THREAT LANDSCAPE REPORT 2023

S21SEC
Cyber Solutions by Thales

INDEX

S21 SEC
Cyber Solutions by Thales

01 VULNERABILITIES

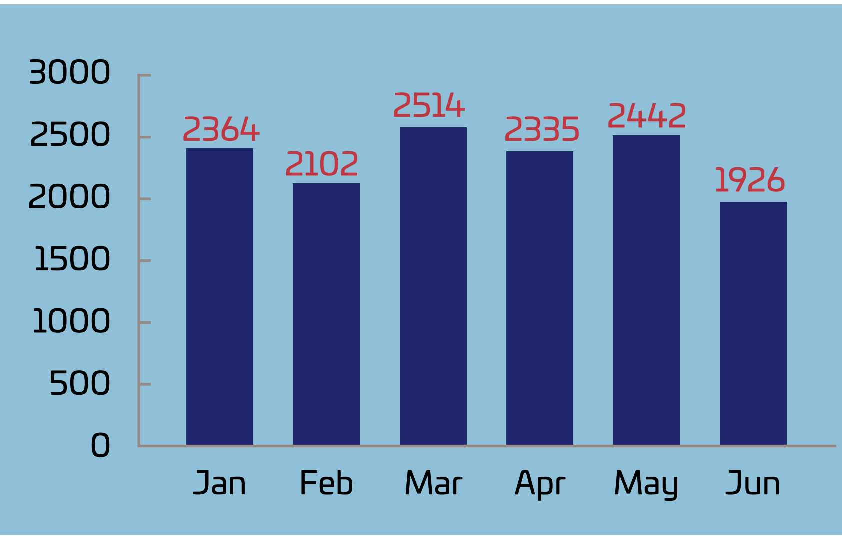
*Cyber vulnerabilities are **weaknesses in software** that can be exploited to compromise systems in cyber attacks.*

During the first half of 2023,

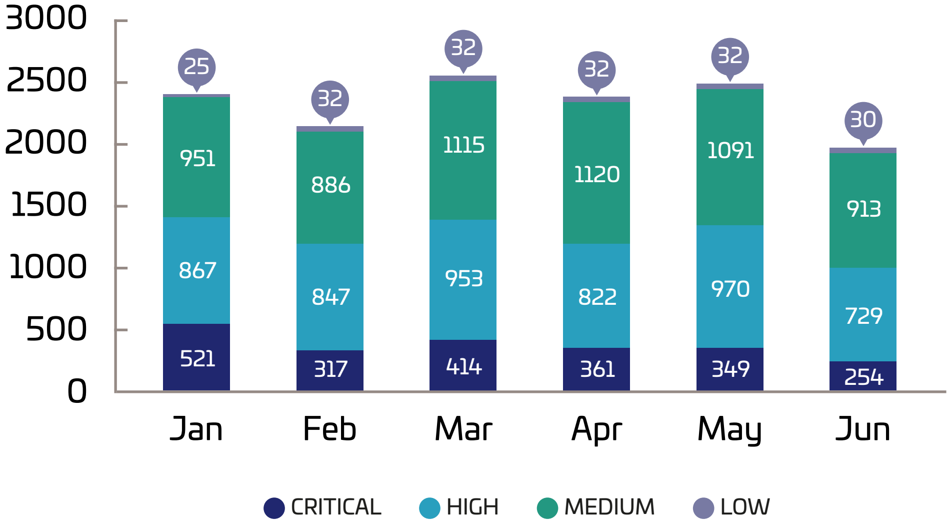
the vulnerabilities in software systems have shown a significant increase over the figures observed in the previous half-year.

According to NIST (National Vulnerability Database) data, ***13683 vulnerabilities classified*** with the Common Vulnerability Scoring System (CVSS) v3.X standard have been disclosed. This is an increase of 3 % over the ***13243 new vulnerabilities published*** in the second half of 2022.

March had the highest number of vulnerabilities disclosed, followed by May and January



Most of the vulnerabilities are of medium and high severity, representing almost 82% of the vulnerabilities reported so far this year. Only 16% were classified as critical flaws.



However, even though the volume of critical severity vulnerabilities is significantly lower compared to medium and high severity vulnerabilities, during the first half of the year it has been observed how threat actors have focused on exploiting this type of vulnerabilities to penetrate target systems and expand or move laterally to escalate attacks.

On the other hand, during the first months of the year, the exploitation of zero-day vulnerabilities in massive campaigns affecting the whole world has occurred.

The range of tactics employed by cybercriminals has expanded dramatically, with ransomware cyberattacks abusing vulnerabilities reaching an all-time high in the first half of 2023, wreaking havoc on businesses and government agencies worldwide. Such is the case with massive exploitation campaigns such as VMWare ESXi, PaperCut, MOVEit, or Barracuda.

MOVEit

An active exploit campaign by threat actors targeting several organizations, particularly in North America and the United Kingdom, was disclosed in late May. ***The campaign abused the zero-day vulnerability CVE-2023-34362 in MOVEit Transfer software***, and the attacks were attributed to threat actor ***Lace Tempest*** linked to the Cl0p ransomware group. Known victims number more than 100, and Cl0p exploited the vulnerability to infiltrate computer networks worldwide and steal sensitive information.

Barracuda

the zero-day vulnerability tracked as CVE-2023-2868 was also the subject of a massive campaign whose exploitation began in October 2022 to gain access to a subset of ESG devices and implement backdoors designed to provide attackers with persistent access to compromised systems. The malware identified in the campaign corresponds to ***a Trojan module known as SALTWATER*** with backdoor functionality and arbitrary file upload and download, command execution, proxy, and tunneling capabilities, ***along with SEASPY***, another ELF64 persistent backdoor that masquerades as a legitimate Barracuda Networks service and sets itself up as a PCAP filter.

PaperCut exploit campaign

An exploit campaign targeting PaperCut servers was also observed in April, which was attributed to ***ransomware operations Cl0p and LockBit***, who used vulnerabilities tracked as CVE-2023-27350 and CVE-2023-27351 in the PaperCut application server for corporate data theft. Exploiting these would allow remote attackers to perform remote code execution and unauthenticated information disclosure. Cl0p had been exploiting PaperCut vulnerabilities since April 13 for initial access to corporate networks ***to deploy the TrueBot malware***, previously linked to the ransomware operation. Some intrusions were also reported to have triggered LockBit ransomware attacks.

Mirai botnet campaign on TP-Link WiFi routers

A massive worldwide exploitation campaign by the Mirai malware botnet was revealed in mid-March through the active exploitation of a vulnerability tracked as CVE-2023-1389, a high-severity unauthenticated command injection vulnerability in the local API of the web management interface of the TP-Link Archer AX21 (AX1800) router, to incorporate devices into the Mirai botnet ***to carry out distributed denial of service (DDoS) attacks***. The first attacks were detected on April 11, 2023, initially localized in Eastern Europe, and subsequently, the malicious activity continued to spread globally.

3CX supply chain attack

An active supply chain campaign called ***SmoothOperator***, attributed to North Korean threat actors, was reported in late March, with the attack chain starting with downloading the MSI installer from the 3CX website or by sending an update to an already installed desktop application on both Windows and macOS from users using the application. Malicious activity in the campaign included signaling to ***actor-controlled infrastructure***, deployment of ***second-stage payloads***, and, in a small number of cases, ***hands-on keyboard activity***.

Fortra's GoAnywhere MFT

Reports surfaced in mid-February regarding the exploitation of the zero-day CVE-2023-0669 ***remote code injection*** vulnerability affecting GoAnywhere MFT, which was being exploited by the ransomware group Clop in a massive campaign targeting the file transfer solution. The group claimed ***to have compromised more than 130 organizations*** in a worldwide campaign.

VMware servers

A massive exploit campaign targeting VMware ESXi servers globally to deploy ransomware was reported in February 2023 by exploiting a ***remote code execution vulnerability tracked as CVE-2021-21974***, discovered in 2021. The exploit campaign deployed ESXiArgs ransomware, a newly discovered malware variant that targeted, at first, more than 500 servers, to later spread globally with an ***estimated reach of more than 3200 VMware ESXi devices/IP addresses*** encrypted by the ESXiArgs ransomware attack.

Other vulnerabilities:

such as CVE-2022-30190, also known as Follina, continue to be highly exploited, with attacks observed during the beginning of the year by different threat actors, including Russian ***hackers*** and ***advanced persistent threat (APT) groups.*** The malicious actors behind Cuba have used vulnerabilities CVE-2022-22965 or Spring4Shell and CVE-2022-41080 and Play ransomware to target vulnerable Microsoft Exchange servers.

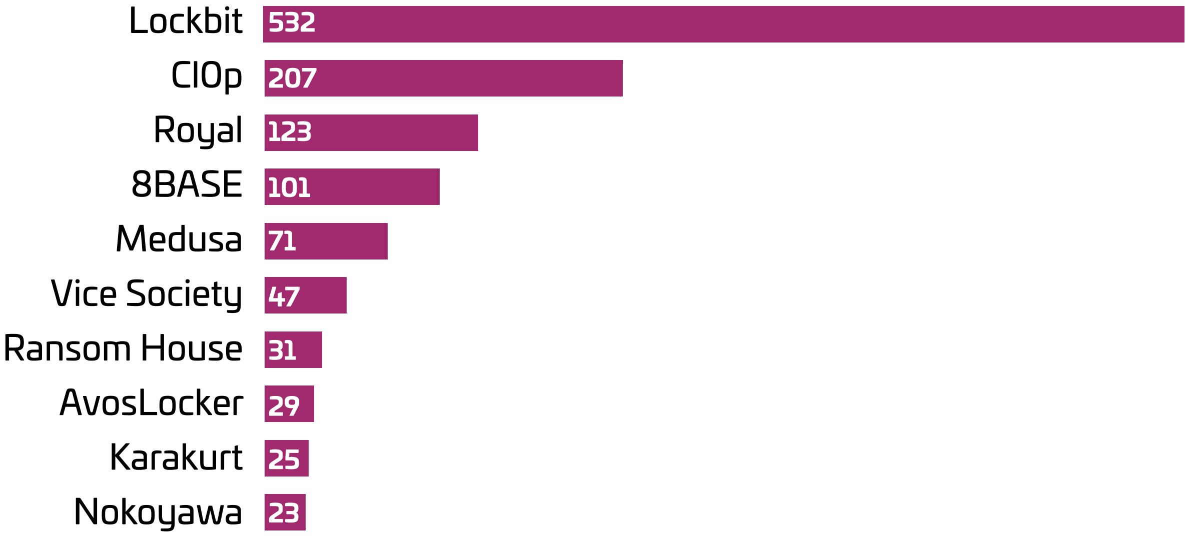
Finally, it is worth noting that the expanding trend of using software vulnerabilities by threat actors in cyberattacks to infect targeted systems continues. Ransomware, Log4shell, Dirty COW, Zerologon, and Drupalgeddon2 vulnerabilities stand out among the remaining observed vulnerabilities that have been exploited for ***malware propagation***.

