

2023

The Ransomware Landscape in Europe



By Swascan

H1

Index

H1 2023	Pg. 03
The most prolific ransomware gangs - the latest data	Pg. 07
European Focus– Q2 2023	Pg. 08
The cyber kill chain: how ransomware becomes pervasive	Pg. 14
Focus Q2 2023	Pg. 14
Reconnaissance	Pg. 16
Compromised devices, credential leaks & social engineering	Pg. 17
Common vulnerabilities and exposures	Pg. 21
Weaponization	Pg. 23
Malware	Pg. 24
Delivery	Pg. 25
Phishing	Pg. 26
Exploitation	Pg. 29
CVE	Pg. 30
Command&control	Pg. 33
Conclusion	Pg. 35
How to Defend Against Ransomware: The Cyber Security Framework	Pg. 36
Action Plan	Pg. 37
Disclaimer	Pg. 40
About us	Pg. 41

H1 2023

The first half of 2023 witnessed a significant increase in targeted cyberattacks aimed at data theft and ransom demands in exchange for the restoration of affected systems. We conducted an in-depth analysis of ransomware and malware scenarios, providing a detailed overview of emerging threats and evolving trends.

During H1, numerous ransomware campaigns were observed, characterized by the distribution of malicious software that encrypts victims' data and subsequently demands a ransom for their recovery. These attacks targeted a wide range of sectors, including financial, healthcare, and government, jeopardizing information security and operational continuity.

The evolution of tactics employed by cybercriminals in these first six months of 2023 has been particularly concerning. Ransomware has become increasingly sophisticated and targeted, and numerous new ransomware gangs have emerged.

In this report, we will analyse the major ransomware attacks, highlighting the operational methods, victims, affected regions, and emerging trends, and we will examine recommended security measures to mitigate the risk of such threats.

Ransomware victims in the first half of this year hail from a wide range of countries and islands, totaling 107 countries involved. This demonstrates that ransomware is a global issue that knows no geographical boundaries: organizations and individuals worldwide have been targeted in attacks, putting data security and operational continuity at risk.

In this context, we have undertaken an analysis of the profile of victims targeted by Criminal Hackers in H1 2023.

In particular, data was collected, through specific OSINT & CLOSINT research, on the victims of the 15 most active ransomware gangs in the second quarter of 2023:

LockBit	Alphav/BlackCat	8Base	CLOP	BlackBasta
PLAY	BianLian	Royal	Akira	SiegedSec
Medusa	Snatch	Nokoyawa	BlackByte	Rhysida

The methodological approach used was as follows:

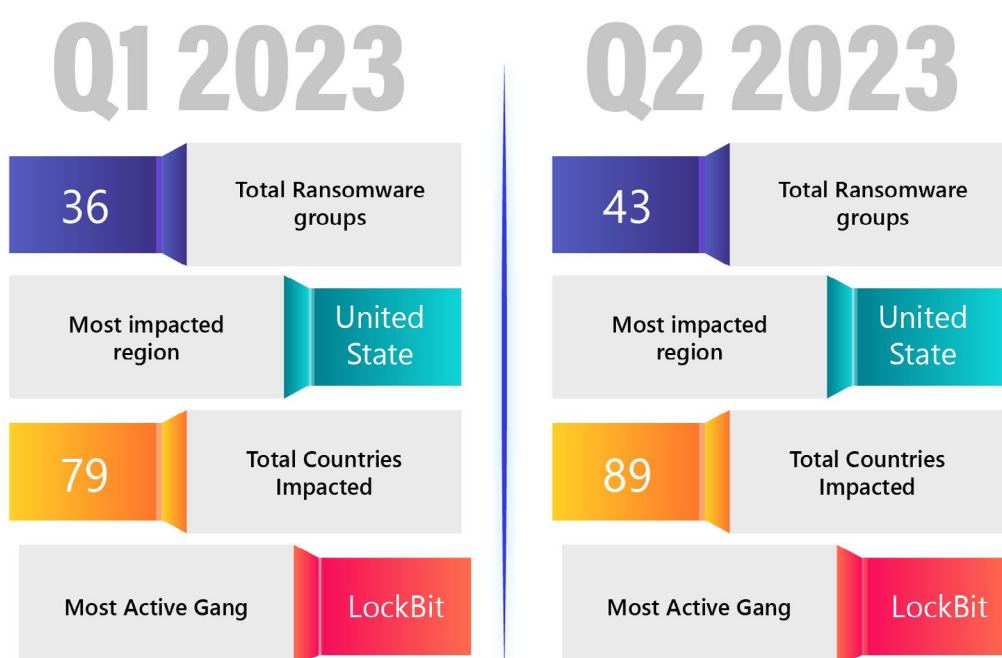
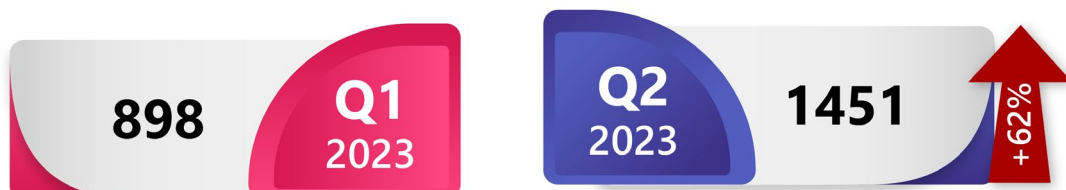
1. Identification of Dark web sites related to ransomware gangs.
2. Identification of victim companies that were published on Dark web portals.
3. Clustering of victim information in terms of:
 - **Geographic area**
 - **Industry sector**
 - **Revenue and number of employees**

The period between the first quarter (Q1) and the second quarter (Q2) of 2023 witnessed a significant increase in ransomware attacks worldwide. During Q1, a total of 36 different ransomware gangs were identified, which had targeted numerous sectors and companies globally. The most affected region was the United States, with a high number of reported attacks.

However, Q2 saw a further increase in ransomware attacks, with a total of 43 groups identified. The United States region continues to be the most affected, but there has been a significant increase in the number of countries worldwide affected by the attacks, rising from 79 (Q1) to 89 (Q2), totaling 107 nations involved. This suggests an expansion of ransomware gang operations, targeting an increasingly wide range of countries.

Among all the ransomware groups active during Q2, LockBit remained the most prolific and aggressive, operating on a large scale and impacting numerous organizations worldwide.

