THREAT LANDSCAPE REPORT

S21SEC

Cyber Solutions by Thales

INTRODUCTION

The second half of 2022 was mainly marked by the presence of previously known threats that pose a risk to both public and private entities, with almost 1,500 attacks publicly recorded by threat actors.

As in the previous semester, the exploitation of vulnerabilities such as Follina or Spring4shell, involving vendors such as Apple, Cisco, Google, or Microsoft Exchange, stands out. The greatest danger of these threats is that many of them have been exploited in zero-day attacks with no patches or fixes and are becoming one of the most used resources by the actors.

According to data from the National Vulnerability Database, 13,243 vulnerabilities classified with the Common Vulnerability Scoring System v3.X standard have been disclosed. A total of 44 ransomware families have been identified this semester, affecting a wide range of industry sectors, highlighting the industrial and healthcare sectors.

The emergence of new operations during the second semester is noteworthy. Compared to the previous half-year in which 10 new groups were observed, during the second half of 2022 15 new ransomware operations have emerged.

Once again, mobile devices remain one of the main targets for cybercriminals, who continue to find ways to introduce their malware on the official Google and Apple marketplaces.

Finally, the second half of 2022 also stands out for the high activity of advanced persistent threat groups of Korean, Russian, and Chinese origin.

TABLE OF CONTENTS

VULNERABILITIES

Cyber vulnerabilities are weaknesses in software that can be exploited to compromise susceptible systems in cyberattacks.

The vulnerability threat landscape for the second half of 2022 is based on the analysis of the most significant vulnerability releases during this period, which has been characterized by the exploitation of vulnerabilities involving vendors such as Microsoft Exchange, Cisco, Google, Apple, and F5, among others.

01

Although exploitation of known vulnerabilities in the first half of 2022 has been observed over the second half, like Follina (CVE-2022-30190), Atlassian Confluence (CVE-2022-26134), Dog Walk (CVE-2022-34713) or Sprin4shell (CVE-2022-22965), other vulnerabilities continue to rank high for continued exploitation despite being disclosed in previous years, such as Log4Shell (CVE-2021-44228) or ProxyLogon (CVE-2021-26855).

Many of the vulnerabilities observed during the period under analysis that have been exploited in zero-day attacks before their disclosure or in attacks in which the vulnerability has been disclosed but not yet patched or corrected in the wild stand out.

In this regard, there has been a rapid capitalization of the weaknesses exploited in the systems, with zero-day exploits being one of the resources most used in attacks in the wild observed during the second half of the year.

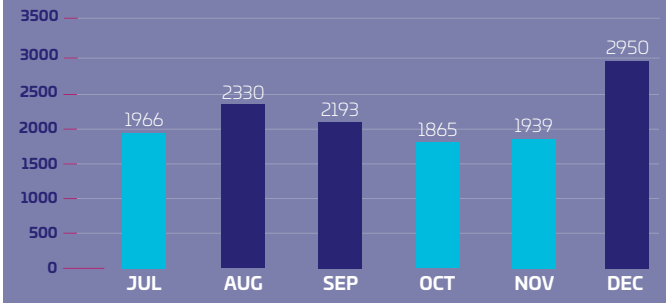
*Social engineering is the **main vector** of initial access.*

DogWalk, Follina, and many other vulnerabilities showing high exploitation through phishing and malspam campaigns by threat actors during the second half of 2022.

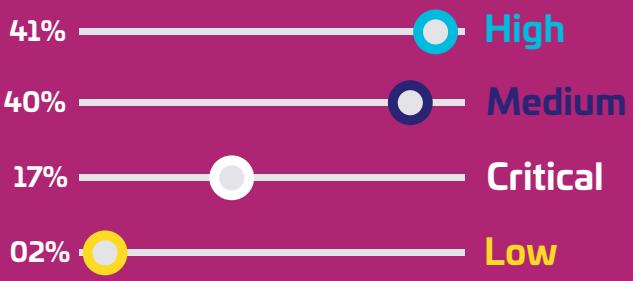
***13214 vulnerabilities** have been disclosed*

According to data obtained from NIST (National Vulnerability Database), 13243 vulnerabilities have been disclosed and classified with the Common Vulnerability Scoring System (CVSS) v3.X standard.

***August**, **September** and **December** have been the months with more published vulnerabilities.*



***Severity level** based on CVSS version 3*



In terms of vulnerability exploitation activity by threat actors, in July, several phishing campaigns were observed exploiting the vulnerability tracked as CVE-2022-30190 (Follina).

The vulnerability was exploited to distribute the Rozena backdoor on vulnerable Windows systems by sending e-mails with malicious Office documents. The backdoor injected a remote shell connection to the attacker's machine The use of exploits targeting vulnerable systems in attacks, thus being able to take complete control of the system. In addition, threat actors exploited the CVE-2022-2207 elevation of privilege vulnerability, allowing code execution as an unprivileged user, which is being used by malicious actors and affects Windows 11 and Windows Server.

In August, the exploitation of Follina in targeted attacks against Russian organizations continued, and threat actors distributed the remote access trojan (RAT) known as Woddy RAT.
DrayTek, Moodle, Palo Alto Networks, Realtek, and VMWare were other affected vendors. On the other hand, vulnerability CVE-2022-34713, known as DogWalk, involved in August 2022, a new trend of criminals exploiting a flaw in the Microsoft Support Diagnostic Tool (MSDT) to operate through a malicious document, which does not require a victim to enable macros.

A zero-day remote code execution vulnerability used attacks in-the-wild by threat actors was shared in late September. The zero-day affects Microsoft Exchange on corporate mail platforms, according to the post published on September 30 for the Microsoft Exchange Server remote code execution vulnerability tracked as CVE-2022-41040 and CVE-2022-41082. Microsoft states that it was aware of the targeted attacks and that these would be limited, confirming that systems were being attacked using the zero-day vulnerability to install backdoors to gain remote access to systems and perform other more targeted, higher-impact attacks.

OCTOBER

In October several zero-day vulnerabilities were detected affecting Apple, Fortinet, Google, and Microsoft were found. Also, Mark-of-the-Web (MOTW) vulnerabilities affecting recent versions of Microsoft Windows and Windows Server appeared to have been actively exploited.

NOVEMBER & DECEMBER

In November and December, the trend of exploiting zero-day vulnerabilities continued. Threat Actors behind the Magniber ransomware exploited CVE-2022-41228 to execute arbitrary code on the infected system with user privileges, together with the exploitation of the CVE-2020-1472, which has been active since 2020 and allows the elevation of privileges using the Netlogon remote protocol (MS-NRPC).

RANSOMWARE

During the second half of 2022 a total of 1487 ransomware attacks were recorded.

According to S21sec Threat Intelligence team investigation, more than 50 ransomware groups have been actively making public its attacks in the deep web.

02

It should be noted that the observed number of attacks covers exclusively recorded public activity that threat actors have carried out.

