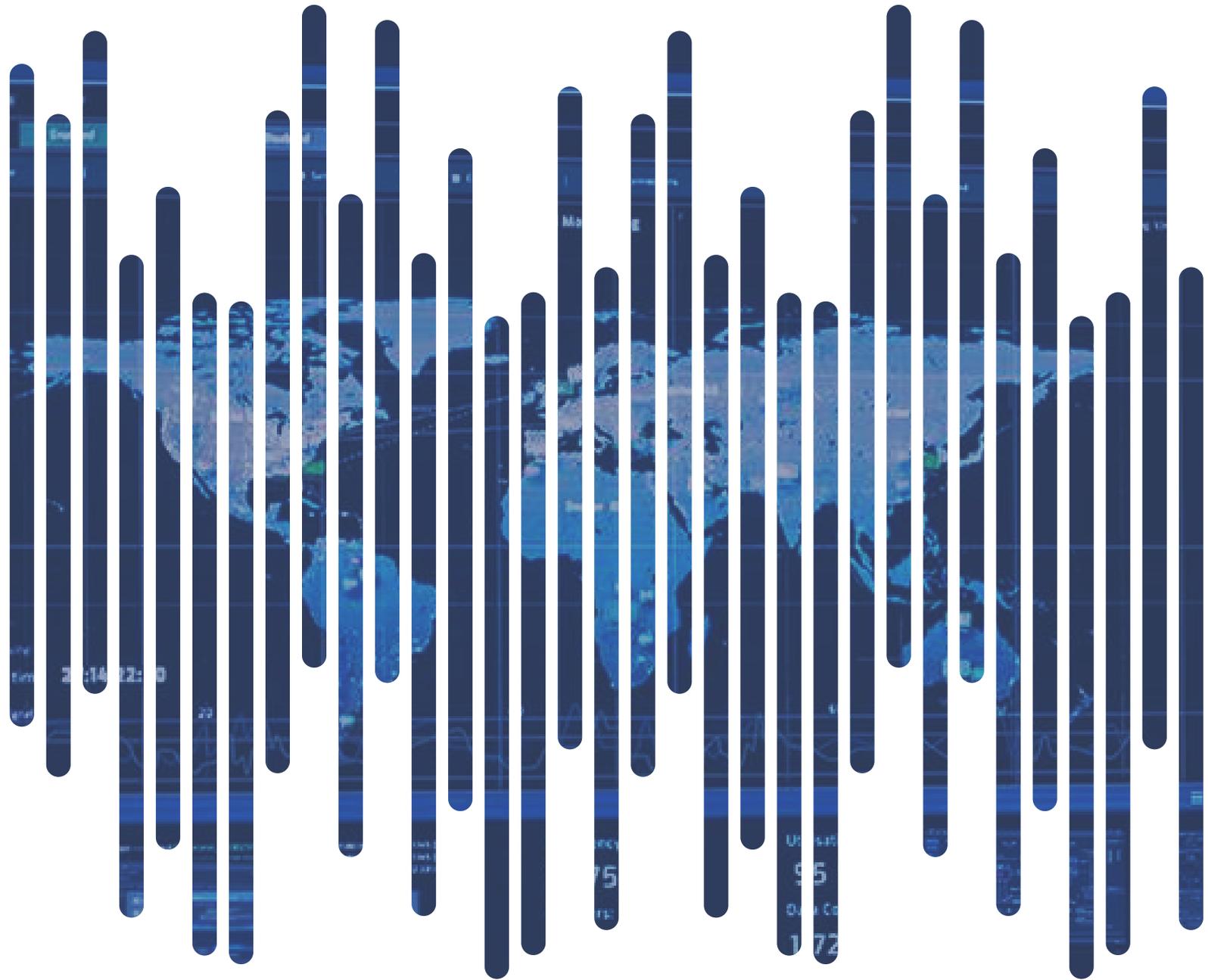


# Threat Landscape Report



**During the first half of 2022, we have identified a significant number of cyber threats that have posed a high risk to public and private entities, which have been affected to a lesser or greater extent by the exploitation of critical vulnerabilities, ransomware cyberattacks, distribution of destructive malware or data breaches.**

In view of these cyberthreats, it is worth highlighting the exploitation of vulnerabilities which, once again, have become one of the most worrying cyber threats due to their consequences.

One of the most relevant situations to analyze in the first half of the year was the cybernetic scenario in the context of the Russian-Ukrainian conflict, where several cyber threats have been identified, such as high participation of hacktivist groups, distribution of wipers (destructive malware), and ransomware attacks.

Threats targeting mobile devices have remained in focus. These threats, through smishing infection campaigns (among others), have targeted cyber espionage, highlighting the Pegasus case.

## TABLE OF CONTENTS

01. Vulnerabilities
02. Ransomware
03. Russian - Ukraine Conflict
04. Banking Sector
05. Energy Sector
06. Industrial Control Systems
07. Healthcare Sector
08. Construction Sector
09. Media
10. Telco
11. Smartphones
12. APT
13. Data Breaches

# Vulnerabilities



During the first half of 2022, several high criticality vulnerabilities that were actively exploited by cybercriminals for different types of attacks have been published.

During this period, most of the cyberattacks that have taken place have had as an initial entry vector the exploitation by cybercriminals of a vulnerability in the target infrastructure.

In April, a vulnerability was disclosed in the Linux Kernel, tracked as CVE-2022-0847, also known as [Dirty Pipe](#) due to the mechanism for communication between Linux processes.

The vulnerability allows improper preservation of permissions affecting the Linux Kernel.

The vulnerability allows a flaw whereby an attacker can write to pages in the page cache backed by read-only files to possibly elevate their privileges.

At the end of March, a zero-day vulnerability, known as [Spring4Shell](#) or [SpringShell](#), marked the security threat landscape as it was linked to a [remote code execution](#) (RCE) vulnerability in the Java Spring web application development environment.

More recently, the security flaw tracked as CVE-2022-30190, also known as [Follina](#), would allow an attacker to install programs, change or delete data, as well as create new accounts in the context allowed by the user's rights.

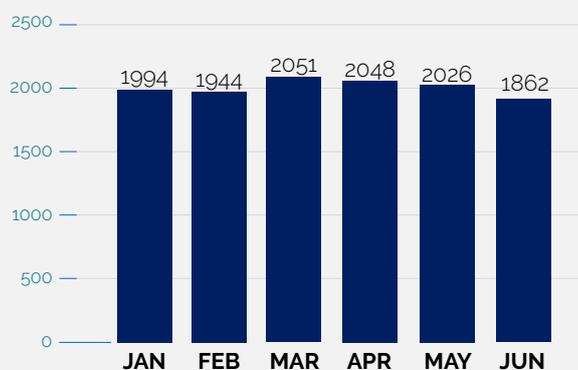
Also, according to the researchers, exploiting this would allow attackers to install malware.

In early June, Atlassian disclosed the existence of a [critical unpatched remote code execution vulnerability](#) affecting all Confluence Server and Data Center supported versions, tracked as CVE-2022-26134, which is being actively exploited in attacks.

## CRITICALITY LEVEL

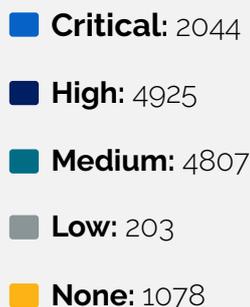
In total, in the first half of 2022, 11.925 vulnerabilities have been published, of which the largest number occurred in March.

### Published vulnerabilities During the second half of 2021



### Severity level

Based on CVSS version 3



The flaw was reported by researchers who discovered its exploitation in attacks against U.S. assets.

After being reported, Atlassian made security patches available to its customers and has warned of active exploitation throughout June.

In the observed attacks, threat actors have been seen [targeting Internet-connected web servers running Atlassian Confluence Server software](#), launching publicly available exploits to achieve remote code execution by activating a zero-day vulnerability affecting updated versions of Confluence Server.