Number of Targets affected by gangs with data leak Q1 2023 vs. Q2 2023 comparison



The threat of ransomware attacks continues to evolve at an alarming pace, with a surge in criminal activity in the second half of 2023. Comparing data from 2022 to 2023 reveals a concerning trend that calls for decisive actions to mitigate damage and protect organizations from severe consequences.

Indeed, the collected data shows a sharp increase in ransomware attacks in every month of 2023 compared to the same period in the previous year. Starting in January, there was a significant rise in attacks, increasing from 112 in 2022 to 175 in 2023. This trend continued in the following months, with February seeing an increase from 200 to 266, March from 232 to 457, and April from 298 to 381.

However, it's in the month of May that one of the most concerning increases is evident. While in 2022 there were 223 ransomware attacks, in 2023, the number surged to 575, representing more than double the previous year's figures. June, the last month under consideration, confirmed this alarming rise, jumping from 187 attacks in 2022 to 495 in 2023.

Comparison of H1 2023 and H1 2022



The most prolific ransomware gangs – latest data

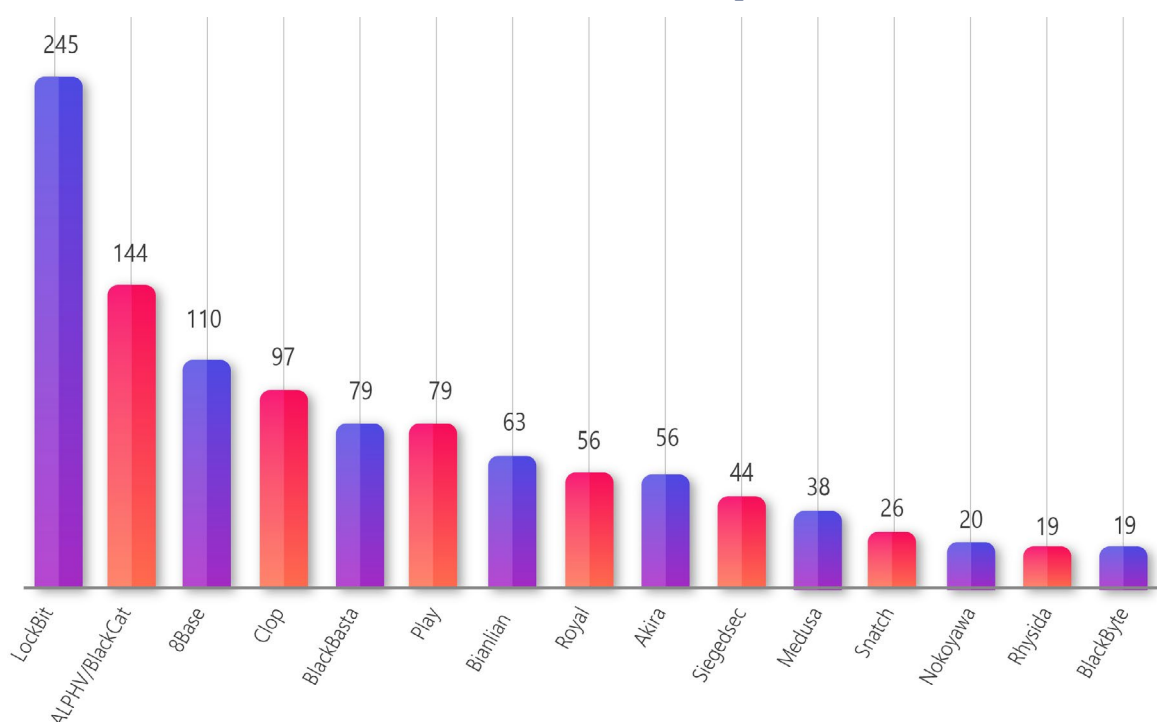
LockBit confirms itself as the most prolific gang in the ransomware attack landscape, with a total of **245 attacks** recorded in Q2 2023. Another gang that has garnered attention is **Alphv/BlackCat**, responsible for **144 ransomware attacks** during the quarter. **8BASE** has also stood out for its aggressiveness, targeting a total of **110 organizations**.

A recently emerged ransomware gang, Akira, has already targeted several victims, with the majority located in the United States. These victims belong to a variety of sectors, including Banking, Insurance, Finance, Real Estate Services (BAFSI), Construction, Education, Healthcare, Manufacturing, and others, underscoring that no sector is safe from these digital threats.

Akira is not the only new gang of the quarter to rank in the top 15: the ransomware gang Rhysida was first observed in May 2023 and secured a spot among the top 15.

Meanwhile, the ransomware gang 8Base is targeting organizations worldwide with double extortion attacks, gaining a steady stream of new victims since early June. The gang first appeared in March 2022, remaining relatively quiet with few notable attacks. However, in June 2023, the ransomware operation recorded a significant increase in activity, targeting numerous companies across different industries.

