Cyber Security Brief (October 2022)

November 3, 2022 - Version: 1.0

TLP:WHITE

Disclosure is not limited.

TLP:WHITE information may be distributed freely.

Executive summary

- We analysed 231 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy and law enforcement**, in Europe, the German government dismissed the head of Germany's national cyber security agency (BSI), for collusion with Russian contacts, France fined two US companies for data protection issues, and the police authorities in several countries arrested a number of cybercriminals for various motives (phishing, keyless car hacking, malware service, hacking and data theft).
- On the **cyberespionage** front, in Europe, a new report exposed a North Korea linked operation against the aerospace sector. Globally, public reports detailed operations by 2 North Korean (codenamed Lazarus and Kimsuky), 6 Chinese (codenamed Mustang Panda, Taidoor, WIP19, APT10, APT41, and DiceyF), 1 Lebanese (codemaned Polonium), Iranian (governmental services deploying mobile surveillance devices against citizens), and 1 Indian (codenamed SideWinder) threat actors.
- Relating to **cybercrime**, ransomware attacks continue to target organisations in all businesses. In Europe, the 3 most active ransomware operations in October have been Lockbit, Karakurt, and Vice Society. In the public sector, ransomware threat actors target in particular municipalities or regional administrations. Threat actors breached organisations in some critical sectors like transportation, healthcare, defence and education.
- Regarding **data exposure and leaks**, in Europe, incidents affected the military sector in Portugal as well as IT companies in the Netherlands and Italy. On the global level large incidents, exposing sometimes the data of millions of users, affected miscellaneous sectors including social media (Meta), telecommunications, gaming, finance (credit cards), IT, automotive, healthcare, secret services, or energy.
- In Europe, we noticed **information operations** with a cyber component following the Nord Stream pipeline incident and another one using deepfake technology to impersonate Ukrainian Prime Minister to undermine cooperation between Ukraine and Turkey.
- On the **hacktivism** front, in Europe, most activity is related to Russia's war in Ukraine. Pro-Russia hacktivists attacked several targets in Ukraine with DDoS or leaks in the government, telecoms, cyber defence and healthcare sectors. In the EU, pro-Russia hacktivists targeted entities in Poland, Slovakia, Estonia and the Czech Republic.

- Regarding **disruptive** operations, in Europe we noted reporting of a German energy company suffering a cyberattack which caused customer service to be unavailable. The pro-Ukraine actor TeamOneFist claimed a new series of disruptive or hijacking attacks in Russia (mobile phone operator, research programmes and routers).
- We included several significant vulnerabilities and associated advisories, reported in October 2022.

Europe

Cyber policy and law enforcement

EU ban Russia from cryptocurrency services *Sanctions*
On October 6, the EU adopted a sanctions package against Russia that includes a full ban on cryptocurrency-related services to Russian nationals or residents in addition to further restrictions impacting the energy, technology, and defence sectors. The EU's sanctions in part were a response to Russia's claimed annexation of the occupied Ukrainian territories Luhansk, Donetsk, Kherson, and Zaporizhzhya.

Arne Schoenbohm, head of German national cyber security dismissed *Dismiss*
The German government has dismissed Arne Schoenbohm, the head of Germany's national cyber security agency (BSI), for collusion with Russian contacts.

France's data protection authority warns about using Google Analytics *Data protection*
The French data protection authority (CNIL) issued a warning, on October 11, to three press publishers for continuing to use Google Analytics. The development follows upon a February ruling, in which the same authority had deemed Google Analytics to be exposing citizens' data, due to unauthorised transfers of personal data to the US in breach of EU privacy law.

France fines Clearview facial recognition company *Data protection*
The French CNIL fined the US-based facial recognition company Clearview AI with 20 million euro for illegal collection and processing of biometric data belonging to French citizens. The amount is the maximum financial penalty the company could receive as per GDPR Article 83. Clearview AI received the same fine from Italian and Greek data protection authorities for the same violations in March and July.

Police tricks DeadBolt ransomware out of 155 decryption keys *Decryption keys*
The Dutch National Police, in collaboration with cybersecurity firm Responders.NU, tricked the DeadBolt ransomware gang into handing over 155 decryption keys by faking ransom payments.

French police arrests five people with stealing 2.5 million euro in NFT *Arrest*
French authorities arrested seven individuals for their alleged involvement in a non-fungible token (NFT)-phishing scheme, but indicted only five of them. According to police, the threat actors caused 2.5 million euro in damages. Media reports suggest the threat actors gained access to the NFTs via a phishing link posted on Discord and then sold the NFTs online immediately following the theft.

German Police arrest one individual for a role in a phishing scam *Arrest*
The German Federal Criminal Police (BKA) arrested one individual for his involvement in a phishing scheme that led to the theft of 4.000.000 euro. The BKA also suggested the suspect engaged in DDoS attacks against different banks to hide the fraudulent transactions.

Police dismantles criminal ring that hacked keyless cars *Arrest*
Authorities from France, Latvia, and Spain arrested 31 suspects believed to be part of a car theft ring that targeted vehicles from two French car manufacturers. The criminals only targeted cars that use keyless entry and start systems and stole them after exploiting their keyless technology to unlock the doors and start the engines without having to use the key fobs.

Spain National Police arrest eight for alleged involvement in a phishing scheme *Arrest*
The Spanish National Police arrested eight people allegedly connected to a criminal organisation behind an SMS and voice phishing ("vishing") scheme. The police reported that the eight individuals imitated bank employees to gain access to victims' login credentials and bank accounts.