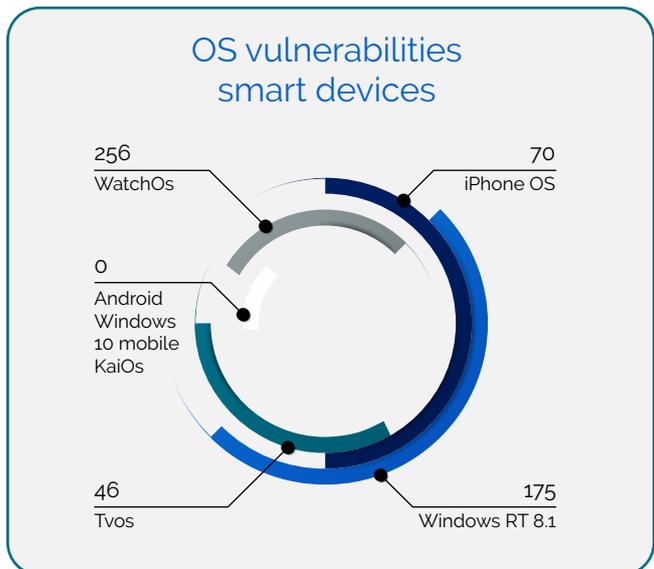
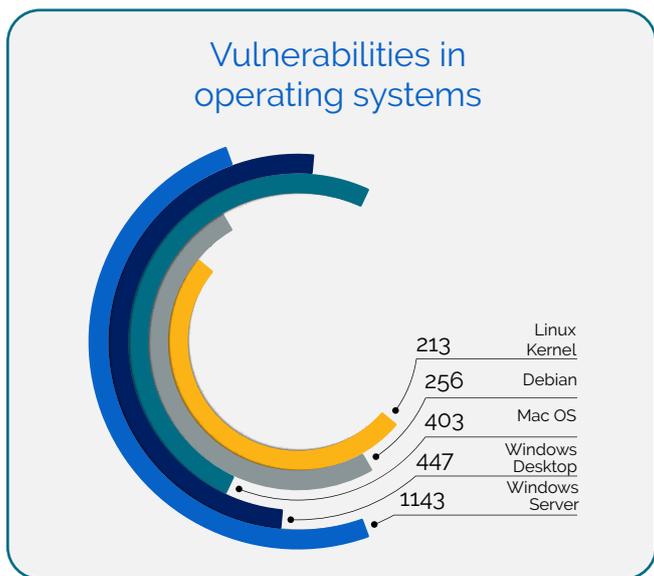
After successfully exploiting Confluence Server systems, the [attacker deploys an in-memory copy of the BEHINDER implant](#), a popular web server implant with source code available on GitHub. BEHINDER provides advanced capabilities to attackers, including memory-only web shells and built-in support for interaction with Meterpreter and Cobalt Strike.

Once BEHINDER is deployed, the attacker uses the in-memory web shell to deploy two additional web shells to disk: [CHINA CHOPPER](#) and a custom file upload shell.

Following the release of the security patches, several media outlets have reported, throughout the month of June, the existence of publicly available PoC, as well as the observation of the exploitation of this vulnerability in several attacks.

**VULNERABILITIES IN OPERATING SYSTEMS AND OS VULNERABILITIES IN SMART DEVICES**

Windows Server and Windows RT 8.1 stand out as the most affected.



## LOG4SHELL EXPLOIT

In June, the U.S. Cybersecurity and Infrastructure Agency (CISA) warned of active exploitation of the Log4Shell vulnerability (CVE-2021-44228) in unpatched VMware Horizon and Unified Access Gateway Servers.

According to investigations conducted by the U.S. Coast Guard Cyber Command (CGCYBER), threat actors, including state-sponsored advanced persistent threats (APTs), have continued to exploit Log4Shell on unpatched VMware Horizon and Unified Access Gateway servers over the past several months to gain initial access to targeted organizations.

As part of this exploitation, APTs deploy loaders on compromised systems with embedded executables that enable remote command and control (C2). In attacks observed over the past few months,

APTs have moved within the network, gained access to an incident recovery network, and collected and leaked sensitive data.

### IN ADDITION TO EXPLOITING THIS VULNERABILITY:

CVE-2022-22954, an RCE vulnerability in VMware Workspace ONE Access and Identity Manager, was observed to be exploited in the same attacks to deploy a web shell.

In the attacks, the threat actors extract sensitive data, some from the production environment of one of the victims.

## DOGWALK

in June, Microsoft patched a zero-day Windows vulnerability in the Microsoft Support Diagnostic Tool (MSDT) through the opatch platform.

The vulnerability, informally called DogWalk, is a path traversal flaw that attackers can exploit to copy an executable to the Windows startup folder when the target opens a maliciously crafted .diagcab file (received via email or downloaded from the web). The implanted malicious executable automatically runs the next time the victim restarts Windows.

Although the vulnerability was disclosed in 2020, the flaw has recently been rediscovered and brought to public attention, prompting Microsoft to patch it.

*Although Microsoft has assured that Outlook users are not at risk because .diagcab files are automatically blocked, researchers and security experts have warned that exploiting this flaw remains a significant attack vector.*

If a threat actor delivers the malicious file through another e-mail client or in hidden downloads through attacker controlled sites, they can actively exploit the vulnerability.

.diagcab files are downloaded from the Internet and include a Web Mark (MOTW), Windows ignores it for this file type and allows opening the file without a warning.

## SOPHOS

During the first half of 2022, security researchers have reported the active exploitation of a critical vulnerability (CVE-2022-1040) in Sophos Firewall to target a set of organizations in South Asia.

Identified as CVE-2022-1040, it is an authentication bypass vulnerability in Sophos Firewall User Portal and Webadmin, which can be exploited by attackers to achieve remote code execution on vulnerable devices.

The vulnerability affects Sophos Firewall v18.5 MR3 (18.5.3) and earlier versions.

*The exploitation of this vulnerability has been observed since the beginning of the year by Chinese advanced persistent threat (APT) groups.*

Their attacks make use of a zero-day exploit to compromise the client's firewall.

In addition, web shell backdoors are deployed, creating a second persistence path, and, ultimately, attacks are launched against the organizations' staff, to further impact cloud-hosted web servers that host the organization's public websites.

# Ransomware



During the first six months, changes in the tactics, techniques, and procedures of some of the ransomware operators have been observed through the introduction of new tactics and improvement of their techniques.

RANSOMWARE STATICS

# RANSOMWARE FAMILIES

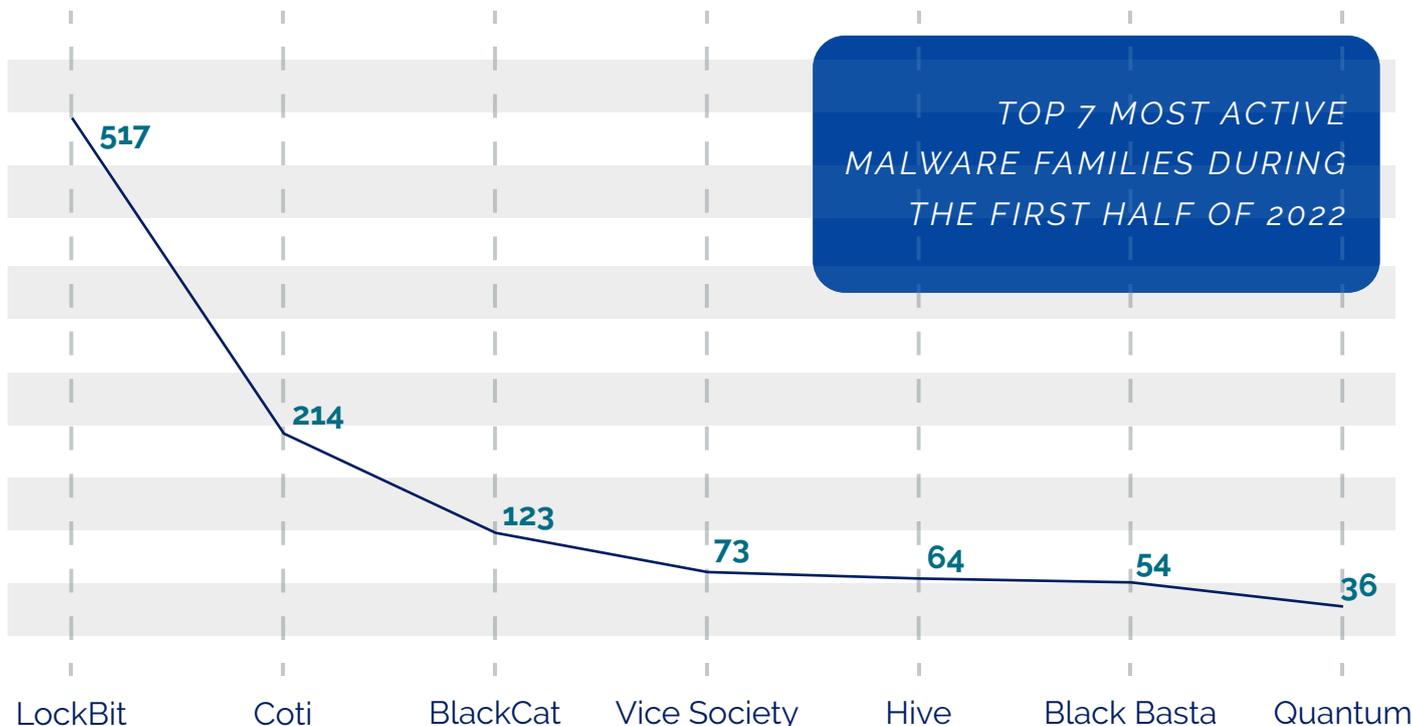
Overall, the three most active ransomware groups during this period were LockBit, Conti and BlackCat (ALPHV), which encrypted a total of 517, 214 and 123 victims respectively, according to the attacks analyzed.