02 RANSOMWARE

During the first half of 2023, S21sec's Threat Intelligence team continued to actively monitor the activity of threat actors on more than 60 ransomware group blogs on the Deep Web, Dark Web and underground forums. According to the telemetry collected, the global ransomware threat landscape has intensified with a total of 2127 attacks.

The number of attacks covers exclusively the observed public activity performed by threat actors through their communication channels or ***Dark Web*** extortion blogs.

Top 10 threat actors during the first half of 2023



If in ***2022*** we witnessed a scenario that reached ***more than 2900 attacks*** (1466 and 1487 attacks observed in the first and second half of 2022 respectively), ***so far this year alone 2127 attacks have been recorded***.

The data shows a worrying trend in terms of the increase in ransomware attacks as, while the number increased slightly from 1H2022 to 2H2022, with an increase of approximately 1.43%, ***2023 has seen an increase of approximately 43% compared to the second half of the previous year***.

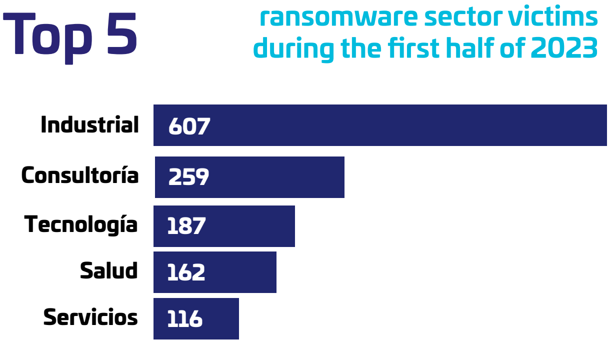
This increase in the number of attacks may also be due to the *increase in new ransomware families* observed so far this year, with a total of 21 new ransomware operations recorded (including *Medusa, DarkBit, Abyss, Vis Vendetta, DarkPower, Dunghill Leak, Money Message, Akira, Trigona, CrossLock, RA Group, Rancoz, 8BASE, Rhysida, BlackSuit, DarkRace, MalasLocker, CryptNet, Abyss, NoEscape, and Cyclops*).

Considering the previous semesters, the number of new ransomware families has been gradually increasing, showing a slight increase in 2022, where 9 and 10 new ransomware groups were observed showing activity in the first and second half of the year. In 2023, the figure rises to a total of *21 new operations observed*, confirming an upward trend in the emergence of new ransomware groups.

MOST AFFECTED SECTORS

Ransomware statistics

As for the most affected sectors during the first half of 2023, manufacturing stands out in first place with 607 attacks, followed by consulting with 259 attacks and in third place the technology sector with 187 attacks.



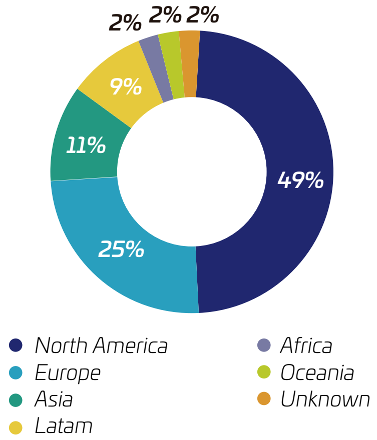
MOST AFFECTED COUNTRIES

Ransomware statistics

As in previous semesters, *ransomware groups* have mostly targeted targets located in North America, especially in the *United States, with a total of 1,009 attacks*.

Europe accounts for 25% of the total, with the *United Kingdom, Germany and France* being the most affected countries with *124, 82 and 68 attacks* respectively.

As for ***Spain***, a ransomware incident figure of ***42 attacks*** was recorded in 2023, with LockBit being the most prominent threat (17 attacks), followed by BianLian (4) and BlackCat along with RansomHouse and Stormous (with 3 attacks each). While the trend analysis at national level shows a 41% increase in terms of the number of incidents during the first and second half of 2022 (34 and 48 incidents), so far this year this trend is slightly down by 12.5% compared to the previous six months.



Portugal shows an affectation of ***11 companies attacked***, which represents a stability in the number of attacks compared to the previous semester. As for the most prominent families that have targeted Portuguese companies, LockBit remains the main threat, matched by the new ransomware group 8BASE, with 2 attacks each.

Finally, ***France*** reflects an affectation of ***68 companies attacked***. The most prominent families are LockBit with 27 attacks, in second position Play with 7, and in third position Cl0p with 5.

MOST ACTIVE RANSOMWARE GROUPS

LOCKBIT

LockBit continues to be the most active threat group of the year, showing an evolution in terms of its increasingly sophisticated tactics, techniques and procedures in its attacks. During 2023, its attacks traced back to *a total of 532 victims*, with a special focus on companies belonging to the manufacturing, consulting and technology sectors, located mainly in *the United States, France and the United Kingdom*, demonstrating its ability to carry out large-scale attacks targeting all industry verticals and sectors.

The ***Ransomware-as-a-Service (RaaS) operation*** emerged in September 2019 and has since been characterized by a focus on data and extortion of its victims with the primary goal of monetizing its attacks through ransom payments. In addition, it has demonstrated its ability to compromise computer systems by encrypting data quickly.

Throughout its evolution, the malware has undergone three substantial updates, moving from LockBit Red to LockBit Black and finally LockBit Green. The LockBit affiliates operate independently, resulting in significant variation in the tactics, techniques and procedures (TTP) used in their attacks. The group has also exploited vulnerabilities in various software, including Fortra GoAnywhere Managed File Transfer, PaperCut MF/NG servers, Apache Log4j2, F5 BIG-IP and BIG-IQ, and Fortinet devices, to gain initial access.

It has recently been observed that the group has ***expanded its reach*** by adapting a new variant of its ransomware capable of compromising systems based on ***Apple M1 chips*** and embedded systems, demonstrating its ability to adapt and abuse new vulnerabilities and potential targets. Among the most common ***TTPs*** employed by ***LockBit*** are infiltration through malicious ***email malspam campaigns, exploitation of known vulnerabilities, unauthorized remote access and use of stolen password management tools***. In addition to the use of evasion techniques to circumvent systems and maintain their permanence for as long as necessary to achieve their objectives.

MOST ACTIVE RANSOMWARE GROUPS

BLACKCAT

The BlackCat ransomware group, also known as **ALPHV**, has been active since November 2021 and is known for employing *double extortion tactics*. Following its emergence, it has established itself as one of the most prominent ransomware operations and has targeted various industries and organizations worldwide, amassing *an extensive history of leaking stolen data* on its Tor extortion websites to pressure victims to pay the ransom.

BlackCat is known to use techniques such as *phishing campaigns and exploiting vulnerabilities* in servers to gain initial access to systems, especially in widely used enterprise software. During 2023 it has been identified exploiting *vulnerabilities in Veritas Backup Exec software* to gain initial access to targeted systems.

In addition to data encryption, the **BlackCat** group has been observed to have adopted *new and much more aggressive tactics* that have involved the public disclosure of stolen data containing sensitive information about their victims to increase pressure on them to pay the ransom. They have also *cloned victims' websites* to publish the stolen information.

The evolution of the **BlackCat/ALPHV** group and the number of attacks observed, amounting to more than ***two hundred victims*** during the first half of 2023 indicates a greater maturity in their operations and an increased ability to carry out ***large-scale attacks***.

So far this year, ***216 officially known ransomware attacks*** have been recorded and claimed by the threat group. Its victimology includes ***companies in the manufacturing sector, followed by consulting and technology***, located primarily in the United States, Canada, the United Kingdom, and Australia.

MOST ACTIVE RANSOMWARE GROUPS

CLOP

Cl0p is a ransomware group that emerged on the threat landscape in February 2019, and employs the *double extortion technique, threatening to leak stolen data on its extortion blog known as "CLOP Leaks"*, to pressure victims into paying the ransom for data recovery.

So far this year **Cl0p** has claimed approximately *207 victims publicly*, with companies in the *financial, consulting, technology and manufacturing sectors* being the most affected, with a geographic focus especially targeting the United States, United Kingdom, and Canada, as well as other countries worldwide to a lesser extent.

Due to its recent activities, the U.S. government has positioned it as a major threat, offering a $10 million reward for information linking **CLOP Ransomware Group** to a foreign government.

Cl0p has a history of exploiting zero-day vulnerabilities in massive worldwide campaigns for data theft and extortion of victims, and among the operations associated with the group observed so far this year, the following stand out:

February

Zero-day exploit campaign in GoAnywhere MFT, in February Cl0p claimed to have targeted more than 130 organizations through attacks exploiting the *zero-day vulnerability CVE-2023-0669 in GoAnywhere MFT*, claiming that, after compromising the victims' vulnerable servers, they could perform lateral movement on their networks and deploy ransomware payloads to encrypt the systems. The attacks were linked to the TA505 threat group, known for deploying Cl0p ransomware in the past.

