# THREAT LANDSCAPE REPORT

S21sec's Threat Intelligence department offers a half-yearly report of the second semester of 2021 explaining the existing threats that can put the security of companies and individuals at risk, informing the reader of the most relevant threats that exist today, such as vulnerabilities, malware, APTs, etc., and that can pose a risk in the medium and short term.

S21SEC

Second semester 2021

The second half of 2021 has been characterized by several high-profile events such as the discovery and exploitation by malicious actors of several vulnerabilities that have been a major headache for IT departments in organizations.

These high-impact vulnerabilities are Printnightmare, Log4j, CVE-2021-40444, and those known as ProxyShell.

This semester has seen an increase in the use of infostealers to obtain personal information, access credentials, or banking data.

Among the most active infostealers, according to S21sec telemetry, Agent Tesla, Vidar and Redline stand out.

The second half of 2021 has also seen a significant increase in attacks on educational institutions and critical infrastructures.

S21SEC

# INDEX


01. Vulnerabilities

02. Ransomware

03. Banking Malware

04. Android Malware

05. SIM swapping

06. Healthcare Sector

07. Educational Sector

08. Critical Infrastructure

09. TELCOM & IT

10. APTs

11. Data Breach

12. Conclusions


Threat Landscape Report

Second semester 2021

# VULNERABILITIES

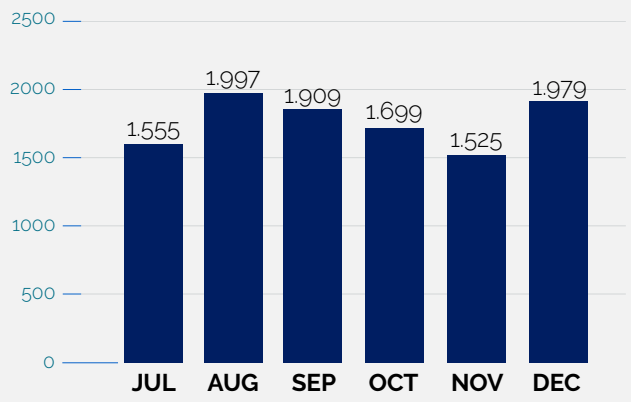
*Vulnerabilities are the conditions and characteristics of an organisation's systems that make it susceptible to threats.*

## CRITICALITY LEVEL

During the first semester of 2020, 10.641 vulnerabilities have been published. Below is an overview of these vulnerabilities.

### Published vulnerabilities

During the second half of 2021




### Severity level

Based on CVSS version 3

- **Critical:** 1.447
- **High:** 4.442
- **Medium:** 4.549
- **Low:** 226
- **None:** 0

During the last half of 2021, several high criticality vulnerabilities that have been actively exploited by cybercriminals to carry out different types of attacks were published.

It is worth noting that, in the vast majority of attacks that have taken place throughout 2021, one of the main entry vectors observed has been the exploitation of existing vulnerabilities in the target infrastructure.

This is why it is important for companies to consider these types of threats and to focus on maintaining and updating their infrastructures.

## PRINTNIGHTMARE

On June 8, Microsoft published CVE-2021-1675, which was a remote code execution vulnerability in Windows Print Spooler, and, in July, published the vulnerability CVE-2021-34527 (named Printnightmare).

This vulnerability exploited the print queue to execute remote code and gain system permissions.

This threat has three key features: it is capable of remote code execution, privilege escalation, and a local attack vector.

Specifically, it can execute code hosted on another machine (remote code execution) with system permissions (privilege escalation), but it is necessary to have access to the machine (local attack vector) to exploit it, as it is needed to run the spoolsv.exe program (print queue).

PrintNightmare exploits the fact that any authenticated unprivileged user can call RpcAddPrinterDriverEx () and specify a driver/dll with arbitrary code, which will be executed with system privileges.

This driver/dll can reside either on the machine itself or on a remote server. This results in the spoolsv.exe print queue service running code in an arbitrary DLL file with system privileges.

## CVE-2021-40444

On September 7, a new vulnerability (CVE2021-40444) was found affecting Office tools where the attacker is able to execute arbitrary code hosted on a remote machine.

CVE-2021-40444 was found in the MSHTML rendering engine of the Internet Explorer browser, which is used by Microsoft Office documents.

MSHTML performs basic browser operability functions, namely filtering and rendering of web documents, HTML, and cascading style sheets among other things.

It also allows integration with other Microsoft Windows applications by exposing an active document API. It is implemented via mshtml.dll.

To exploit the vulnerability, an attacker could create a malicious ActiveX control to embed it in a Microsoft Office document that hosts the browser rendering engine and convince the victim to open the malicious document.

ActiveX is a framework used to define reusable software components independently of the programming language used by Office, such as Internet Explorer, but not Edge.

# APACHE LOG4J

In early December, a critical vulnerability known as Log4Shell or LogJam remote code execution was disclosed in the Apache component log4j, a logging library written in Java.

The critical vulnerability tracked as CVE-2021-44228 in Apache Log4j allows a remote actor to send a crafted HTTP packet to Apache servers running software before Log4j 2.15.0.

The vulnerable software will store the HTTP request as a legitimate log, which then executes the payload embedded in that log.

Successful exploitation of the vulnerability would allow an attacker to initiate LDAP traffic to an attacker-controlled node from the Java Naming and Directory Interface (JNDI).

The attacker-controlled node would respond with a malicious Java class file that would then begin running on the targeted server.

On December 14, a second vulnerability tracked as CVE-2021-45046, involving Apache Log4j, was published.

This is due to the fix to address this vulnerability, which was incomplete in certain non-default configurations, recommending upgrading to the latest version of Log4j 2.16.0 to avoid attacker-controlled JNDI lookups.

The vulnerability affects all versions from 2.0-beta9 to 2.12.1 and 2.13.0 to 2.15.0.

On December 16, a third vulnerability emerged in Apache Log4j 2, CVE-2021-45105, a denial-of-service (DoS) vulnerability in a JavaScript WebSocket to trigger remote code execution (RCE) in internal and locally exposed unpatched Log4j 2 applications.

On December 18, Apache Foundation released additional Log4j 2.17.0 updates on December 18, 2021, replacing the vulnerable 2.16.0 and 2.12.3 to fix the security flaw.

Since Log4j is an open-source Java logging library used worldwide in a wide variety of enterprise Java applications and software services, within days of its release, numerous threat groups (APT35, Hafnium, and Conti), as well as individual actors, exploited this vulnerability.

The targets of these actors were varied, ranging from the installation of crypto miners to different types of malware.

## PROXYSHELL

During this semester, malicious actors have explored and exploited several vulnerabilities in Microsoft Exchange. These vulnerabilities are called ProxyShell and allow an actor to bypass authentication and execute code as a user with privileges.

ProxyShell comprises three separate vulnerabilities used as part of a single attack chain:

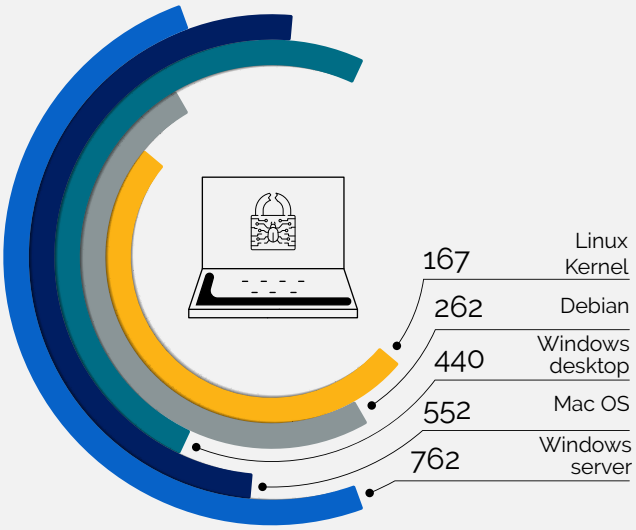
CVE-2021-34473: Remote code execution vulnerability with a CVSSv3 score of 9.1.

CVE-2021-34523: Elevation of privilege vulnerability in the Exchange PowerShell backend

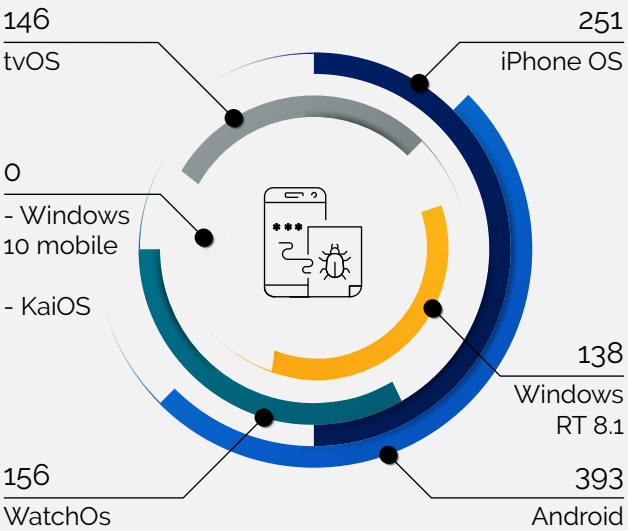
CVE-2021-31207: Remote code execution after authentication via arbitrary file writes.

It should be noted that ProxyShell vulnerabilities have been used to deploy malware, such as the LockFile ransomware.