Numbers of victims - Q2 2023

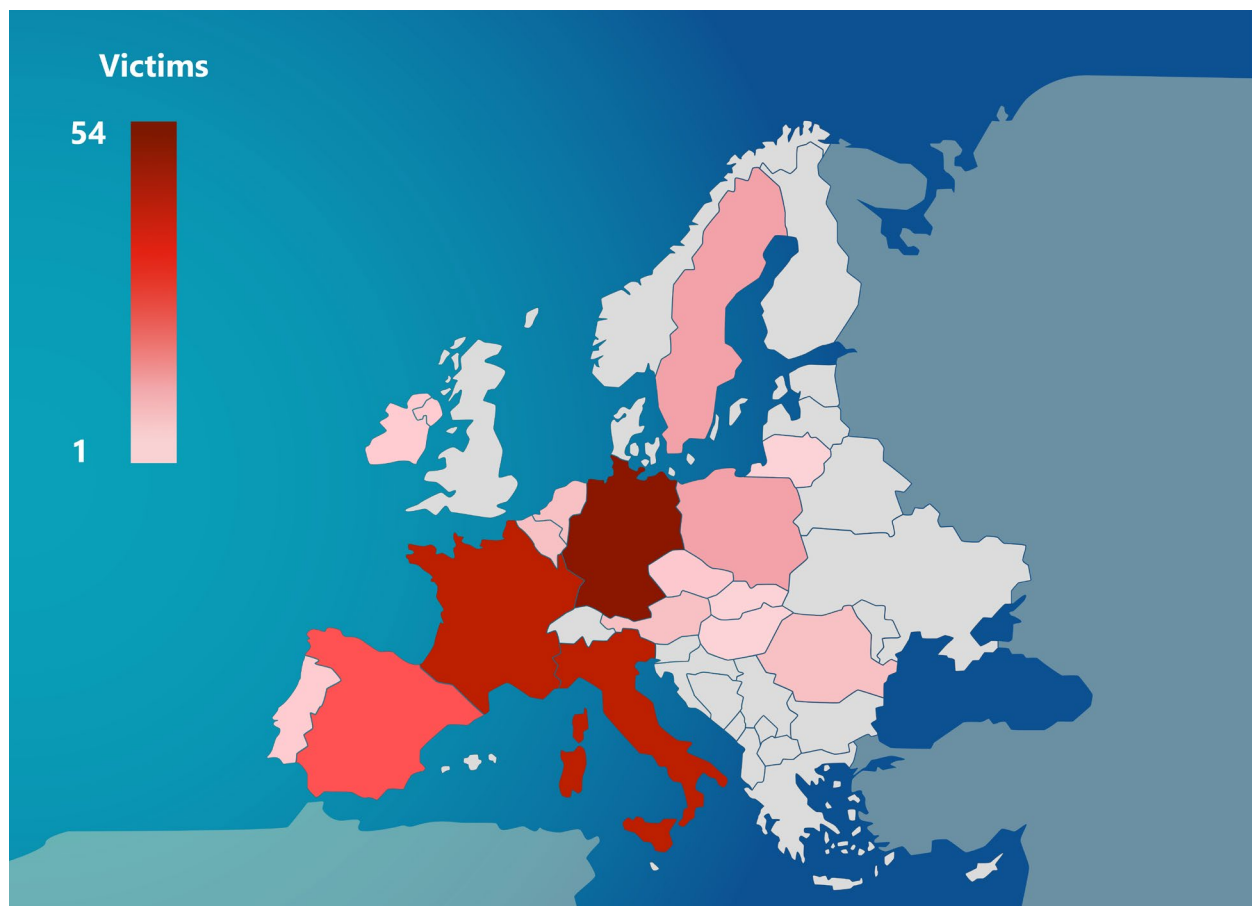


European Focus – Q2 2023


The increase in ransomware attacks within the European Union has highlighted the need for international cooperation to counter these digital threats. This involves promoting the exchange of information and adopting preventive measures to protect digital infrastructure and sensitive data.

Countries such as **Germany, France, Italy, and Spain** have been particularly affected. **Germany**, in fact, experienced a total of **54 ransomware attacks** during this period, signalling a significant increase compared to previous quarters. **France** and **Italy** closely follow Germany with **39 and 35 attacks**, respectively. Both of these countries are important economic and commercial hubs, making them prime targets for attackers.

Ransomware Attacks Europe - Q2 2023



*Most affected countries
in April:*

1. Germany 

2. France 

3. Italy 

*Most affected countries
in May:*

1. Germany 

2. Italy 

3. France 

*Most affected countries
In June:*

1. Germany 

2. France 

3. Spain 

Top Gang Q2 by country (number of attacks)

France LOCKBIT3 (11)

Italy MONTI (09)

Spain LOCKBIT3 (08)

Germany PLAY (07)

Austria LOCKBIT3 (06)

Republic Czech PLAY (04)

Netherlands LOCKBIT3 (04)

Sweden LOCKBIT3 (03)

Romania LOCKBIT3 (02)

Poland LOCKBIT3 (02)

Luxembourg LOCKBIT3 (02)

Belgium LOCKBIT3 (02)

Slovenia BLACKBASTA (02)

Slovakia VICESOCIETY (01)

Greece VICESOCIETY (01)

Denmark VICESOCIETY (01)

Portugal PLAY (01)

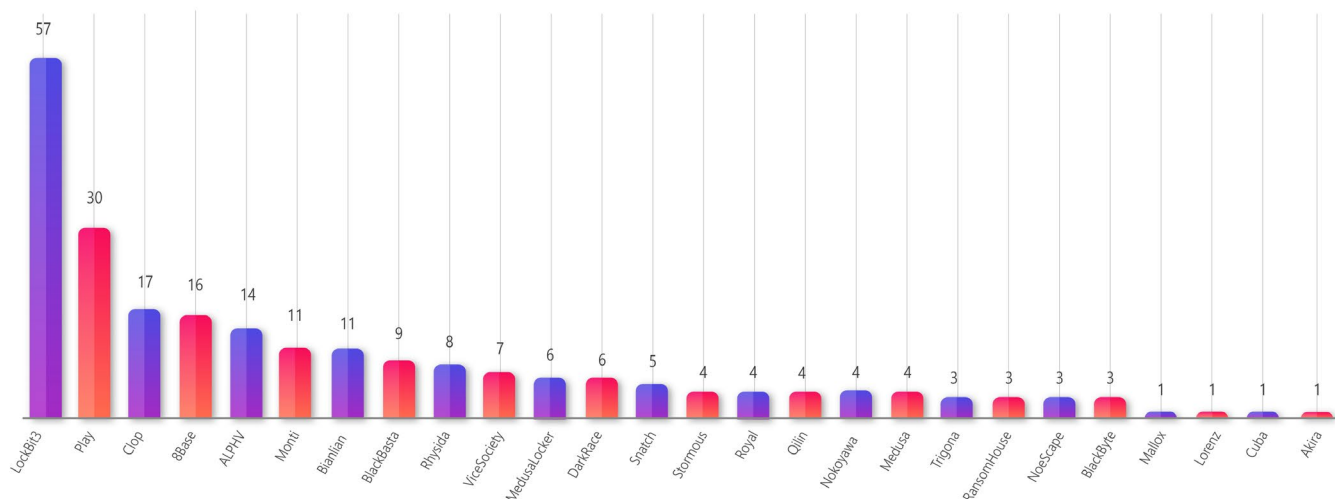
Ireland PLAY (01)

Hungary PLAY (01)

Cyprus MEDUSA (01)