April

PaperCut exploit campaign, information was disclosed last April regarding a massive exploit campaign exploiting vulnerabilities in the *PaperCut application server for data theft, tracked as CVE-2023-27350 and CVE-2023-27351*, which allowed attackers to perform remote code execution and unauthenticated information disclosure. Cl0p had been exploiting PaperCut vulnerabilities since April 13 for initial access to corporate networks and deploying the TrueBot malware, previously linked to the ransomware operation.

May

MOVEit Exploitation Campaign, at the end of May, a massive *zero-day vulnerability campaign tracked as CVE-2023-34362* was reported is a zero-day vulnerability in MOVEit Transfer software. According to Microsoft the exploitation of the vulnerability was attributed to the threat actor tracked as Lace Tempest (Storm-0950, overlaps with FIN11, TA505), a financially motivated actor known for ransomware operations and linked to running the Cl0p ransomware group's extortion site on the Tor network. In terms of victims, Cl0p has claimed more than 100 companies via its Dark Web leak blog, with the total number of affected companies unknown.

MALWARE

03

Malware-as-a-Service has become a widespread practice among cyber criminals. This model allows attackers to rent or purchase access to malicious tools and services. This has enabled less sophisticated threat actors to launch complex attacks. The availability of off-the-shelf malicious services has increased the number and diversity of threats in today's landscape. Following this business model, infostealers have become increasingly prominent.

Infostealers

Infostealer malware is a malicious program that can be installed on victims' computers through phishing techniques, downloading, or accessing malicious software or websites. This type of malware is aimed at *stealing information* such as login credentials, usernames, clipboard credentials, and cookies, obtaining 2FA or credentials stored in browsers.

Many infostealers are for sale under a ***Malware-as-a-Service*** model in underground forums. They have also managed to establish a botnet-like structure, where a threat actor has control of infected computers or bots, e*stablishing persistence and maintaining constant communication* with the C2, allowing it to continue to retrieve credentials and information from computers while deploying other malware.

Lumma Stealer

Lumma is an infostealer that can be purchased from Russian-speaking hacking forums. The malware's operators advertise that the stealer has *an average success rate of 80%* and includes information on the type of files it steals, the operating systems it operates on (from Windows 7 x32 to the latest Windows 11 x64 updates), and its price. Regarding this last aspect, there are different plans to purchase it, depending on the number of services the client wants. It also has technical assistance, which shows *the great structure behind this stealer*.

The C2 servers store the data extracted from the victims and are structured to make it easy for the attacker to manage the stolen data. Among the capabilities of C2 is the ability to employ various filters to divide the data by nationality of the victim, IP, type of data extracted, etc.

Typhon Reborn Stealer

A recent version of Typhon Stealer, a .NET application that, like other stealers, focuses on *collecting sensitive user information* stored on the device.

Typhon Reborn only affects the Windows operating system. Its previous version had keylogger, mining, and worm functionalities, but these have been removed in Typhon Reborn to move them to separate projects. However, this stealer can still steal information from browsers, from cookies to credit card and autofill data, and information from crypto wallet browser extensions that may exist on the device. It also steals information related to user sessions from instant messaging apps, gaming apps, and VPN providers.

Amadey

Amadey is a sophisticated malware of Russian origin, first discovered in 2018. It has been used in targeted attacks against government organizations and critical infrastructure companies. It is known for its advanced capabilities, which include *evading detection and exfiltrating sensitive data.*

Amadey is available on the Dark Web or underground marketplaces under the ***Malware-as-a-Service*** model. This malware is typically distributed through spam e-mails with malicious attachments or links. However, a major infection vector for **Amadey** is exploit kits such as RigEK and Fallout EK.

Once installed on a victim's system, **Amadey** can perform a variety of malicious actions, such as *stealing sensitive information, installing additional malware, and executing commands on the compromised system*.

Rhadamanthys

Rhadamanthys is an infostealer active since mid-2022. The malware is designed *to steal information, such as login credentials, from several applications, like web browsers, e-mail clients, and cryptocurrency wallets*. It is primarily distributed through malicious Google ads from which an executable file is downloaded, posing as a legitimate installer.

This malware can steal credentials stored in browsers and from different applications (such as KeePass, Outlook, Thunderbird) and services (FTP, Discord, Tox, or Telegram), in addition to stealing from cryptocurrency wallets belonging to services such as ByteCoin, Bitcoin, Binance and Armory.

04

MOBILE MALWARE

Mobile devices have become an essential part of our daily lives. The growth of smartphone users has gone hand in hand with a worrying increase in the proliferation of mobile malware, especially on the Android operating system.

From malicious apps to ransomware and Trojans, the Android ecosystem has been flooded by a variety of malware that seeks to exploit the security vulnerabilities present in these devices.

However, 2023 has seen an increase in malware on the iOS operating system, used on iPhone and iPad devices.

Malware Nexus

At the beginning of March this year, a new Android malware family was detected, ***a new SOVA variant called Nexus.*** This new banking Trojan could be seen on several hacking forums using the ***MaaS (Malware-as-a-Service)*** model to offer its services on a rental or subscription basis. These services can be found through private Telegram channels or on underground forums. In this case, Nexus malware can be rented for $3,000 per month. This business model is useful for non-technical threat actors who need support for the malware and is widely used in Android malware, where developers use this MaaS model to offer their services to a wider audience. This model allows for more efficient monetization of the infrastructure used by customers.

This banking trojan has the typical functionalities of this malware family, such as *credential theft or SMS interception*. In addition, it has been proven that this malware *can impersonate 450 banking institutions*, which makes it potentially dangerous.

Fleeceware Joker

Joker is a family of fleeceware. It is one of the most well-known malware families in the Android environment, capable of *defrauding via SMS and payments through WAP* (Wireless Application Protocol).

The Joker malware has a JavaScript interface that runs on the pages that make use of the WAP protocol to carry out the fraud and allows the following commands to be executed in the application: close web page, send SMS, delete collected messages, check communication with C2, send a request to the C2, etc.

WAP is a specification for a set of communication protocols to standardize how wireless devices like cell phones can access the internet. Its use disappeared under the HTTP protocol. *It works similarly to the traditional client-server model* but uses an additional WAP gateway as an intermediary between the client and the server. This gateway belongs to the carrier and allows charging for services directly on the carrier's bill.

In this way, the fleeceware makes money by silently subscribing its applications to premium services without the user being aware of it.

Gigabud RAT

At the beginning of 2023, a ***new remote access trojan (RAT)*** campaign called ***Gigabud*** was distributed in Thailand, the Philippines, and Peru.

The distribution was carried out by *impersonating mobile applications of government entities, banking institutions, and online stores*, forcing the user to subsequently enter their access credentials, being able to have accessibility permissions. It can also record and capture screenshots and screen overlays.

SpyNote & Hook malware

A new variant of the SpyNote banking spyware started to be distributed in early 2023 *to infect specific banking applications* to steal the user credentials of its customers.

SpyNote malware, also known as ***CypherRAT***, launched this new version called SpyNote.C *to increase its attack capabilities* and obtain more data and information from victims' devices. In this way, SpyNote.C has been distributed against banking institutions mainly in Asia but also slightly affecting Germany.

Its techniques include *keylogging* and overlay techniques *to obtain the victim's personal information*, banking/financial data, and social network credentials.

Operation Triangulation

In June 2023, an espionage campaign targeting devices with the iOS operating system called ***Operation Triangulation*** was made public.

Researchers of this campaign revealed *a general infection sequence* in which a targeted iOS device could receive a message via the iMessage service with an attachment containing an exploit. Without user interaction, the message *triggers a vulnerability that allows malicious code execution*.

Through the exploit, several successive stages were downloaded from a Command and Control (C&C) server, which include *additional exploits for privilege escalation*. After a successful exploitation, a payload was downloaded from the C&C server that runs with root privileges and can *collect system and user information*, as well as *execute arbitrary code* downloaded from the C&C server.

05 FINANCE SECTOR

*In the first half of 2023, several **banking malware families focused on using the ATS (Automatic Transfer System) framework**. This helps them automate the fraud chain, both the infection process and the exfiltration of data/information.*

In this sense, the following are the banking malware identified using ATS:

PixPirate

Identified in February 2023, this Android banking Trojan, allegedly Brazilian, is encompassed in a new generation of malware that can exploit the Pix instant payment platform to insert malicious money transfers through the Automatic Transfer System (ATS) process.

Its capabilities focus on compromising legitimate banking credentials to perform ATS attacks, intercepting SMS messages, and deploying measures to prevent uninstallation.

PixPirate's actions have mainly focused on Latin American countries, specifically Brazil, Mexico, and Peru, while its distribution in those countries is through malicious apps hosted on Google Play that impersonate other legitimate apps.

Xenomorph.C

A new version of the Xenomorph banking Trojan, named Xenomorph.C, is found making full use of the ATS framework.

This new capability allows Xenomorph.C to automate processes in the attack chain, enabling operators to steal cookies from web browsers, augment their accessibility services, and implement the ATS process to insert malicious bank accounts into the payment processes of banking applications. Moreover, Xenomorph.C's targets are broad, focusing on banking applications and crypto wallets from countries like Italy, Spain, Portugal, Canada, Poland, and the United States.

GoatRAT

Like PixPirate and Xenomorph.C, the GoatRAT banking Trojan has also been observed using the ATS framework, previously obtaining accessibility permissions on the victim's device.

Although GoatRAT was created as a remote tool to take control of the victim's device, the new version of the banking Trojan allows its operators to have additional capabilities to obtain data and information from banking applications. In this case, this new version of GoatRAT can transfer money from infected devices to cybercriminals' bank accounts.

Its victimology is mainly focused on Brazil, using the Pix instant payment system to carry out the ATS process.

Apart from the malware targeting the ATS framework, other banking malware campaigns have taken place in these first six months, with several being identified as very aggressive and having specific targets and victimology.

Given the increase in such activity, some of these campaigns that have had a relevant impact are presented below.

Qbot

During this period, a new Qbot banking Trojan campaign was identified, using fake corporate e-mails to send spam with an infected attachment. These attachments were previously stolen files (mostly PDF) infected with Qbot.