During this first semester, a total of **41 different families of ransomware** have been observed.

In general terms, it is worth noting the trend toward the appearance of new ransomware groups in the threat landscape, including Pandora, Night Sky, Haron, Black Basta, Mindware, Cheers, Industrial Spy, Crimson Walrus, and Axxes.

In addition to the activation of the well-known REvil3.0 ransomware group, which has shown signs of activity since March, following the arrest in January of several of its members and the cessation of its infrastructure.

Other threat groups have ceased operations, such as the Conti ransomware which, after declaring its support for Russia in February this year, suffered a leak by one of its members, known as ContiLeaks, which released the group's internal records and has allowed researchers to reveal the ransomware's workings, operations, victims, code, etc.



RANSOMWARE STATISTICS

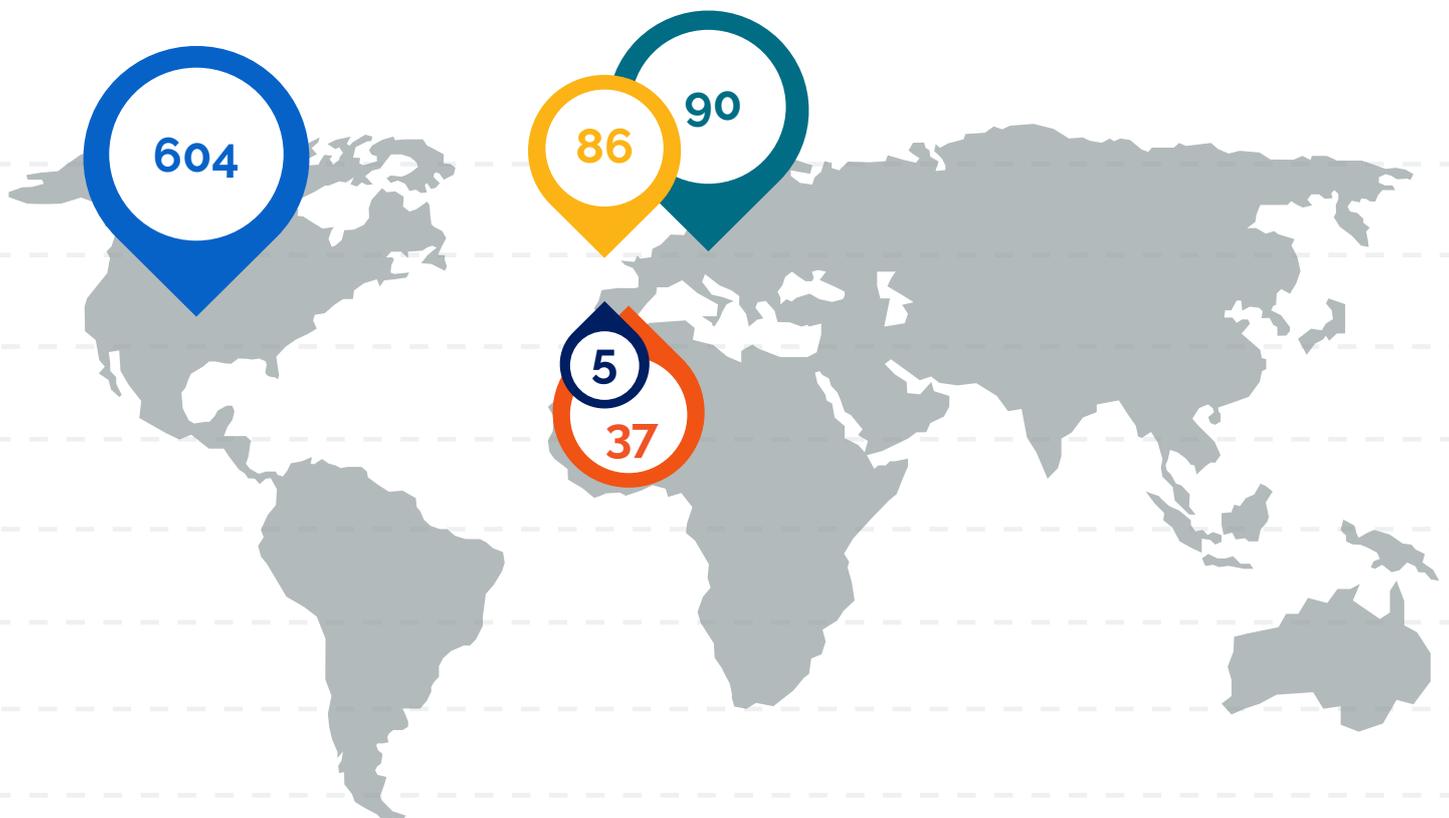
**COUNTRIES**

S21sec's Threat Intelligence team has monitored the activity carried out by threat actors on more than 50 ransomware group blogs on the Deep Web, Dark Web, and underground forums. It should be noted that the observed number of attacks covers only the observed public activity carried out by threat actors.

With a total of 1.466 attacks worldwide during the first half of 2022, the most affected continent is North America, with a total of 689 attacks, followed by Europe with 485, and Asia, which has suffered 161 attacks during this period of time.

Focusing on the countries, the United States registers the highest number with 604 attacks, followed by Germany and the United Kingdom, with 90 and 86.

Spain has received 34 attacks during the first half of 2022 and Portugal, 5, placing them in position 7 and 37 in the world ranking of cyber attacks, respectively.



RANSOMWARE STATISTICS

**SECTORS**

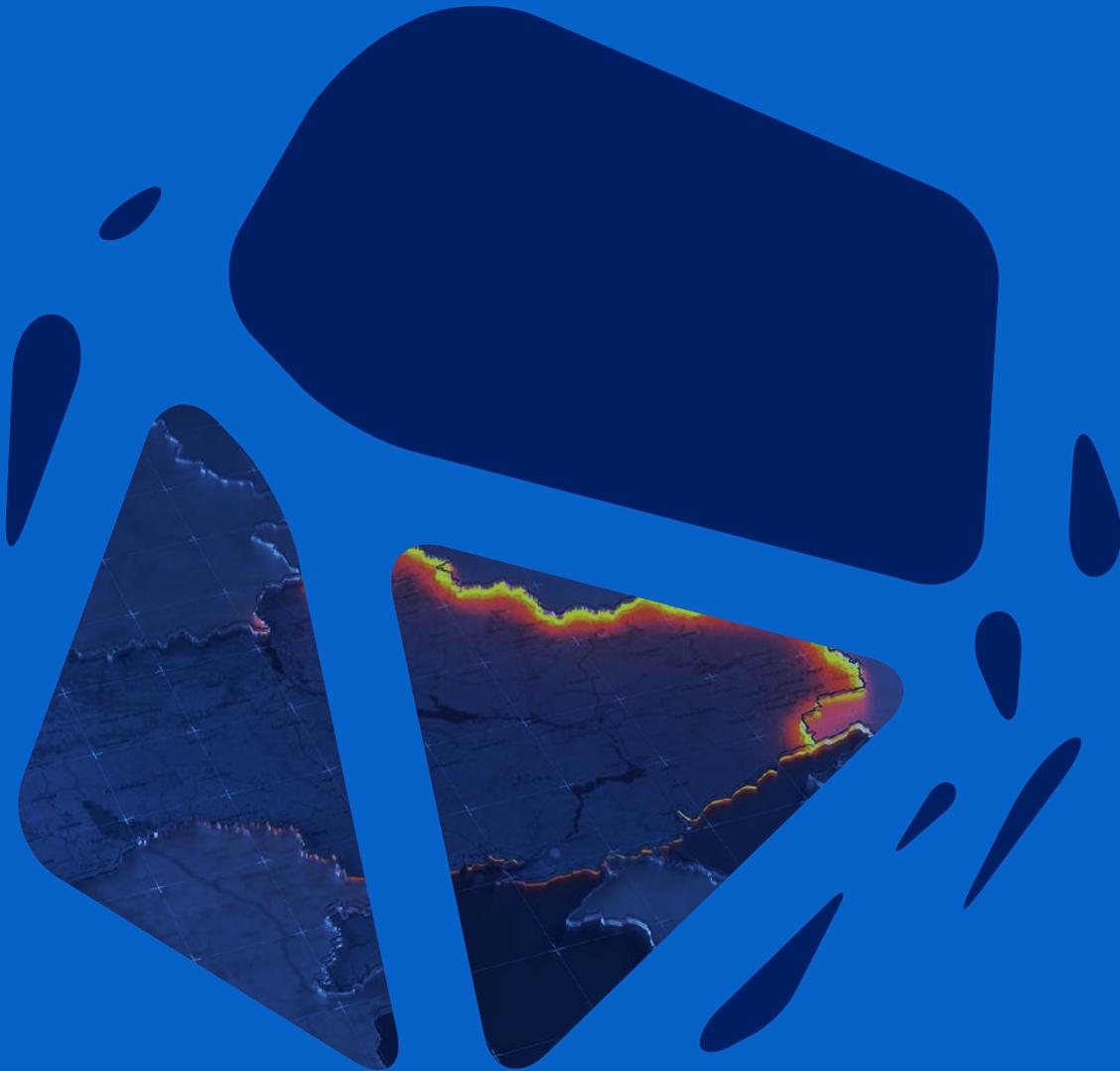
The results show a total of 1,466 ransomware attacks registered between January and June 2022. As for the verticals of the most prominent industries to which the 1,466 victims of these ransomware belong, they are mainly companies in the technological, industrial, retail, and construction.