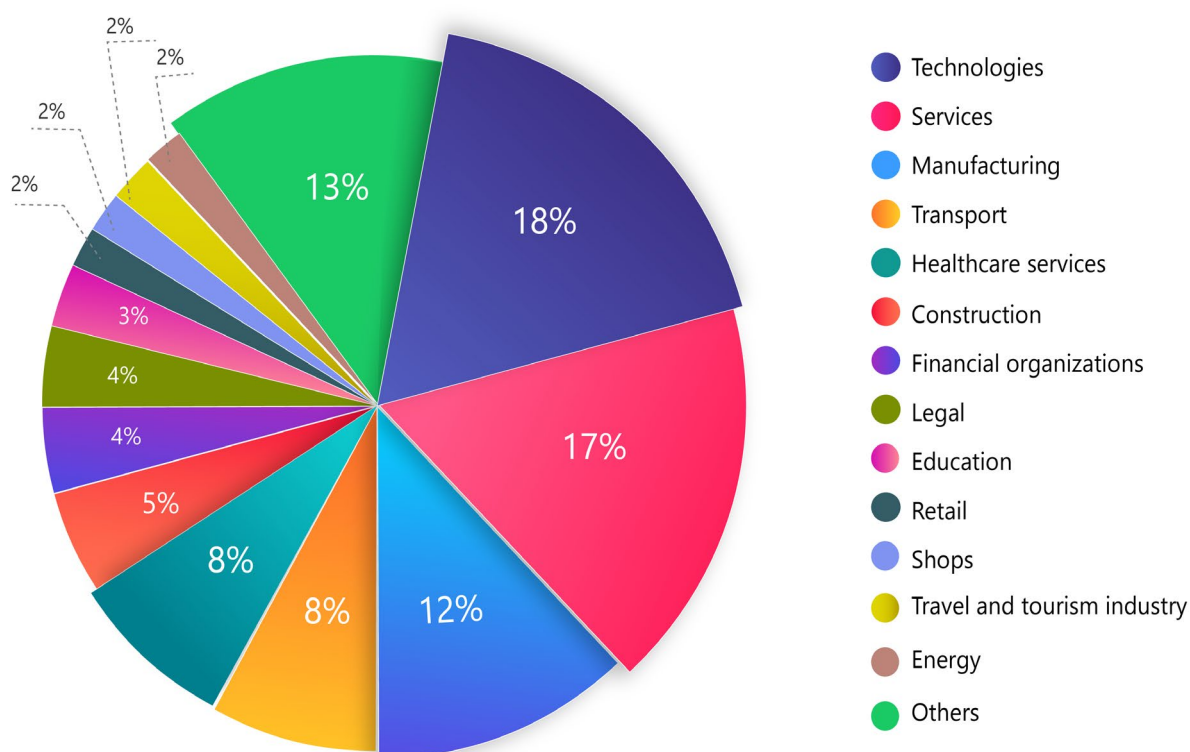
Lithuania CUBA (01)

Gang Attacks - Europe Q2 2023



Below is the graph of the most affected services in Q2 2023 in the European Union:

Attacks by sector - Europe





Top 5 sectors
affected in April

Top 5 sectors
affected in May

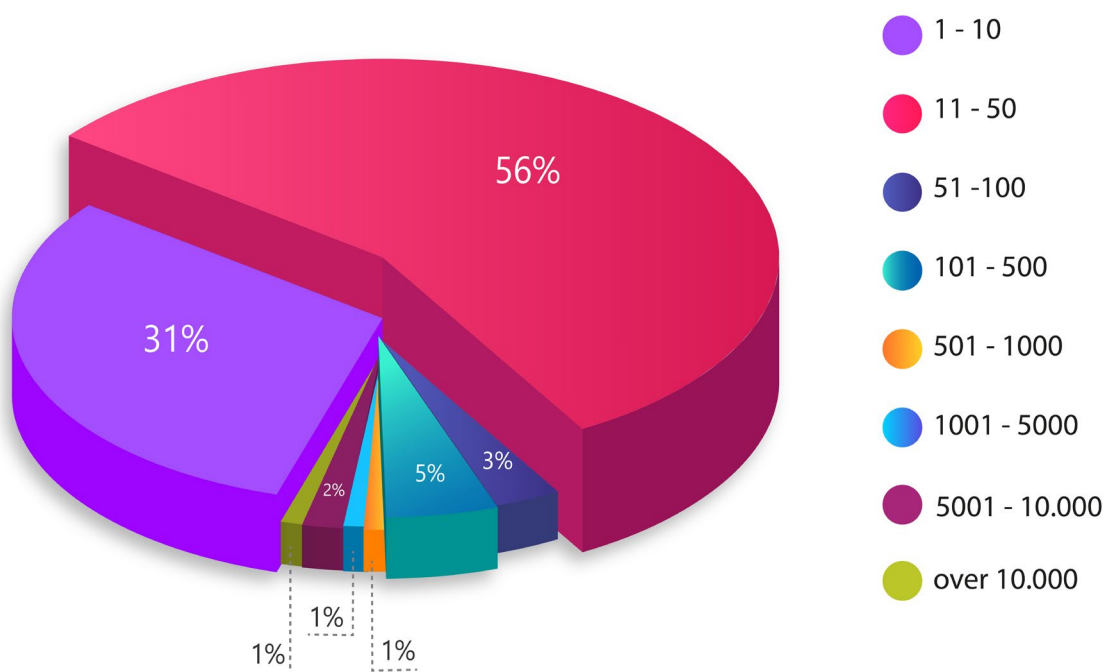


Top 5 sectors
affected in June

Among all companies, as previously mentioned globally, small and medium-sized enterprises (SMEs) continue to face a growing threat from ransomware attacks, jeopardizing the security of their data and business operations.