The attachments used in the Qbot campaign had the characteristic that they were addressed to the recipient with their name, which could lend greater credibility to the email and document. Once the victim opened the document and downloaded a WSF file, the malware was executed and could extract passwords and cookies from web browsers, intercept and view emails from the inbox, intercept device traffic, and access the device's system.

CMDStealer campaign

In the CMDStealer campaign, the perpetrators deploy Living Off the Land Binaries and Scripts tactics, i.e., they recognize executable files, scripts, or libraries that already exist on the target/infected system and can later manipulate them to activate malware functions. Likewise, CMD scripts allow cybercriminals to avoid detection by security measures on the target device.

The attack vector, as seen in previous campaigns, is mainly phishing. Victims receive e-mails in Portuguese or Spanish with attachments about urgent matters, such as warnings and notifications from official agencies that lead the potential victim to enter their banking credentials.

Operación Magalenha

One of the most recent campaigns identified is "Operation Magalenha", executed in the first four months of 2023, impacting more than 30 banking entities in Latin America, Spain, and Portugal. Likewise, its development and distribution are attributed to cybercriminals from Brazil due to the use of Portuguese in the infrastructure configuration and the malware distribution actions.

The campaign process began with phishing e-mails impersonating various energy and governmental organizations. These e-mails could contain a URL redirected to a malicious login page or a compromised document.

The infection process was based on entering credentials on the malicious login page or downloading the compromised document. Once one of the two actions was performed, a malicious Visual Basic script was executed, which was used to download and run a loader that, in turn, executed two variants of the Peeping-Title backdoor.

Once both variants of PeepingTitle were loaded and executed, the malware could obtain login credentials, personal information, and device access to compromise banking applications. In turn, the backdoor would have spyware functions, full control of the infected device, screenshot capabilities, execution of complementary malware, and reconfiguration of the device, among others.

APT activity against the banking sector

Advanced Persistent Threats (APTs) are among the most relevant cyber threats due to the complexity of their actions and operations, as well as the deployment of their TTPs.

In this regard, the ***APT Blind Eagle*** (APT-C-36) has been identified as being involved in extensive cyberattacks against financial institutions and banking entities in Latin America and Spain, among other countries.

The attack starts with an e-mail impersonating a national financial regulatory body. The potential victim receives the e-mail with an attachment that, once downloaded, starts a second download of a malicious file from ***Discord's Content Delivery Network*** (CDN) with the final ***AsyncRAT*** payload.

With the final injection of AsynRAT into the financial institution's computers, cybercriminals could create persistence, connect to endpoints, and perform tasks such as information exfiltration and privilege escalation.

Regarding ***APT-C-36***, the group defines itself as a South American collective focused on cyber espionage and active since 2018, focusing its actions mostly on the financial sector.

HACKTIVIST TREND

The focus of hacktivist actions and operations has centered on the conflict between Ukraine and Russia, which has had a *significant impact on the banking and financial sector*, that has been affected by various cyberattack campaigns.

In the first half of 2023, a large number of cyber operations against European, American, and Russian banking institutions were observed. Notable among these campaigns are those carried out by the **NoName057(16), KillNet, Anonymous Sudan, Kvazar, Bloodnet, IT Army of Ukraine, and CyberArmy of Russia groups,** among others. The vast majority of operations carried out by pro-Russian hacktivist groups such as **NoName057(16), CyberArmy of Russia and KillNet** against European banking entities mainly respond to four actions:

- **Sanctions packages** approved and executed by the European Union and the United States.
- **Alleged activities** of organizations and entities from Russophobic European countries.
- **Planning and delivery** of military, logistical or economic aid by the EU (European Union) to Ukraine.
- **Ukrainian cyber activity** against Russian interests and infrastructures.

In the context of these actions, the pro-Russian groups have activated their cyber operations against banking entities in countries such as *Denmark, Sweden, Latvia, Lithuania, Estonia, Finland, Germany, Romania, France, Italy, Switzerland, the United Kingdom, Poland, and Italy*, among others. Some of these operations are specifically directed against the banking system due to its criticality and importance, or simply involve mass cyberattacks with multiple impacts on the sector.

Regarding the type of cyberattack, the persistence of *DDoS attacks has been observed*, although in various cases database publications, defacement attacks, and use of botnets have been identified. In this case, one of the most recent large-scale cyberattacks by KillNet and Anonymous Sudan against the Bank of Investments of Europe stands out, which suffered disruptions in its web services.

On the other hand, more sophisticated cyberattacks against Russian banking entities and systems have been carried out by the **IT Army of Ukraine** collective. These attacks, *mostly DDoS in nature*, were also accompanied by actions of disruption of payment systems and network intrusion, causing banking applications and systems to become inaccessible.

In one of the most recent operations carried out by another pro-Ukrainian hacktivist collective, called **Cyber Anarchy Squad**, various cyberattacks were launched against the Russian provider JSC Infotel, who handles online interactions between Russian banking entities. This type of cyberattack, as mentioned above, *demonstrates the capacity for action of these collectives and the impact* they can have on financial systems.

06 ENERGY SECTOR

*Considering the threat landscape targeting the energy sector in H1 2023, the **cyber risk to the industry increased** because the sector is still an attractive target for cybercriminals. 2023 has seen **a wide range of threats** ranging from data breaches to ransomware attacks to malware and advanced persistent threat (APT) groups targeting the industry for the interests of other nation-states or simply politically, ideologically, or economically motivated threat groups or actors.*

Threats are attacking oil, gas, electricity, renewable energy, nuclear, and utility companies and are likely to remain one of the most targeted, according to forecasts for the rest of 2023. This is due to the interest of threat actors in the sector and the change and evolution seen in ***APT groups***, which target the industry by targeting critical infrastructure, operations technologies (or OT networks), SCADA (Supervisory Control and Data Acquisition) systems, or Industrial Control Systems (ICS) data control technology, with increasingly sophisticated capabilities.

In addition, the global geopolitical situation and the increase in hacktivist activity by groups working in favor of Russian interests is yet another element in the scenario of risks and threats to the sector.

Within the cyber activity by APTs, the following stand out:

► Sandworm

BE2 APT, Quedagh, UAC-0082

A Russian-sponsored advanced persistent threat group. The group has been operational since 2014 and consists of 3 subgroups, each focused on specific activities. Kamacite serves as an access and enablement group. Electrum performs actions on targets, including disruption of Industrial Control Systems (ICS), and TeleBots performs cyber sabotage against a wider range of targets. Earlier in the year, Sandworm has been seen targeting companies and industry bodies in attacks in which it has deployed a group of wipers through Active

► Lazarus

Bluenoroff, Stardust Chollima, BeagleBoyz

Is a North Korean state-sponsored threat group that primarily conducts financial cyber operations and has been active since at least 2014. In March 2023, it was credited with deploying the VEILEDSIGNAL multi-stage modular backdoor activity designed to execute shellcode and steal corporate credentials from the device of an employee of stock trading automation company Trading Technologies and used them to move laterally through 3CX's network and conduct an attack on 3CX's supply chain.

▶ In April 2023, Microsoft posted a report detailing past campaigns perpetrated against U.S. critical infrastructure by a subgroup of the Iranian-linked group APT35 (Mint Sandstorm), who reportedly targeted U.S. seaports, energy companies, transit systems, and major gas and electric utilities between late 2021 and mid-2022. The group specializes in cyberespionage and theft of sensitive information from high-value targets. Its operations aim to gain initial access by exploiting vulnerable public devices through phishing campaigns.

▶ In mid-May, malicious activity targeting critical infrastructure organizations in the United States developed by the Chinese-sponsored threat actor Volt Typhoon was reported, aimed at intelligence gathering, focusing on developing capabilities to disrupt Asia-U.S. communications for future geopolitical issues.

DATA BREACHES

In data breaches, the sector has also been the victim of *confidential and sensitive information leaks* because the companies are highly profitable and can pay a ransom in case of extortion. In addition, the energy sector is vital to the functioning of a country's society and economy, so, in many cases, attacks *can cause significant disruptions to services*. Data breaches are particularly interesting to threat actors with political or ideological objectives who intrude and sabotage industrial systems to gain greater recognition in the cybercrime ecosystem.

MAIN THREAT ACTORS

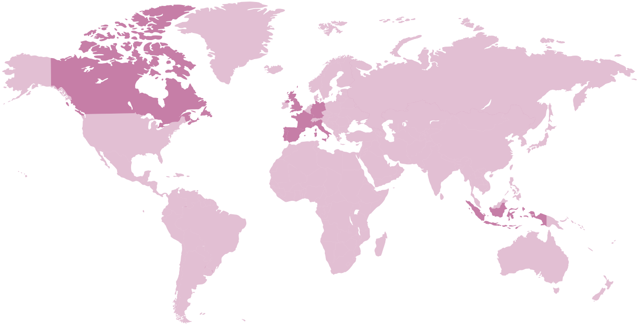
Among the observed threat actors, the group known as Dark Angels stands out, who in March announced a data breach of 3 TB of e-mails and corporate information of more than 10,000 employees of a company in Latin America, specialized in Infrastructure, Energy, Oil and Gas, Mining and Industry projects.

Another actor that has been involved in massive leaks is SiegedSec, a group that appeared the alleged affectation of the U.S. company dedicated to hydrocarbon exploration on its Telegram channel in February 2022 as a branch of the GhostSec hacktivist group, linked to the well-known hacktivist collective Anonymous, specialized in gaining access to confidential information of targeted organizations to leak data, as well as in carrying out the defacement of their victims' websites. On April 16, 2023, the group posted the alleged affectation of the U.S. company dedicated to hydrocarbon exploration on its Telegram channel.

As for the threat from ***ransomware groups***, this continues to be a growing risk in the industry. Several new variants were identified in 2023 that affected organizations and demanded large financial sums for data recovery, and *approximately 50 public cyber incidents were recorded* that have affected the industry.