## VULNERABILITIES IN DESKTOP AND SERVER OPERATING SYSTEMS




## VULNERABILITIES SO SMART DEVICES



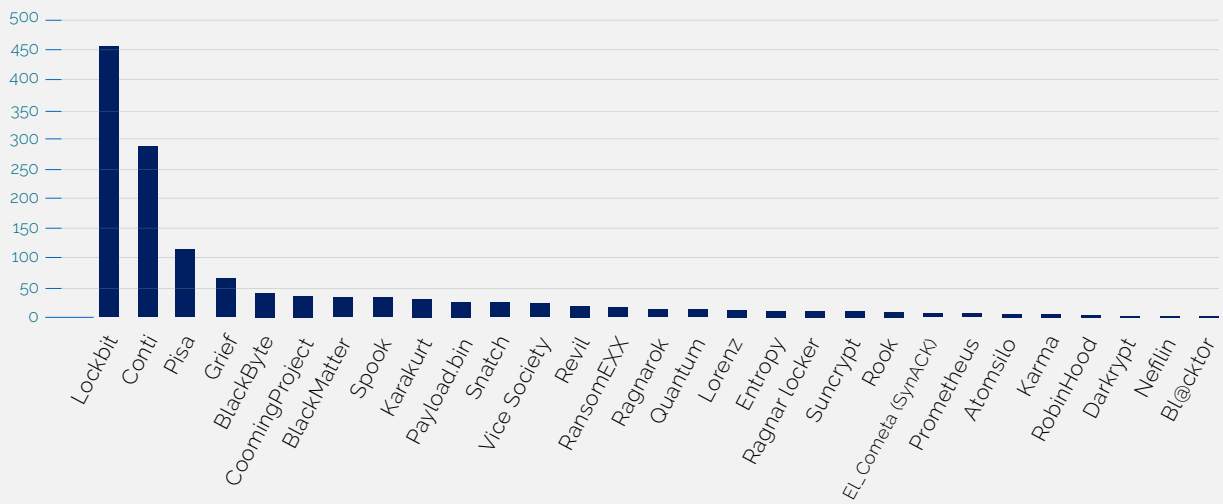
# RANSOMWARE

*In the last few years, ransomware has become one of the most common types of malware used by financially motivated malicious actors.*

## RANSOMWARE STATISTICS

In the second half of 2021, the Threat Intelligence team at S21sec tracked a total of 1,694 ransomware victims being threatened on TOR websites managed by the operators of various ransomware.

### Ransomware families relevant in the second half of 2021



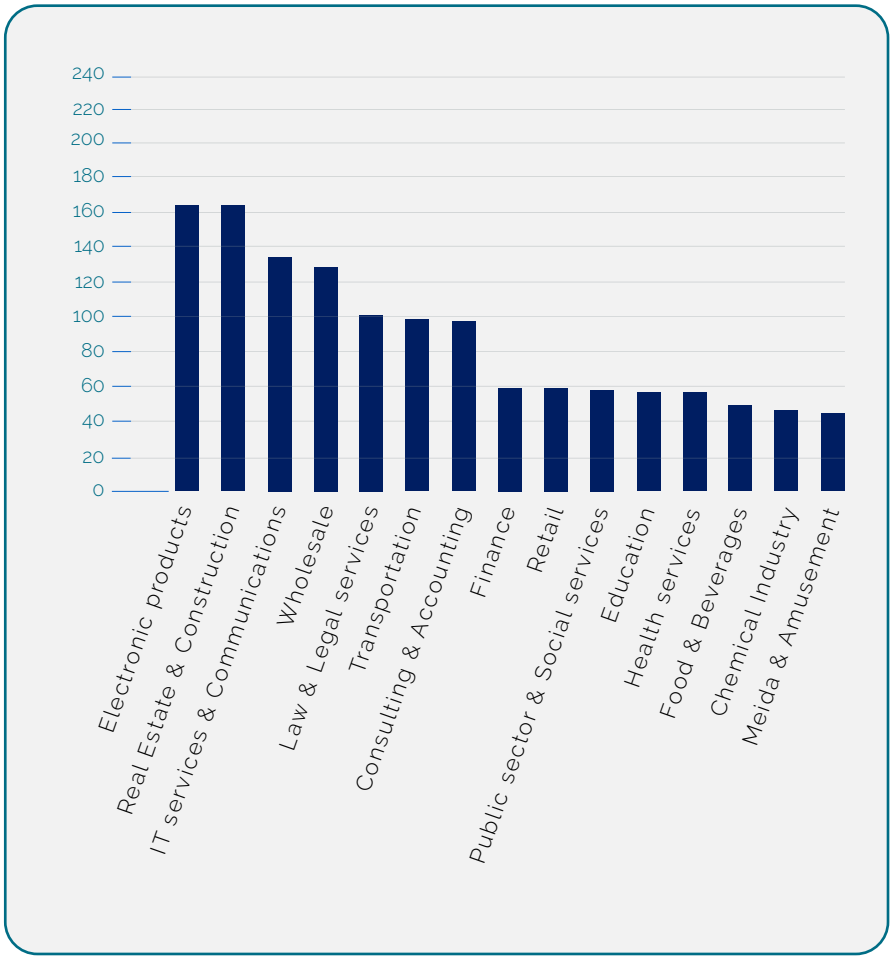

As it has been common for the last two years, most ransomware operates under a so-called ransom-as-a-service (RaaS) scheme, where a core group of developers (operators) sells or rent seats to gain access to control panels and tools.

These positions are mostly limited and are generally filled by users (called affiliates) who have previously shown the operators that they have enough technical knowledge to achieve a successful attack.

## RANSOMWARE IMPACT BY SECTORS

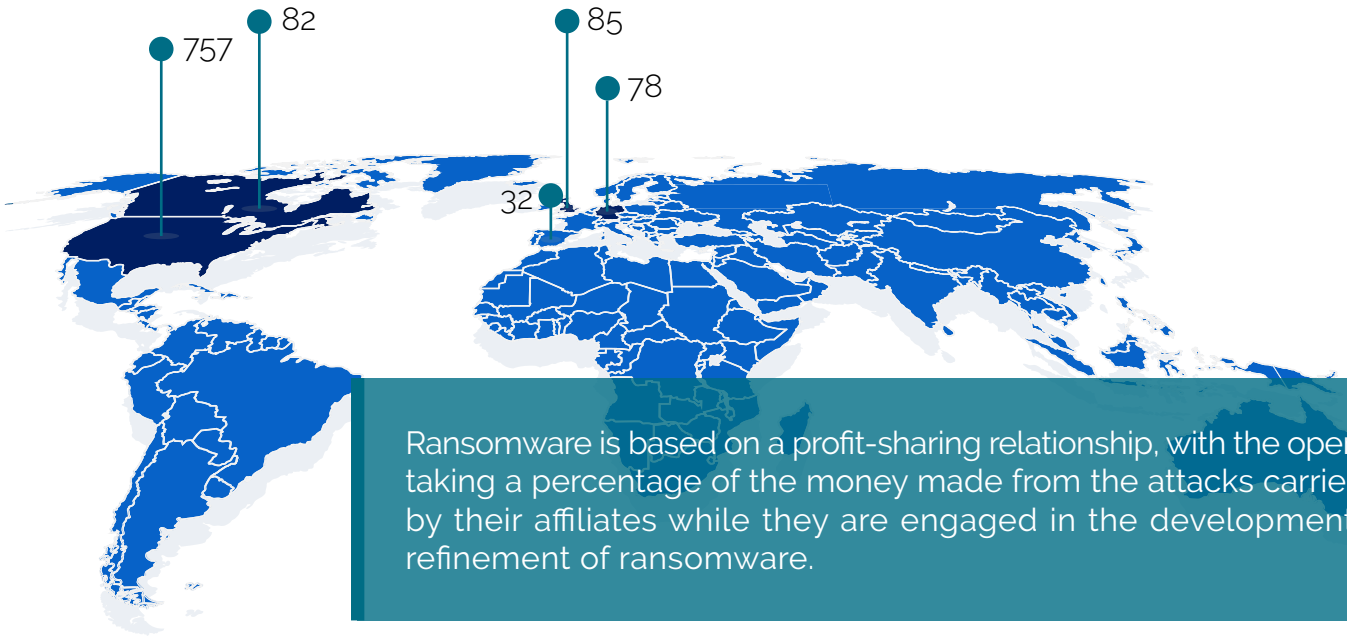
From most to least affected, the main sectors that have suffered ransomware attacks are:

- Electronic products
- Real Estate & Construction
- IT services & Communications
- Wholesale
- Law & Legal Services
- Transportation
- Consulting & Accounting
- Finance
- Retail
- Public sector  & Social Services
- Education
- Health services
- Food and beverages
- Chemical industry
- Media & Amusement




## RANSOMWARE IMPACT BY COUNTRIES

The attackers have mostly targeted targets located in the United States, followed by the United Kingdom, Canada and Germany, with Spain in seventh place.