A total of 44 ransomware families have been identified during the second half of the year, targeting a wide range of sectors and industry verticals globally.

The most active groups were LockBit, BlackCat (ALPHV), and Black Basta.

S21SEC Cyber Solutions by Thales

RANSOMWARE FAMILIES

Ransomware Statistics

The following graph shows the activity of the ten most active ransomware families during the six months under analysis. The attacks carried out by these 10 families gathers over the 70% of the ransomware attacks during the six months.

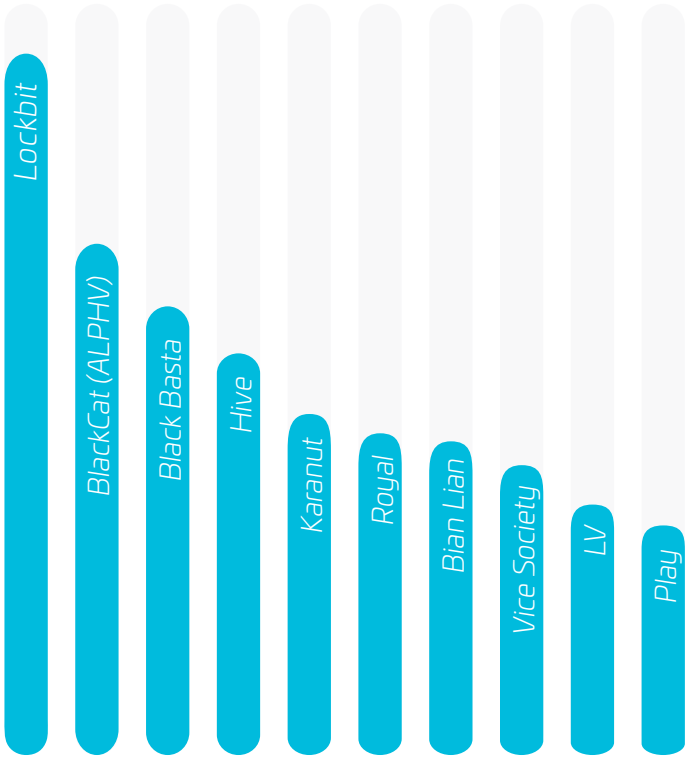
The trend regarding the appearance of new ransomware operations stands out. There was a significant increase on the number of new groups. During the first half of 2022, approximately ten groups were observed between January and June, and in the second half 2022, more than fifteen new operations have emerged.

Thus, in July, the groups known as Haron, Omega, RedAlert, BianLian BlOOdy, and Play emerged, all with intense activity worldwide and a broad targeting approach. Other operations were Donuts Leak, IceFire, Play, or Sparta. The latter operation whose activity began on September 13, 2022 was directed exclusively on Spanish targets and the group used the Deep Web extortion site Sparta Blog to leak data and extort its victims.

Another notable operation is the Royal ransomware. Although it emerged in early 2022, in November the group made its attacks public via the leak site hosted on the Deep Web. Royal targets victims through phishing attacks, impersonating software providers or legitimate delivery services. The ransomware encrypts the victim's files using the .royal extension, leaving a ransom note, named README.TXT, on infected systems. The ransomware is capable of encrypting files on the virtual disk (VMDK).

Finally, among the most recent operations is the one known as Nokoyawa, which was detected in March 2022. However, it showed activity on a Deep Web leak site opened at the end of the year. It is highly possible that the Nokoyawa group is linked to the Hive ransomware operation, sin it shares similarities in their tactics, techniques, and procedures (TTP), such as the chain of attacks and tools used.

Top 10 most active ransomware families in the second half of 2022.



MOST AFFECTED SECTORS

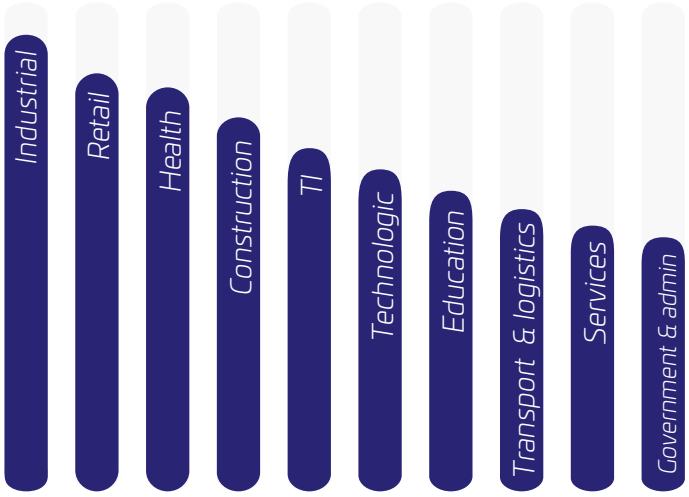
Ransomware Statistics

In terms of impact by sector, during the second half of 2022, the activity was primarily directed at companies belonging to the industrial (14%), retail (7%), and healthcare (7%) sectors.

The following chart shows the ten most affected sectors from the wide range of industry verticals exposed during the period under analysis.

Overall, the impact of the ransomware threat amounts to more than 65 % of the monitored attacks.

Top 10 victims of ransomware by sector in the second half of 2022



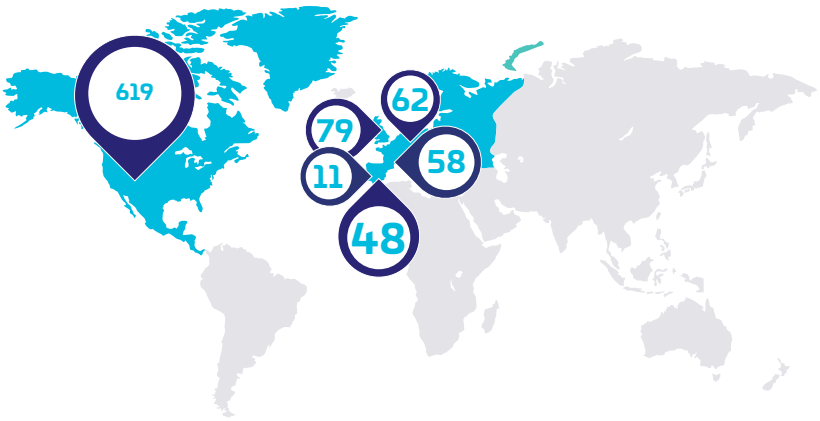
MOST AFFECTED COUNTRIES

Ransomware Statistics

In terms of geographic targeting, ransomware groups have mainly targeted targets in North America (United States, Canada, Greenland, and Mexico), with a total of 696 attacks recorded. US victims were the most affected, with 619 attacks representing 42% of the total attacks claimed in the year's second half (1487).

Spain suffered 48 attacks during the second half of 2022, an increase of 41% compared to the previous six months. The same applies to Portugal, which recorded 11 attacks, representing a 120% increase in ransomware incidents.

Ransomware victims by country in the second half of 2022.