Attacks monitored on the ransomware groups' extortion blogs show that the most active families have been **LockBit** (18), **BLackCat** (5), and **Royal** along with **Cl0p** (4 attacks each). The remaining ransomware groups that have attacked energy companies include **Vice Society** (3), **Play** (3), **Medusa** (3), **Qilin** (2), **Monti** (1), **Stormus** (1), **BianLian** (1), **Black Basta** (1), **Unsafe** (1), **Mallox** (1), **8BASE** (1), and **RansomHouse** (1).

Geographical focus shows that ransomware groups mainly target companies in the United States (15), accounting for 30 % of all targeted attacks, followed by countries such as Germany, Indonesia, the United Kingdom, France, and Italy (3 attacks each). Spain and Portugal have 2 attacks each so far this year.



Given valuable information such as *intellectual property data, critical infrastructure information, contract data, and customer and supplier information,* ransomware groups carry out encryption and extortion on their victims, with the following ***examples being the most prominent in 2023***:

January

A municipal company in Portugal was the victim of a cyber incident that affected some of its customer services. According to sources from the municipal agency, the attack did not affect the operation of essential public services such as water supply and sanitation. However, given the temporary suspension of some citizen attention services, the company enabled contact channels (via WhatsApp) for citizen formalities.

March

Two Spanish companies which provide energy services such as electricity production, were affected by the Stormous and Vice Society ransomware groups.

June

The Canada's leading integrated energy company, has suffered a cyberattack that affected payment operations at gas stations nationwide.

MALWARE-AS-A-SERVICE

On the other hand, the presence of malware in the energy industry also is still a concern, especially in a massive cybercrime ecosystem where the ***Malware-as-a-Service (MaaS)*** trend has allowed the entry of many low-skilled, technical players who contract these services, thus optimizing their efforts to target the industry in highly professional, targeted attacks.

Examples of malware that have specifically targeted industries include:

▶ Regarding the use of ***wipers***, a new variant of data-wiping malware called ***SwiftSlicer***, which targeted unknown Ukrainian organizations, was reported in February 2023, in addition to a new wiper called ***NikoWiper***, which was used to attack an undisclosed Ukrainian energy provider in October 2022. Russian-aligned threat actors have been deploying data wipers since the initial invasion of Ukraine in February 2022. The wipers' deployment aligns with previous Russian-sponsored cyber operations against Ukraine and other countries, in some cases targeting critical infrastructure.

▶ A new malware threat called *COSMICENERGY*, which targets operational technology (OT) and industrial control systems (ICS), was reported in March, linked to a threat actor of Russian origin. The malware is designed to cause power outages by interacting with IEC 60870-5-104 (IEC-104) devices, such as remote terminal units (RTUs), commonly leveraged in electrical transmission and distribution operations in Europe, the Middle East, and Asia. Among the most significant similarities found, it compares to *INDUSTROYER* and *INDUSTROYER.V2*, both malware variants deployed in the past to affect electricity transmission and distribution. *COSMICENERGY* also has technical similarities to other OT malware families developed or packaged with Python or used open-source libraries for OT protocol implementation, including *IRONGATE*, *TRITON*, and *INCONTROLLER*.

▶ In March, a campaign to spread a new stealer called ***SYS01stealer*** was reported, targeting employees in critical government infrastructure and other sectors. Threat actors targeted Facebook business accounts by using Google ads and fake social network profiles promoting games, adult content, decrypted software, etc., to download malicious files to steal confidential information, login data, cookies, business account information, and Facebook ads.

▶ In May, security researchers reported a new version of ***PowerStar***, a malware reportedly used by the cyber-espionage group known as Charming Kitten to target companies in the industry. ***PowerStar*** features advanced techniques, including IPFS (Inter-Planetary File System) and public cloud hosting for decryption and configuration. It is distributed through sophisticated spearphishing attacks and is an updated version of the ***CharmPower*** backdoor.

HACKTIVIST GROUPS

As for the threat coming from ***hacktivist groups***, since the outbreak of the war conflict of Russia's invasion of Ukraine, pro-Russian hacktivist threat groups have executed targeted operations and attacks *against Ukraine and NATO (North Atlantic Treaty Organization) countries*, especially on those companies in the energy sector, not only to undermine Ukraine's resistance persistently but also as an ideological claim through cyber-attacks on humanitarian aid and shipment of military equipment and infrastructure to the country. The most prominent groups are **KillNet, Anonymous Sudan, Anonymous Russia, NoName057(16), and Cyber Army of Russia**.

It is worth noting that, during the first half of the year, there has been a tendency to collaborate and create alliances between these groups, *targeting European energy company websites* to vindicate their attacks. Likewise, an effort has been made to align these ***groups with APTs, ransomware groups, or other cybercriminal actors***, including outstanding collaborations that include the use of *tools and botnets* (TeslaBotnet, DDoSia Project) that allow a greater reach and impact in their attacks.

Other hacktivist groups that have staged attacks against the energy sector include the group known as **GhostSec**, who claimed earlier this year to have carried out the first ransomware attack against an RTU (Remote Terminal Unit) used in ICS environments during the *operation known as* ***#OpRussia*** *in support of Ukraine*.

It is also worth mentioning the use of vulnerabilities in attacks by threat actors, which has put the sector at risk from the massive exploitation of zero-day vulnerability exploitation campaigns or vulnerabilities already known in unpatched systems, in some cases due to obsolete technology. Some examples:

February

In February, the ***ClOp ransomware group*** claimed to have stolen confidential data from more than 130 organizations by exploiting a zero-day vulnerability CVE-2023-0669 in Fortra's file transfer software, GoAnywhere MFT, days before the vulnerability was disclosed. Some energy companies confirmed that they had been affected by the campaign.

The same month warned of *a massive campaign targeting VMware ESXi* servers globally to deploy ransomware by exploiting a remote code execution vulnerability tracked as CVE-2021-21974. According to researchers, the ransomware campaign may have affected thousands of organizations worldwide since Feb. 2, and among the victims was an Italian energy company which generates and supplies electricity and delivers natural gas.

May

In late May, news broke of a massive exploitation campaign of ***MOVEit***, a critical zero-day vulnerability tracked as CVE-2023-34362, in the secure managed file transfer ***(MFT) software MOVEit Transfer***. Among the victims were some energy companies who confirmed that they were affected by the campaign.

Finally, supply chain attacks stand out, where companies in the sector are affected due to their dependence on a wide network of suppliers, which can provide access and multiple entry points for cybercriminals. Examples of supply chain attacks:

SmoothOperator

In late March, energy organizations in the United States and Europe were the victims of cyberattacks targeting their communication systems through an attack on the supply chain of a of a technology company to push Trojanized software versions of Trading Technologies' X_TRADER software. The active supply chain campaign begins when the MSI installer is downloaded from the 3CX website, or an update is pushed to an already installed desktop application on Windows and macOS from users using the application. Malicious activity includes *signaling to actor-controlled infrastructure*, *deployment of second-stage payloads*, and, in a small number of cases, *hands-on keyboard activity*.

DEFENSE SECTOR

07

The escalation in the Russian-Ukrainian war has resulted in a spike in cyber activity against the defense industry by various actors, making it a sector hit by actions of various kinds, such as cyberattacks and information leaks, among others.

In the last 6 months, such actions against the defense industry have remained at the levels of the last half of 2022, while in the first six months of September, it has been possible to highlight the activity of the so-called insiders, as well as APT groups, and the realization of more complex cyberattacks whose goal is cyberespionage.

S21SEC
Cyber Solutions by Thales

Cyberthreats and cyberincidents

APTs

One of the biggest cyber threats identified has been the activity of ***APT groups***, whose relevance remains active, as do their actions in the defense industry environment.

In the first six months of 2023, these groups have been noted for deploying *malware and intrusion into systems* and servers motivated by information gathering (cyber espionage) and the possible deployment of additional malware to make lateral moves and distribute to other systems.

It is worth noting the presence and activity of the following APT groups in the defense industry:

Transparent Tribe (APT36)

This APT group, sponsored by ***Pakistani*** government agencies, directs its cyberattacks in Asia, with Indian government agencies as its main target. Among its latest actions, it has been possible to identify the ***deployment of malware*** in Indian Armed Forces agencies acting in conjunction with an Indian insider actor that leaked defense information to Pakistani agents.

APT28

this group, sponsored by the ***GRU*** (Russia), is one of the most active in this scenario, especially in the wake of the Russian invasion of Ukraine. Its latest actions have focused on launching ***spearphishing campaigns*** against government agencies abusing Roundcube servers by exploiting vulnerabilities CVE-2020-35730, CVE-2020-12641, and CVE-2021-44026. In this case, the campaign's main purpose was to gather military intelligence for military operations in the Russian-Ukrainian war.

Core Werewolf

Although ***Core Werewolf*** has not been categorized as an APT group, it is likely to be supported or sponsored by one or more countries. The group's activity dates to 2021, and in this first half of the year, it has carried out several actions against Russian organizations in the military industry. Its entry vector is ***phishing***, and those responsible for the campaign use the ***UltraVNC*** remote access program to perform additional malware deployment and privilege escalation actions. Their attacks include phishing mailings to Russian military agencies and offices. The phishing e-mails contained official documents opened by the victim, which led to the execution of malicious actions and persistence by creating tasks in the Windows Scheduler.

Kimsuky

The North Korean APT group Kimsuky has carried out high-impact actions in the last six months of 2023, one of them targeting ***the US Department of Defense*** login portal. In this case, it has been identified that the group spoofed the login page of the agency and may have obtained the login credentials of several DoD employees.

GALLIUM

Cyber threats from ***China*** are also among the most relevant when identifying cyberattacks against the defense industry. In this case, the ***GALLIUM*** group has maintained an active campaign against military organizations in Africa and Asia, highlighting its actions against the services of the South African Special Forces and military organizations in Nepal. For this purpose, ***GALLIUM*** has used ***PingPull*** to carry out cyberespionage tasks.