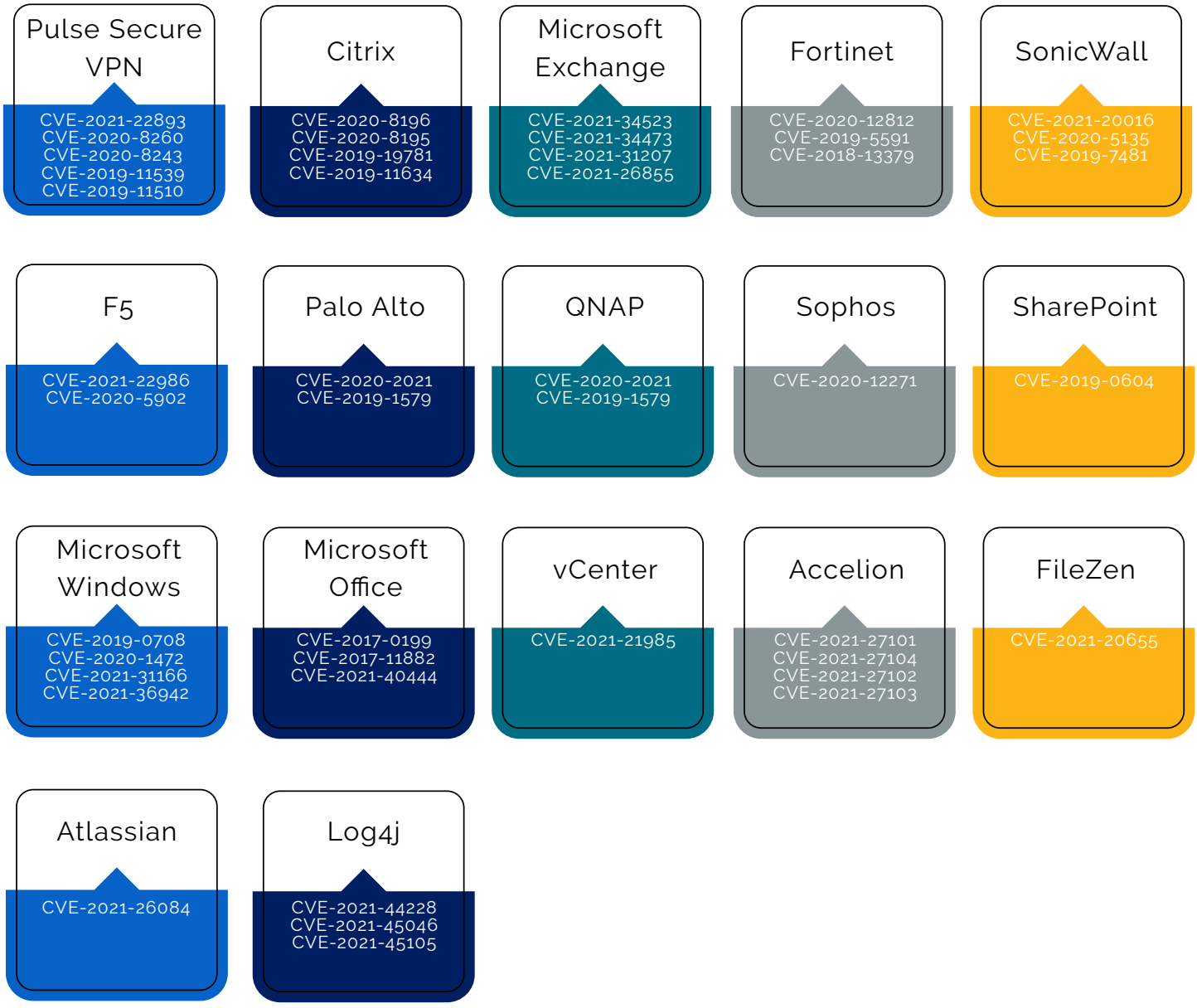



Ransomware is based on a profit-sharing relationship, with the operators taking a percentage of the money made from the attacks carried out by their affiliates while they are engaged in the development and refinement of ransomware.

## USED CVEs

Ransomware uses e-mail (through messages with malicious attachments) and the exploitation of vulnerabilities as its main entry vectors.

It has been observed in recent years that the following vulnerabilities are the most commonly used by the actors behind ransomware.




Another trend that has remained stable in terms of ransomware this year has been the double extortion technique: first, they encrypt computers, rendering them unusable and even affecting the productivity of the companies, and then they threaten to publish the files obtained during the attack.

## SUNCRYPT

SunCrypt is a ransomware that targets organizations and users worldwide.

The ransomware operators act on a double extortion model: in addition to encrypting your files, they threaten to disclose the sensitive information obtained if the victims do not contact them within a period of less than 72 hours.

In addition, they promise to provide a security analysis showing the security weaknesses used for the attack.

The ransomware uses network vulnerabilities to gain access to corporate servers and lock files stored on them.

After encryption, the ransomware displays a ransom note named "YOUR_FILES_ARE_ENCRYPTED.HTML", available in several languages such as English, French, German, or Japanese, suggesting interest from operators in North America, Europe or Japan.

## PYSA

The ransomware currently known as PYSA, whose acronym comes from the term "Protect Your System Amigo", is a variant of the Mespinoza ransomware, which appeared in October 2019 and is attributed with several attacks that led to the infection of large corporations' networks.

According to the French CERT, evidence of the existence of this ransomware has been found since 2018, also linking it to the attack on institutions in the same country.

It is worth noting that, in March 2021, the FBI also issued a statement reporting increased PYSA activity against educational organizations in the United States, and the United Kingdom.

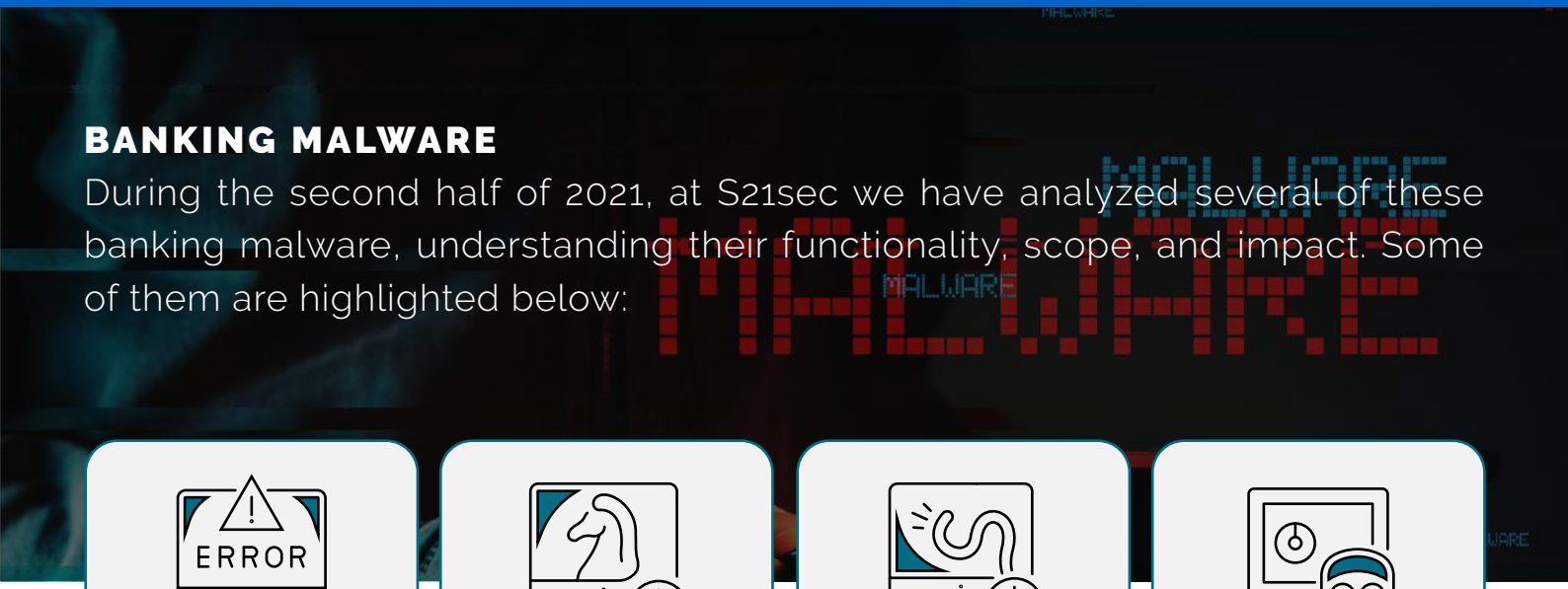
The cybercriminal group behind this ransomware has focused its attacks since March 2020 on educational institutions, K-12 schools, seminaries, government entities around the world, the healthcare sector and private companies.

Currently, the countries most targeted by PYSA are the United States, United Kingdom, Brazil, Spain, and Canada.

In addition, the last few months have seen an increase in what would be considered triple extortion: some ransomware have included DDoS attacks among their features and threaten their victims with DDoS attacks for several days until they pay the ransom.

# BANKIG MALWARE

*Banking malware remains one of the most relevant cybersecurity threats during the second half of 2021, having a high impact on its victims.*



## BANKING MALWARE

During the second half of 2021, at S21sec we have analyzed several of these banking malware, understanding their functionality, scope, and impact. Some of them are highlighted below:




**SQUIRREL WAFFLE**



**NUMANDO**



**GUILDMA**



**INFOSTEALERS**

Due to the increase in attacks and the consequent acquisition of data and access to infected computers, S21sec has increasingly identified the sale of this data and access to computers and networks by cybercriminals in markets in the Deep and Dark Web, mainly in Genesis Market, Russian Market, and 2easy Market, among others.

These sales are made for various prices and may include access to infected machines, credentials, and sensitive data.

## SQUIRREL WAFFLE

In September, a campaign to distribute the SquirrleWaffle banking malware via email was detected, where the use of other malicious programs such as Cobalt Strike could be observed.

The SquirrleWaffle distribution is carried out via e-mail malspam campaigns using existing e-mail threads and probably stolen "subjects".

The working model of this campaign is similar to that observed in similar campaigns: in the first phase, the e-mail includes a URL that redirects to a web page that downloads a ZIP file, which contains a malicious office document, mostly in Word and Excel formats.

Once the ZIP file is downloaded, the embedded macros of the documents are enabled and, after the execution of these documents, a second phase of the malware is downloaded.