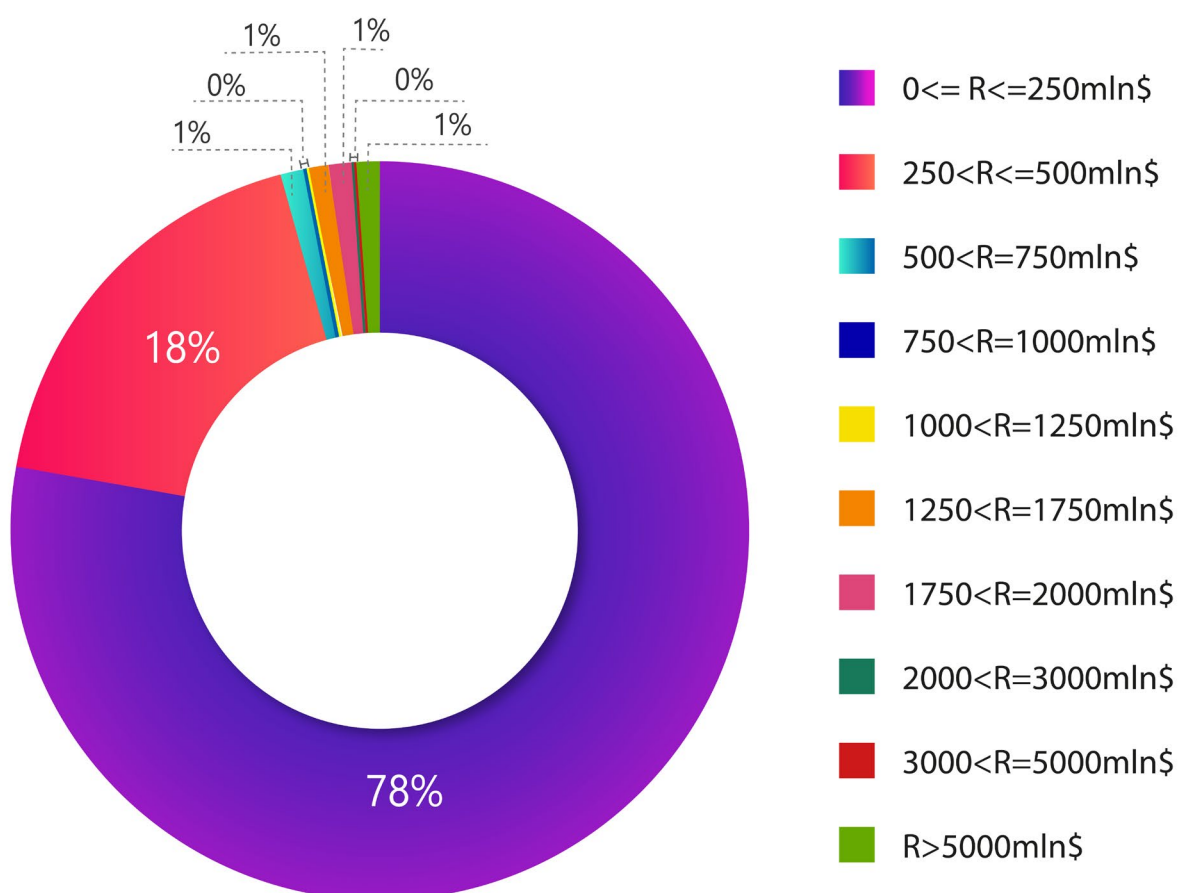
When analysing the number of employees, the data confirms that SMEs with a smaller workforce are the most affected. Specifically, companies with a staff size ranging from 1 to 50 employees constitute the most affected group, accounting for a total of 87% of the involved companies.

Number of Employees of Affected Companies - Europe



The same data is also confirmed in the turnover of the affected companies:

Split of Affected Companies By Revenue - Europe



Of all the ransomware gangs active in Italy in the second quarter of 2023, Monti proved to be the most prolific, accounting for around 26% of attacks in the country, demonstrating an impressive presence in Italy. Lockbit3 was also confirmed as one of the most active ransomware gangs in Italy, accounting for 20% of attacks.

THE CYBER KILL CHAIN: HOW RANSOMWARE BE- COMES PERVERSIVE

Focus Q2 2023

In the increasingly complex and frequent landscape of cyberattacks, the Cyber Kill Chain emerges as a fundamental tool for identifying and countering threats from criminal hackers. This defense methodology, inspired by the concept of the Kill Chain used in the military field, has been adopted in the cybersecurity sector to identify the stages through which an attack unfolds and to prepare an appropriate defensive strategy. It consists of seven well-defined phases. These phases represent the steps that a potential criminal hacker would need to take to carry out an attack, allowing for an understanding of the attackers' modus operandi, the detection of attack signals, and the implementation of necessary countermeasures.

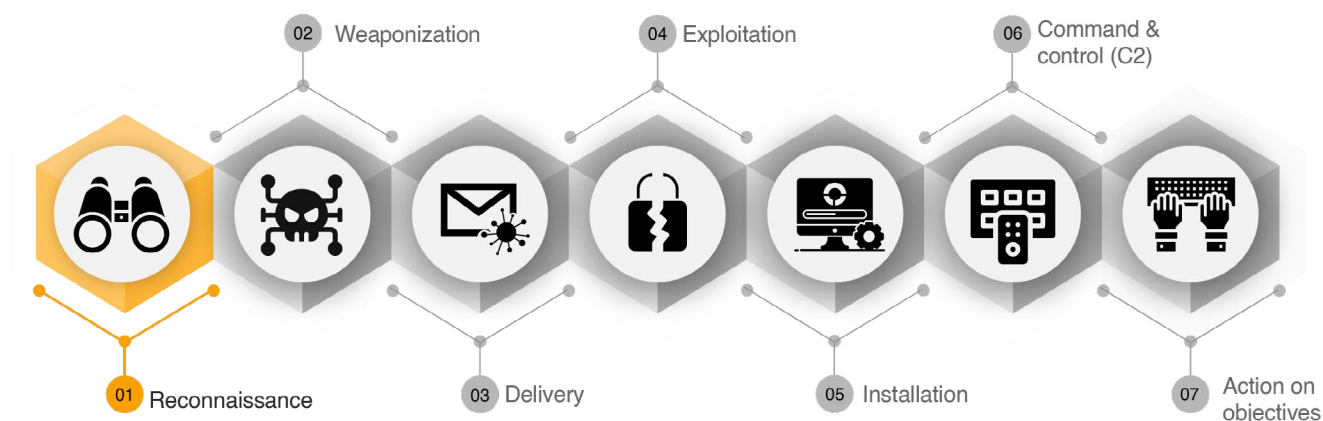


The seven phases of the Cyber Kill Chain are as follows:

1. **Reconnaissance:** In this phase, the criminal hacker identifies the target and conducts in-depth research to identify vulnerabilities in the target's security system. This phase is of fundamental importance as it determines the success of subsequent phases.
2. **Weaponization:** In the second step, the attacker uses the information gathered in the previous phase to select the most suitable tools for creating remote access to the target system.
3. **Delivery:** In this phase, the malware created is delivered to the target through various vectors, such as phishing emails or links on compromised websites.
4. **Exploitation:** Once delivered to the target, the malware is activated and exploits system vulnerabilities to gain unauthorized access or perform other malicious actions.
5. **Installation:** During the installation phase, the attacker ensures that the malware is installed and running on the target system. This allows them to bypass security controls and maintain access to the system. The installation of malware is facilitated by the exploit selected during the weaponization phase and is executed during the exploitation phase.
6. **Command & Control:** In the sixth step of the chain, attackers establish a connection between the victim system and the remote machine from which they operate. This connection allows them to gain persistent control and continuous access to the victim's environment.
7. **Actions on Objectives:** In the final link of the chain, attackers carry out the attack on the predetermined target, which can involve data manipulation, exfiltration of sensitive information, data destruction, or unauthorized access to confidential resources.

