operations if they so choose.

Social media

Information operation about Russia’s war on Ukraine targets Chinese audience

Social media

Radio Free Asia, a US-funded think tank, reported that an influential account with more than 6 million followers on Weibo conducted an information operation. The account reportedly spread a conspiracy theory alleging that NATO members had donated HIV and hepatitis-infected blood to Ukraine. Researcher at Asia Fact Check Lab report that a pro-Russia Telegram channel, Breaking Mash, is the source. Further inquiries by a Ukraine-based fact-checking organisation StopFake caused the Ukrainian government to release a formal statement debunking the disinformation.

Nuisance content floods Twitter during Chinese protests

Social media

Media report that on November 27, Twitter’s anti-propaganda team grappled with a flood of nuisance content in China that researchers said was aimed at reducing the flow of news about widespread protests against coronavirus restrictions.

Data exposure and leaks

Unauthorised access to Dropbox GitHub causes leak of internal data

Code sharing platform

On November 1, Dropbox, a data storage provider, disclosed a data leak. Threat actors accessed the Github repositories of Dropbox employees. The investigation revealed that threat actors accessed code containing credentials, including API keys.

Numerous mobile applications were hosting code developed by suspicious company

Supply chain, Mobile applications

On November 14, news reports claimed that thousands of smartphone applications for both the iOS and Android platforms contain code developed by Pushwahs, a Russian company falsely portraying itself as an American company. Code from the company reportedly exists among others, on applications of the US army and the US Center for Disease Control. Several organisations subsequently withdrew their applications citing security concerns.

US hospital leaks personal health data

Healthcare

In November, the US Presbyterian hospital of New York disclosed a data breach. Personal health data of 12.000 individuals leaked. The threat actor was able to access and exfiltrate files at the hospital’s Queens and Hudson Valley locations.

US Healthcare provider suffers data leak

Heathcare

On November 18, the Community Health Network in Indianapolis informed the US government that it suffered unauthorised access to the personal data of 1.5 million data subjects who used its website’s tracking code.

Amazon database suffers data leak

Cloud

In November, security researchers reported that they found hundreds of databases on the Amazon Relational Database Service exposed personal data.

Mobile applications leaking API keys

Mobile applications

CloudSEK security researchers report having discovered that 1550 mobile applications are leaking Algolia API keys. These keys can provide access to system and user information stored on the device. The Algolia API is a widely used proprietary platform that integrates search engines with discovery and recommendation features in websites and applications.

Leak of airline passenger information

Airline

Daixin Team, a cybercrime group, claimed to have stolen personal data of five million passengers and employees from the Malaysian airline AirAsia Group. The operation reportedly involved data encryption and deletion as well.

Collaboration company and affiliated password management company breached *IT*

LastPass, a company selling password management solutions, publicly said that unknown threat actor breached its cloud storage using information stolen during a previous security incident from August 2022. According to the company, the threat actors were able to gain access to certain elements of our customers' information. The remote access and collaboration company GoTo also disclosed that they suffered a security breach where threat actors gained access to their development environment and third-party cloud storage service. LastPass is an affiliate of GoTo.

Significant vulnerabilities

Several High Vulnerabilities in Splunk Enterprise *Splunk*

On November 2, 2022, Splunk released the quarterly Security Patch Update which included nine HIGH severity vulnerabilities. The most severe vulnerabilities, which have a CVSS score of "8.8" out of 10, are "CVE-2022-43571" for Remote Code Execution (RCE) through dashboard PDF generation component, "CVE-2022-43570" for XML External Entity Injection through a custom View and "CVE-2022-43568" for Reflected Cross-Site Scripting via the radio template. See CERT-EU's SA 2022-077.

Severe Vulnerabilities in Citrix Gateway and Citrix ADC *Citrix*

On November 8, 2022, Citrix released a Security Bulletin regarding three severe vulnerabilities affecting its Citrix Gateway and Citrix ADC products. Under specific configurations, the three vulnerabilities can enable attackers to gain unauthorised access to the device, perform remote desktop takeover, or bypass the login brute force protection. See CERT-EU's SA 2022-078.

Exploited 0-days and Critical Vulnerabilities in Microsoft Windows *Microsoft Windows*

On November 8, 2022, Microsoft released its Patch Tuesday advisory which contains information about 68 flaws, for which 11 are rated as critical, and 6 are exploited 0-day vulnerabilities. The exploitation of these vulnerabilities could lead to elevation of privilege, security feature bypass, remote code execution, information disclosure, denial of service and spoofing. See CERT-EU's SA 2022-079.

Remote Code Execution Vulnerabilities in F5 Products *F5*

On November 16, 2022, F5 released an advisory on F5 Big-IP and Big-IQ concerning two CVE with high severity. The first one, "CVE-2022-41622", is a cross-site request forgery (CSRF), for which the exploitation can allow an unauthenticated attacker to perform critical actions on the system, even if the management interface is not exposed on the internet. The second vulnerability, "CVE-2022-41800", can allow an attacker with administrative privileges to execute arbitrary commands on the device. See CERT-EU's SA 2022-080.

Critical Vulnerabilities in Atlassian Products *Atlassian*

On November 16, 2022, Atlassian released two advisories for critical vulnerabilities in the Crowd Server and Data Center identity management platform, and in Bitbucket Server and Data Center. Tracked as "CVE-2022-43782", the first vulnerability allows an attacker to authenticate as the Crowd application and subsequently call privileged endpoints on the Crowd platform. The second vulnerability, tracked as "CVE-2022-43781", is a command injection vulnerability in BitBucket that lets an attacker with permission to control their username to exploit this issue and execute arbitrary code on the system. See CERT-EU's SA 2022-081.

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.