In the second phase, during installation, the malware downloads the final payload containing Cobalt Strike, although matches with the Qakbot/Qbot malware have also been identified.

Once the system is infected, the malware would have the ability to collect information from the affected system, load malware configuration, and enable infections to deploy additional malware, such as Qakbot and Cobalt Strike.

## NUMANDO

The Numando malware is positioned as one of the most used banking trojans, having a relevant impact in Latin American countries and Spain.

Although its activity dates back to 2018, updates in its TTPs have been less dynamic than those of other malware of the same family, such as Mekotio.

In the latest campaigns observed in 2021, new operating techniques have been identified.

The main attack vector of the campaign is based on sending malspam e-mails. In these e-mails, a ZIP file with an MSI installer (where the malware is hidden or downloaded) is attached with a CAB file containing a legitimate application, an injector, and a DLL encrypted with the Numando Trojan.

When the MSI is run, the legitimate application is executed in parallel, and the injector is sideloaded.

After this execution process, Numando can perform backdoor functions, such as simulating mouse and keyboard actions, rebooting and shutting down the machine, displaying overlay windows, and taking screenshots.

Among the new techniques employed is the use of an unwritten injector in Delphi language and the use of public platforms to store its remote configuration in applications such as YouTube or Pastebin.

# INFOSTEALERS

Information-stealing malware (known as infostealer) also posed a significant threat to users and banks during the second half of 2021.

As in the first half of 2021, infostealers continue to maintain their activity on the rise, with several targeted campaigns being detected to obtain banking credentials.

The use of infostealers to obtain personal information, login credentials, or banking data continues to be used by malicious actors, who are continuously developing and improving the capabilities of this type of malware.

Among the infostealers detected in S21sec, Agent Tesla, Vidar and Redline stand out. Through monitoring and detection tasks it has been observed that the activity of these infostealers is focused on the infection of computers and networks to obtain sensitive information, credentials, and data from the target.

Some of these infostealers are often distributed together with other malware or ransomware, such as Vidar, which is distributed together with several ransomware families.

Vidar is considered to be one of the most used infostealers during 2021 and had an increase during the last half of 2021 due to its increased buying and selling in Deep Web marketplaces.

In the case of Agent Tesla, it is one of the infostealers that has been distributed among users for the longest time.

However, it continues to grow in prevalence as Agent Tesla variants emerge with improved capabilities, using phishing as its main attack vector.

On the other hand, Redline infostealer is considered a recent malware whose distribution was detected in 2020 but has only noticed a remarkable growth in the last half of 2021.

Its distribution is done through social engineering, including phishing campaigns, attaching files in different formats to proceed with the execution of malicious programs.

It is also positioned as one of the 10 emerging threats in the infostealer category.

One of the characteristics of the identified infostealers is the ease with which they are bought or sold in Deep and Dark Web forums.

Their use has spread due to their low purchase or sale prices, increasing the number of attacks with this malware.

## GUILDMA

At the beginning of the second half of 2021, S21sec detected a new Guildma banking trojan campaign that distributed malware among its targets, mostly financial institutions in Latin America, Portugal, and Spain.

In this case, in July 2021, a new distribution campaign of this malware was identified against financial institutions in Latin American countries, Portugal and Spain.

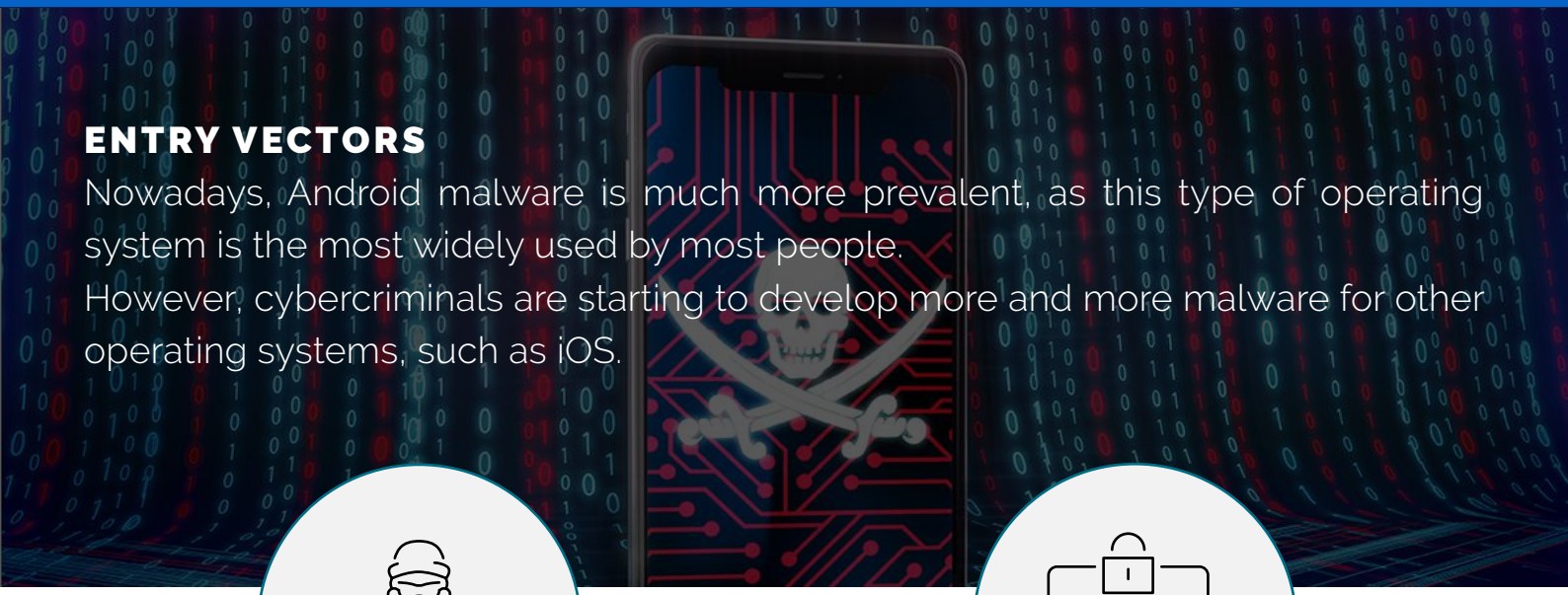
In this campaign, the banking trojan spread through emails where a malicious URL is attached, which contains a ZIP file with a fake executable and from where the attack is launched.

Although Guildma's activity dates back to 2017, banking Trojans often develop new attack techniques to keep their assaults active.

In the case of Guildma, the ZIP file to which the user is directed contains an additional ZIP file with a Windows shortcut from where the CMD command is executed and a Windows start menu shortcut is created to keep the infection persistent.

# ANDROID MALWARE

*Cybercriminals have added smartphones and tablets to their list of top targets, leading to an increase in threats, specifically targeting these types of devices.*



## ENTRY VECTORS

Nowadays, Android malware is much more prevalent, as this type of operating system is the most widely used by most people.

However, cybercriminals are starting to develop more and more malware for other operating systems, such as iOS.

### SOCIAL ENGINEERING

Cybercriminals use messages (SMS) with a link that redirects to a malicious URL from which an application that looks legitimate but is actually malware is downloaded.

### DOWNLOADING APPLICATIONS

The user downloads an app that is considered legitimate but is trojanized.

Such apps are available from official app stores (Google Play, Apple Store) or unofficial marketplaces and developers' websites.

## PEGASUS

Another mobile malware called Pegasus, which also affects iOS devices, has also had a major impact this semester.

It is a commercial malware with spyware functionalities attributed to the Israeli group NSO.

Pegasus operators could, by installing different modules, read or get hold of their victim's text messages, read e-mails, listen to and record audio or calls by secretly activating microphones, record keystrokes, access browser history, learn about contacts in the address book, etc.

## SOVA

In mid-September 2021, several media outlets reported the existence of a new Android Trojan called SOVA (Russian for owl).

The analyzed samples of this Trojan by the S21sec Threat Intelligence team were samples that spoofed security updates of widespread applications, such as Adobe Flash Player.

After the victim downloads the application, the malware asks the user to grant it a series of permissions that will allow it to perform different actions in the future, for example, the BIND_ACCESSIBILITY_PERMISSION accessibility services.

It is through the use of these services that SOVA performs its overlay attack.

## OSCORP

Oscorp is an Android malware from the banking trojan family that emerged in early 2021 with campaigns mainly targeting Italy.

This malware has banking trojan, keylogger, RAT and infostealer functionalities.

Oscorp has a service for requesting access to accessibility services.

If it gains access to these services, it will be able to grant itself a series of other permissions that will guarantee, for example, persistence on the device.