Dutch police arrest hacker who breached a healthcare software vendor *Arrest*
The Dutch police arrested a 19-year-old man suspected of breaching the systems of a healthcare software vendor in the country, and stealing tens of thousands of documents. These documents might contain sensitive personal and medical data of patients of healthcare providers using the company's systems.

German student arrested for operating a darknet market *Arrest*
The Federal Criminal Police Office in Germany arrested a student suspected of being the administrator of Deutschland im Deep Web, one of the largest darknet markets in the country.

Ukrainian charged for operating Raccoon Stealer malware service *Arrest, Charge*
US authorities charged 26-year-old Ukrainian national Mark Sokolovsky for involvement in the Raccoon Stealer malware-as-a-service (MaaS) cybercrime operation. The Dutch police had arrested him in March 2022 and he is currently jailed in the Netherlands while waiting to be extradited to the US.

Cyberespionage

Amazon-themed campaigns of Lazarus in the Netherlands and Belgium *North Korean threat actor*
ESET uncovered a set of malicious tools that the North Korean threat actor used in attacks during the autumn of 2021. The campaign started with spearphishing emails containing malicious Amazon-themed documents and targeted an employee of an aerospace company in the Netherlands, and a political journalist in Belgium.
***Analyst note**: We observe Amazon-theme phishing emails on regularly in our constituency. Most of the time these phishing emails are from low sophistication cybercrime actors.*

Former British Prime Minister Liz Truss 's phone allegedly hacked by Russian threat actors *Russian threat actor*
According to the Daily Mail tabloid, threat actors suspected of working for the Kremlin hacked the personal mobile phone of British Prime Minister Liz Truss. Reportedly, the threat actors compromised Truss's phone during the summer's Tory leadership campaign when Ms Truss was Foreign Secretary.

Cybercrime

Ransomware

Municipality in Portugal hit with ransomware — *Public administration*
The ransomware threat actor HiveLeak claimed responsibility for an attack targeting the Portuguese municipality of Louros. The attack reportedly took place on September 22 and the threat actor released stolen data between October 9 and 10.
***Analyst note**: We observe that the majority of ransomware attacks against public administrations in Europe target local administrations (municipalities, regions, etc.). We assess that this due in part to the extended attack surface they offer and the limited resources they have to secure their networks.*

French department services hit with ransomware — *Public administration*
On October 10, authorities of the French department of Seine-Maritime issued a press release announcing that they would cut off networks and be forced to degrade services severely. The cybercrime prosecutor's office has opened an investigation. Although no ransom demand has been communicated for the moment, the modus operandi of the attack strongly suggests ransomware.

French city of Chaville targeted with ransomware — *Public administration*
During the night of October 14 to 15, a large-scale cyberattack targeted the servers of the Chaville Town Hall. The cyberattack caused the interruption of the main services associated with the Town Hall. The cybercriminal group Cuba claimed responsibility for the attack on October 18.

French municipality victim of a cyberattack — *Public administration*
The French town of Maison Alfort in the Paris region has announced that it has been the victim of a cyberattack. The attack would have blocked the internet and telephone network maintained by the town. The modus operandi of the attack strongly suggests ransomware.

German regional administration suffers cyberattack — *Public administration*
On October 24, the district administration of Rhein-Pfalz in Germany requested an investigation after a cyberattack paralysed them. Users could not access the services provided by the Ludwigshafen authorities. The administration shutdown IT resources, forcing civil servants to work without them.

Snatch ransomware threat actor adds Hendsoldt France to their victim list — *Defence*
On October 30, the Snatch ransomware group claimed to have attacked the Hensoldt France company. Hensold is a leading company in the European defence industry, particularly in the areas of cyber, data management and electronic product development.

UK IT service provider confirms incident — *Healthcare*
Advanced, an IT service provider of the UK's National Health Service (NHS), confirmed that an August 2022 cyber incident resulted from ransomware. Advanced also confirmed that the attackers stole data during the incident. However, the company has not disclosed whether this information includes patient data.

Hospitals hit with ransomware in Barcelona — *Healthcare*
On October 8, a ransomware attack targeted the computer systems of three hospitals in Barcelona. The attack affected the computer systems of all departments of the Consorci Sanitari Integral (CSI), which includes several health centres, nursing homes and hospitals.

Portugal-based hospital hit with Everest ransomware *Healthcare*
The threat actor Everest Ransom Team named a Portugal-based hospital as a victim on their data leak site (DLS). The threat actor claimed to have access to 37 GB of customer and employee data and other hospital documents. The threat actor also provided a password-protected link to access the allegedly stolen files.

French maternity hospital hit *Healthcare*
On October 9, the threat actor Vice Society breached the French maternity hospital Les Bluets in Paris. At time of writing, the impact is still unknown.

Prestige ransomware targets Ukrainian and Polish organisations *Transportation*
Microsoft said threat actors used the new Prestige ransomware to target transportation and logistics organisations in Ukraine and Poland. The threat actors first used this new ransomware in the wild on October 11, in attacks detected within an hour of each other.

German educational institute breached *Education*
On October 19, the ransomware threat actor Ragnar Locker claimed responsibility for an attack on the German Leibniz Institute for Educational Research and Information. Ragnar Locker made approximately 241 GB of the company's data publicly available. The organisation provides empirical educational research, digital infrastructure and targeted knowledge transfer, thus helping to address educational challenges.

German university hit *Education*
On October 20, the German University of Ansbach was the target of a cyberattack. As part of the response, the university blocked all access for staff and students. The university partially cancelled virtual seminars. The modus operandi of the attack strongly suggests ransomware.

UK high school hit *Education*
The Bishop of Hereford's Bluecoat School (BHBS), a UK-based high school, experienced a cybersecurity incident that disrupted the school's IT systems. According to a school spokesperson, there is no evidence that incident has compromised personal data of students or staff. On October 28 cybercriminals operating the Vice Society ransomware named BHBS as a victim on their DLS.