The previous ones have been highlighted for exceeding 90 victims in this period; however, other sectors such as health, transport and logistics, government and administration and finance, exceed 70 victims as a whole.

**TOP 5 SECTORS MOST AFFECTED BY RANSOMWARE DURING THE FIRST HALF OF 2022**



# Russia-Ukraine Conflict



The conflict between Russia and Ukraine has become a clear example of what is called a hybrid war, in which the battlefield is not exclusively in the physical realm but has also moved into cyberspace.

**In this case, before Russia entered Ukraine, cyberattacks were using destructive malware against Ukrainian organizations and critical infrastructure, the so-called wipers.**

Such destructive attacks are carried out by government-sponsored APT (advanced persistent threat) groups with high technical capabilities.

Due to the Russian threat in cyberspace, the Ukrainian government conducted massive recruitment of computer security experts that involved the participation of hackers worldwide.

These cyber volunteers joined an army called the IT Army of Ukraine.

In this cyber conflict, individual actors, pro-Russian or pro-Ukrainian hacktivist groups have been involved in conducting cyberattacks against the opposing side.

It is also noteworthy that the scope of the attacks has extended to other countries and international organizations that are not actively participating in the armed conflict.

## THREATS

The threat landscape arising from the war in Ukraine is broad and includes :

- Destructive malware attacks.
- Ransomware.
- Phishing campaigns.
- Malspam.
- Hacktivist attacks.

### DESTRUCTIVE MALWARE ATTACKS

During the conflict, the use by Russia of different types of wiper-type malware has been observed, the main objective of which is to destroy the targeted systems or the deletion of data within them, causing great damage to the affected companies and organizations.

The first wiper observed in the context of the war was the so-called Whispergate, on January 13, 2022, before the invasion. Subsequently, on February 24, Russian attackers launched the IsaacWiper malware. On March 14, an attack with CaddyWiper was observed.

In addition, other malware known as Hermetic Wiper, HermeticWizard, and HermeticRansom were also observed.

In March, DoubleZero and Cyclops Blink malware were also detected.

Subsequently, in mid-April, a large-scale cyberattack was reported against power substations of a Ukrainian energy company, which used a new variant of the Industroyer malware deployed by Russia in Ukraine in 2016, known as Industroyer2.

## HACKTIVISM

In this conflict, there has been a reactivation of international hacktivism, with [Anonymous as one of the most relevant actors in this category](#).

Anonymous showed its support for Ukraine from the beginning of the conflict, carrying out a large number of attacks [based on defacements of websites, DDoS attacks, and leaks of databases and confidential information](#) of government agencies and companies in various sectors.

These attacks are part of the so-called [#OpRussia](#), an operation that not only targets Russian companies or institutions, but also Western companies operating in Russia.

The collective formed through the Ukrainian government's call, the [IT Army of Ukraine](#), has also carried out numerous hacktivist attacks targeting Russian institutions.

The [AgainstTheWest/BlueHornet](#) collective has also carried out several cyberattacks, including data breaches and leaks against targets belonging to countries that have shown their support for the Kremlin.

On the other hand, we also find [hacktivist collectives that support Russia](#), such as XakNet, a hacktivist collective that calls itself a "group of Russian patriots", and KillNet, one of the most active collectives in this conflict, with attacks targeting Latvia, Italy, Germany,

Poland, Romania, Ukraine, the United States, the Czech Republic, among others.

It should be noted that in mid-May, Killnet published a threat directed at Italy and Spain through its Telegram channel, after which they carried out [numerous Denial of Service attacks on Italian sites](#).

# Banking Sector



During the first half of 2022, different banking Trojan distribution campaigns have been detected, which have been known about for several years before and have starred in some of the most significant campaigns in 2021.

The detection of new distribution operations of these banking Trojans reflects the prevalence of these malicious codes, which have remained active and have been distributed throughout the first half of 2022 using new templates and themes in their fraudulent communications, impersonating various services, companies, and organizations and making use of new artifacts that facilitate their distribution.

## GRANDOREIRO

The Grandoreiro trojan has become a relevant threat in the banking sector in Spain and several European Union countries since 2021. As a trojan, this malware is designed to have multiple utilities. The most common is to create a backdoor in the infected computer to download updates and new functionalities.

Developed in Delphi language, this trojan carries out the [capture and exfiltration of sensitive information from the compromised computer](#), using as a distribution vector the sending of phishing emails with attached files that trigger the user's interaction installation of this trojan in the computer.

Among its characteristics, [the speed with which its authors update their code stands out](#), with different variants that have spread internationally since 2019 and have affected banks in Spain, Mexico, and Portugal.

During the first half of 2022, Grandoreiro's distribution campaigns have remained active, reusing e-mail templates used in 2021 operations and introducing new victim deception themes.

In addition to malspam e-mails pretending to contain invoices and financial information from impersonated companies, such as cell phone providers or service providers, Grandoreiro's most significant distribution operations have impersonated public institutions and organizations.

### THE INFECTION HAS SEVERAL STAGES

Distribution takes place via fraudulent e-mails containing a URL to a malicious page or an attachment.

When the link is accessed, an installer file is downloaded, which in turn downloads the payload containing the banking trojan.

## Iced ID

IcedID, also known as BokBot, is a banking trojan that appeared in 2017. This malware has different capabilities, such as stealing personal information and credentials.

Operated by the APT by Luna Spider, also known as [Gold Swathme](#), this malware has been used as a means of distribution in REvil/Sodinokibi ransomware campaigns. This link to ransomware operations, in addition to its exponential distribution in 2021, has led the expert community to suggest that this malware may act as a successor to Emotet in its mass infection campaigns.

Its means of distribution include [phishing operations](#) through which malware operators send victims phishing e-mails containing a malicious Microsoft attachment with Macros 4.0 (XML), which leads to a second phase to download the malware after opening the document and enabling the macros.

In addition to this means, distribution has been detected through the sending of contact forms. This means of infection allows attackers to perform [tracking activities](#), as well as move laterally across affected networks to continue distributing additional malicious code.

In February, new IcedID activity was detected linked to the loading of Cobalt Strike within a short time of just 20 minutes after infection. In this operation, once executed, IcedID applies discovery commands to [capture system, domain, and network information](#).

These are common commands executed by precursor malware and are likely used to prioritize footholds for future intrusion actions.

Less than 20 minutes after the initial infection, the host executes remote PowerShell commands to deploy Cobalt Strike.

In March, the use of [compromised Microsoft Exchange servers](#) for the distribution of malspam designed to infect computers with IcedID was also detected. This operation targeted organizations in the [energy, healthcare, legal and pharmaceutical sectors](#).