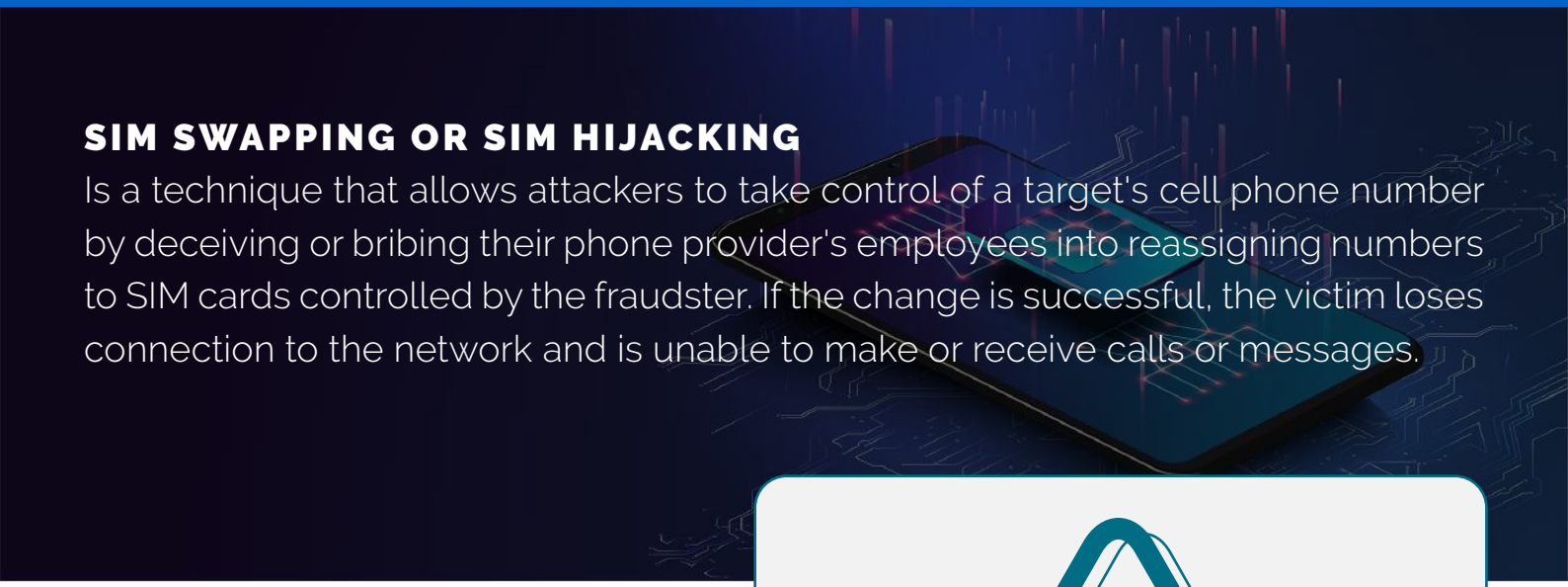
As a banking Trojan, it has overlay attack techniques. Oscorp has a service that is responsible of detecting the foreground application on the device at any given time.

For Android versions lower than Android 5.0, it uses the system activity manager to obtain the package name of the running activity and, from Android 5.0 onwards, it uses the device usage statistics to access the same information.

Once it has detected the application of interest (generally banking apps), the trojan's overlay attack begins, consisting of loading the contents of a phishing kit, which will mimic the appearance of the legitimate application in a WebView view superimposed on the legitimate application.

# SIM SWAPPING

*During the last few months of 2021, there has been an increase in the number of phone attacks by changing the SIM cards of mobile devices.*



**SIM SWAPPING OR SIM HIJACKING**

Is a technique that allows attackers to take control of a target's cell phone number by deceiving or bribing their phone provider's employees into reassigning numbers to SIM cards controlled by the fraudster. If the change is successful, the victim loses connection to the network and is unable to make or receive calls or messages.

This type of attack targets the user's banking transactions particularly, but not exclusively.

It also seeks to gain access to cryptocurrency wallets, social networks, messaging applications, and email accounts.

For an attacker to successfully carry out the scam, he must first obtain data from his victim.

## MODUS OPERANDI IDENTIFIED IN SIM SWAPPING

Throughout 2021, a substantial increase has been observed in the number of complaints made by users. They report unauthorized banking transactions or sudden loss of control of their telephone number.

Some people have pointed out the type of scam or robbery to their bank accounts, explaining that, after receiving unsolicited codes on their cell phones, they suffer the extraction of all or most of the money from their bank accounts.

The modus operandi identified in SIM swapping has three phases:

### THEFT OF USER CREDENTIALS THROUGH SOCIAL ENGINEERING TECHNIQUES

Fake or duplicate web pages, phishing emails, malware installation through applications, or by impersonating a banking institution's app.

Information is also obtained through OSINT or footprinting techniques, or by exploiting illegally obtained data breaches.

### ONCE THE INFORMATION IS COLLECTED, THE ATTACKER ATTEMPTS TO CLONE THE VICTIM'S SIM CARD TO RECEIVE HIS SINGLE-USE-PASSWORDS (2FA CODES) AND TAKE CONTROL OF THE TELEPHONE NETWORK

The scammer physically presents himself or contacts the telecom company to duplicate the card.

Once the change is made, the user loses the signal on his mobile device, a situation that can be interpreted as an intermittency of the device and not a break-in.

### ONCE THE 2FA CODES ARE CONFIRMED, THEY REACH THE DUPLICATE SIM, THUS GAINING CONTROL OF THE PHONE NETWORK

The next lateral movement is the theft of email accounts, identity theft or, if necessary, the withdrawal of money in the victim's name.

# HEALTHCARE SECTOR

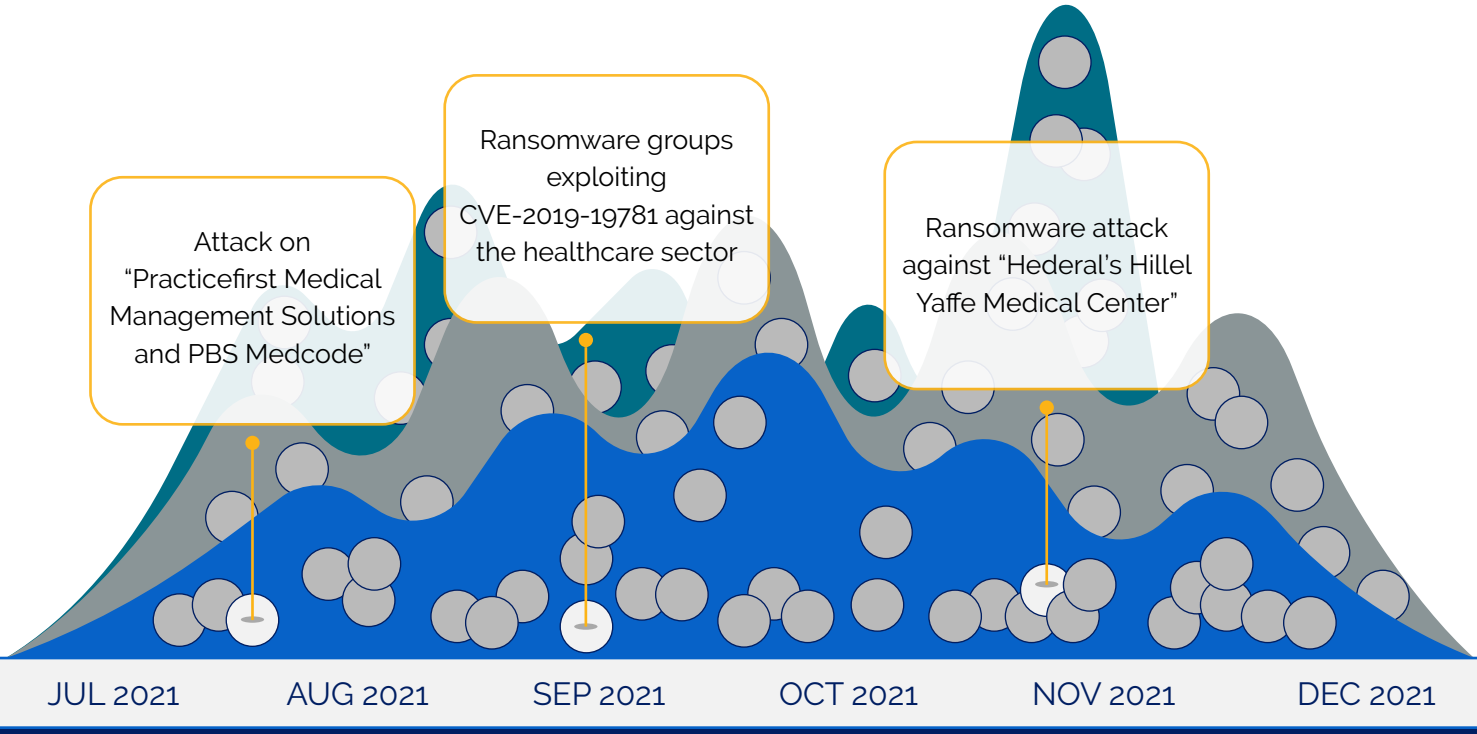
*The computer networks of the health sector have been affected in the second half of 2021 by various ransomware cyberattacks and the distribution of other types of malware.*

## SARS-CoV-2 (COVID-19)

The trend in cyber-attacks against the healthcare sector remains on the rise following the SARS-CoV-2 pandemic declaration (COVID-19).

According to the information monitored and collected in the second half of 2021, the healthcare sector has suffered more than 60 ransomware attacks, which include hospitals, private clinics, health centers, and laboratories.

When analyzing all cyberattacks suffered by the healthcare sector in the last half of 2021, this figure increases significantly, being able to distinguish between computer attacks of various types (trojans, security breaches, infostealers, spyware, ransomware).