Newspaper's printing system disrupted by ransomware *Newspaper*
A ransomware attack impacted the printing system of the Baden-Wurttemberg, Germany-based Heilbronn Stimme newspaper on October 14 and forced the victim to release a 28-page e-paper. The newspaper issued a six-page "emergency" edition on October 15 and posted obituaries on its website as a workaround.

Other cybercrime

Ticketing service discloses 2,5 year-long breach *Payment cards*
The Europe-based ticketing service provider See Tickets disclosed a data breach and informed customers that cybercriminals might have accessed their payment card details via a skimmer on its website. The investigation showed that the infection happened on June 25, 2019, so the total duration of the exposure was just over 2,5 years.

Spain's Telefonica breached *Telecoms, End user equipment*
The Spanish telecommunication's company Telefonica issued notices to customers, on October 28, stating that it had suffered an intrusion. The incident allowed access to technical data or configurations of customer equipment.

Hacktivism

Pro-Russia hacktivists target Slovakia — *Government, Transportation, Web hosting*

On October 4 and 5, We Are Clowns, Anonymous Russia and Killnet, three supposed pro-Russia hacktivists, claimed cyberattacks against Slovakian targets. These cyberattacks in reality only consisted of DDoS attacks. DDoS attacks were operated against the websites of some government institutions such as the Slovak Ministry of Defence, the Human Rights Centre in Slovakia, airports, web hosting companies and airport taxi companies.
***Analyst note**: We assess a huge part of cyberattacks claimed by pro-Russia hacktivists aims to gather public attention and causes only limited damages.*

Pro-Russia hacktivists target Estonia — *Government*

On October 8, supposed pro-Russia hacktivists such as Anonymous Russia and Cyber Army of Russia, claimed to have conducted DDoS attacks against Estonian government websites in retaliation for the Estonian Foreign Minister congratulating Ukrainian special forces for damaging the Crimean Bridge.

Pro-Russia hacktivists target Czech Republic — *– ' –*

On October 21, the supposed pro-Russia hacktivist group Cyber army of Russia reborn claimed to have conducted a DDoS attack against the Pardubice airport in the Czech Republic.

Pro-Russia hacktivists target Poland — *Finance*

On October 24, Killnet claimed to have conducted a DDoS attack on the Polish stock exchange in Warsaw.

Pro-Russia hacktivists attack Polish and Slovakian Parliaments — *Legislature*

A spokesperson for the Polish Senate confirmed service disruptions, on October 28, due to DDoS attacks. According to news reports, similar attacks also blocked the Slovakian Parliament. Both parliamentary sessions had planned votes in which they would declare Russia a terrorist regime.

Pro-Russia hacktivists target Ukraine telecoms — *Telecoms*

On October 5, Xaknet, a supposed pro-Russia hacktivist, claimed be leaking data belonging to Kyivstar. Kyivstar us a Ukrainian telecom operator. The exposed data appears to contain big data analysis, contracts and mobile identities but it is unclear if they are authentic and belong to Kyivstar or not.

Pro-Russia hacktivists target Ukraine Ministry of Social Policy — *Government*

On October 12, Zarya, a supposed pro-Russia hacktivist affiliated with Killnet, leaked data supposedly belonging to the Ukrainian Ministry of Social Policy. The data contained names, email addresses, postal addresses and phone numbers.

Pro-Russia hacktivists claim intent to target Ukraine energy producer — *Energy*

On October 12, Cyber Army of Ukraine, a supposed pro-Russia hacktivist, claimed it would conduct unspecified cyber operations against Naftogaz is a Ukrainian energy producer involved in the transportation of natural gas, as well as the extraction, refining and transportation of oil. The threats coincided with Russian missile strikes on Ukraine.

Pro-Russia hacktivists target Ukraine cyber defence — *Cyber defence*

On October 20, Ukrainian Ministry of National Defence cancelled a hackathon following DDoS attacks by the group Noname057. A hackaton is a social computer programmers' event. Noname057 is a supposed pro-Russia hacktivist.

Pro-Russia hacktivists target Ukrainian hospital *Healthcare*
On October 31, the pro-Russian hacktivist groups Phoenix and WeAreClown claimed responsibility for an attack on a Ukrainian hospital in Kiev. The threat actors claim to have caused damage to the hospital's systems.
***Analyst note**: The impact of the attack is currently unknown to us. As in most previous cyberattacks by pro-Russia hacktivists, it is likely that the attack was a DDoS attack on websites.*

Disruption and hijacking

German energy company suffers cyberattack *Energy*
On October 27, Enercity, a German company in the energy sector suffered a cyberattack. The incident caused customer service to be unavailable. There is no indication that the incident has impacted power grids and related power plants.

Operations disrupted at copper smelter *Industry*
Europe's largest copper smelter, the German company Aurubis, reported, on October 28, that a cyberattack had resulted in the shutdown of its IT systems. It is possible the attack had a Russian origin due to statements by Aurubis, prompting the Western industry to ban the use of Russian metal.

Information operations

Nord Stream pipeline disinformation *Energy*
Within hours of Nord Stream pipeline explosion, Russian officials, Twitter users and Tucker Carlson began circulating disinformation suggesting that the Biden administration was responsible for the apparent act of sabotage. Some viral tweets included old footage of US military jets flying over Germany to support Russia's claims that the US was the culprit. While there is not yet evidence to say exactly who is responsible for the Nord Stream attack, however, plenty of officials are pointing at Russia.