Gamaredon

One of the most active and impactful groups since the start of the Russian-Ukrainian war has been Gamaredon, whose activities have ***focused on Europe, NATO (North Atlantic Treaty Organization), the United States, and international organizations.*** During 2023 the group has been active in several ***spearphishing*** campaigns, one targeting the Latvian Ministry of Defense. This campaign attached a malicious document impersonating Latvian government agencies. Also, once the document was executed, access to the device's systems was obtained through the exploitation of the CVE-2017-0199 to obtain sensitive and confidential information about the victim in the different phases of the attack chain.

Cyberthreats and cyberincidents

Hacktivists

Regarding ***hacktivist activity***, these actions have focused on cyberattacks against defense agencies and industry companies in the context of the Russian-Ukrainian war. Among the most active groups are ***KillNet, Anonymous Russia, and CyberArmy of Russia***.

Among ***the most relevant cyberattacks***, we can highlight the compromises of the websites of *the National Security and Defense Council of Ukraine*, the intrusion into a company that manufactures ships for *the US Armed Forces*, and the cyberattack carried out against the company *Rheinmetall* (Germany).

All these hacktivist actions were ***aimed at shutting down the websites of the targeted companies/agencies***. In contrast, the actions were motivated by the support of these companies to Ukraine with the delivery of offensive weaponry.

Cyberthreats and cyberincidents

Insider

Insider activity within the military and defense agencies is one of the threats the defense industry has faced over the past six months.

This scenario where insiders are positioned as a threat, which is estimated to have a high impact, has had relevance due to the ***leak of several confidential documents of the Pentagon (United States)*** with content about the Russian-Ukrainian war. This leak, carried out by a member of the U.S. Air National Guard, was shared in numerous Internet forums and blogs with a high reach and whose content was exploited by other national organizations and ***hacktivist or APT groups*** to focus their possible new campaigns.

Similarly, ***authorities in Chile*** arrested a member of the Chilean military for introducing ***ransomware*** into the computer systems of the Chilean Armed Forces, which damaged personnel operations.

Likewise, both cases focus on how the organization's employees can jeopardize the entity's information, operability, and computer systems. Although their motivations were different, with the former having personal satisfaction as a supposed objective while the member of the Chilean Armed Forces had an ***economic motivation***, there is no doubt that a shutdown of the IT services of a military organization or the leak of its confidential information can compromise national security and allow external actors ***to take advantage of the vulnerabilities*** of the affected organization.

Cyberthreats and cyberincidents

Cyber-espionage

Cyberespionage tasks are positioned as one of the ***main actions carried out by external actors*** during political, geopolitical, social, or economic tension.

In this case, due to the current situation caused by the Russian-Ukrainian war and the instability generated at the international level, ***APT groups*** are carrying out ***cyber espionage operations against various military organizations***.

In this case, as happened in the last half of 2022 with the cyber actions ***against HIMARS missile systems***, between May and June, a campaign was identified with the deployment of ***PowerDrop malware*** that aims to perform cyber-espionage work on U.S. defense providers, specifically on aerospace agencies, coinciding with the development of missile programs.

PowerDrop has different capabilities and is not categorized as malware with new TTPs. Still, those responsible for its development and deployment have improved its ***initial access and persistence***, especially using PowerShell to facilitate other malicious actions to ***obtain administrator permissions*** while simultaneously exploiting the WM protocol.

In this sense, although its ***attribution remains uncertain***, it is not excluded that APT actors are behind its deployment due to the strategic nature of its objectives and the moment in which it has begun to be deployed.

HEALTHCARE SECTOR

08

Cyber activity in the healthcare sector has increased in the last two years, especially after the pandemic.

Although various cybercriminal groups, especially those aligned with ransomware groups, communicated that their cyberattacks would not target the sector, such statements are no longer valid because, since the end of 2021, more hospitals, clinics, hospital centers, and medical product providers have been compromised by cyberattacks of various kinds.

The first half of 2023

is no exception, as ***the healthcare sector has suffered several cyber incidents***, most notably in the United States and Europe, where cybercriminals and APT groups seek financial gain or use such cyberattacks for ***cyberespionage or simple disruption***.

Cyber threats

Gootkit

Australian authorities warned about the presence and distribution of ***Gootkit malware*** in the country's healthcare sector, ***causing disruptions and infections*** in the computer systems of several medical centers and hospitals.

To successfully carry out this infection process, the cybercriminals responsible for the campaign, through social engineering, trick the potential victim into downloading a malicious ZIP file from a WordPress website. Once the file is downloaded, another JavaScript file will be executed, allowing the cybercriminals ***to steal information from web browsers, use keylogging techniques, and take screenshots, among other functions***.

In this sense, medical centers and hospitals can see their internal information and patient and employee data and information compromised. Furthermore, the distribution of Gootkit against the healthcare sector *has only been detected in Australia* since the operators have added keywords against this sector in Australia. However, it is not ruled out that it could be reproduced in other countries.

Cyberespionage operations of the APT group Andariel

A document drafted by various U.S. and South Korean government agencies, including CISA (Cybersecurity and Infrastructure Security Agency) and South Korea's National Intelligence Service, shows how ***North Korean threat actors, sponsored by the DPRK*** (Democratic People's Republic of Korea), have an active cyberattack campaign against the healthcare sector in the U.S. and South Korea.

The main group suspected of such activity is the ***Lazarus Group***, which serves as an umbrella for many other subgroups attached to various government offices of the DPRK. In this case, the ***disruption and cyber espionage*** campaign is attributed to the Andariel Group.

Andariel, specifically in this campaign, has shown no signs of aiming for financial gain through ransomware distribution. Still, one of its main motivations is to perform disruptive cyberattacks ***to cripple medical services*** in hospitals and medical centers and perform cyberespionage tasks ***to collect sensitive information***.

In this sense, Andariel's TTPs are like those of other groups in the North Korean cyber scheme. These include having their ***own infrastructure***, initial access through exploiting vulnerabilities (CVE 2021-44228, CVE-2021-20038, CVE-2022-24990), performing lateral movement ***to distribute malware and collect information***, and using ***ransomware*** tools.

RedGolf APT

Continuing with the ***APT*** cyber threat, throughout the first half of 2023, suspicious activity was identified from the Chinese-sponsored ***RedGolf (Earth Longzhi) group***, a subgroup of APT41, *targeting healthcare sector entities in Southeast Asia and Eastern Europe*.

The group has been active for X years, using as initial access the exploitation of vulnerabilities in Internet-exposed devices such as *Citrix, Cisco, and Zoho*, allowing them to install malware such as ***Keyplug*** or ***PlugX*** on Windows and Linux systems.

However, during this new RedGolf activity, it was detected that the group has new techniques, such as ***exploiting vulnerable drivers*** or implementing high-impact targeted ***DDoS attacks***. Likewise, exploiting vulnerabilities continues, focusing on ***compromising Internet Information Services (IIS) servers or Microsoft Exchange servers*** to subsequently deploy ***CroxLoader*** or ***SPHijacker*** malware.

TimisoaraHacker Team

Following recent cyber incidents identified in the United States, U.S. government authorities warned about the growing activity of the ***cybercriminal group TimisoaraHacker Team (THT)***, which targets the healthcare sector globally.

Said group, active since 2018, would use ***ransomware*** as the final stage of its cyberattacks to have a greater impact while its actions against the healthcare sector remain active. In addition, it focuses on ***exploiting legitimate tools such as Microsoft BitLocker and Jetico's BestCrypt***.

Although information about the THT group is scarce, it is not excluded that its members come from Romania (due to the language of the source code and the name of the group, which refers to a city in Romania). THT could also have links to other more experienced cybercriminal groups such as DeepBlueMagic or APT41 (China).

In this case, the activity of this group, in conjunction with other APT groups, ***can lead to aggressive campaigns against the healthcare sector***, with various motivations, including ***financial gain*** and the ***collection of information*** for subsequent sale or use in malicious actions against third parties.

DDoS attacks via DNS NXDOMAIN

As we have seen, threat actors, whether cybercriminal groups or APT groups, have a wide range of techniques and tactics to carry out their malicious actions against the healthcare sector in this case.

However, these groups use various cyberattack techniques in their attack chain to have a greater impact and obtain more damaging results for the organization/affected party.

The US Healthcare Cybersecurity Coordination Center warned about some of these techniques, highlighting ***DDoS cyberattacks via DNS NXDOMAIN***.

These cyberattacks fall into the DDoS typology and ***target an organization's DNS servers***. Threat actors aim to overload the DNS server with a high level of requests, which may be invalid or non-existent, so the DNS server will spend resources and time locating non-existent requests. This would slow down the DNS server, ***making it impossible to access the web resources of the target entity***, impacting web pages, applications, and programs that hospitals can use to carry out any type of management.

Data Breaches

- One of the biggest concerns in the healthcare sector is ***data breaches*** after a cyberattack on the hospital or a hospital provider.

- In the first half of 2023, ***22 data breaches*** related to the healthcare sector have been counted by ***S21sec's Threat Intelligence team***, ***54.54% more*** than in the last half of 2022.

- These data breaches correspond mostly to cyberattacks of the ***ransomware type*** or simply due to the ***intrusion of third parties into the hospital's internal networks***. It is also worth mentioning that at least half of the data breaches recorded in the first half of 2023 correspond to hospital providers who initially suffered a cyberattack and subsequently saw their information and that of their customers in the healthcare sector compromised.

- These ***suppliers*** include ***manufacturing, software, and technology or consulting companies*** that work with the healthcare sector in automating processes and implementing technological improvements in their internal processes.

Hacktivist Trend

As for hacktivist activity directed against the healthcare sector, two groups have stood out for their actions against hospitals and medical centers in various countries.

Anonymous Sudan

Anonymous Sudan has carried out *cyberattack campaigns against Sweden, Denmark, and France* in response to the burning of the Koran by various groups. Anonymous Sudan's retaliation took the form of ***DDoS attacks*** against more than thirty private and public hospitals in Sweden and later in France, with minor impact.

Anonymous Sudan also focused on India, deploying cyberattacks against several hospitals and medical centers in that country in response to the treatment of the Muslim population in India.