LOCKBIT 3.0

Since the release of the 3.0 version of the ransomware in June 2022, the operators behind LockBit have employed new tactics, techniques, and procedures (TTP) in their attacks deployed during the second half of the year.

Once LockBit encrypts the victim's files, the new version 3.0 of the ransomware changes the wallpaper of infected computers to black (LockBit Black), leaving a file named [random_text].README.txt with instructions on how to proceed with the ransom payment.

In September, LockBit was the victim of a leak of the LockBit 3.0 builder by an alleged affiliate of the group.

The leaked builder consists of four files, an encryption key generator, a builder, a batch file to build all the files, and a modifiable configuration file that allows anyone to customize and modify the ransom note to create a new infrastructure.

The leak means a potential rise in threat actors who can employ the builder to launch their ransomware operations and attacks, as in the case of BlOODy Ransomware Gang, which has been observed using the builder to create the BlOOdy encryptor in an attack targeting a Ukrainian organization during September.

BLACKCAT (ALPHV)

During the second half of the year, it has been observed that the ransomware threat group uses the BruteRatel tool for the Intrusion stage in its attacks, along with other commercial remote access tools such as AnyDesk and TeamViewer, as well as the open-source tool called nGrok. BlackCat (ALPHV) is characterized by the exploitation of unpatched firewalls and VPNs on internal systems, along with the use of known vulnerabilities.

BLACK BASTA

It is another one of the most active threat groups during the second half of 2022. Discovered in April 2022, it targets organizations around the world. Black Basta ransomware is written in C++ and is cross-platform, targeting Windows and Linux operating systems through a variant of VMware ESXi targeting virtual machines running on Linux servers.

Although Black Basta showed novel code, it shared some similarities with the Conti ransomware. In November, the operation released its new Black Basta 2.0 version with some updates regarding its file encryption algorithms via the GNU Multi-Precision Arithmetic Library (GMP), the Crypto++ encryption library, the introduction of stack-based string obfuscation and per-victim file extensions.

Once Black Basta 2.0 encrypts victims' files, it changes the file names by appending the victim-encrypted extension such as .agnkdbd5y, .taovhsr3u, or .tcw9lnz6q to them, unlike the previous version of the ransomware that used .basta as the encrypted file extension.

The image of the icon used to encrypt the files has changed from a white square (in the first version of the malware) to a red square.

The Black Basta 2.0 ransom note has changed its name and text content (previously named readme.txt and now renamed to instructions_read_me.txt), which is opened in Windows Notepad using the command cmd.exe /c start /MAX notepad.exe.

Black Basta 2.0 also no longer implements the change of the victim's desktop wallpaper, nor does it terminate processes and services that may interfere with file encryption.

USED TIPS

Ransomware groups have evolved in their use of new tactics, techniques and procedures in their operations, most notably Black Basta's use of the new detection evasion method known as 'intermittent encryption'. It allows systems to be encrypted more quickly, encrypting only parts of the zrecoverable without the use of the decryption key. The technique also reduces the chances of detecting attacks.
In early October, researchers found evidence of wiper functionality added to a previously used data exfiltration tool employed by ransomware operators.

The evidence points to a possible version of Exmatter, a data exfiltration tool associated with BlackCat intrusions, which is notable in this period for its use of the QakBot banking Trojan as an initial entry point and payload for lateral movement, as well as its use of a persistence method based on hijacking a legitimate service by deleting it and recreating a new malicious service with the same name.

Russia-Ukraine V Conflict

2022 has been marked by the Russian invasion of Ukraine, a conflict that has moved from the physical to the cyber terrain and has led to an increase in cyberattacks not only in the contending countries but globally.

In the first half of 2022, attacks such as the one attributed to the Sandworm APT against a Ukrainian energy provider company using the Industroyer malware and different destructive wiper malware against Ukrainian organizations were observed.

This typology of attacks has continued throughout 2022, with at least seven wiper strains observed in attacks by actors allegedly linked to the Russian government.

03

The Security Service of Ukraine claims that cyberattacks directed against the country tripled in 2022 compared to previous years.

The targets of these attacks are the critical infrastructure sectors, such as energy, communications, logistics, military, and government databases. During December 2022, the energy sector has been the most affected by cyberattacks.

Governments of Western countries allied with Ukraine have also been affected by an intensification of cyberattacks.

According to Microsoft, Russian intelligence services have tried to intrude into the networks of 128 targets from 42 countries.

Most of these attacks aim to obtain sensitive information from government agencies of countries with an essential role in NATO, so their targets are usually public entities.

For this reason, the Council of the European Union posted a warning of the risks of Ukrainian war-related cyberattacks on European countries that can be carried out by actors involved in the conflict.

During this conflict, the most common cyberattacks sought to destroy data and systems, disrupt the regular operation of critical infrastructure, and exfiltrate a significant volume of data.

HACKTIVISM IN THE UKRAINIAN CONFLICT

The hacktivist landscape has been altered since the beginning of the war in Ukraine, with the participation of so-called pro-Russian and pro-Ukrainian groups.

This disruption has affected not only the countries directly involved in the military conflict (Russia and Ukraine). NATO member states have also suffered the consequences of cyberattacks against their defense organizations and public entities.

TYPOLOGY OF CYBER ATTACKS

Most of these cyberattacks have been DDoS and intrusions to collect sensitive information. However, no significant actions by hacktivist groups that could have caused severe computer damage to the networks of different organizations have been detected.

The most recognised pro-Russian groups over the past 6 months have been NoName057(16), KillNet, Anonymous Russia, Cyber Army of Russia and XakNet Team. Pro-Ukrainian groups have also mobilised under hacktivist operations, notably IT Army of Ukraine, Studen Cyber Army, AnonGhOst, Belarusian Cyber-Partisans and NB65. Cyber-attacks are identified against Russian military entities and drone factories, volunteer platforms (Dobro), military shops and armaments (Arsenal Army, Kapterka), as well as military transport logistics companies (Dostavka-Krym).

S21SEC Cyber Solutions by Thales

KILLNET

KillNet, the leading pro-Russian hacker group, has carried out multiple cyberattacks on Ukraine and any country that took a position in its favor.

This group emerged in the wake of the Russian invasion of Ukraine and is believed to be sponsored by the Russian government, although they may also be financially motivated.

Most of these have been DDoS attacks, their speciality, against non-combatant targets around the world perceived as hostile to the Russian government, in order to put pressure on them.

In July 2022, it launched a DDoS attack against the US domain congress.gov, which briefly affected public access.

In August, KillNet attacked U.S. aerospace company Lockheed Martin again using DDoS, stealing employee data from the company.

In November, the European Parliament's website was the victim of a cyberattack carried out by KillNet, shortly after a resolution calling Russia a "state sponsor of terrorism" was passed.

FINANCIAL SECTOR

Digitalization processes have made the financial sector be among the most targeted industries by cybercriminals in recent years, especially by those whose primary interest is making an economic profit. The most common attacks targeting companies in the financial sector are ransomware, unauthorized server access, and data theft.