Deepfake impersonation of Ukrainian Prime Minister *Ukraine, Government*
On October 9, the Ukrainian Defense Ministry's Main Intelligence Directorate (GUR) announced it disrupted an operation utilising deepfake technology to impersonate Ukrainian Prime Minister Denys Shmyhal. The imposter posing as Shmyhal purportedly believed they had contacted the founding director of a major private Turkish defence company specialising in unmanned aerial vehicles (UAVs). However, the imposter apparently spoke with GUR operatives. The GUR claimed the threat actor sought to undermine cooperation between Ukraine and Turkey.

Data exposure and leaks

NATO confidential data leak *Hack and leak*
In early August, a cyberattack against the Portuguese army allowed an unknown actor to steal hundreds of confidential NATO files. According to the Portuguese TV station, a second attack took place in the last week of September, creating a new leak of sensitive data, without specifying the nature of the data.

IT service provider to Dutch government suffers leak *IT service provider*
ID-ware, an IT service provider who produces access badges, suffered a data leak in September. The company services the Dutch government, including the first and second chamber of Parliament, with the Rijkspas, an access card.

Italian WIFI provider reportedly suffers data leak *IT service provider*
On October 25, Kelvinsecurity leaked data purportedly belonging to Italian organisation Filomeno WIFI on a dark web forum.

Dutch software vendor discloses data breach *IT service provider*
Dutch technology vendor Nedap disclosed a data breach related to Carenzorgt, a Dutch medical portal with more than 9 000 affiliated healthcare providers and 497 000 active users. Nedap clarified that the threat actor exploited an unidentified vulnerability to access and download documents from the portal

World

Cyber policy and law enforcement

Interpol arrests Black Axe members *Arrest*
Interpol has arrested over 70 suspected members of the Black Axe cybercrime syndicate, with two believed to be responsible for 1,8 million US dollar in financial fraud. An international law enforcement operation arrested the suspects between September 26 and 30 in South Africa.

Brazil arrests suspect linked to the Lapsus$ group *Arrest*
As part of Operation Dark Cloud launched in August, the Brazilian Federal Police arrested a Brazilian suspect in Feira de Santana, Bahia, believed to be part of the Lapsus$ extortion gang. The police suspects the individual to have participated in the December 2021 breach of the Brazilian Ministry of Health. In this incident Lapsus$ deleted files and defaced the Ministry of Health website to display a message where the group claimed it had stolen data from the ministry's network.
***Analyst note**: Lapsus$ is a group that has conducted data theft extortion operations since mid-2021. They are motivated by both financial gain and a desire for notoriety. They breach IT systems, exfiltrate data and threaten to publish on their Telegram channels. They use such channels to both shame victims and leak information when they are unsuccessful in coercing a victim.*

Operator of darkweb marketplace arraigned *Charges*
On October 26, the US Department of Justice arraigned a British citizen for allegedly running The Real Deal, a darkweb marketplace. The allegations relate to illicit services conducted in 2015 and 2016. Threat actors used this platform to sell stolen data and hacking tools as well as drug and weapons.

Malware-as-a-service operator extradition from NL to US granted *Charges*
On October 25, the US Department of Justice unsealed an indictment containing charges against a Ukrainian national for developing and operating the Raccoon Stealer Malware-as-a-Service (MaaS). The individual is being held in the Netherlands and is awaiting extradition to the United States. The Amsterdam District Court granted extradition on September 13.

US government indicts for violating sanctions *Sanctions*
On October 19, the US Department of Justice announced charges and arrests in two cases involving export violation schemes to aid the Russian military. The charges involved a dozen individuals and several corporate entities for participating in unlawful schemes to export powerful, civil-military, dual-use technologies to Russia.

Google Translate is disappearing from China *Censorship*
Google has decided to shut down Google Translate services in China. The translator was one of the few digital services still operating in China, which has now censored and blocked access to it. The Google Translate website and mobile app, as well as the Chrome extension, when accessed from mainland China, redirect users to the Hong Kong-based Google Translate website, which is blocked in the People's Republic of China.

FBI and CISA say cyberattacks targeting election systems unlikely to affect results *Elections*
In the US, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a public announcement in which they assess that any attempts by cyber actors to compromise election infrastructure are unlikely to result in large-scale disruptions or prevent voting.

US administration announces cybersecurity labelling for IoT devices *Regulation*
The US government announced on October 11 its plans to develop a cybersecurity labelling programme for internet-of-things (IoT) devices. The programme aims to improve digital safeguards for such devices. The programme will be followed by three to four recommendations that will be developed in consultation with the private sector.

Google sued over biometric data collection without consent *Data protection*
In the US, Texas attorney general has sued Google for allegedly collecting and using biometric data belonging to millions of Texans without proper consent.

Cyberespionage

Kimsuky targeting Android devices with newly discovered mobile malware *North Korean threat actor*
Security researchers found three new types of malware that target Android devices. They named the malicious APKs FastFire, FastViewer, and FastSpy. They attributed the malware to the North Korea-linked actor Kimsuky and they asses that Kimsuky's mobile targeting strategy is getting more advanced.

China-linked Mustang Panda targets Myanmar *Chinese threat actor*
Researchers at BlackBerry uncovered a campaign by the China-linked Mustang Panda threat actor that is leveraging the PlugX malware family to target the Southeast Asian state of Myanmar.

TrendMicro detail malicious toolset used by cyberespionage threat actor Earth Aughisky *Chinese threat actor*
According to TrendMicro, the China-linked threat actor named Earth Aughisky (aka Taidoor) has been using an increasingly sophisticated toolset in cyberespionage attacks targeting entities in Taiwan and Japan.