KillNet y NoName057(16)

On the other hand, the other leading hacktivist groups directing their cyberattacks ***against the healthcare sector are KillNet and NoName057(16)***.

Their actions have been directed *against hospital centers in the United States and Europe* in response to the shipment of offensive military weaponry from these countries to Ukraine in the framework of the Russian-Ukrainian war.

In addition, ***KillNet has been involved in other international operations*** affecting the health sector, including one set up by various groups against Israel in response to that country's policy against Palestine.

09

INDUSTRIAL CONTROL SYSTEMS

*The conflict between Ukraine and Russia **has significantly increased cyberattacks** targeting critical infrastructure. Since the outbreak of the conflict in 2022, tensions have escalated, and cyber actions have become an important tool both sides use.*

***Cyberattacks on critical infrastructure**, such as power plants, transportation networks, and communication systems, have proven to be an effective way to weaken the opposing side and undermine its ability to defend itself.*

The first half of 2023

has seen actors supporting Russia in the conflict against Ukraine carry out attacks against critical infrastructure:

Cosmic Energy Malware

In May this year, a ***new malware*** called ***Cosmic Energy*** was discovered that is *capable of exploiting vulnerabilities in ICS protocols to gain access* to and control critical infrastructure systems. According to some experts, the malware could be linked to the Russian government.

This latest family of operational technology (OT)-targeted malware is *designed to interact with IEC 60870-5-104 (IEC-104) devices*, sending remote commands to alter the actuation of power line switches and circuit breakers to cause power disruption. The malware has two main components: ***Light Work***, which implements the IEC-104 protocol to modify the RTU state to on/off, and ***PieHop***, which connects to a specific remote MSSQL server to upload files and issue remote commands to an RTU using LightWork.

The malware *infiltrates the ICS network* and ***aims to disrupt or sabotage the operation of the power grid*** by exploiting vulnerabilities within the protocols used to communicate between different system components.

The threat posed by ***Cosmic Energy*** and other ICS malware ***is serious***. ICS systems are vital to operating critical infrastructure systems, such as power grids, water treatment plants, and transportation systems. A successful attack on an ICS system ***could have a devastating impact on the economy and public safety***.

RedStinger

The ***RedStinger APT group***, also linked to Russia, was discovered in the first half of 2022 but has been *targeting Eastern European* targets since 2020, especially the military, transportation, and critical infrastructure sectors. Depending on the campaign, the attackers ***would steal screenshots and recordings from microphones and the keyboard***.

RedStinger primarily used ***spear-phishing*** emails to attack its victims. These phishing emails usually had a file with a name that tricked victims into opening the email and downloading the malicious attachment. The attachments downloaded the ***DBoxShell malware*** onto the compromised systems.

Pipedream Malware

Also, during the first half of 2023, it became public that a Russian ***cybercriminal group*** called ***Chernovite*** was using a new malware to *target industrial control and automation systems* called ***Pipedream***. According to researchers, this malware has been used against at least one U.S. company in the energy sector.

This malware can manipulate various industrial *control programmable logic controllers* (PLCs) and *industrial software*, such as Omron and Schneider Electric. This means that Pipedream can infect a significant portion of industrial assets worldwide.

Its existence demonstrates that the capabilities of ICS attackers have increased considerably. Among their capabilities are the ***disruption, degradation and potential destruction of physical processes in industrial environments***.

10

TELECOMMUNICATIONS SECTOR

The telecommunications sector has been another of the most targeted sectors during this period. Both companies in the sector and the technologies have fallen victim to cybercriminals.

Among the main threats to the telecommunications sector are the botnets, since most attacks on mobile telecommunications networks are linked to botnets targeting IoT devices that seek vulnerable hosts to expand, and subsequently carry out distributed denial of service (DDoS) attacks.

A botnet is a collection of Internet-connected devices known as bots, which have been infected with malware, are remotely controlled by an attacker, and can be used together to perform malicious activities.

Mirai

Mirai malware belongs to the botnet family and primarily aims at ***infecting IoT devices***, especially routers and IP cameras, to carry out ***DDoS attacks***.

Mirai continuously scans IoT devices and infiltrates them *via Telnet* with default login credentials. Once infected, it loads its malicious code into the device's main memory.

This malware family is designed to attack devices running *Linux operating systems*, common in data centers, web servers, cloud services, and a wide range of network, mobile, and IoT devices. While **brute-force attacks** to access Internet-connected devices remain the preferred method for spreading Mirai variants, there is also *a shift towards more powerful devices* running Linux due to the availability of broadband connections and greater computing power.

Mirai variants have adopted ***many original malware features***, such as establishing a signal-based control flow to make dynamic analysis difficult, automatically deleting the executable, and renaming the process and command line to avoid detection. They also prevent system reboots, stop processes related to remote administration tools such as SSH and Telnet, neutralize other malware, and look for new targets to infect. However, more recent variants ***feature slightly different implementations*** or add new exploit capabilities to increase their attack surface.

Zerobot

Zerobot is a Go-based ***botnet*** that spreads primarily through ***vulnerabilities in IoT devices and web applications***. Its operators constantly add new capabilities and exploits to the malware.

Zerobot spreads through ***brute-force attacks and vulnerability exploitation***. This malware can infect devices based on various architectures and operating systems, such as firewall devices, routers, and cameras, to aggregate them into a distributed denial-of-service (DDoS) botnet.

Once it gains access to the device, Zerobot injects a ***malicious payload*** and uses various persistence tactics to maintain access. The latest version of the malware, Zerobot 1.1, includes new attack capabilities and exploitation of vulnerabilities in Apache and Apache Spark.

Zerobot 1.1 features new ***DDoS attack*** capabilities and can customize the target port based on the attacker's target. In addition, new previously undisclosed attack capabilities have been identified, such as ***UDP packet forwarding and customized TCP attacks***. Once it achieves persistence on a device, Zerobot scans for other exposed devices on the Internet to infect them.

APTs

11

In the first half of 2023, APT groups emerged as one of the most critical threats to organizations. Advanced Persistent Threats (APTs) are organized groups, sometimes funded by nation-states, whose main objective is information theft, industrial espionage, and obtaining information that provides a competitive advantage for the country.

These groups have greater capabilities of action and infection than other malicious actors and are continuously working on updating their Tactics, Techniques, and Procedures (TTP).

The international and regional interests of the various states sponsoring these types of threats have led to various campaigns throughout the first half of 2023 in which their opponents have been targeted.

In general, these campaigns are based on cyberespionage or information theft, and to a lesser extent, they seek the destruction of their targets' systems.

Among the actions of APT groups in the last six months, Russian, Chinese and North Korea, stand out.

Russian origin

Due to the current geopolitical landscape, it has been observed during the first half of 2023 an increase in the activity of Russian state-sponsored groups, which are directed at Western targets, mainly NATO members or countries supporting Ukraine in the conflict.

APT28

APT28 is also linked to the Russian intelligence service (GRU), and is especially dedicated to ***espionage tasks***.

In May of this year, UK and US security agencies warned about this group because the group was ***exploiting Cisco routers to deploy malware***. The group performed reconnaissance on their victims by using their infrastructure to mask access to the Simple Network Management Protocol (SNMP). They then configured the compromised routers to accept SNMP v2 requests. APT28 exploited an old Cisco vulnerability CVE-2017-6742 and deployed the ***Jaguar Tooth malware***.

Cadet Blizzard

In June 2023, Microsoft researchers published that they had discovered the emergence of a GRU-affiliated APT group called ***Cadet Blizzard***. This group has been conducting destructive cyber operations aimed at ***military targets in Ukraine***.

According to reports, Cadet Blizzard has been the creator of the ***WhisperGate wiper***, which was used at the beginning of the war against Ukrainian targets and was intended to delete the Master Boot Record (MBR) of the devices.

Sandworm

The ***Sandworm*** group operates under the control of Unit 74455 of the Main Center for Special Technologies of the Russian GRU. In January 2023, the activity of the Sandworm group was reported using different types of malware specially ***directed against Ukrainian targets***.

In January it was discovered that the group would be using since the end of 2022 a destructive type of malware (wiper) against the Ukrainian energy infrastructure and against a government agency. The malware used in these campaigns were ***NikoWiper, CaddyWiper, and ZeroWipe***. In these campaigns, a legitimate tool called ***SDelete*** has been used to execute the malware. SDelete is a Microsoft command line utility used to delete files securely.

Chinese origin

In February 2023, the EU Cybersecurity Agency (ENISA) and the CERT for EU institutions (CERT-EU), made a joint alert on several Chinese state-sponsored groups which have been directing their activities over the past years against EU companies and governments, such as APT27, APT30, APT31, Ke3chang, GALLIUM, and Mustang Panda.

Mustang Panda

Since January 2023, activity of this Chinese state-sponsored ***APT*** has been observed ***exploiting TP-Link routers to gain access to organizations*** using these devices.

The attacks are being carried out by deploying ***malicious firmware*** specially designed for TP-Link routers and a ***backdoor***, called ***Horse Shell***, allows attackers to gain control of infected devices and access compromised networks undetected.

It is also worth noting that during the first six months of 2023, numerous Chinese APTs have appeared that had not previously been reported targeting governments or critical infrastructures, such as **Volt Typhon** or **LanceFly**.

LanceFly

Lancefly is a recently discovered ***APT*** of Chinese origin that has been deploying the ***Merdoor malware*** in different organizations located in South and Southeast Asia in the aviation, government, and telecommunications sectors since mid-2022.

Merdoor is a malware that allows cybercriminals to track actions, ***record keystrokes and communicate with infected devices***. The initial attack vectors of this group are believed to be mainly ***phishing*** emails, ***brute-force*** SSH-like credentials and ***exploiting vulnerabilities***.

Volt Typhon

Volt Typhon is a recently discovered APT related to the government of the People's Republic of China. Its ***main target is critical infrastructures***.