The main attack vectors are exploiting vulnerabilities in the targeted systems, supply chain attacks, prior compromise of other malware, phishing, and compromised credentials.

04

The most active infostealers in the last six months worldwide have been Formbook, Agent Tesla, Raccoon Stealer, Lokibot, and Vidar.

In this regard, the last half of 2022 has seen an increase in attacks on companies in the financial sector by infostealer malware, designed to steal information from the victim's computer, such as login credentials, usernames, clipboard credentials, cookies, and obtain 2FA or credentials stored in browsers.

Once it obtains this information, it extracts it to a command-and-control server under the cybercriminal's infrastructure, where it receives all this information.

AGENT TESLA

Agent Tesla is a RAT (Remote Access Trojan) and infostealer distributed as Malware-as-a-Service (MaaS). Since its appearance in 2014, this RAT has continued adapting to steal credentials and data from its victims, such as cookies or keystrokes.

The most frequent entry vector for Agent Tesla are phishing emails containing a malicious file attachment. When the user downloads and executes this file, the infection is initiated. In the last six months, campaigns have been observed in which Agent Tesla malware is being used to distribute Nanocore malware.

RACOON STEALER

The first version of Raccoon Stealer was sold as a MaaS (Malware-as-a-Service) on underground forums in early 2019, was written in C++, and priced around $75 per week or $200 per month, which helped it become popular among the rest.

A new version of this family started to be observed at the beginning of July 2022. Unlike the old version, this new version is written in C and assembler.

This stealer can obtain information from the infected computer, such as passwords, cookies, autofill information, and cryptocurrency wallet information.

On the other hand, over the past six months, trends observed within the threat landscape relative to a previous compromise show that cybercriminals continue to generate revenue from the development or sale of malware families or botnets that incorporate keylogging functionality to steal information. This kind of malware leverages multiple attack vectors to steal information from financial institutions and execute fraudulent bank transfers.

EMOTET

Emotet has been one of the most popular botnets in recent times, and the second half of 2022 has seen an increase in its activity compared to the first half of the year.

In these months there was multiple campaigns from this botnet targeting countries worldwide using a new malware variant that has credit card theft capabilities and targets Chrome browser data theft.

FAUPPOD

Fauppod is a very obfuscated malware that is also used to spread FakeUpdates and writes Raspberry Robin to USB drives.

On July 27, 2022, Microsoft identified some samples detected as Fauppod, which had process trees similar to the Raspberry Robin LNK infection, with DLL files written in similar locations and using similar naming conventions.

Their infection chain also released the FakeUpdate malware. However, the victims exposed to these samples did not have the traditional LNK file infection vector launched from an infected USB drive.

QAKBOT

QakBot, also known as QBot or Pinkslipbot, is a banking trojan primarily used to steal victims' financial data, including browser information, keystrokes, and credentials.

- Once QakBot has successfully infected an environment, the malware installs a backdoor that allows the threat author to launch additional malware, such as ransomware.

- QakBot is usually delivered via phishing campaigns and then executed in memory.

- QakBot has multiple modules to help monetise its intrusions, including propagation, web injections, email harvesting and other data theft.

- Recent campaigns have seen actors using QakBot to gain initial access to a system and then move laterally within an organization's network and deploy the Black Basta ransomware.

- In addition, it is worth noting that during this semester, a new threat to companies in the financial sector has been observed that spreads via USB, called Raspberry Robin, which in turn has been detected in conjunction with the Fauppod malware.

RASPBERRY ROBIN

Raspberry Robin is ransomware with worm-like functionality that spreads via infected USB devices and was first detected in September 2022.

Microsoft claims to have found this recently detected Windows worm on the networks of hundreds of organizations in several industry sectors worldwide.

This malware was using QNAP NAS devices as command-and-control servers in early November.

Infected USB devices often contain .LNK files that, after being executed by the user, unwittingly download other files, such as MSI installers, using msiexec.exe to contact their control servers.

MOBILE MALWARE

Smartphones continue to be one of the main targets of cybercriminals in the second half of 2022, with numerous malware families targeting the most common operating systems, such as Android and IOS.

Despite manufacturers' security measures in official marketplaces such as Google's PlayStore, cybercriminals continue to find new ways to introduce malware into these marketplaces. This make it easier for them to obtain thousands of downloads. However, there are also other ways of distributing this threat, for example through the use of advertisements or the use of websites that impersonate legitimate companies, where the user is tricked into downloading the malware.

Mobile malware developers generally seek financial gain, and they often designed the malware to steal banking credentials when someone accesses its banking application from the infected device.

05

MALIBOT

An Android banking trojan was discovered in 2022 while investigating another malware family that has been very active in recent years, called FluBot.

The developers of this malware camouflage the malicious application by masquerading as legitimate applications such as Mining X or TheCryptoApp, MySocialSecurity or Chrome.

Infected victims appear to have been lured to fraudulent websites where they are tricked into downloading the malware in their devices. In addition, the attackers send bulk SMS messages to all the infected user's contacts to distribute the fraudulent page and get more downloads.

Once a device is infected, it has the ability to perform overlay attacks prompting a phishing website that impersonates the authentication process of a legitimate application. This technique is used to carry out credential theft. In this case, the malware focuses on stealing banking credentials.

THE GODFATHER

At the end of 2022, a new Android banking Trojan appeared, targeting more than 400 banking institutions worldwide, but in most banking apps.

It targets the US (49), Turkey (31), Spain (30), Canada (22), France (20), Germany (19) and the UK (17).

The malware is distributed via Google's app marketplace and, once installed, pretends to be Google Protect and scans the device.

The malware requests access to accessibility permissions, which gives it full control over the device.

In this way, it generates fake notifications from banking apps that are installed on the victim's device to take the victim to a phishing page, so that the victim does not have to wait for the app to be actively opened.

06 ENERGY SECTOR

Cyber threats targeting the energy sector in the second half of 2022 have included state-sponsored operations by advanced persistent threat (APT) groups, most notably the People's Republic of China and the Russian Federation, along with threats from hacktivist groups and actors who have executed massive denial-of-service attacks, intrusions and data breaches of companies and institutions in the sector.

During the second half of the year, an increase in cyberthreats has been observed, especially in terms of ransomware attacks targeting this type of infrastructure, from several ransomware families such as LockBit, BlackCat (ALPHV), Hive, Daixin, Ragnar Locker, Everest, Lorenz, Industrial Spy, Snatch, BianLian, Royal, Quantum, Vice Society, Play or Cuba.

Threat actors have targeted companies from all economic areas. However, there was a focus on organizations belonging to the energy sector, such as renewable energy providers and oil and gas companies.

In August and September 2022, there was a wave of cyberattacks targeting companies and organizations belonging to the Italian energy sector claimed by the BlackCat (ALPHV) ransomware family. Among its victims were the Gestore Dei Servizi Energetici (GSE S.p.A.) agency, the Italian multinational oil company Eni SpA, and the Canarbino Group, which operates in the gas and electricity sector.