New Chinese APT targets IT service providers *Chinese threat actor*
A new threat cluster tracked as WIP19 has been targeting telecommunications and IT service providers in the Middle East and Asia. According to SentinelLab, it is highly likely espionage-related and WIP19 appears to be a Chinese-speaking threat group. WIP19 utilises a legitimate, stolen certificate to sign novel malware, including SQLMaggie, ScreenCap and a credential dumper.

Chinese APT continues to target Hong Kong *Chinese threat actor*
Researchers at Symantec reported a likely continuation of a cyberespionage campaign against Hong Kong dubbed Operation CuckooBees, which they attribute to the Chinese cyberespionage threat actor APT41. Cyberreason first reported on this campaign in May 2022. In Operation CuckooBee, the threat actors breached government agencies in Hong Kong and remained undetected for a year in some cases.

Likely Chinese APT targets casinos in Southeast Asia for cyberespionage purpose *Chinese threat actor*
According to researchers at Kaspersky Lab, a threat actor named DiceyF has been targeting online casinos based in Southeast Asia since at least November 2021. DiceyF does not appear to be targeting financial gains from the casinos but instead conducting stealthy cyberespionage and intellectual property theft. DiceyF activity aligns with Operation Earth Berberoka reported by Trend Micro in March 2022, both pointing to the threat actor being of Chinese origin.

APT10 continues targeting Japan *Chinese threat actor*
Researchers from cybersecurity company Kaspesky uncovered new activity and techniques by the Chinese APT10 threat actor against Japanese organisations. The threat actor abused security software to install a new version of their LODEINFO malware.

Lebanon-based Polonium threat actor targets Israel with new malware *Lebanese threat actor*
According to cybersecurity firm ESET, the Lebanon-linked Polonium threat actor has targeted more than a dozen organisations in Israel since at least September 2021 and until September 2022. Sectors targeted by this threat actor include engineering, information technology, law, communications, marketing, media, insurance, and social services.

Iranian services install malware on phones of Iranian protesters following their arrest *Iranian threat actor*
Germany's cybersecurity agency reportedly took down a web server used to control malware deployed by the Iranian government. The government used the malware, an Android remote access trojan dubbed L3MON, to monitor opposition supporters. The Iranian military manually installed the malware on the phones of arrested protesters. Although the German authorities have decommissioned the server used by the malware, they say the danger remains and potential targets should reset their smartphones, as the trojan does not have a persistence feature.

Android malware for surveillance operations against Iranian citizens *Iranian threat actor*
Researchers from ESET identified a new version of the Android malware FurBall which the threat actor Domestic Kitten uses to conduct mobile surveillance operations against Iranian citizens. Since June 2021, the threat actors are reportedly distributing the malware as a translation app via a copycat of an Iranian website that provides translated articles, journals, and books. The Domestic Kitten campaign is still ongoing, dating to at least 2016.

Indian threat actor targets Pakistan *Indian threat actor*
Researchers at Zscaler discovered that the India-linked SideWinder threat actor is using a new malware, dubbed WarHaw, in campaigns targeting Pakistan. SideWinder has been active since at least 2012, with a history of targeting government, military, and businesses throughout Asia, particularly Pakistan.

Suspicious activities of France-based company *PSOA*
News outlet Mediapart uncovered that a France-based private company called Avisa Partners is involved in misinformation activities on behalf of miscellaneous public or private customers in France and in foreign countries. Mediapart also says that the company is involved in the hack of an African telecommunication operator. The cyberattack reportedly aimed to spy on communications of opponents to the regime in Chad. Avisa Partners claims, however, that the Chadian government hacked the phone system and Avisa Partners were only a recipient of the report.

State-backed hackers stole data from US defence organisation *Unspecified threat actor*
On October 4, the US government released an alert about state-backed hackers using a custom CovalentStealer malware and the Impacket framework to steal sensitive data from a US organisation in the Defense Industrial Base sector. The compromise lasted for about ten months and it is likely that multiple advanced persistent threat groups likely compromised the organisation, some of them gaining initial access through the victim's Microsoft Exchange Server in January last year.

Budworm returns to targeting in the Middle East, Asia and US *Unspecified threat actor*
According to Symantec, a threat actor dubbed Budworm has mounted attacks over the past six months against strategically significant targets, including the government of a Middle Eastern country, a multinational electronics manufacturer, and a US state legislature. The latter attack is the first time in some years Budworm is targeting a US-based entity. Along with the above targets, the group also conducted an attack against a hospital in South-East Asia.

Cyberespionage campaign targeting Russian companies *Unspecified threat actor*
The Russian company Kaspersky Lab found that a large-scale cyberespionage campaign is targeting Russia. The attackers use phishing techniques with malicious Word documents sent by email to employees of Russian companies.

Cybercrime

Ransomware

Decryptor for Hades *Decryptor*
The Antivirus company Avast released, on October 4, a free decryptor for variants of the Hades ransomware. The decryptor operates thanks to a flaw discovered in the encryption scheme.

Guatemala Ministry of Foreign Affairs breached by ransomware *Diplomacy*
Onyx, a ransomware threat actor, claimed responsibility for the breach of Guatemala's Ministry of Foreign Affairs. The incident caused temporary system outages. The threat actor offered a link to leaked files.

Cybercriminals hit Australian Defence communications platform with ransomware *Defence*
Cybercriminals hit the Australian Defence's ForceNet external service, which Australian military personnel and defence staff use, with a ransomware attack. According to Assistant Minister for Defence Matt Thistlethwaite, the incident has not compromised data. Reporting from the Australian Broadcasting Corporation, however, cites an unidentified source with knowledge of the investigation who asserts that some private information such as dates of birth and enlistment information belonging to military personnel may have been stolen.