Volt Typhoon has gained initial access to various target organizations through ***Fortinet FortiGuard*** devices with Internet access. This APT leverages the privileges offered by the Fortinet device, ***extracts credentials*** from an Active Directory account used by the device and then attempts to authenticate to other devices on the network with those credentials.

Volt Typhoon sends all its network traffic to its targets through compromised SOHO network edge devices. After gaining access to the victim's network, this APT uses ***living-off-the-land commands*** to find information on the system, discover additional devices on the network, and leak data.

North Korean origin

The U.S. Cybersecurity Agency (CISA) recently published that North Korea conducts operations worldwide, primarily using ransomware against critical infrastructure and the healthcare sector.

Lazarus

In early 2023, the ***Lazarus*** group targeted medical research agencies and energy companies using the ***BianLian ransomware***. The group gained initial access and privilege escalation by exploiting vulnerabilities CVE-2022-27295 and CVE-2022-37042 on Zimbra servers with unpatched Internet access.

The ***Lazarus*** group has directed attacks in recent years against companies dedicated ***to exchanging cryptocurrencies***, thus managing to finance their activity. In fact, this semester, they published that in one of the attacks they were able to obtain more than one hundred million dollars stolen from users of these companies.

In April the group changed its tactics and tools in a campaign called ***DeathNote***, targeting the defense, automotive, academic and diplomatic services sectors. In this campaign they used bitcoin-themed ***phishing*** emails to lure their victims into opening documents with macros to install the ***Manuscrypt backdoor***.

Also, during this semester, the group has had relevance after the attack it carried out on the supply chain through the ***VoIP software of the company 3CX***.

Kimsuky

Kimsuky is a North Korean state-sponsored advanced persistent threat (APT) group that has been active since 2012 and is known to perform social engineering attacks.

In June, several international security agencies issued a joint advisory warning that Kimsuky has been conducting a ***phishing*** campaign this year, posing as journalists and academics and targeting employees of research centers, think tanks, academic institutions, and media organizations. The campaign aimed ***to obtain confidential information***.

The initial messages of this campaign were free of any malicious attachments or links; however, the threat actors developed a personal connection with the target to send subsequent emails with malicious content that could trick the victim into opening them.

12 HACKTIVISM

Hacktivist activity refers to attacks by an individual or group of individuals for social or political motivations. The actions by these groups are generally denial of service, defacement attacks, or the publication of confidential data.

Since the beginning of 2022, hacktivism has seen a worldwide increase, especially due to the beginning of the conflict between Ukraine and Russia. During the first semester of 2023, hacktivist attacks have targeted governments, companies belonging to NATO countries, and even critical infrastructures such as ports and airports.

One of the most active hacktivist groups within the hacktivism born out of the Russian-Ukrainian conflict is Killnet, but Noname057 also stands out.

KillNet

KillNet is a ***pro-Russian hacktivist group*** active since at least January 2022, known for its ***Distributed Denial of Service (DDoS) attack campaigns*** targeting countries supporting Ukraine, especially countries belonging to the North Atlantic Treaty Organization (NATO) since the military conflict between Russia and Ukraine broke out in February 2022.

In its early days, ***KillNet*** became known for selling a tool specialized in DDoS attacks promoted under the same name to focus on a hacktivist group with an internal structure organized by squads or divisions structured according to the typology of attacks and cyber operations to become one of the most prominent pro-Russian cybercriminal groups by international authorities on cybercrime.

Killnet was organized as a group of cyber soldiers structured in squads or divisions with assigned tasks, operations and targets to attack. In recent months it has been moving towards the independence from the original group. The squads have become independent entities that collaborate with each other on specific attacks, campaigns or targets.

At the end of April, ***KillNet*** announced through its Telegram channel that they were ending their hacktivist activities and becoming part of a "private military hacking company" called Black Skills, to continue cyberattacks against their targets but accepting orders from private and public entities in exchange for money. However, KillNet's activities have continued, and in June, they participated in a campaign aimed at breaking the European infrastructure of the SWIFT banking system, the Wise international bank transfer system, the SEPA intra-European payment service, and several central banks in Europe and the United States. This campaign was carried out with the threat groups **REvil** and **Anonymous Sudan**.

Noname057(16)

Noname057(16) is a ***hacktivist threat actor with pro-Russian ideology***, which emerged on the threat landscape in March 2022, following the military conflict after Russia's invasion of Ukraine the previous month.

The main activity of the actor is to carry out ***DDoS-type attacks directed against Ukraine***, as well as against those NATO countries which have supported the country during the conflict.

The group has its own tool, called ***DDosia***, which is intended for the ***removal of websites*** of alleged enemies of Russia. ***DDosia*** is a cross-platform tool, and variants have been observed for most operating systems (*Windows, macOS, Linux and Android*).

It is worth noting that in the first half of 2023, the group has carried out more than a thousand denial-of-service attacks, many of them using ***DDosia***.

While hacktivism in the Russian-Ukrainian conflict has accounted for most of the attacks carried out during this period, there have also been other significant hacktivist operations on the international scene, such as **#OpColombia**.

OPColombia

The ***#OpColombia*** is one of the ***oldest hacktivist operations in Latin America***, and since 2020, the activities of groups linked to this operation have increased.

The hacktivist activity of ***#OpColombia*** is directed to targets of different typology, highlighting mainly ***public institutions and authorities***. As is common among these groups, their attacks are published through social networks such as Twitter or Telegram.

In May 2023, an event that led to the intensification of the campaigns collected within ***#OpColombia*** took place, leading to the arrest of *OrgOn*, a member of the *Lulzsec Colombia community*. Following his arrest, global hacktivist collectives such as **GhostSec** or **Siegedsec** have directed their attacks on Colombian targets using the hashtags #OpColombia and #FreeOrgOn. These attacks include the ***attack on GNSS*** and radio stations in Colombia on May 19, the ***data breach*** of Colombian authorities on May 26, the attack on a Colombian energy company on May 28, and the breach of the database of the Colombian National System for the Registration of Precautionary Measures in June.

SiegedSec

This hacktivist group has been heavily ***involved in OpColombia***, but has also carried out attacks against the governments of other countries, such as Cuba, the United States or the Philippines.

SiegedSec first appeared in 2022, led by a renowned hacktivist named *YourAnonWolf*.

The modus operandi of this group derives from the hacktivist actions of other groups, which are mainly based on ***defacement or DDoS attacks***.

SiegedSec focuses on c***ompromising its victims' networks and the subsequent data publication***, without seeking financial gain. In fact, in February 2023, the group announced that it had gained access to the networks of an Australian software company and published the information obtained on underground forums.

RELEVANT ATTACKS 13

The most relevant attacks of the first semester of 2023 are detailed, classified by date, victim sector, attack typology, and perpetrating actor.

S21 SEC
Cyber Solutions by Thales

Relevant Attacks First Quarter

Date	Sector	Attack Type	Threat Actor
jan-23	Insurance	Data breach	NotPetya
jan-23	Government & administration	Ransomware attack	LockBit 3.0
jan-23	Government & administration	Ransomware attack	Conti
jan-23	Government & administration	Ransomware attack	Cuba
jan-23	Telecommunications	Data breach	Okta
jan-23	Education	Ransomware attack	Royal
jan-23	Telecommunications	Data breach	IntelBroker
jan-23	Government & administration	Ransomware attack	LockBit 3.0
feb-23	Pharmacy and drugs	Data breach	Lorenz
feb-23	Telecommunications	Data breach	pompompurin
feb-23	Entertainment industry	Data breach	BlackCat (ALPHV)
feb-23	Government & administration	Data breach	pompompurin
feb-23	Entertainment industry	Data breach	CVE_2022_30190
feb-23	Air transport	DDoS	Anonymous Sudan
feb-23	Government & administration	Ransomware attack	BlackCat (ALPHV)
feb-23	Consulting	Ransomware attack	LockBit 3.0
mar-23	Retail	Data breach	Hy####ad
mar-23	Technologies	Data breach	kernelware
mar-23	Healthcare	Ransomware attack	RansomHouse
mar-23	Healthcare	Data breach	Unknown
mar-23	Finance	Data breach	Unknown
mar-23	Energy	Ransomware attack	Cl0p
mar-23	Healthcare	Intrusion	Unknown
mar-23	Industry	Data breach	RansomExx

Relevant Attacks Second Quarter

Date	Sector	Attack Type	Threat Actor
apr-23	Energy	Ransomware attack	LockBit 3.0
apr-23	Technologies	Ransomware attack	BlackCat (ALPHV)
apr-23	Healthcare	Data breach	Bian Lian
apr-23	Insurance	Ransomware attack	BlackCat (ALPHV)
apr-23	Automotive	Ransomware attack	Nokoyawa
apr-23	Insurance	Ransomware attack	BlackCat (ALPHV)
apr-23	Automotive	Ransomware attack	Nokoyawa
apr-23	Insurance	Data breach	Royal
apr-23	Maritime transport	Ransomware attack	LockBit 3.0
apr-23	Pharmacy and drugs	Ransomware attack	Karakurt
may-23	Healthcare	Data breach	Cl0p
may-23	Government & administration	Ransomware attack	BlackByte
may-23	Logistics	Ransomware attack	Royal
may-23	Defense	Ransomware attack	Black Basta
may-23	Telecommunications	Data breach	LAPSUS$
may-23	Insurance	Ransomware attack	Trigona
may-23	IT Consulting	Ransomware attack	BlackCat (ALPHV)
may-23	Legal Consulting	Ransomware attack	BlackCat (ALPHV)
jun-23	Telecommunications	Ransomware attack	LockBit 3.0
jun-23	Education	Intrusion	Unknown
jun-23	Energy	Data breach	8Base
jun-23	Telecommunications	DDoS	Anonymous Sudan
jun-23	Technologies	Ransomware attack	Bian Lian
jun-23	Technologies	Data breach	Cl0p
jun-23	Oil & Gas	Ransomware attack	Cl0p
jun-23	Air transport	Data breach	Cl0p

S21 SEC

Cyber Solutions by Thales

www.s21sec.com