The Cyber Kill Chain provides a strategic framework for understanding cyberattacks and acting accordingly. There is no one-size-fits-all approach to dealing with an attack, but this model allows one to think like an attacker and adopt a similar approach to prevent or mitigate intrusion.

RECONNAISSANCE

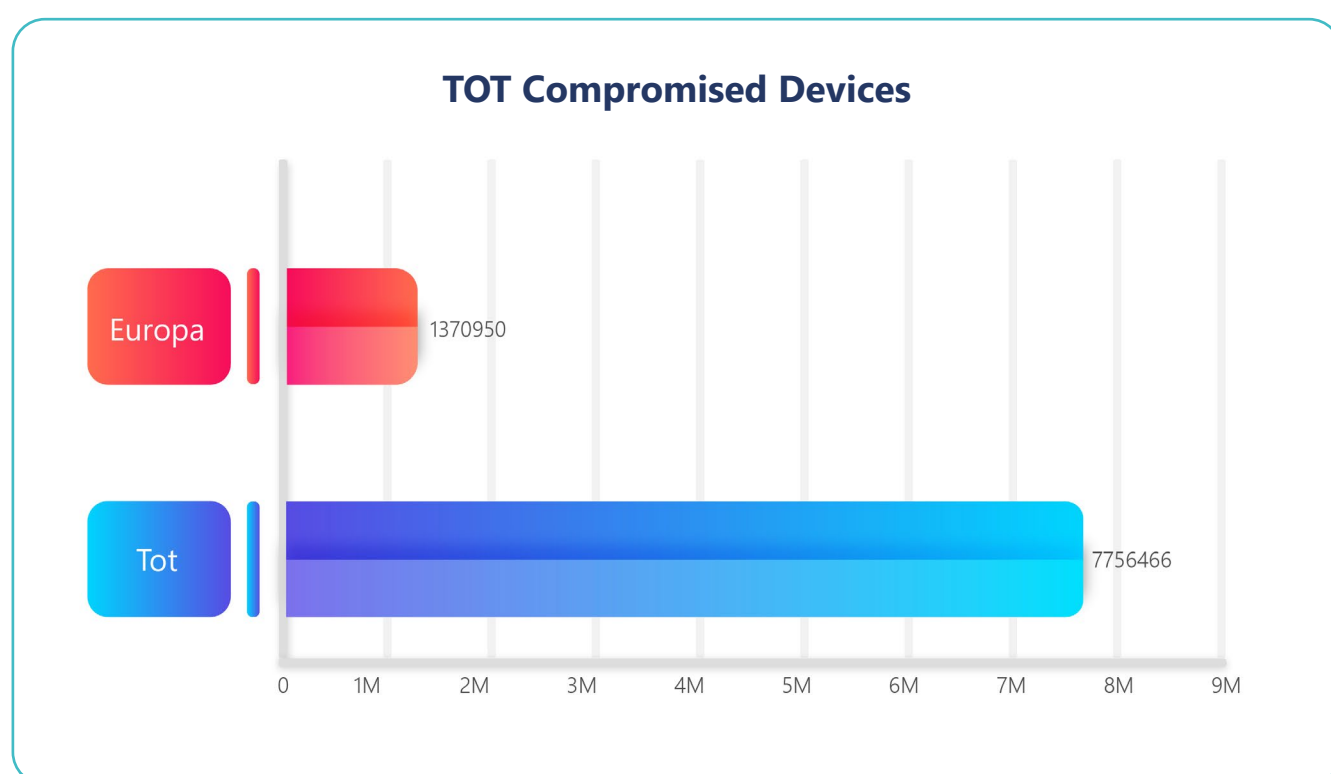


The reconnaissance phase is the first significant stage within the Cyber Kill Chain, during which attackers gather valuable information to plan a targeted attack. During this phase, various strategies are employed, including the collection of credentials from dark web markets, the identification of new vulnerabilities (CVE), and the use of social engineering campaigns.

Attackers can acquire sensitive credentials from markets on the Deep and Dark Web, where stolen information such as usernames, passwords, and access details to systems or online accounts is illegally traded. These credentials can originate from previous data breaches or phishing techniques and can be used to gain unauthorized access to systems or impersonate a legitimate user.

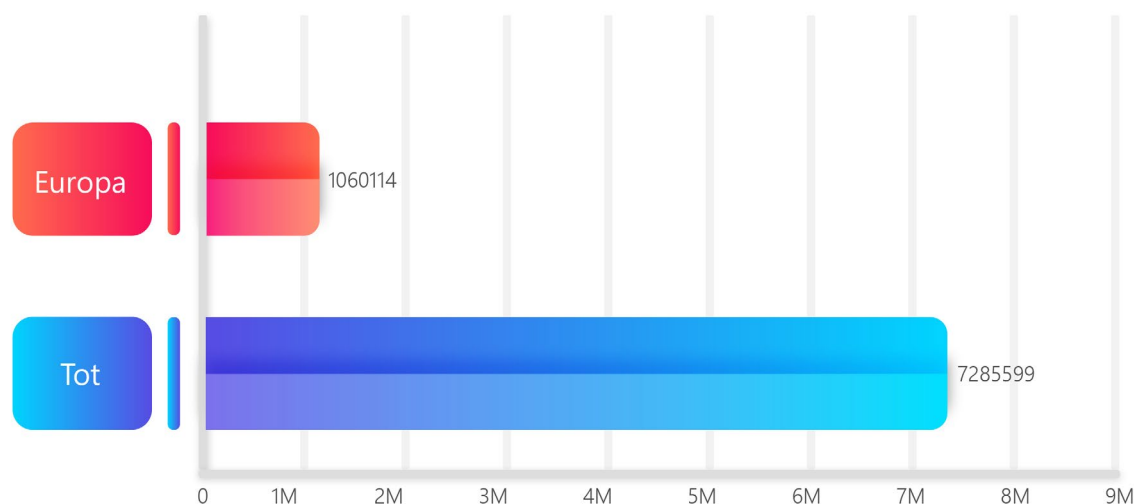
Compromised Devices, Credential Leaks & Social Engineering

Referring to two well-known credential markets for sale, a total of **7,756,466** compromised devices were detected from which credentials were exfiltrated. The focus on Europe detected a total of **1,370,950**.