The distribution made use of outdated servers, which allowed the criminals to exploit ProxyShell vulnerabilities to take over computers and send malspam with the IcedID code.

### IN ADDITION TO THESE INFECTIONS, AT THE END OF MAY WERE DETECTED

New distribution and infection vectors were detected at the end of May, involving the use of a ZIP archive containing an embedded .lnk (Microsoft Windows shortcut file) file that used the legitimate mshta.exe binary to download IcedID to the target computer.

This operation also made use of DarkVNC, a malicious distribution of the VNC (Virtual Network Computing) program that allowed the malware to remotely control a victim's computer.

# Energy Sector



In the first half of 2022, there have been cyberattacks of various kinds against companies in the energy sector. It should be noted that a country's energy infrastructures are considered critical infrastructures, and an attack against them can pose risks not only for the company attacked but also for the public.

As mentioned above, during this period there have been attacks against companies in the energy sector by actors with different objectives. Some of them sought financial gain, while others were aimed at destroying or paralyzing electrical infrastructures to cause the greatest possible damage.

*Among the most significant attacks during this period were those that occurred in February.*

The sector was the victim of a series of cyberattacks targeting the German companies Oiltanking GmbH and Mabanft GmbH and the Belgian company Sea-Invest, to which were added another series of attacks targeting critical infrastructure, such as the ransomware attack suffered by the Italian group Dolomiti Energia that rendered its IT systems inoperative or the Swiss-based aviation services company Swissport International.

The attacks targeted companies in the supply chain, suppliers, facilities, or systems, by primarily financially motivated threat actors.

### **Other companies were allegedly attacked by LockBit 2.0 ransomware**

The Southeast Energy Group (GES Group), located in Campeche (Mexico), which is part of the Wholesale Oil and Petroleum Products Industry, in addition to the National Petroleum Group of Vietnam (Petrolimex), who was a victim of the actors of threats behind BlackByte ransomware in February.

### **Hive ransomware attacks**

In early March, Rompetrol, a Romanian oil company operating in Europe, Central Asia, and North Africa, specialized in the refining of petrochemical products, was the victim of a ransomware attack by Hive operators, impacting most IT services.

Another company mentioned by the Hive ransomware during March has been Pan American Energy S.L., Argentinian Branch, the country's main gas producer. So far no company information has been leaked. In addition to the company Noble Oil, a privately held used motor oil, antifreeze, and filter recycling services company located in the United States.

## *Russia - Ukraine conflict*

Since the beginning of the war conflict following Russia's invasion of Ukraine, the cyber threat landscape targeting the strategic sector and critical infrastructure has been increasing, and threat actors have been expanding their targets to other European countries, especially those that have provided support to Ukraine.

Some cybercriminal groups have pledged support for both Ukraine and the Russian government. In the case of Russian-aligned cyber actors, they have threatened to conduct operations in cyberspace in retaliation for alleged cyber offensives against the Russian government or the Russian people, in addition to cyber operations directed against countries and organizations that provide support to Ukraine.

The vast majority of attacks observed during the development of hybrid warfare are hacktivist motivated and consist of website defacements, DDoS and DoS attacks, and leaks of databases and confidential information from government agencies and critical infrastructure such as airports.

In this context, 43 ransomware attacks against companies in the energy sector have been observed during the months of January to February 2022.

February saw three cyberattacks on European companies involved in wind power generation by ransomware groups that have declared themselves to be aligned with the Russian government, such as Conti or Black Basta. These attacks occurred in the initial phase of the conflict between Russia and Ukraine and, although the incentive behind these groups is generally economic, it cannot be ruled out that they may also have had political motivations, to disrupt the operation of power generation companies in Europe.

Also, at the beginning of the conflict, the Blackcat ransomware, linked to cybercriminal groups of Russian origin, targeted companies involved in oil and gas production and transportation.

## **Malspam campaigns**

On the other hand, the sector has been affected by malspam campaigns, in which threat actors were distributing the Formbook malware, targeting oil and gas companies, by sending malicious e-mails impersonating Saudi Arabia's state-owned oil and natural gas company, Saudi Aramco, containing malicious PDF and Excel files containing the Formbook malware.

## BLACKCAT

The Blackcat ransomware, also known as ALPHV, started its activity in November 2021, being distributed via e-mail. When the victim downloads and opens the file attached to these emails, the malware starts executing on the machine.

Blackcat encrypts its victim's files and renames them by adding the .sykffle extension. As is common with other ransomware samples, BlackCat will drop ransom notes on compromised systems to inform the victim of what has happened and how to proceed to restore their data.

Text files with the name RECOVER-sykffle-FILES.txt showing the ransom note will be found on the compromised system and will contain information and instructions for the victim to follow.

**BEFORE ENCRYPTING  
THE FILES, THE ATTACKER  
WILL EXFILTER THE FILE  
CONTAINED IN THE MACHINE**

It applies the double extortion technique, threatening to publish the extracted data on his blog on the Deep Web.

In addition, if the previous extortion method does not work, the attacker will use another extortion method, which consists of threatening the victims with a DDoS attack against their assets to get them to pay. Through this triple extortion technique, the attacker ensures that the victims pay the ransom.

# Industrial Control Systems



In the first half of 2022, industrial control systems have become one of the priority targets for different threat actors internationally.

The widespread use of industrial control systems (ICS), from manufacturing and processing facilities to power plants, has made this technology one of the targets for threat actors to impact large and strategically positioned organizations.

Over the past few months, campaigns, tools, malicious code, and tactics have been uncovered to target these systems and create major disruptions to the organizations that use them.

In the context of the conflict between Russia and Ukraine, disruptive activities have been detected in these systems to massively impact the organizations that make use of these technologies.



**INCONTROLLER**



**INDUSTROYER<sub>2</sub>**

# INCONTROLLER

During this period, several toolkits called Pipedream or Incontroller have been discovered, which allow full system access to multiple Industrial Control System (ICS) devices.

Last April, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE) issued a joint cybersecurity advisory warning of threats backed by a government or advanced persistent threat (APT) actors, using these tools,

which allow access to Schneider Electric programmable logic controllers (PLCs), OMRON Sysmac NEX PLCs, and open platform communications unified architecture (OPC UA) servers.

With these tools, threat actors can perform lateral movement, privilege escalation, and service disruption after gaining full access to ICS/SCADA device environments.

The Incontroller toolkit is essentially made up of 3 main tools.



## TAGRUN

This tool is used to search for OPC servers. It enumerates and tags OPC structures and generates brute force attacks.



## CODECALL

This module communicates via Modbus and CodeSys. It contains functionalities to interact, scan, and attack, at least, three different models of Schneider Electric logic controllers (PLC).



## OMSHELL

Contains functionalities to interact with and scan some Omron PLC types via HTTP, Telnet, and Omron FINS. This tool can also interface with Omron servo drives.

## INDUSTROYER2

In April, a Ukrainian CERT investigation into a large-scale cyberattack against power substations of a Ukrainian energy company that reportedly took place during the same month was made public, which could be attributed to the Russian-origin APT known as Sandworm.

The malware deployment in the Industrial Control Systems (ICS) of the affected power substation probably occurred on April 8, 2022.

However, the cybercriminals would have gained access weeks earlier, so it is not excluded that they were performing actions to gain persistence and get lateral movement to distribute the Industroyer2 malware.

The Industroyer2 malware is deployed as a Windows executable named 108\_100.exe.

In this case, the malware only makes use of the IEC-104 protocol through which it communicates with the industrial equipment.

After connecting to the targeted devices and computer equipment, the malware starts adding the .MZ extension to the applications used in the daily operations of the affected computers and devices.

After this process, Industroyer2 could access the control of ICS systems for a variety of purposes, such as cutting off the power supply.

*The information presented shows that the April 8, 2022, attack chain was initiated as follows:*

- Deployment of the CaddyWiper malware on Windows, Linux, and Solaris systems of the target energy provider.
- The Sandworm group initiates the sequence for the deployment of the Industroyer2 malware to cut off the electricity supply in a region of Ukraine.
- Subsequent execution of the CaddyWiper malware on the same machines affected by Industroyer2 to eliminate traces of the latter.

# Healthcare Sector



Since the start of the COVID-19 pandemic in 2020, the healthcare sector (including hospitals, medical research centers, private clinics, and health centers) has positioned itself as one of the main targets of cyberattacks, highlighting the sensitivity of this sector to cyberattack threats.