Large Brazilian health insurance provider breached *Healthcare, Insurance*
On October 18, the ransomware threat actor RansomEXX named Unimed Belem, one of the largest health insurance networks in Brazil, as a victim. The threat actor posted the announcement to their site along with 12 ZIP file links containing data allegedly obtained from the company. On October 13, Unimed Belem had announced it was the victim of a cyberattack and its internal monitoring detected a system breach.

Brazil's government services portal breached *Government*
The threat actor Everest Ransom Team claimed the breach of Brazil's federal government service portal and offered 3 TB of data up for sale. The data included documents and personal data of employees as well as VPN login details, credentials, and RDP access. Additionally, the post offers access to a company that serves 5.5 million users.

Vice Society targets the education sector with multiple ransomware families *Education*
Vice Society's ransomware and extortion campaigns impact the global education sector, particularly in the US. Their ransomware payloads have shifted over time from BlackCat, QuantumLocker, and Zeppelin to a Zeppelin variant.

Microsoft Exchange servers exploitation led to LockBit ransomware *ProxyNotShell*
The South Korea-based firm AhnLab reported that cybercriminals compromised Microsoft Exchange servers through ProxyNotShell with a then zero day vulnerability and deployed the Lockbit ransomware on the victim's network.

Links between Ransom Cartel and the REvil gang *Ransomware rebranding*
Security researchers report links between the Ransom Cartel ransomware operation and the REvil gang. The researchers make this assessment based on code similarities in both operations' encryptors. The REvil gang had shut down in October 2021 following intense pressure from law enforcement. Ransom Cartel emerged in December 2021.

US government warns of ransomware attacks against public health sector *Healthcare*
CISA, the FBI, and the US Department of Health and Human Services warned that a cybercrime group known as Daixin Team is actively targeting the US Healthcare and Public Health sector with ransomware attacks.

Other cybercrime

Live support service spreads malware in supply chain attack *Supply chain attack*
As part of a new supply chain attack, threat actors trojanised the official installer for the Comm100 Live Chat application, a widely deployed SaaS which businesses use for customer communication and website visitors.

Cybercriminals built a credential-stealing enterprise on code hosting platform *Supply chain attack*
LofyGang, a cybercrime group, conducted stole credentials by distributing 200 malicious packages and fake hacking tools on code hosting platforms. The code hosting platforms included NPM and GitHub. Many of the malicious packages have removed, but others are still available for download at the time of writing.

Private npm packages disclosed via timing attacks *Supply chain attack*, *Timing attack*
A new form of supply chain attack leverages npm (Node Package Manager) packages. Npm is a package manager for the JavaScript programming language. Using a technique called timing attack, threat actors detect organisation-scoped private packages and then masquerade public packages, tricking employees and users into downloading them.

Hundreds of Microsoft SQL servers backdoored *Backdoor*
Security researchers have found a new piece of malware targeting Microsoft SQL servers. Maggie, the backdoor, has already infected hundreds of machines all over the world. Threat actors controlled Maggie through SQL queries which instruct it to run commands and interact with files. Its capabilities extend to brute-forcing administrator logins to other Microsoft SQL servers and doubling as a bridge head into the server's network environment

Cybercrime group stole 2 million Binance Coins *Cryptocurrency*
A cybercrime group stole 2 million Binance Coins (BNB), worth 566 million US dollar, from the Binance Bridge. On October 6, the attacker's wallet received two transactions, each consisting of 1.000.000 BNB. A few hours later, the CEO of Binance tweeted that the cybercriminals had used an exploit in the BSC Token Hub to transfer the BNB to threat actor controlled accounts.

Cryptocurrency platform reportedly suffered a loss of 14,5 million US dollar in cryptocurrency *Cryptocurrency*
A threat actor reportedly abused the cryptocurrency platform Team Finance. The incident resulted in reportedly 14,5 million dollar of stolen cryptocurrency.

Threat actors steal 100 million US dollar from Mango Markets DeFi trading platform *Cryptocurrency*
Solana-based cryptocurrency trading platform Mango Markets confirmed a cybersecurity incident resulting in the theft of 100 million US dollar. Mango Markets reported via Twitter that the threat actors drove up the price by 5 to 10 times in a matter of minutes using an Oracle pricing manipulation and then extracted 100 million US dollar, which was the total equity available on the platform.

Fake WhatsApp distributed through legitimate apps *Mobile app*
An unofficial WhatsApp Android application named YoWhatsApp reportedly stole access keys for users' accounts. YoWhatsApp is a messenger app that uses the same permissions as the standard WhatsApp app and is promoted through advertisements on popular Android applications like Snaptube and Vidmate.

Hackers hit cybersecurity conference *Phishing*
Threat actors reportedly targeted the online cyber conference organised by the Australian Institute of Company Directors and forced the organisers to cancel the event. Participants attempted to access the conference via the LinkedIn video streaming service on October 24, but the conference never went live. Instead, participants received an Eventbrite link via the messaging section of the LinkedIn video streaming platform. The link directed individuals to a likely phishing page, asking participants to input their credit card details.

Caffeine PhaaS platform provides to target Russian and Chinese-speaking individuals *Phishing as a service*
Caffeine, a phishing-as-a-service (PhaaS) platform, reportedly is providing phishing templates designed to target Russian and Chinese end users. Caffeine allegedly has subscriptions ranging from 250 US dollar for one month to 850 US dollar for six months. The PhaaS kit reportedly can also generate lures imitating a Microsoft 365 login page, which aims to steal Microsoft 365 account credentials.