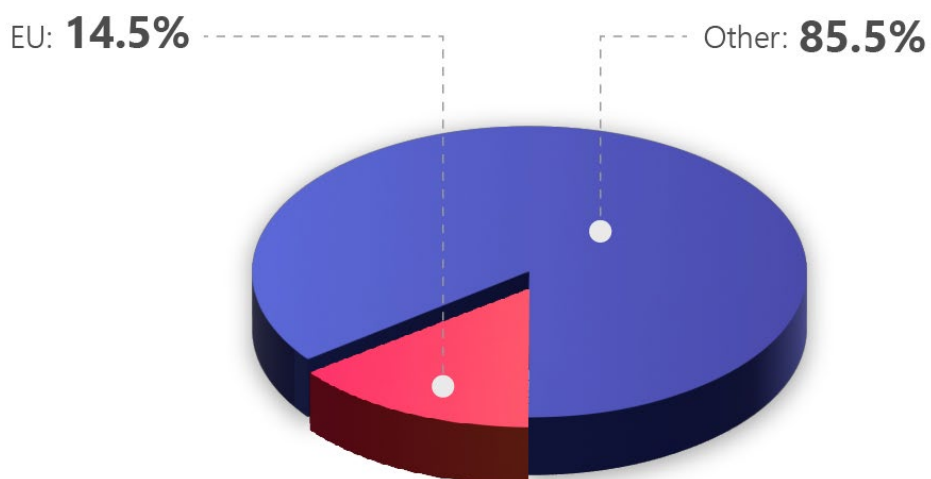
An in-depth analysis of the first portal revealed a total of 7,285,599 compromised devices from which access credentials were exfiltrated. Focusing on Europe, the total is 1'060'114 compromised devices.

Compromised Devices Market n.1



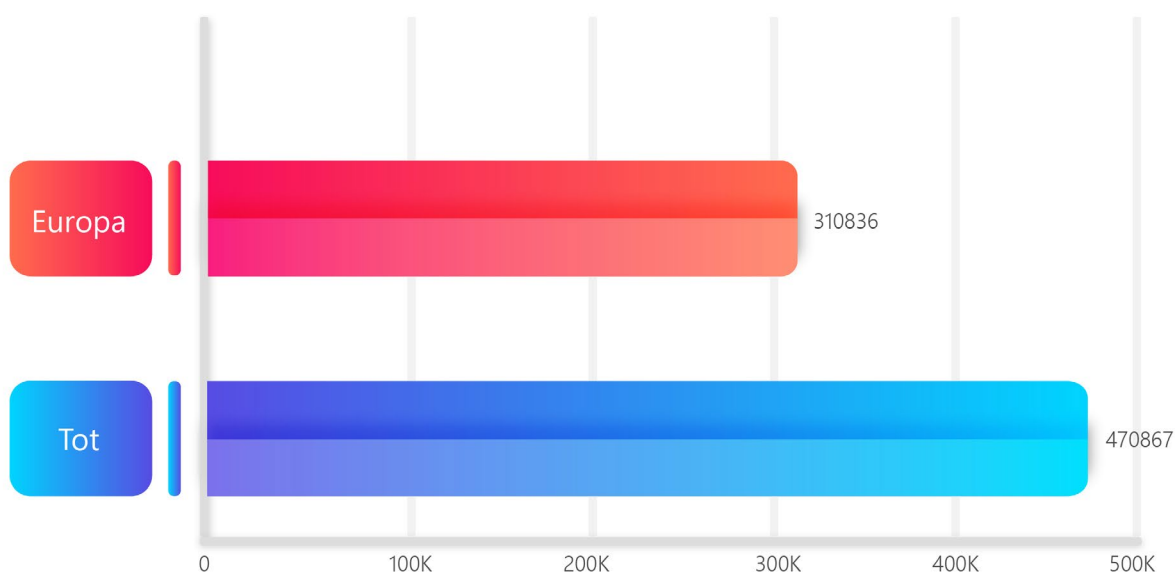
Europe accounts for 14.55% of the total compromised devices:

Global vs Europe

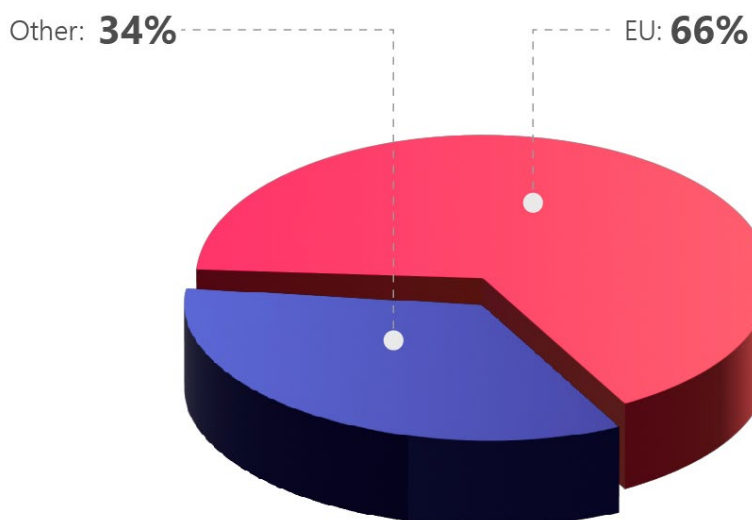


The second portal under analysis presents a total of 470,867 compromised devices, of which **310,836 (66%)** related to Europe.