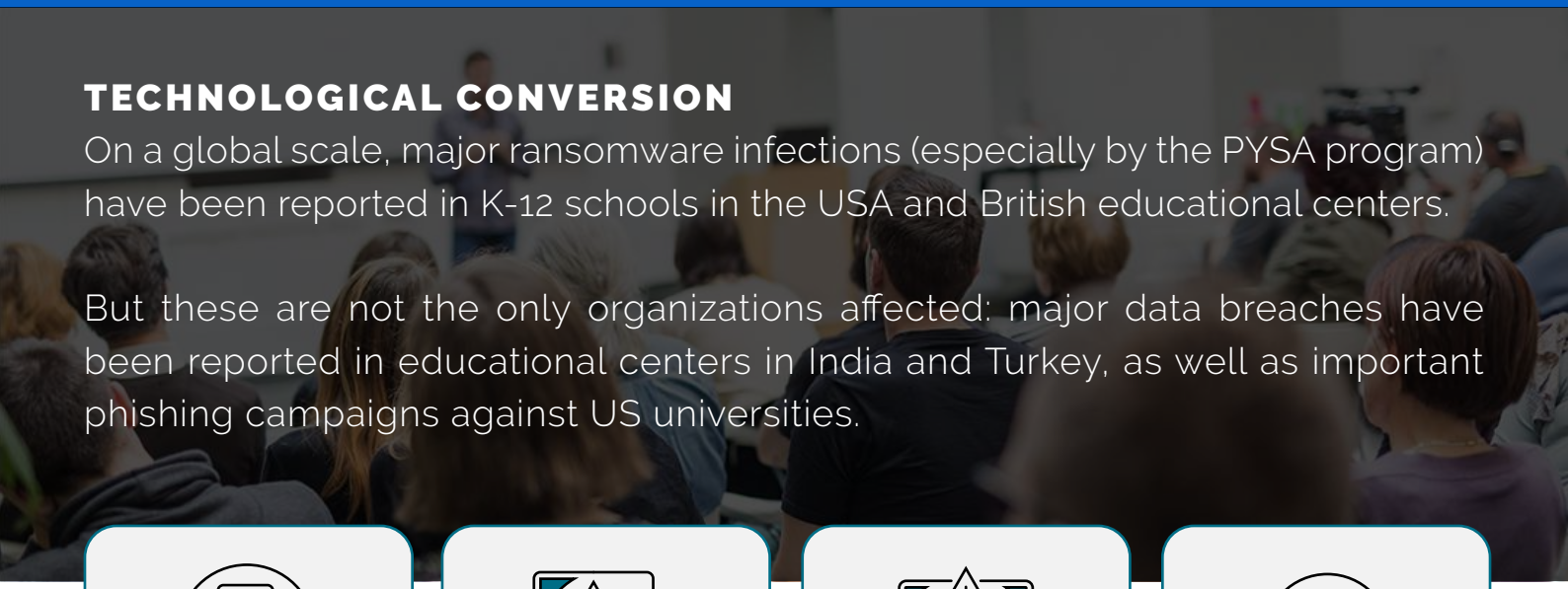


# HIGHLIGHTS OF CYBERATTACKS ON THE HEALTH SECTOR DURING THE SECOND HALF OF 2021

- During this period, there have been more than 300 security incidents in the healthcare sector at international level.
- High peaks are observed in the months of July, September, October, and early December.
- Several cyberattacks had a considerable impact on the healthcare sector, particularly on hospitals and their laboratories, such as the attack on the Macquarie Health Corporation (MHC) and various medical centers in Israel.
- These types of attacks often have long-term consequences
- Following the ransomware attack on the Irish Health Service Executive that took place in May 2021, Irish hospitals have not yet returned to full normal operation in the second half of 2021
- In December, Coombe Hospital in Dublin suffered a new cyberattack and the HSE has warned another Dublin hospital about a potential cyberattack in the near future.
- The healthcare sector has also suffered during the second half of 2021 an increase in security incidents involving personal or corporate information and data theft.
- Healthcare organizations such as public or private hospitals worldwide have reported data breaches, such as the healthcare system of Lazio (Italy), which suffered disruptions to its regional health portal and vaccination network, putting at risk personal and clinical data of Italian citizens (records, addresses, telephone numbers, and emails).

# EDUCATIONAL SECTOR

*It is estimated that the educational sector has been one of the most affected during the last six months in terms of cyberattacks.*



## TECHNOLOGICAL CONVERSION

On a global scale, major ransomware infections (especially by the PYSA program) have been reported in K-12 schools in the USA and British educational centers.

But these are not the only organizations affected: major data breaches have been reported in educational centers in India and Turkey, as well as important phishing campaigns against US universities.


**MALSPAM & SPEARPHISHING CAMPAIGNS**

**DDoS ATTACKS**


**DATA BREACHES**

**MALWARE & RANSOMWARE INFECTIONS**

Throughout the second half of 2021, malicious actors have taken advantage of this rapid sector reconversion to exploit existing vulnerabilities in organizations and deploy a wide range of attacks.

In recent months, it has become clear how the sector is facing a number of general risks that jeopardize the cybersecurity of organizations.

## THESE TYPE OF ORGANIZATIONS FACE A SERIES OF CONDITIONS THAT MAKE THEM VULNERABLE TO ATTACK BY MAILICIOUS ACTORS

Use of vulnerable technologies, such as the Zoom videoconferencing platform, which is widely used for online teaching.

Outdated systems and with weak defense systems.

User communities with a low level of cybersecurity awareness, making organizations a target for attacks such as data breaches or phishing campaigns.

It is estimated that the educational sector has been one of the most affected during the last six months in terms of cyberattacks.

On a global scale, major ransomware infections (especially by the PYSA program) have been reported in K-12 schools in the USA and British educational centers.

But these are not the only organizations affected: major data breaches have been reported in educational centers in India and Turkey, as well as important phishing campaigns against US universities.

## SOME OF THE MAJOR ATTACKS IN THE LAST SIX MONTHS HAVE BEEN:

**Cyberattack on the Autonomous University of Barcelona**

**Cyberattack on the University of Lisbon**

**Computer attack on the Pontifical Xavierian University**

## CYBERATTACK ON THE AUTONOMOUS UNIVERSITY OF BARCELONA

Last October, the UAB publicly reported having been the victim of a ransomware attack, attributed to the PYSA encryption program, which would have caused the encryption of files and confidential information, impacting more than 650,000 files.

Although the entry vector of the attack is unknown at the moment, the institution took measures to contain the attack including the disconnection of campus networks, as well as blocking access to its platforms.

The institution also set up a complete Microsoft online environment in order to be able to continue its activity and is working to fully reestablish it.

Although no information has been leaked so far, the authorities do not rule out the possibility that internal data or that of members of the educational community may be published on PYSA's Deep Web blog.

## CYBERATTACK ON THE UNIVERSITY OF LISBON

At the end of October, the University of Lisbon was the victim of a cyberattack against the institution's Windows servers.

According to public media, the incident occurred after a ransomware infection of the university systems, which were suspended as a preventive measure.

Although the university has made public that no personal or financial information of the academic community was compromised and that it was limited to the collection of access credentials of e-mail accounts, up to six colleges were involved in the incident, and access to their e-mail servers was suspended.

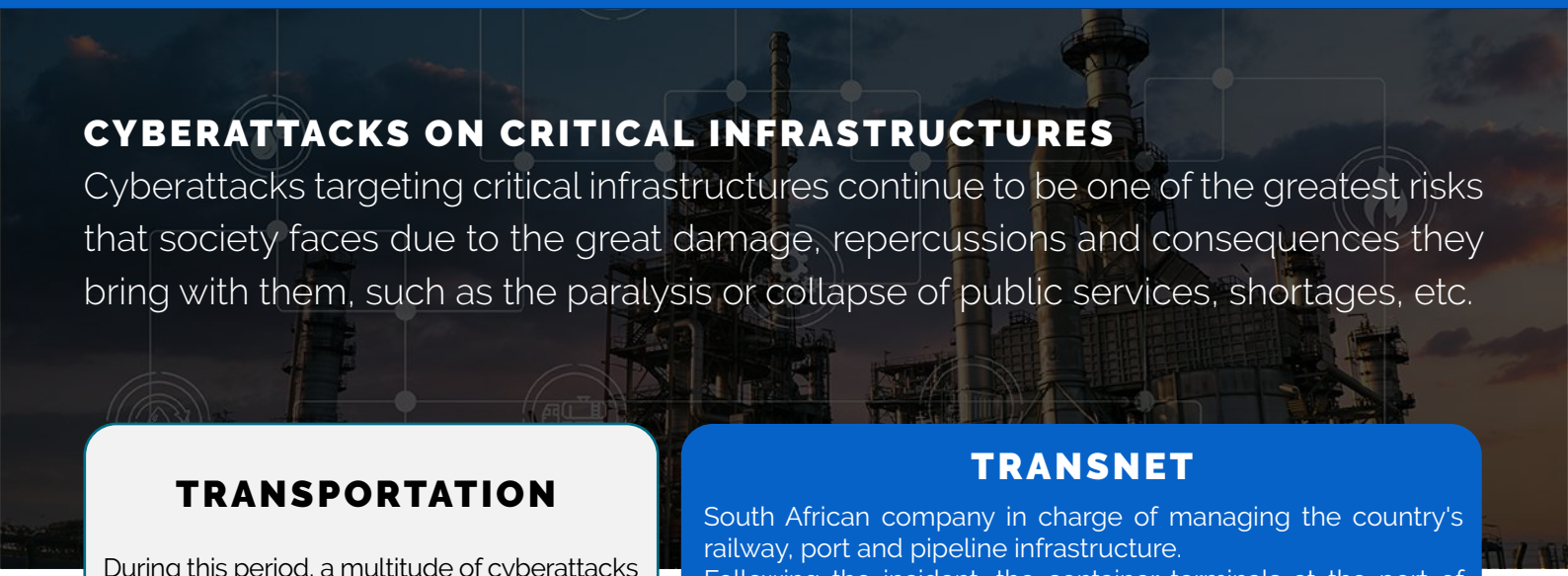
## COMPUTER ATTACK ON THE PONTIFICAL XAVIERIAN UNIVERSITY

Last November, the Xavierian University made public the news of a computer attack against its systems that would have forced the organization to disable some of its technological services to protect the operation.