Within the advanced persistent threat group landscape, malware campaigns conducted by the North Korean-sponsored Lazarus group (also known as Hidden Cobra or ATP38) targeting energy providers in the United States, Canada, and Japan, as well as other energy organizations globally stand out. The main goals were to infiltrate to establish network permanence and conduct espionage operations in support of North Korean government.

Also, due to the global energy crisis in the wake of Russia's military conflict in Ukraine, threat actors have been taking advantage of the issue to target consumers in phishing campaigns. On exemple is a campaign recorded in September in which British regulatory bodies were impersonated through malicious emails and SMS text messages to trick victims into obtaining an alleged discount on their energy bills for the theft of personal data.

HACKTIVISTS GROUPS

In the mid of Russia's military invasion of Ukraine in February 2022, which ushered in an unprecedented cyber threat landscape for the sector, cyber activity has continued during the second half of the year.

While the first half of last year saw major attacks such as the one targeting US and international satellite communication networks (SATCOM), the second half of 2022 has been marked by leaks in critical infrastructure of the Nord Stream pipelines owned by Gazprom, a Russian state-owned energy company.

Given the evolving geopolitical landscape after the outbreak of the war, there is a high probability that Russia will use the threat of gas supply disruptions, as it did in June 2014. Russia could use this threat to increase its leverage over other European countries that depend on Russian gas.

DISTRIBUTED DENIAL OF SERVICES (DDoS)

The most prominent threat groups and actors are KillNet, XakNet, and Cyber Army of Russia.

Distributed Denial of Service (DDoS) attacks have disrupted services and websites of various industry, electricity and gas distribution companies in countries such as Ukraine. The victimis of these attacks include the Ukrainian electricity supplier, the country's largest oil producing company, the largest electricity producer and operator of nuclear power plants, as well as the Lithuanian electricity and gas distribution company.

DATA BREACHES

Among the data breaches suffered by entities in the sector, in early November, a Spanish electricity trading company was the victim of a cyber incident following unauthorized access to its IT systems, after which sensitive information of a limited number of the company's customers was compromised.

DEFENSE SECTOR

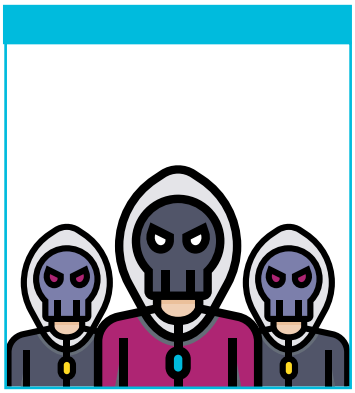
In the wake of the military conflict between Russia and Ukraine, various threat actors have directed their actions for the Defense industry.

With the prolongation of the conflict and the increase of operations and activities around the defense sector, in the last six months threat actors of various kinds and from different latitudes have been involved in cyber actions that have had an impact on the defense industry, including state agencies, defense companies, and military technology assets, among others.

07

When mentioning the threat actors responsible for such cyberattacks, it is necessary to identify their nature, objectives, and motivations.

During this last semester, the following threat actor groups have been identified as being involved in operations against the Defense industry:



Organized cybercriminal groups

Hacktivist groups

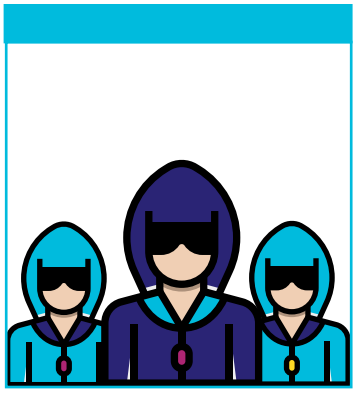
Advanced Persistent Threats

Organized cybercriminal groups include both ransomware groups and groups or individuals with lesser operational capabilities but with a significant impact on the target entity.

- In the first case, since the beginning of the Russian-Ukrainian conflict, ransomware groups have directed their activity against the defense sector, mainly affecting companies in the sector.

- The positioning of some ransomware groups in the conflict and the international and regional tension arising from it has created a scenario where ransomware cyberattacks have become one of the biggest threats to companies and organizations in the sector. The most relevant and active ransomware are LockBit 3.0, BlackCat (ALPHV), and Black Basta.

Organized cybercriminal groups



Hacktivis groups

Advanced Persistent Threats

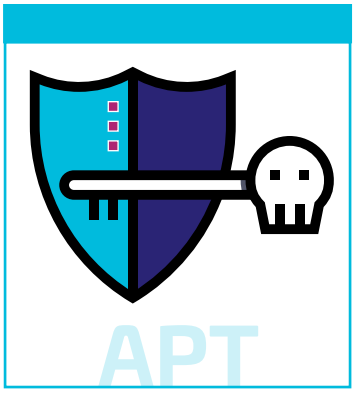
Outside the conflict between Russia and Ukraine, the group known as Guacamaya stands out, whose activity has focused on Latin America and against companies or targets in the defense sector.

Among its attacks are those against the websites and servers of the Armed Forces of Chile, Peru, Colombia, El Salvador, and Mexico, exploiting vulnerabilities in Exchange and Zimbra.

Similarly, the Adrastea group has also become one of the main threats in the sector in the second half of 2022 following its attack on a European missile manufacturing company. Following the attack, the group managed to exfiltrate confidential project information from the company and posted some of the information on underground forums.

Organized cybercriminal groups

Hacktivist groups



Advanced Persistent Threats

APT groups have positioned themselves as one of the threats with the highest level of criticality, having increased capabilities of action and infection and maintaining a constant process of updating their Tactics, Techniques, and Procedures (TTP).

the sponsorship they receive from their States of origin and their involvement with security and intelligence agencies creates a scenario in which APTs focus on carrying out high-level cyberattacks targeting critical entities and organizations, such as those in the defense sector.

In this regard, the current international and regional situation has given rise to numerous APT groups, mostly of Russian and Chinese origin, carrying out various operations against military and defense targets.

These operations are based on cyberattacks with destructive malware (wipers), cyber espionage campaigns, and malware injection to steal information or maintain persistence to identify possible vulnerabilities.

With the increase in APT groups' activity, several actions against the defense sector have been identified during the last six months.

In August 2022, several news stories were posted about the "possible hacking" of HIMARS missile launch systems operated in Ukraine, stemming from a joint operation between pro-Russian hacktivist groups and an unidentified Russian government group.

On the other hand, a campaign by the Russian group Callisto (AKA COLDRIVER) was identified between July and August. They started sending fraudulent emails with PDF attachments to military officers and defense agencies to collect credentials and extract sensitive information.

HEALTH SECTOR

VVVV

Cybercriminals keep a very high level of activity targeting the healthcare sector. Recent years have seen high rates of cyberattacks and disruptive actions against the IT systems of hospitals, healthcare centers, medical equipment suppliers, and private clinics, among other organizations in the sector.