Previous editions of the S21sec Threat Landscape have mentioned the cyberthreats to which the healthcare sector has been exposed and proposed future scenarios around this situation.

Among the cyberthreats shown in the document, ransomware attacks and phishing campaigns for credential theft are the most common, which continue to be a cyberthreat with serious repercussions.

**However, with the beginning of the year 2022, 2 cyberthreats have been identified whose notoriety has increased and have attracted attention:**

- Hospital and clinic data breaches.
- Sales / auctions of access to healthcare entities .

In the case of data breaches, these usually occur after a previous cyberattack, either by phishing campaigns, intrusion, ransomware, or infection by other malware. In addition, threat actors can perform mere intrusion actions to collect information/data to use it for malicious purposes.

According to data compiled by S21sec, data breaches are considered to be among the main cyber threats against hospitals, clinics, and private clinics of any specialty, among others.

With this, S21sec has been able to identify more than 50 data breaches in the first half of 2022.

However, the number of these could be higher, doubling the figure of 50, while some of them have not been identified due to 2 main casuistry:

- several clinics do not report the data breach to the relevant agencies due to ignorance of it or for reasons of reputational damage.
- Cybercriminals responsible for the data breach do not announce in blogs and underground forums the sale or exposure of the stolen data, being unknown without a previous computer analysis if it has been the victim of an intrusion and data theft.



For example, in the first 6 months of 2022, the data breaches of the [Hospital Centro de Andalucía](#), which reported a data breach following a cyberattack last January.

The US hospital group [Shields Health Care](#), which suffered a data breach in early June that affected more than 2 million patients following a cyberattack that occurred in March, having a significant impact on its infrastructure and patient and employee data, can be highlighted.

On the other hand, through forums and chats on the Deep and Dark Web, it has been possible to identify an [increase in the sale and / or auction of access](#) with administrator privileges to hospitals and clinics in the healthcare sector. These sales are usually carried out in 2 ways:

- As a step following the infection of the target entity's computer equipment where access credentials to critical / sensitive systems of the target entity are collected.
- Following a previous data breach where threat actors extract victims' data to sell or auction such data and information on underground forums on the Deep and Dark Web.

In the second case, threat actors publish databases for free on more accessible forums (without having to create an account or interact).

Likewise, the sale and subsequent acquisition of the stolen data can be used for different reasons by other malicious actors, such as performing other cyberattacks, impersonating users, launching phishing campaigns against compromised users, or proceeding to compromise banking data to divert the victim's money to the threat actor's accounts.

### ADDITIONAL INFORMATION

According to data compiled by S21sec, in the first few months, 33 publications of sales/auctions of access related to the healthcare sector have been detected, although it is not ruled out that there may be more sales of this type through forums with greater restrictions or through private channels.

In the first half of 2022 various threat actors have published the sale and auction of access with administrator privileges to several hospitals in the US, Canada, France, and the UK, for an initial price of between 3,000 and 5,000 dollars. The sale of access to biotech and pharmaceutical companies has also been identified, especially to companies in Southeast Asia.

Including the healthcare sector medical web platforms (web and mobile applications), technological entities exclusively dedicated to the healthcare industry, and pharmaceutical and biotech companies, the cases of data breaches and access sales skyrocket. This is because threat actors focus more on these types of entities due to the profitability, as well as the fact that various cybercrime groups are aligned in not carrying out actions against hospitals and medical centers.

As for the consequences of the 2 cyberthreats exposed, data breaches and access sales are distinguished by having a greater potential impact on citizens, specifically the patient. In this type of cyber incident, in addition to compromising access credentials, medical information, medical records, and banking data are also breached, which poses a threat to the affected person.

# Construction Sector



The construction industry represents one of the fundamental pillars of the global economy, representing one of the fastest growing and most stimulating areas of some of the world's major economies, such as the European Union.

In this region, the sector provides 18 million direct jobs and contributes around 9% of the EU's GDP.

This makes the construction sector one of the main targets of cybercriminal groups, especially ransomware groups looking for financial gain, and APT groups aimed at cyber espionage.

## RANSOMWARE

One of the main threats against the construction sector has been the danger posed by ransomware attacks. During the last six months, the construction sector has been one of the sectors most impacted by this type of attack, accounting for 95 of the total number of attacks recorded.

Among the most active ransomware groups targeting organizations in the industry are the following:

### LOCKBIT

LockBit attacks during the first half of 2022 have focused on organizations located in the United States, with incidents that made the companies lose millions of dollars due to the disruptions in their services and the importance of the leaked information.

### CONTI

Has been one of the most active threat actors in the first half of 2022 in impacting organizations in the construction sector, mainly located in the United States. Of its attacks, the infection of a company dedicated to the development of construction materials that are among the 500 most influential companies in the Middle East, stands out.

### BLACKCAT (ALPHV)

Launched in November 2021, has been distributed through e-mails, which has allowed the malware to spread worldwide, affecting organizations in different sectors and countries. Its attacks against the construction sector have focused primarily on U.S. corporations.

## CYBERESPIONAGE

Concerning cyberespionage campaigns targeting the construction sector, the main cybersecurity risk for organizations in the industry is posed by APT campaigns.

These attacks are characterized by the use of a wide range of advanced techniques designed to steal confidential information from organizations.

Tracking APT campaigns against the sector shows the growing interest of Chinese-sponsored threat actors against organizations in the sector. APT campaigns stand out:

01

### APT20

Also known as Twivy, exploits the compromise of strategic websites by party-hosted websites that address issues such as democracy, human rights, press freedom, ethnic minorities in China, and other topics.

02

### APT24

Also known as PittyTiger, it targets organizations in countries such as the US and Taiwan. It exploits the RAR archive utility to encrypt and compress stolen data before transferring it outside the network. The data theft extracted from this actor focuses on documents with strategic importance, suggesting that it is intended to monitor the movements of various states on issues applicable to China's ongoing territorial or sovereignty dispute.

03

### APT31

This Chinese cyberespionage actor is focused on obtaining information that can provide the government and state-owned companies with political, economic, and military advantages. APT31 has exploited vulnerabilities in applications such as Java and Adobe Flash to compromise victims' environments.

# Media



The media and entertainment industry is one of the main strategic sectors for different countries and a growing business area that accumulates millions of euros in revenue worldwide.

This key role has made industry organizations one of the main cyberattack targets for threat actors, state-sponsored cyber actors, cybercriminals, and hacktivists seeking visibility.

In the first half of 2022, this sector has experienced an increase in the number of cyber threats, malicious activities, and incidents against its IT systems. Some of the main incidents against media and audiovisual industry have been:



**RANSOMWARE  
ATTACKS**



**ATTACKS BY  
CYBERCRIME  
GROUPS**



**ATTACKS BY  
HACKTIVIST  
GROUPS**

## RANSOMWARE ATTACKS

---

Ransomware attacks against the media industry have increased exponentially during the first half of the year, with international incidents such as the attack against Nikkei in May.

**Different ransomware groups have been behind these attacks, including identified groups such as Everest or Conti, which have leaked information on their victims.**

## ATTACKS BY CYBERCRIME GROUPS

---

Cybercrime groups have also been at the forefront of attacks against media outlets in the first half of the year, with significant attacks.

In January this year, the Portuguese media group Impresa, owner of the SIC television channel and the Expresso newspaper, was the victim of a cyberattack by the Lapsus\$ group, in which the cybercriminals allegedly obtained private information that they would leak if they did not receive a ransom.

In addition, they also performed defacement actions, a type of targeted attack on a website, characterized by modifying the visual appearance of a web page.

## ATTACKS BY HACKTIVIST GROUPS

---

In the first half of the year, the media industry has been one of the main targets of attacks by hacktivist groups, especially in the context of the Russian invasion of Ukraine.

Both Russian and Ukrainian media have been victims of organized hacktivist groups that have used attacks for a wide range of politically motivated activities: disrupting services, distributing fraudulent or propagandistic content, or stealing information.

From intrusion and sabotage attacks to defacement activities, the media of countries involved in armed conflict have become targets of these collectives.

Some of the most relevant attacks include the hacking of the Russian television and video content provider RuTube or the all-Russian state television and radio broadcasting company VGTRK.

# Telco



The onset of the war in Ukraine has led to the proliferation of various attacks on critical infrastructure and companies in the sector.

In May, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) made public the attribution of several cyberattacks that occurred at the end of February against commercial satellite communication networks to Russian state-sponsored threat actors.