Disruption and hijacking

Hacktivists claim to compromise Russian mobile phone operator's routers *Satcoms*
On October 10, TeamOneFist, a supposed pro-Ukraine hacktivist, claimed to have concluded Operation Cataclysm. The operation reportedly targeted Megafon. Megafon is a Russian mobile phone operator that aims to provide data access to on-the-ground users from low-earth orbit satellites. This is the third time that TeamOneFist claims to have attacked Russian satellite systems. They claim to have disrupted two Moscow-based satellite ground stations by sending a high volume of cellular traffic to both satellite constellations in three attack waves. They claim to have caused day-long outage to have compromised the configuration of the underlying routers.
_**Analyst note**: These are unverified claims

Pro-Ukraine TeamOneFist targets Russian research programmes *Research*
On October 16, TeamOneFist claimed to have launched a new operation against several research programmes of the Russian Academy of Sciences in Moscow. TeamOneFist claims that one of the routers connected to the academy's network was misconfigured and connected to the internet, which allowed them to access the Russian network.

Pro-Ukraine TeamOneFist targets Russian routers *Routers*
On October 27, TeamOneFist announced that it was conducting a cyber operation called Kazimierz Pulaski. The aim of the operation was reportedly to destruct 224 Russian routers. The team claims to have developed a technique to monitor compromised routers to help confirm their destruction. To do this, the hacktivists claim to have exploited a zero day vulnerability which makes it impossible to fully boot up the router, thus rendering it irreparable. TeamOneFist also announces that for this operation, two Polish cyber actors helped.
***Analyst note**: None of these claims are confirmed or corroborated.*

2,5 Tbps DDoS attack against Minecraft server *Gaming*
A DDoS attack against Minecraft servers reached a rate of 2,5 Tbps, which lasted for about two minutes and consisted of UDP and TCP packets.

Indian energy company Tata Power's IT infrastructure hit by cyberattack *Energy*
A cyberattack targeted Mumbai-based Tata Power Limited and affected some of its IT systems. According to a Tata Power filing with the National Stock Exchange of India, in response to the attack, the power company took steps to restore impacted systems and implemented improved security procedures for customer-facing portals in an effort to prevent further unauthorised access.

Data wiper pretends to be ransomware, frames security researchers *Data wiper*
According to news media, on October 30, an unspecified threat actor was using the SmokeLoader malware botnet to deliver a new wiper, called Azov. The wiper pretends to be a Ukrainian-origin ransomware. It also mentions a number of known security researchers as contact points, in an effort to frame them. There is no known decryption method, making the malware a wiper.

Information operations

Disinformation before 2022 US midterm elections *Elections*
The US FBI issued a warning, on October 6, on foreign influence operations that intend to spread disinformation to influence the November 2022 US midterm elections. The agency pointed to the use of spoofed websites, fake social media personas, and publicly available media channels to spread and amplify the intended messages

Chinese disinformation operation targeting the US elections *Political system, Elections*
Mandiant has reported, on October 26, that they observed an influence campaign targeting the US political system, to promote narratives favourable for China (PRC). The campaign aimed to compromise US interests and affect the US midterm elections.

Data exposure and leaks

Large data leak dubbed BlueBeed caused by misconfigured data buckets *Microsoft Azure*
SOCRadar discovered six large public buckets, containing information of more than 150.000 companies in 123 different countries. SOCRadar dubbed the leaks BlueBleed. The first part of the collection (BlueBleed Part I) is due to a misconfigured Azure Blob Storage (an optimised data depository for storing big volumes of unstructured data).

Modified apps stealing user data *Social media*
Meta sued Chinese software development companies for allegedly using unofficial WhatsApp Android apps to steal over one million user accounts from Meta's platform. The operation, which started in May 2022, was using modified versions of WhatsApp, delivered outside Google's Play store and reportedly managed to steal more than one million WhatsApp accounts.

Optus confirms data breach exposed the ID numbers of 2,1 million customers *Telecommunications*
Optus, an Australian telecom provider, disclosed a cybersecurity incident in September. The company has now confirmed that the incident caused unauthorised access to approximately 2,1 million customer identification numbers.

2K Games user data for sale online *Gaming*
Video game publisher 2K warned users that threat actors leaked personal and put them up for sale online following a September 19 security breach.

Darkweb marketplace releases massive dump of credit cards to promote its operations *Credit cards*
A darkweb marketplace named BidenCash has released 1.221.551 credit card numbers, aiming to promote its position in the cybercriminal market.

Intel's Alder Lake BIOS source code leaked *IT*
Intel has confirmed that a source code leak for the UEFI BIOS of Alder Lake CPUs is authentic. Alder Lake is the name of Intel's 12th generation Intel Core processors, released in November 2021. The leak contains 5.97 GB of files, source code, private keys, change logs, and compilation tools.
Analyst note: *According to researchers, the data can help the security researchers, bug hunters (and the attackers) find the vulnerability and understand the result of reverse engineering easily, which adds to the long-term risk to the users.*

Toyota customers' personal data exposed *Automotive*
Toyota discovered that a portion of the T-Connect site source code was mistakenly publicly available on GitHub for almost five years. Toyota T-Connect is the carmaker's official connectivity app that allows owners of Toyota cars to link their smartphone with the vehicle's infotainment system. The published source code contained an access key to the data server that stored customer email addresses and management numbers. The company warned that the incident may have exposed data of more than 296.000 customers.

Personal data of 3 million patients exposed *Healthcare*
Advocate Aurora Health (AAH), a healthcare IT system used by 26 hospitals in the US notified its patients of a data breach that exposed the personal data of 3.000.000 patients. An improper use of Meta Pixel on AAH's websites, where patients log in and enter sensitive personal and medical information, was the cause of the incident. Meta Pixel is a JavaScript tracker that helps website operators understand how visitors interact with the site, helping them make targeted improvements.