This trend continued during the second half of 2022. During the six months of analysis covered in this document, several types of cyberattacks and actors involved have been identified.

08

RANSOMWARE

On the one hand, ransomware remains one of the most severe and high-risk threats to the healthcare sector. Its consequences have resulted in the paralysis of services, operation cancellation, and disconnection of medical monitoring and management devices.

During the second half of the year, operators of various ransomware groups have targeted medical centers and suppliers of medical equipment, most notably the Karakurt attack in July against a hospital group in the United States and the attack by the operators of the Sparta ransomware in September against a company specializing in providing radiofrequency technology for medical use.

In addition, between September and December, several hospitals in France were affected by ransomware attacks of varying severity, impacting hospitals and medical service providers.

The involvement of Daixin and Royal ransomware groups is highlighted for their alleged participation in cyberattacks against healthcare organizations, mainly in the United States.

DATA BREACHES

During the second half of the year, data breaches in the healthcare sector have continued their trend, mainly upwards.

Such data breaches happened due to some of the cyberattacks that previously occurred and where cybercriminals could obtain data for sale or malicious use in phishing campaigns.

Given the distribution of different cyberattacks globally against the healthcare sector by cybercriminal groups of different specializations and APT groups, it is likely that during the next six months, the trend of related cyber incidents will remain constant and may increase against companies in the supply chain.

Furthermore, further exploitation of vulnerabilities by threat actors, such as APTs, cannot be ruled out and could impact the sector.

APT GROUPS

On the other hand, threats from APT groups have attracted the attention of national and international government agencies for their alleged involvement in cyberattacks against hospital centers and companies providing services to such centers.

In this case, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), as well as the U.S. Healthcare Cybersecurity Coordination Center, warned about the different actions being carried out by APT groups in conjunction with Ransomware groups, having an impact on the healthcare sector.

Through communications from these agencies, as well as the analyzed activity of APT groups, several groups of interest have been detected:

- North Korean APT groups, which can steal information in the healthcare field and obtain data.
- APT41, for its activity against diagnostic systems and hospital centers in different countries.
- Mustang Panda, APT10, and Winnti, for their use of specialized malware developed by these groups to target healthcare entities and research centers.

09

In terms of cyberattacks, the industrial production sector was the most targeted by ransomware groups during the second half of 2022, with an increase of 34% compared to the first half of the year.

INDUSTRIAL SECTOR

During the second half of 2022, industrial control systems (ICS) and operational technology (OT), responsible for monitoring and controlling the devices and processes of physical operating systems, have presented different vulnerabilities that allowed cybercriminals to take control of them or access them to obtain sensitive information from the companies.

Some of the most relevant events during this period have been:

01 The vulnerability known as AttachMe, a cloud isolation vulnerability in Oracle Cloud Infrastructure (OCI) that allowed attackers to perform various destructive acts such as obtaining and leaking sensitive data or changing code and escalating privileges.

02 The vulnerability known as CVE-2022-38465 in the Siemens Simatic programmable logic controller (PLC), which allowed attackers to retrieve encrypted global private cryptographic keys and take control of the devices.

03 Critical vulnerabilities in Advantech's R-SeeNet: The vulnerabilities identified as CVE-2022-3386 and CVE-2022-3385 allowed attackers to remotely delete files on the system or execute code on affected versions. These vulnerabilities affected critical infrastructure sectors such as critical manufacturing, energy, water, and wastewater systems worldwide.

04 F5 vulnerabilities in BIG-IQ and BIG-IP products: In November, F5 Networks published a post about two vulnerabilities affecting several of its products, such as BIG-IP and BIG-IQ network devices, which could lead to remote code execution.

05 In December, a tool known as Simantic-Smackdown was posted, which allowed the operations of SIMATIC S7 programmable logic controllers (PLCs) to be interrupted by sending a signal that shut down the PLC's central processing unit (CPU).

10 HACKTIVISM

Over the past few years, there has been a reduction in hacktivist-type attacks targeting businesses, as actors focused their activity against government entities or even individuals.

However, the second half of 2022 has seen an increase in hacktivist actions around the world targeting businesses, such as hacktivist actors involved in the war in Ukraine, but also groups in other geographic locations whose actions have had a major impact.

Hacktivism refers to an individual or a group abusing a network or a web application to promote a social or political cause. Group attacks are generally based on carrying out denial-of-service attacks, defacement attacks, or data breaches.

GUACAMAYA

Guacamaya is a hacktivist group that has been active since at least March 2022 and whose members have conducted cyber operations based primarily on data breaches.

Their original name, or by which they became known in their first leak, is Guacamaya Roja, a characteristic bird of Central America. The motivation for their attacks points to an ideology marked by anti-capitalist environmentalist concepts.

According to the group, the reasons for their attacks range from injustice in general, criminal offenses against the population and the territory, the system, and multinationals, considering that the struggle of a region is the defense of life, the human species, and living beings that inhabit the planet.

According to the group's observed attacks, its targets are located in North America (Mexico), Central America (Guatemala, El Salvador), and South America (Venezuela, Colombia, Brazil, Chile, Peru, and Ecuador).

GHOSTSEC

Ghostsec is a hacktivist group that has been active since 2015 and was formed to conduct hacktivist attacks against terrorist organizations, carrying out doxing attacks (posting personal information) of Daesh, Boko Haram, or Al-Qaeda affiliates.

Although the group began with these objectives, it has changed its political agenda in recent years. It has become critical of the governments of Israel and Iran, countries at which it has directed most of its activity in the last six months.

In September, the group announced that it had compromised 55 Berghof programmable logic controllers (PLCs) used by Israeli organizations as part of a hacktivist campaign called #FreePalestine.

Following the death of Mahsa Amini and the ensuing protests, Ghostsec members have carried out multiple attacks against the Islamic country, even claiming to have gained access to industrial and governmental systems.

The group has also supported other hacktivist causes, such as #OpNicaragua and #OPRussia, against the Nicaraguan government and in support of Ukraine.

11 APTs

Such attacks are carried out by state or nationally-sponsored actors with the purpose of state or nationally sponsored actors for the purpose of espionage or sabotage against organisations organisations that pose a (strategic or political) competition against the interests of the sponsor.

KOREAN APTs

In the second half of 2022, there has been a high activity of advanced persistent threat groups of Korean origin, especially cyberattacks by North Korean APT groups targeting South Korea, most notably Lazarus, Kimsuky, and APT37 groups.

LAZARUS GROUP

Lazarus Group, also known as Guardians of Peace or Whois Team, is undoubtedly the most active APT group of North Korean origin in the second half of 2022. It is an advanced persistent threat group funded by North Korean military intelligence with numerous subgroups, such as AndAriel and BlueNorOff.

In the latter half of 2022, Lazarus has been observed exploiting a Log4j vulnerability in VMWare Horizont to gain an initial foothold in targeted organizations, many of which were in the energy sector in the United States, Canada, and Japan.