Although the origin or nature of the incident is unknown, the center urged the community to refrain from using the infrastructures or computer network to avoid the spread of the attack.

# CRITICAL INFRAESTRUCTURES

*During the second half of 2021, there have been numerous attacks targeting critical infrastructures in different countries, involving means of transport, entities related to wind energy, oil supply companies, gas stations, etc.*



## CYBERATTACKS ON CRITICAL INFRASTRUCTURES

Cyberattacks targeting critical infrastructures continue to be one of the greatest risks that society faces due to the great damage, repercussions and consequences they bring with them, such as the paralysis or collapse of public services, shortages, etc.

### TRANSPORTATION

During this period, a multitude of cyberattacks have been detected against large transport companies that form an integral part of a country's critical infrastructure: Iran's railway network together with the Ministry of Transport, airlines such as Mahan Air, Toronto's public transport system, etc., although two incidents stand out due to the magnitude and the number of people affected.

### TRANSNET

South African company in charge of managing the country's railway, port and pipeline infrastructure.
Following the incident, the container terminals at the port of Cape Town stopped functioning and the registration of container movements had to be carried out manually. In addition, the port of Durban was also affected by the cyberattack, which resulted in greatly increased logistics congestion, impacting the country's economy.

### DEV-0343 THREAT GROUP

According to information released by the Microsoft Threat Intelligence Center (MSTIC), was responsible for spreading the passwords of more than 250 customers using Office 365.

Some of those customers were U.S. and Israeli defense technology companies, Persian Gulf gateways or global shipping companies with a commercial presence in the Middle East.

## "CONTI" RANSOMWARE

During these last 6 months, the "Conti" ransomware has been used in different cyberattacks targeting a multitude of companies or entities belonging to the critical infrastructure sector (electricity, oil, etc.).

In most of the successful attacks using this ransomware, the cybercriminals obtained confidential and personal information of the companies' employees and different samples were published by the Conti group on its Deep Web site "Conti News" for later sale.

Some of the companies affected by the "Conti" ransomware during this period were: a Kansas oil and gas exploration and production company, an Italian natural gas and electricity operator, a Chinese photovoltaic company and an electricity supplier in Australia.

## LOCKBIT & LOCKBIT 2.0 RANSOMWARE

In the second half of 2021, both Lockbit and Lockbit 2.0 ransomware were used in different cyberattacks related to critical infrastructure.

Major cyberattacks using the Lockbit ransomware include those suffered by the first wind energy operator in Italy, a natural gas service provider operating in Indonesia, a wind turbine manufacturer or the airline Bangkok Airways.

In most attacks, they obtained confidential company or customer information and put it up for sale on their Dark Web site.

Following this and with the 2.0 version of the malware, a German wind farm operator, a French multinational company offering digital energy and automation solutions, and a renewable energy group based in India were all affected.

# IT SECTOR AND TELECOM

*The telecommunications sector has been one of the main sectors targeted by cyberattacks during the second half of 2021. During this period, several campaigns were uncovered against companies in this sector in Europe, the United States and Asia, with special mention of the REvil group.*

## CYBERATTACKS INCREASE OVER THE YEARS

Since the incident at a nuclear power plant in Iran, caused by the Stutnex malware, occurred in 2010, these types of attacks have become more and more common.

Since the beginning of 2019, this sector has suffered an increase in cyberattacks, carried out by all kinds of actors: from those seeking financial gain, to those who want to steal confidential information, APTs, etc.

**KASEYA**


**REVIL**

**GODADDY**


**CIBERESPIONAJE CHINO**

**MALKAMAK**

The telecommunications sector has also been one of the most affected sectors during the coronavirus outbreak, from the shared hoaxes in social networks over 5G networks to phishings in which telephone companies are supplanted to offer "free gigs for the coronavirus".

## KASEYA

In early July, the multinational software and IT services company Kaseya was the victim of a ransomware cyberattack.

The initial attack vector was a zero-day vulnerability (CVE-2021-30116) in Kaseya VSA, which allowed attackers to remotely execute commands on the VSA device.

This solution is commonly used by these service providers to manage their customers' systems.

The number of companies affected by the attack is unknown, and it is estimated that the total number of companies affected is between 800 and 1,500 distributed around the world, most of them being suppliers and small or medium-sized businesses.

The REvil group proclaimed its authorship through its official blog, demanding 70 million dollars to publish the tool that will allow the decryption of the information breached.

In mid-July, Kaseya obtained a universal decryption key for the ransomware attack from an unknown "trusted third party" and began distributing it to affected customers.

## REVIL

One of Spain's most consolidated telecom operators announced in early July that it had suffered a ransomware cyberattack.

The REvil group published on its official blog that it had compromised the company, having accessed and downloaded its data bases and confidential information.

Several images of the stolen files were published in order to prove the attack.

After the attack, no ransom demand was issued by the criminals, nor was it reported by the company, and the existence of the ransom demand is unknown.

The telephone provider reported that several servers were affected by the attack, although its importance was low: "no information was lost."

## GODADDY

The GoDaddy hosting platform suffered an intrusion, through the use of a compromised password, to the WordPress hosting environment in early September.

The breach was detected in mid November and security and mitigation measures were implemented.

The company reported that more than 1.2 million customers were affected by the incident, with data such as email addresses, passwords, names, private SSL keys and customer numbers having been leaked.

The hosting company suffered further cyberattacks in March and May 2020, with more than 28,000 customer accounts affected.

## CHINESE CYBERESPIONAGE

In September, a cyber espionage campaign against companies in the telecom sector in Southeast Asia was detected by ATPs related to the Chinese government.

This possible involvement is carried out using techniques, tactics and procedures employed, and its objectives are aligned with the interests of the Chinese government.

The actors are known to have exploited vulnerabilities in Microsoft Exchange servers, gaining access to sensitive communications carried out on the affected telecom services.

Some of the targets include political and governmental corporations, law enforcement agencies and dissident organizations for the Chinese state.

## MALKAMAK

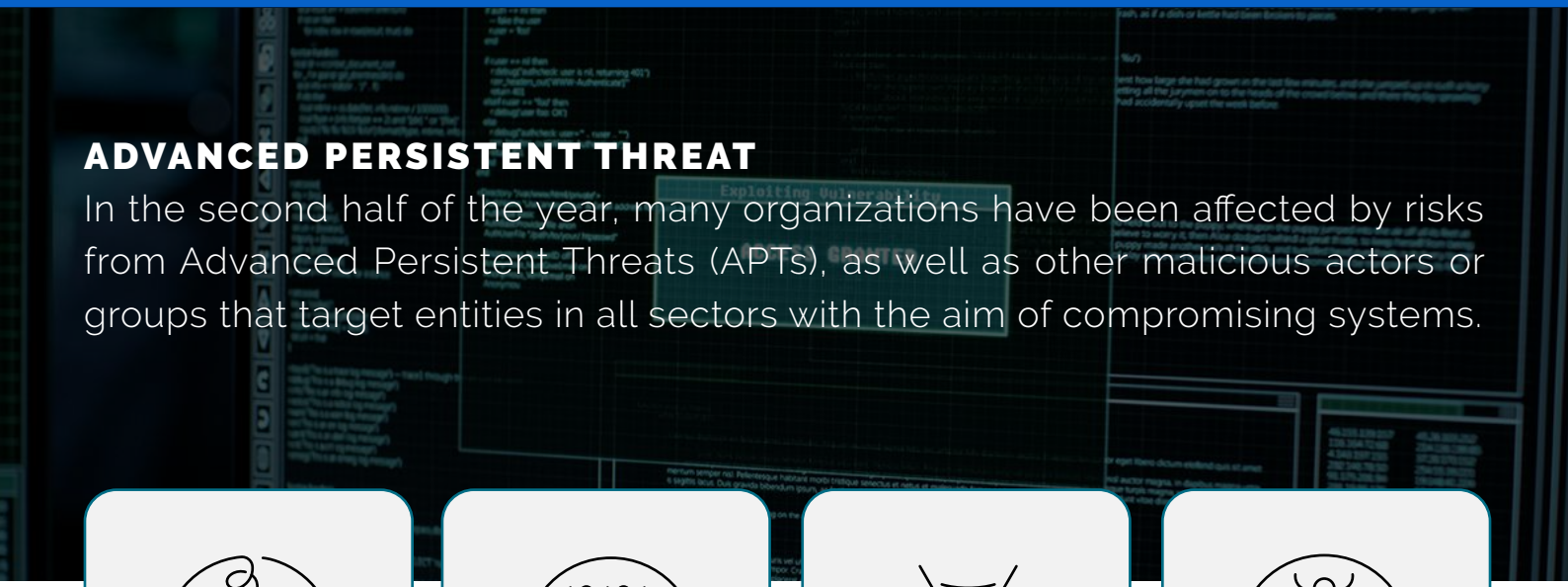
In October, a new threat actor called MalKamak was discovered related to a cyber espionage operation targeting telecommunications and aerospace companies since 2018.

MalKamak operates through a remote access trojan called ShellClient, capable of evading security devices to gain command and control.

The main targets of this group are focused on the Middle East, the United States, Russia and Europe. Various connections with Iranian APTs such as Chafer APT or Agrius APT have been detailed.

# APT

*New threat actors such as groups or APTs have appeared, as well as the return of the Emotet botnet, which have managed to evolve in terms of tactics, techniques and procedures.*



## ADVANCED PERSISTENT THREAT

In the second half of the year, many organizations have been affected by risks from Advanced Persistent Threats (APTs), as well as other malicious actors or groups that target entities in all sectors with the aim of compromising systems.