According to the report, Russia allegedly launched cyberattacks in late February against commercial satellite communications networks that affected the Viasat KA-SAT broadband satellite service to erase SATCOM modems, to disrupt communications in Ukraine during the invasion.



The attacks indirectly impacted other European countries, rendering terminals in Ukraine and throughout Europe inoperable and affecting services and infrastructure that support wind turbines and provide Internet services.



Cyber threats to satellite communication networks internationally can pose risks to customer and network provider environments.



In the current geopolitical situation and hybrid warfare cyber scenario, critical infrastructure organizations and other organizations that are suppliers or customers of the SATCOM network need to increase their cybersecurity defenses.

# Smartphones



Cell phones have become one of the main targets of cybercriminals, and as has been the case in recent years, the first six months of 2022 have seen an increase in mobile malware activity.

It should be noted that malware targeting cell phone users is distributed mainly via **four routes**:

 <p>Smishing attacks in which cybercriminals impersonate applications, banking entities, or messaging companies.</p>	 <p>Use of pop-ups or advertisements on web pages urging users to download an application.</p>	 <p>Unofficial application markets are one of the main places for malware distribution.</p>	 <p>Official markets like Google Play or Apple Store.</p>
---	---	---	--

These messages include a link to a fraudulent page where the user will be asked for personal information to steal credentials, or a URL that directs to a page where malware will be downloaded.

Many cases have been observed in which cybercriminals urge to install fake updates of common software, such as Adobe Flash Player or anti-virus.

Numerous applications appear in these markets that look legitimate or even a copy of the real application but to which the actors have added malicious code.

Although these official app markets have internal security measures in place to prevent apps with malicious code from being available for download, there are still cases where an app that looks legitimate is an app that contains some type of malware.

## WITHIN THE ATTACKS ON SMARTPHONES THE FOLLOWING STAND OUT:

**PEGASUS**  
Spyware

**XENOMORPH**  
Banking Trojan

**FLUBOT**  
Malware

## PEGASUS

The Pegasus spyware, developed by the Israeli security company NSO Group, has gained prominence in the last three years for its use against members of state and regional governments, as well as journalists, prominent citizens, and diplomatic personnel. The purpose of this malware is espionage.

The exploitation of the three vulnerabilities allowed the attackers to infect the device when the user accessed the URL previously sent by the attackers through a smishing attack. These messages, sent either as SMS or as a message on social networks, used airline and public institution advertisements as lures.

Once the user accesses the malicious URL, the malware performs actions to execute the exploits and proceeds to perform a jailbreak

attack has been performed, the spyware package is automatically installed.

After installation, the spyware compromises applications previously installed by the user to collect information and data.

Through the hooking technique, Pegasus can modify the behavior of applications and operating systems.



Pegasus is also capable of compromising Apple devices by sending fake images in GIF format via the iMessage application.



For this infection, the attackers use zero-click exploits and exploit vulnerabilities in the CoreGraphics PDF parser.

## XENOMORPH

Xenomorph is an Android banking trojan first discovered in February 2022, distributed under the name FastCleaner application.

Upon installation of the application, the user is prompted with a window asking them to give accessibility service permissions to the application. The accessibility services permission should only be used to assist in the development of applications for users with disabilities.

When the FastCleaner installation is finally

complete and the user has enabled accessibility services, the application appears to have no behavior. If a user attempts to open the application, it simply returns the user to the home screen, and, if the user attempts to uninstall the application, the pop-up window to confirm whether the user wants to uninstall it closes automatically.



As with other Android banking Trojans, when the user opens their banking app, the Xenomorph malware will perform an overlay attack, superimposing a fake page that impersonates the bank's login page, to get victims to enter their login keys.



The cybercriminals will use these passwords to access the account and steal money.

## FLUBOT

Discovered in December 2020 and with a significant expansion in the last two years, FluBot was distributed via SMS text messages, impersonating different entities to spread malicious links where malware was downloaded as fake tracking programs for parcel deliveries or other services.

FluBot operators use SMS messages that claim to contain links to voicemail, missed call notifications, or alerts about incoming money from an unknown financial transaction.

The links in these messages take the victim to a website that hosts the FluBot APK, which victims must download and install to learn the details of the transaction.

Once downloaded, the application prompts victims for certain permissions, such as accessing SMS data, managing phone calls, and reading the user's address book.

Threat actors use the victim's contact list to send an SMS with a message containing a malicious link.

Because these messages come from a known source, recipients are more likely to open them and infect their devices.



Last May, the infrastructure behind FluBot was disabled by the Dutch police and in early June Europol announced the complete removal of the FluBot Android malware.



European law enforcement authorities detailed how the international police operation reportedly involved eleven countries to dismantle the malware.

# APT



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

This type of attack is carried out by the state or nationally sponsored actors with the aim of espionage or sabotage against organizations that compete (strategically or politically) against the interests of the sponsor.

Their activity is based on persistence, seeking to remain undetected for prolonged periods. APT activities take place within the framework of strategic socio-political events, as well as in specific geopolitical scenarios.

In this sense, the main APT activities during the first half of 2022 have been framed by different ongoing strategic scenarios, such as the bid for Chinese international leadership or the Russian invasion of Ukraine.

*Among a large number of threats, one set of threats has been the most significant incidents and campaigns in the first few months of 2022:*

## Russian APT

Advanced Persistent Threat (APT) groups of Russian origin have been remarkably active in their actions before the invasion of Ukraine and in the context of the conflict between Russia and Ukraine.

## Chinese APT

Over the past few months, it has been observed how Chinese APTs have starred in some of the major international incidents and campaigns in the cyber threat landscape.

## Emotet

In the first months of 2022, there has been a significant increase in computer threats, resulting from the return of the Emotet malware.

# Russian APT

Following the monitoring and detection of activity in the first half of 2022, it is considered that the distribution of the so-called Wiper by Russian APTs, among strategic targets in European countries and NATO member states, has been one of the [main threats to critical infrastructures](#) due to its destructive potential in the cybernetic field.

**The scenario of the military conflict between Russia and Ukraine has led to an increase in the cyber activity of Russian APTs such as APT28, APT29, and Gamaredon, distributing infection campaigns with destructive malware and cyber espionage.**

Likewise, limited information has been obtained from Russian APTs such as Turla or DoppleSpider, known for their activity in cyberespionage and extortion tasks, which could demonstrate the opacity of their activity, although it is not ruled out that their actions have been limited to internal reasons of the group.

*In this regard, S21sec highlights the activity of the APT28 group (Fancy Bear, Strontium, Pawn Storm, Sednit, Tsar Team, Iron Twilight, Sofacy). The following are some of the group's identified characteristics:*

The origin of APT 28's activities dates back to 2007-2008 when several cyberattacks involving malware distribution for cyberespionage purposes were identified in the context of the Russia-Georgia conflict.

It acts as a state-sponsored entity (Russia, in this case) and is attributed to personnel of military unit 26165 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

The main motivation of APT 28 in its actions is focused on obtaining privileged and confidential information of strategic sectors of the target country or industry for geopolitical reasons.

Likewise, the existence of economic motivation has not been identified.

The targets of the threat actor in question are distinguished by being of high strategic level such as aerospace, government, technology, and energy, among others.

Its activity for 14 years has resulted in cyberattacks against government entities of countries aligned with the European Union and NATO, highlighting its latest actions in the context of the Russian-Ukrainian conflict with the distribution of phishing campaigns with destructive malware and cyber espionage.

The APT 28 group is characterized by the use of various malware since 2008 in which it has implemented constant improvements with the primary objective of making the victim's systems unable to detect the execution and presence of the malware.

The impact of these attacks is considered high risk for the targeted entities due to the ability of the APT to evade defenses and gain persistence, the ability to exfiltrate confidential information, the collection of credentials and access, as well as the dissemination of malware in critical systems.

*Given the capabilities of Russian APTs and their latest actions in scenarios of geopolitical disputes, it is considered likely that their activity will remain at a high level with potential cyberattacks that could diversify their TTPs, which would pose a risk to critical target infrastructures.*

# Chinese APT

These threat actors are credited with sponsorship from the Chinese nation-state, which [provides resources and support for intrusion, espionage, and sabotage activities](#) to be carried out against various strategic targets for the country.

With major campaigns over the last few years, in the first half of 2022, they have expanded their targets by taking advantage of the international threat scenario, exploiting new vulnerabilities, and using new tactics to carry out [attacks on major organizations around the world](#).

## MAY

Several actors linked to China have been identified exploiting the Follina vulnerability (CVE-2022-30190) in the Microsoft Support Diagnostic Tool (MSDT) against organizations in different countries, including Belarus and Russia, as well as the Tibet region.