The successful exploitation of this vulnerability allows the deployment of custom malware by the threat group, such as the VSingle backdoor, the YamaBot malware, or MagicRAT, a previously unknown malware implant.

Also during this period, Microsoft has reported that Lazarus was using legitimate open-source software (PuTTY, KiTTY, TightVNC, Sumatra PDF Reader, and the muPDF/Subliminal Recording software installer) to address its targets via the BLINDINGCAN backdoor, also known as ZetaNIle, in social engineering attacks targeting engineers and technical support professionals working in IT and media organizations in the UK, India and the US.

Lazarus subgroups have also been active in the last six months of 2022. A new ransomware called Maui, attributed to the Lazarus subgroup AndAriel, was discovered in mid-August. This subgroup, active since at least 2015, would have used this ransomware since April 2021 to target cyberattacks on South Korean companies in the construction, manufacturing, and media sectors and network service provider companies

This is not the only ransomware detected in this period affecting South Korea. A new ransomware called GwisinLocker, used by threat actors to encrypt Linux ESXi and Windows servers of only South Korean companies, was detected in August 2022. It has yet to be assigned to any known APT group, although everything points to it being a tool made by an advanced persistent threat group of North Korean origin.

On the other hand, in December 2022, a phishing campaign targeting startup employees attributed to the BlueNorOff subgroup of Lazarus was detected, for which they would have created more than 70 fake domains imitating well-known banks and venture capital firms of Japanese, Vietnamese and American origin.

KIMSUKY

Kimsuky, also known as Thallium, Black Banshee, or Velvet Chollima, is an advanced persistent threat group of North Korean origin that has been active since at least 2012.

During this period, the phishing campaign known as GoldDragon, which took place in early 2022, has been attributed to this APT group, targeting cyberattacks on political and diplomatic entities located in South Korea to implement a Windows backdoor for information theft (lists of files, user keystrokes, and stored web browser login credentials).

Moreover, the group has been observed using three different strains of Android malware called FastFire, FastViewer, and FastSpy. The FastFire malware masquerades as a Google security plug-in, FastViewer hides as Hancom Office Viewer, and FastSpy is a remote access tool based on AndroSpy.

Finally, a spear-phishing campaign has been detected targeting more than 900 South Korean Western foreign affairs experts to obtain information about possible Western policy movements toward North Korea. The e-mails included a link to a fake website and an attachment that triggered malware downloads.

APT37

APT37, also known as Scarcruft or Reaper, is a North Korean state-sponsored APT group that has been active since at least 2012. Since then, the group has targeted cyberattacks on South Korea and countries located in the Middle East.

In October 2022, this advanced persistent threat group deployed a phishing campaign to target users located in South Korea using malicious files that exploited a zero-day vulnerability in Internet Explorer's JavaScript interpreter named CVE-2022-41128.

They used as filename "221031 Seoul Yongsan Itaewon accident response situation (06:00).docx", alluding to the Seoul Halloween stampede. Microsoft patched the vulnerability in November 2022.

Also, in November 2022, a campaign was detected in which APT37 used a backdoor called Dolphin to compromise the systems of users in South Korea to carry out cyber espionage.

RUSSIAN ATPs

While the Russian-Ukrainian conflict has been one of the factors responsible for the increased activity of APT groups of Russian origin during the second half of 2022, this is not the only motivation of the groups that have directed cyberattacks during this period. Of particular note is the activity of APT28, APT29, TA505, Sandworm, FIN7, and UAC-0142 groups.

APT28

Researchers from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) discovered in late 2022 that the advanced persistent threat group APT28, of Russian origin, was infiltrating the systems of a U.S. company providing satellite communications.

Many of the affected entity's customers are companies in the U.S. critical infrastructure sector, which could be related to the group's motivations.
The infiltration, which went unnoticed for several months in 2022, may have resulted in the exfiltration of sensitive data.

FIN7

In November 2022, the Russian-origin advanced persistent threat group FIN7 was linked to the Black Basta ransomware, one of the most widely used ransomware in 2022. In addition, it has been noted that this group has been exploiting Microsoft Exchange vulnerabilities to create a platform called Checkmarks.

This attack system scans Microsoft Exchange vulnerabilities to discover vulnerabilities within the networks of its potential victims that can be exploited to gain access to their systems.

APT29

APT29 added in mid-2022 to its arsenal of tactics the use of cloud storage services such as Google Drive or DropBox to deploy malware on the compromised systems of its targets.

Also, in November 2022, a spear-phishing attack carried out by this advanced persistent threat group against an unknown European diplomatic entity was detected.

To do so, they exploited a Windows feature called Credential Roaming.
Credential Roaming is a mechanism that allows users to securely access their credentials (private or certificates) on different workstations in a Windows domain.

In addition, a new malware used by this APT group called MagicWeb, an evolution of the FoggyWeb malware, has been observed during this time, affecting Microsoft's authentication software called Active Directory Federation Services (ACFS).

Its mechanism consists of replacing a legitimate DLL used by ADFS with a malicious version to manipulate user authentication certificates and modify the claims passed in the tokens generated by the compromised server.

TA505

Two botnets associated with the TA505 group, also known as Evil Corp, have been identified in this period. These botnets implement malware such as the FlawedGrace Trojan, Cobalt Strike, or Clop ransomware and have impacted entities worldwide, particularly those in the United States, Mexico, Pakistan, and Brazil.

New tactics have also been associated with the group, such as using the Raspberry Robin malware, exploiting the vulnerability known as CVE-2022-31199 affecting the Netwrix Auditor software, and using the TeslaGun software control panel used to implement a backdoor called ServHelper.

SANDWORM

This APT group, also known as Iridium, has directed most of its cyberattacks to Ukraine during this period.

This half-year period has seen the group exploited the CVE-2022-30190, which affects the Microsoft Windows Support Diagnostic Tool (MSDT) to target cyberattacks on Ukraine.

They have also targeted organizations in the country using ransomware-type cyberattacks, such as the new ransomware called RansomBoggs, whose ransom note refers to the Pixar movie Monsters, Inc (2001).

UAC-0142

This APT group directed a cyberattack in December 2022 on the Ukrainian Ministry of Defense's Center for Innovation and Development of Defense Technologies.

The attack involved sending a spear phishing email using a compromised email address of a member of the country's Ministry of Defense urging the recipient to update the certificates of the DELTA system, a military software used by the Ukrainian government.

Attached to the e-mail were a PDF document and a malicious ZIP file hosted on a fake Delta domain that included two files named FateGrab and StealDeal, which collect and exfiltrate data from compromised systems.

CHINESE APTs

APT groups sponsored by China or with Chinese origin have positioned themselves in the last six months as one of the most active groups globally, to carry out cyberespionage and intrusion campaigns. Their actions have been focused on strategic sectors such as financial, industrial, telecommunications, defense, manufacturing, and government. The Chinese APT cyberattacks could have serious consequences. In this regard, activity during the last six months of 2022 has focused on three APT groups: APT41 and Mirror Face.