**NOBELIUM**


**CHAMELGANG**

**EMOTET**


**TRICKBOT**

The term APT or "Advanced Persistent Threats" refers to a highly sophisticated cyberattack, as well as to state-sponsored groups that carry out these malicious campaigns.

During the last few years, several security incidents related to the action of these APTs have been observed, which have made it possible to contemplate the global scope of the campaigns carried out by these actors.

## NOBELIUM

The Russia-linked threat group, known for the supply chain attack against SolarWinds, has shown activity during the second semester.

In October, Microsoft observed a campaign targeting more than 600 customers, leveraging a diverse range of techniques such as token theft, API exploitation or spear-phishing to divert credentials associated with privileged service provider accounts, enabling lateral movement in cloud environments.

During December, attacks continued to target several French organizations.

Furthermore, according to security researchers, the group made use of a new malware variant, codenamed "CEELOADER" and incorporated into its arsenal with the ultimate goal of breaching government and corporate networks globally.

Finally, new suspicious server infrastructure, likely associated with the group, has been identified and is known as SOLARDEFLECTION.

The infrastructure is in its operational phase and is likely already in use or will soon start to be used for operations.

## CHAMELGANG

A new cybercriminal group not associated with any existing threat actor has been exploiting vulnerabilities known as ProxyShell in Microsoft Exchange Server and using new malware to compromise networks in attacks targeting Russian energy and aviation companies.

The group hides its network infrastructure and malware under the legitimate services of companies such as Microsoft, TrendMicro, McAfee, IBM and Google using legitimate lookalike domains and by using SSL certificates that mimic well-known companies.

According to the reported attacks, one of them targeted the network of an energy company through the supply chain by compromising a vulnerable version of a subsidiary company's web application, as well as compromising networks in other countries such as the United States, Japan, Turkey, Taiwan, Vietnam, India, Afghanistan, Lithuania and Nepal, including government servers as targets.

## EMOTET

It has been one of the most relevant threats in this period.

In mid-November, there was evidence of the return of Emotet, a botnet that had been dismantled earlier in the year, but has been reactivated by malicious actors, showing spreading activity via the Trickbot malware.

In addition, it was observed that Emotet is currently dropping a Cobalt Strike beacon, which would make it easier for ransomware to take action.

## TRICKBOT

The Trickbot modular banking Trojan is another of the most relevant threats in the current cybercriminal landscape.

According to S21sec data, Trickbot has attacked 194 countries. 36.67% of Trickbot attacks are on machines on US soil, followed by Germany with 8.25% and Italy with 6.85%.

Spain is the twelfth country with the highest number of endpoints attacked by Trickbot, with 1.06%; Portugal is 52nd with 0.07% of all attacks.

# DATA BRECH

*The second half of 2021 was marked by high-profile incidents involving vendor software that led to widespread data security breaches and malware attacks.*

## DATA BREACH

Organizations across multiple sectors (finance, government, education, telecom, healthcare, energy, technology and manufacturing) have suffered data breaches as a result of the compromise of systems by threat actors.

**LINKEDIN** | **ZURICH SPAIN** | **FORTINET** | **EPIK**

**ACER** | **ACCENTURE** | **TELEFÓNICA**

The results of this type of cybersecurity incident include reputational and financial damage for the affected company, as well as phishing attacks, ransomware or identity theft in the case of victims affected by the compromised personal information.

## LINKEDIN

"TomLiner," an actor on the RaidForums forum, posted for sale in late June an alleged data dump relating to 700 million users of LinkedIn's professional network users.

The data included names, gender, e-mails, phone numbers and industry information.

LinkedIn issued an official statement on its website providing information about the investigation regarding the incident, stating that it was data that had been extracted from LinkedIn and other websites that included the same data that had been previously reported.

## ZURICH SPAIN

In August, the Spanish division of Zurich Seguros was victim of the theft of its customers' databases, following a cyberattack that took place between August 12 and 13, in which information was extracted and put up for sale on an underground hacking forum.

A total of 4,260,757 registration lines of the threat actor, a database relating to private vehicle policies, with data ranging from ID number, address, telephone number, e-mail, and even license plates or the model of the vehicles.

The stolen information was offered for sale on the Internet for $1000 in bitcoins.

## FORTINET

A financially motivated threat actor nicknamed Groove, active since August 2021, leaked approximately 500,000 compromised Fortinet VPN credentials in September.

The credentials were likely collected by exploiting a restricted directory-type vulnerability (CVE-2018-13379) in Fortinet FortiOS running on Fortigate devices.

The leaked credentials could allow threat actors to compromise organizations' networks with compromised VPN devices and perform malicious activities such as deploying ransomware or stealing sensitive data.

Among the countries affected globally by this breach are Portugal, Mexico and Spain.

## EPIK

The US company Epik, specialized in domain registration and web hosting, was the victim of a security incident claimed by the hacktivist group Anonymous as part of an operation known as "#OperationJane" or "Operation Epik Fail" announced in September.

Anonymous leaked 180 GB of data and the hacktivist group "Distributed Denial of Secrets" stated that they had obtained a copy of the stolen database, which was published through their digital channels.

Shortly after, the second part of the data was leaked, a total of 300 GB of information in which, according to them, at least 59 API keys and login credentials of Epik's systems and its official accounts on Twitter, Coinbase and PayPal were exposed.

## ACCENTURE

In mid-October, Accenture disclosed a data breach following the LockBit 2.0 ransomware attack that occurred in August 2021.

Cyble reported that the ransomware gang stole databases containing more than 6 TB of data and demanded a ransom of $50 million.

## ACER

October was marked by a data breach posted on a publicly accessible cybercriminal forum.

A group called "Disorder" claimed to have stolen 60 GB of databases and other files from breached Acer India servers.

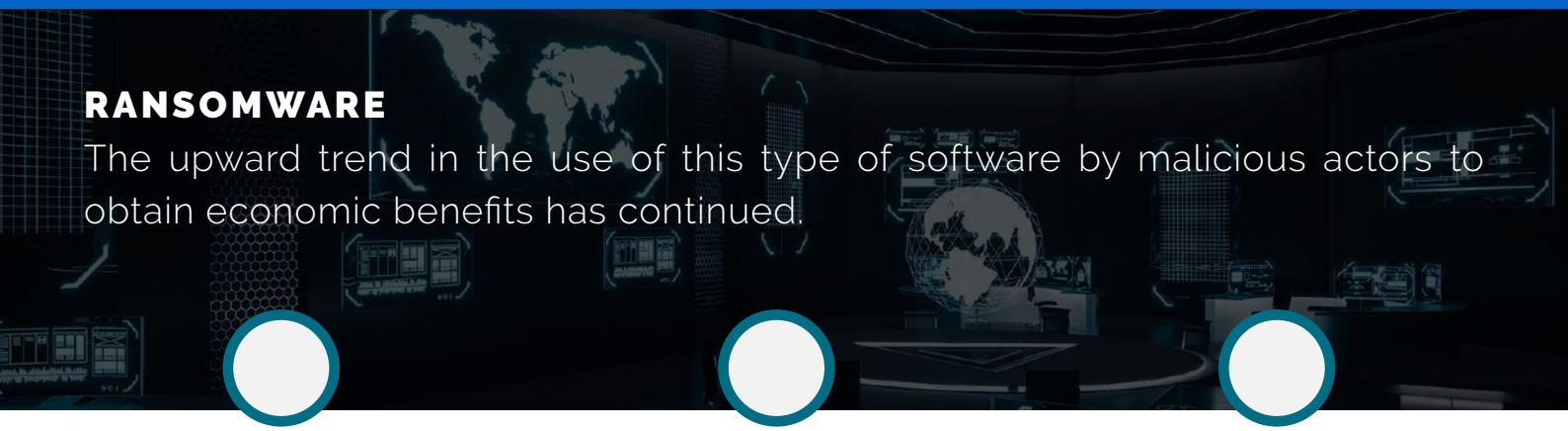
The hackers shared a link to a sample of the stolen data and posted a video showing the allegedly stolen files that included information on millions of customers, login credentials used by thousands of Acer retailers and distributors, as well as corporate, financial and audit documents.

## TELEFÓNICA

Movistar was affected by a security incident, after which unauthorized third parties accessed a database with personal information of the company's customers.

According to research data, the breach affected around 1% of customers, exposing information related to names, telephone numbers and products contracted with the company.

# CONCLUSIONS



## RANSOMWARE

The upward trend in the use of this type of software by malicious actors to obtain economic benefits has continued.

Some ransomware that has been very active during the last few years has ended its activity .

New ransomware has emerged during this period and has become a threat to corporate networks.

The report has shown the different vulnerabilities exploited by ransomware operators.

## BANKING MALWARE

The threat known as SquirrelWaffle stands out, a malware that is distributed through e-mails with malicious attachments that download a final Qbot or Cobalt Strike payload.

## MOBILE MALWARE

Android is the main operating system targeted by these malware.

iOS has also received numerous mentions following the discovery of the Pegasus spyware, which enables a jailbreak in the device and allows reading text messages, tracking calls, etc.

## SIM SWAPPING

There has been an increase in SIM swapping attacks, especially in the Americas. This technique allows attackers to take control of a target's cell phone number by tricking or bribing their phone provider's employees into reassigning numbers to SIM cards controlled by the scammer.

## HEALTHCARE SECTOR

The upward trend of the last two years of attacks on healthcare centers and hospitals continues

In addition, malicious actors keep taking advantage of the social and healthcare situation and the different variants of COVID-19 to deceive victims.

# THREAT LANDSCAPE REPORT

S21SEC

www.s21sec.com