Among the threat actors exploiting the vulnerability, the Chinese APTs Twisted Panda and TA413 have been identified.

## JUNE

Experts identified activity allegedly attributed to the Chinese state-sponsored APT, BackdoorDiplomacy (CloudComputing), which exploited the same vulnerability in phishing campaigns targeting Saudi Arabia.

The infection chain first loaded an HTML file containing the Follina exploit from a compromised infrastructure associated with Saudi Arabia's Effat University and eventually retrieved a secondary payload, the group's custom backdoor, Turia.

*During these six months, Chinese APTs have also developed different malicious codes to perpetrate attacks against specific targets*

During this period, for example, it was discovered that the WinDealer malware, spread by the LouYu APT, can be introduced through a man-on-the-side attack.

This innovative development makes it possible to modify network traffic in transit to insert malicious payloads.

**These attacks are particularly dangerous and harmful because they do not require any interaction with the target for the infection to succeed.**

In addition to exploiting vulnerabilities and using new malicious code, Chinese APTs have diversified their activity, moving into conducting sophisticated cryptocurrency theft scams that use social engineering tactics to lure victims from dating applications (apps) to fraudulent platforms.

**These types of campaigns have been carried out by Chinese APT groups such as APT41, which in recent months have been involved in financially motivated cybercrime, such as cryptocurrency theft.**

# Emotet

This threat, which spreads through malicious e-mails (malspam) with massive infection campaigns, returned to activity after attempts to disrupt its operation last year.

*After cessation of activity for several months, since the beginning of 2022, its operations have multiplied exponentially.*

its operators have carried out constant malspam campaigns in Latin America (with particular impact on Mexico) and Europe (with activity in countries such as Italy or Germany) in the first quarter of 2022.

In addition, due to the characteristics of its campaigns and the mechanisms it uses to distribute itself, Emotet has diversified the use of downloaders, and the use of threats via e-mail (mainly phishing).

These new operations have made use of lures as diverse as electronic notifications of alleged bank invoices or greetings for social and festive events.

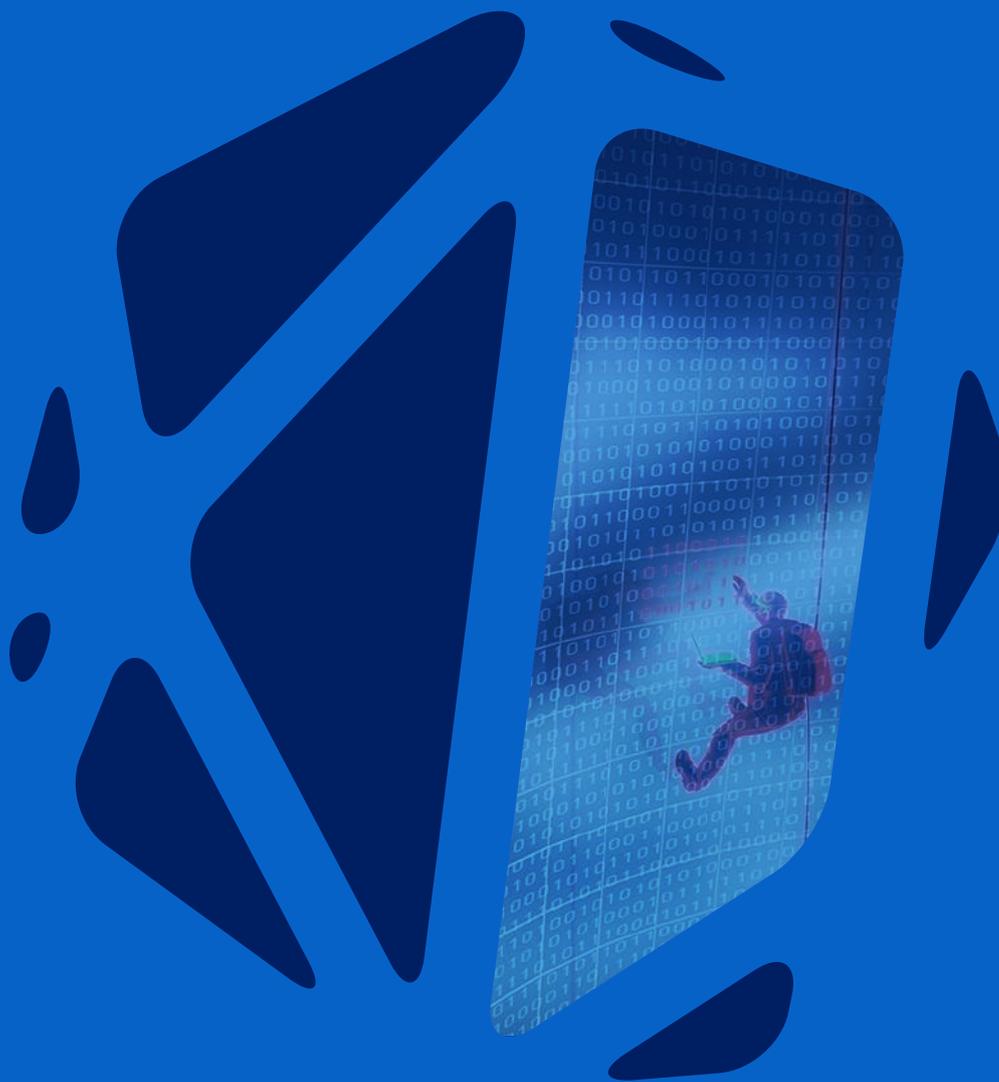


This malware is distributed via e-mails containing an Excel or Word file with macros (or as a password-protected Zip file containing such a file).



Recently, cases have been detected where malicious Excel and Word files are downloaded via links in the body of the email or via links pretending to contain Windows application installers.

# Data Breaches



During the first half of 2022, in the case of security incidents that have resulted in data breaches due to the nature of the information exposure, they mainly respond to economic motivations on the part of cybercriminals, who aim to make a profit for the information extracted from victims.

The main techniques used are social engineering, brute force attacks, credential stuffing, malware, or other types of attacks.

Among the data compromised in the data breaches during the first half of the year, personal information (full names, addresses, e-mails, telephone numbers, etc.) stand out.

*Among the main data breaches by sector affected, the following stand out:*

**JANUARY**



Red Cross was the victim of a cyberattack that exposed the data and personal information of more than half a million people. The data came from at least 60 Red Cross and Red Crescent societies worldwide. According to official reports, the attack targeted an external company in Switzerland that the ICRC contracts to store data on the Red Cross and Red Crescent societies worldwide.

**FEBRUARY**



The Croatian telephone operator A1 Hrvatska was the victim of a security incident in which confidential information affecting approximately 200,000 customers was exposed. The information accessed included full names, personal identification numbers, physical addresses, and telephone numbers.



T-Mobile, a U.S. telecommunications provider. It disclosed that an unknown attacker gained access to customer account information, including personal information and personal identification numbers (PINs), adding that an unknown number of customers were affected by SIM swapping attacks.

**MARCH**



Ikea Canada confirmed that in March it suffered a data breach involving the personal information of approximately 95,000 customers.

## APRIL



The multinational company Coca Cola in April began investigating a large-scale data breach allegedly carried out by the Stormous group. The group posted on its website this week that it had successfully hacked into the soft drink giant's servers and stolen 161 GB of data. It also offered the data for sale for more than \$64,000, or 1.6467 bitcoins.



U.S. automaker General Motors revealed it was the victim of a credential stuffing attack in April that exposed some customers' information and allowed hackers to redeem reward points for gift cards.

## MAY

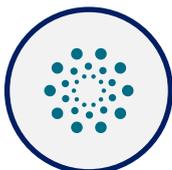


The Peruvian Association of Banks (Asbanc) warned about a possible leak of personal data of a Peruvian public agency, which is being marketed through social networks such as Facebook, WhatsApp, and Telegram.



In May 2022, a state audit revealed a data leak at the Texas Department of Insurance that compromised 1.8 million individuals. The data in question, including Social Security numbers and other sensitive personal information, was widely available on the department's website from March 2019 through January 2022

## JUNE



The pharmaceutical company Novartis suffered a data breach after a security incident carried out by the threat group Industrial Spy, a collective that has a market on the deep web in which it offers for sale information extracted in its attacks. In this case, the group mentions having obtained 7.7 MB of information.

# S21 SEC



[www.s21sec.com](http://www.s21sec.com)