APT41

This group maintains significant operability and adds new subgroups to its team of operators, such as Earth Longhzhi, Earth Baku, Grayfly, and Blackfly.

Although no new active APT41 campaigns have been identified, they likely maintain their operations with previous campaigns and through subgroups.

MIRRORFACE

This APT launched a spear phishing campaign targeting political entities and personalities as part of Operation LiberalFace.

Among the targets of the campaign was the election body of the Japanese House of Councillors.

Using proprietary tools such as MirrorStealer creates a higher risk scenario for possible information theft and intrusion campaigns with cyber espionage objectives.

12 TELECOM

During the year's second half, many cyberattacks against telecommunications companies have been observed, as well as a large number of customer data leaks of large telecommunications companies in European Union member countries such as Spain and Portugal.

Earlier in September, user PoCExploiter, Admin (owner) of the Telegram channel of the threat group known as KelvinSecurity, reported that he had and offered for sale 309 GB of data from a phone company in Italy containing around 295,969 files.

Among the information, the user offered as a sample, identity documents, subscription proposals, and telephone contracts were found.

In September, Samsung issued a statement indicating that in late July 2022, an unauthorized third party obtained information from several of the company's U.S. systems.

In the same statement, they indicated that the attacker did not obtain information about Social Security numbers or debit and credit card information. Still, he could have accessed other sensitive information such as name, demographic and contact information, date of birth, or product registration information.

This is the second incident related to data breaches that the company has suffered in recent months, following the breach last March.

During the first week of November, a Spanish telecommunications company reported that one of its suppliers had been the victim of a cyberattack through which the threat actor could have gained access to customers' data such as name, surname, postal address, ID card number, IBAN code of current account, etc.

Large Australian telecommunications companies were victims of cyberattacks during September and October.

In September, the data of +10,000 customers of Optus, a company that is a subsidiary of Singtel (Singapore Telecomm Ltd), was leaked by the actor known as optusdata for a short period on the Deep Web forum Breachforums.

Subsequently, in September, Dialog, an IT services consulting company based in Australia and a subsidiary of Singtel, was the victim of a cyberattack in which cybercriminals obtained information from various customers and employees of the company and then posted it on the Deep Web in October.

Lastly, Telstra, one of Australia's largest Telcoms companies, disclosed a data breach through one of its third-party vendors.

The company made a statement informing that the data that had been leaked dated back to 2017 and included the first names, last names, and e-mail addresses of employees who had signed up for an employee rewards program that was now obsolete.

There is no evidence that the incidents are related to each other, as the actor behind the Optus leak removed the content and apologized to affected users.

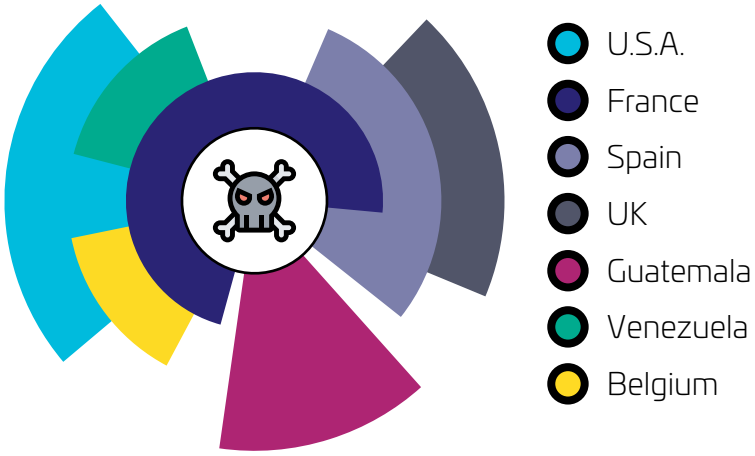
INSURANCE SECTOR

Overall, the number of cyber threats impacting the insurance industry has increased in the second half of 2022.

>> 13

From July through December 2022, the insurance industry has been primarily affected by an increase in ransomware-type cyberattacks, targeting especially companies in the United States, followed by France, Spain, and the UK.

Ransomware attacks affecting the insurance sector by country



Insurance industry affected by ransomware group

The ransomware group that affected this sector the most in the second half of 2022 was LockBit, followed by Royal and BlackBasta.

The most commonly sold accesses to entities in this sector are RDP, VPN or Citrix vulnerability exploits.

The cybersecurity event within the insurance industry that most marked the year 2022 was the ransomware-type cyberattack suffered by one of Australia's largest private health insurance providers. Thus, in October 2022, the entity suffered a ransomware attack perpetrated by the REvil threat group, resulting in the post of 5G of files that included the personal data of about 9 million customers.

The cyber incident has marked a before and after in the history of cybersecurity law. As a result of the attack, the Australian government has passed a bill called the Privacy Legislation Amendment Bill 2022, which increases the financial penalty for all those companies that suffer data breaches.

This bill is being considered by other countries around the world, which are studying whether to adopt a similar measure to increase the cybersecurity of entities and whose purpose is to significantly by companies, as they are forced to invest in cybersecurity.

The Spanish Data Protection Agency and the Central Technological Investigation Brigade of the National Police dealt with the matter.

RELEVANT ATTACKS

IN THE SECOND HALF OF THE YEAR

14

S21SEC
Cyber Solutions by Thales

From the Cyber Threat Intelligence department of S21sec, we present a summary of the most talked-about attacks in the second half of 2022.

The most commonly used attacks range from data breaches, distributed denial of service (DDoS) attacks and ransomware, the latter being the most widely used by cyber attackers.

DATA BREACHES

DATE	SECTOR	THREAT ACTOR
JULY 2022	Hospitality	Group with No Name (GNN)
DECEMBER 2022	Financial	APT group of unknown Chinese origin

DDoS

DATE	SECTOR	THREAT ACTOR
OCTOBER 2022	Transport	KillNet
OCTOBER 2022	Government	KillNet
NOVEMBER 2022	Government	KillNet
NOVEMBER 2022	Religious	Hacktivist group of unknown Russian origin

RANSOMWARE

DATE	SECTOR	THREAT ACTOR
JULY 2022	Telecommunications	LockBit
JULY 2022	Construction	BlackBasta
JULY 2022	Research	Vice Society
JULY 2022	Technology	LockBit
AUGUST 2022	Manufacturing	LV
AUGUST 2022	Government	Play
AUGUST 2022	Oil & Gas	ALPHV Black Cat
AUGUST 2022	Government	Conti
SEPTEMBER 2022	Manufacturing	RansomHouse
SEPTEMBER 2022	Transport	Ragnas Locker
OCTOBER 2022	Insurers	REvil
OCTOBER 2022	Energy	Hive
NOVEMBER 2022	Retail	BlackBasta
NOVEMBER 2022	Transport	Daixin Team Group
NOVEMBER 2022	Healthcare	WannaCry
DECEMBER 2022	Technology	LockBit


S21
SEC
Cyber Solutions by Thales
www.s21sec.com