Australian Clinical Lab suffers data breach *Healthcare*
Australian Clinical Labs disclosed a February 2022 data breach that impacted its Medlab Pathology business, exposing the medical records and other sensitive information of 223.000 people.

Australian police secret agents reportedly exposed in Colombian data leak *Government*
Threat actors leaked documents stolen from the Colombian government, which caused the exposure of identities of secret agents working for the Australian Federal Police (AFP).

Iranian government suffers data leak *Energy*
The Iranian Atomic Energy Organisation reportedly confirmed that one of its subsidiaries' email servers suffered a data leak.

Singaporean online marketplace suffers data leak *Online marketplace*
Cybercriminals are selling data of 2,6 million Carousell accounts on the darkweb. Carousell is a Singaporean online consumer-to-consumer and business-to-consumer marketplace.

Large personal and health data breach affecting Australian insurance firm *Insurance, Health*
Australian insurance firm Medibank confirmed that hackers accessed all of its customers' personal data and a large amount of health claims data during a recent ransomware attack.

Amazon leaks data of viewing habits for Prime service *Steaming platforms*
A security researcher discovered a database of user viewing habits in the Amazon Prime service to be accessible over the internet. According to news reports, on October 27, the database contained about 215 million entries but data was anonymised.

Significant vulnerabilities

New Microsoft Exchange Zero Day Vulnerabilities *Microsoft Exchange*
The security researchers at Vietnamese cybersecurity vendor GTSC published a blog post claiming they have discovered an attack campaign which utilised two zero day bugs in Microsoft Exchange that could allow an attacker a remote code execution. The attackers are chaining the pair of zero day to deploy web shells, notably China Choppers, on compromised servers for persistence and data theft, as well as move laterally to other systems on the victims' networks. Microsoft had identified the vulnerabilities as CVE-2022-41040, a Server-Side Request Forgery (SSRF) vulnerability, while the second, identified as CVE-2022-41082, allows remote code execution (RCE) when PowerShell is accessible to the attacker. See CERT-EU's SA 2022-068.

Update: Remote Code Execution in Zimbra Collaboration Suite *Zimbra*
A remote code execution vulnerability similar to CVE-2022-30333 (SA2022-063) was reported for Zimbra Collaboration Suite. Tracked as CVE-2022-41352 since September 25, this yet-unpatched flaw is due to an unsafe use of a vulnerable "cpio" utility by the Zimbra's antivirus engine Amavis. The exploitation of this vulnerability allows a remote unauthenticated attacker to execute arbitrary code on a vulnerable Zimbra instance. Proofs of Concepts (POC) are publicly available for this vulnerability and reported actively exploited. See CERT-EU's SA 2022-069.

Update: FortiOS and FortiProxy Critical Vulnerability *Fortinet*
Fortinet released a security advisory to warn about a critical vulnerability (CVSS v3 score: 9.6), tracked as CVE-2022-40684, impacting the FortiOS, FortiProxy and FortiSwitchManager. The exploitation of this vulnerability allows an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests. Fortinet is aware of at least one instance where this vulnerability was exploited and hence it is recommended to remediate this vulnerability with the utmost urgency. A proof-of-concept (PoC) exploit and a technical root cause analysis for this vulnerability has been published by the Horizon3.ai security researchers. See CERT-EU's SA 2022-070.

Junos OS: Multiple Vulnerabilities in J-Web — *Junos OS, J-Web*
Multiple vulnerabilities have been found in the J-Web component of Juniper Networks Junos OS. One or more of these issues could lead to unauthorised local file access, cross-site scripting attacks, path injection and traversal, or local file inclusion. See CERT-EU's SA 2022-071.

Apache Commons Text Vulnerability — *Apache*
A vulnerability, tracked as CVE-2022-42889 with a CVSS score of 9.8 was found in Apache Commons Text packages in versions 1.5 through 1.9. The affected versions allow an attacker to benefit from a variable interpolation process contained in Apache Commons Text, which can cause properties to be dynamically defined. Server applications are vulnerable to remote code execution (RCE) and unintentional contact with untrusted remote servers. See CERT-EU's SA 2022-072.

OpenSSL Critical Vulnerability — *OpenSSL*
On October 25, the OpenSSL project team announced the upcoming release of OpenSSL version 3.0.7, planned to be available on November 1. This version will fix a critical vulnerability. While there is no technical details about this vulnerability, the team urged organisations to inventory systems using OpenSSL and prepare for immediate patching when the fix is released. See CERT-EU's SA 2022-073.

DoS Vulnerabilities in Pulse Secure Products — *Ivanti Connect Pulse Secure*
On October 13, Ivanti released an advisory regarding two vulnerabilities affecting Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), and Ivanti Neurons for Zero-Trust Gateway that could lead to DoS conditions if exploited. It is recommended to upgrade to the latest version of these products. See CERT-EU's SA 2022-074.

Type Confusion Vulnerability in Chrome Browser — *Chrome*
On October 27, Google released a new version of its Chrome browser fixing a high-severity flaw, identified by "CVE-2022-3723". Google is aware of reports that an exploit for CVE-2022-3723 exists in the wild. It is highly recommended to apply the update. See CERT-EU's SA 2022-075.

Critical Vulnerability in VMware Cloud Foundation — *VMware Cloud Foundation*
On October 25, 2022, VMWare released a new version of Cloud Foundation (NSX-V) fixing a critical Remote Code Execution vulnerability. VMware has confirmed that exploit code leveraging "CVE-2021-39144" against impacted products has been published. It is highly recommended applying the last version. See CERT-EU's SA 2022-076.

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.

TLP	Disclosure	Message
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.