Compromised Devices Market n.2

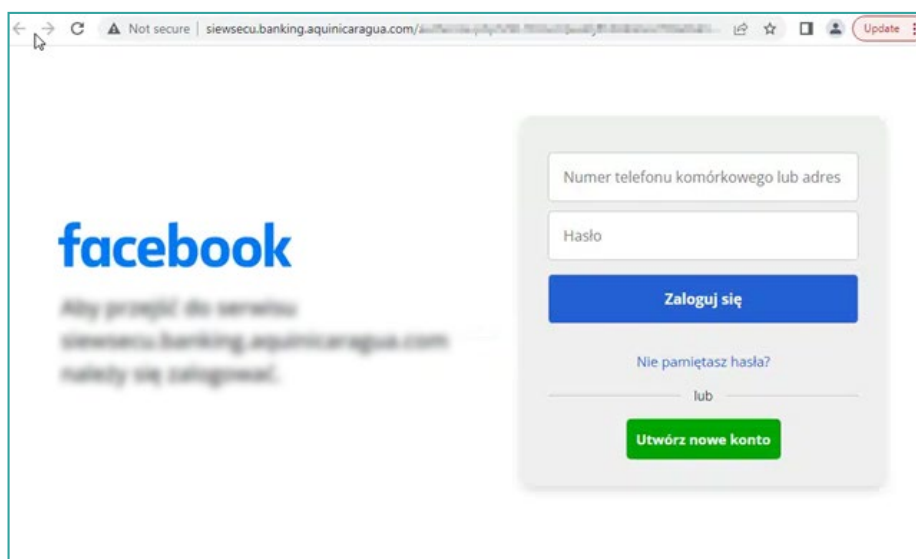
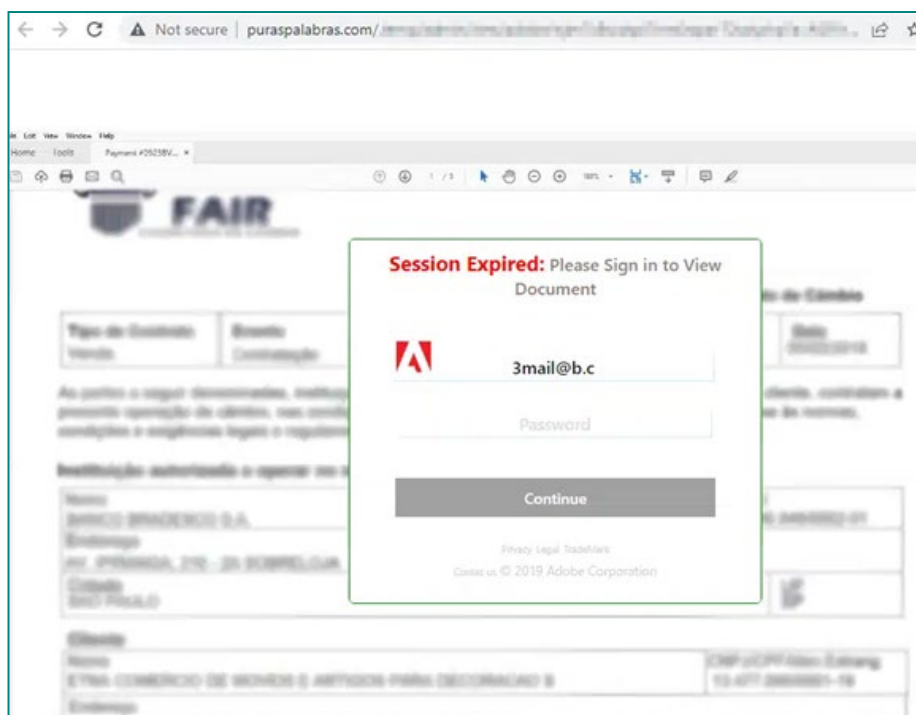


Global vs Europe - Compromised Devices Market n.2



Social engineering campaigns represent another common tactic in the Reconnaissance phase. Attackers seek to gather valuable information about users or organizations through deception and psychological manipulation. This can involve sending fraudulent emails or text messages that request sensitive information or induce users to click on malicious links. In Q2, a total of 155,683 phishing campaigns were observed. Through these tactics, attackers aim to gain access to confidential information or deceive users to facilitate subsequent phases of the attack.

Among the analyzed campaigns, it is possible to notice some examples where the attempt is made to deceive the victim by pretending to be real products or services:

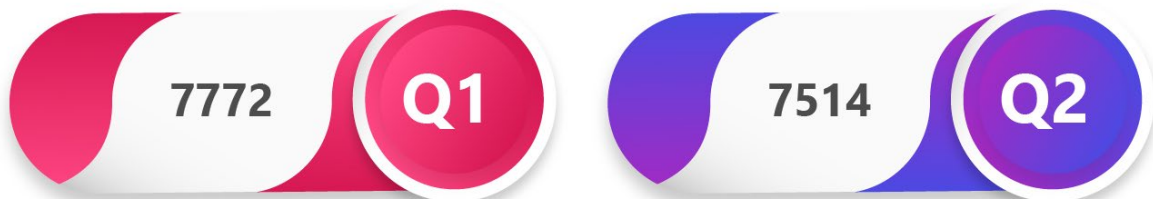


Common Vulnerabilities and Exposures

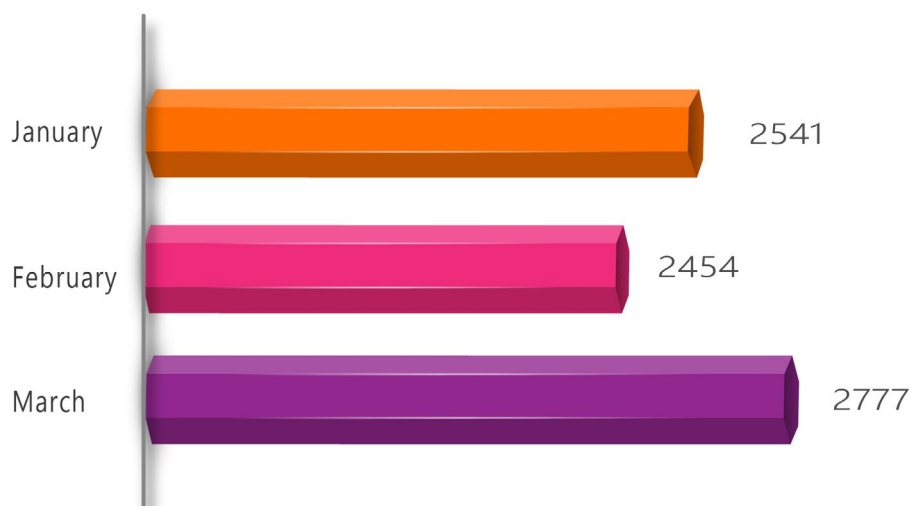
The identification of new vulnerabilities, known as CVEs (Common Vulnerabilities and Exposures), is another critical component of the Reconnaissance phase. Attackers continuously monitor newly discovered vulnerabilities in software, operating systems, or applications. This allows them to identify weaknesses in target systems and exploit them later during the attack.

In Q1 of 2023, a total of 7,772 new CVEs were published, compared to the 7,514 published in Q2:

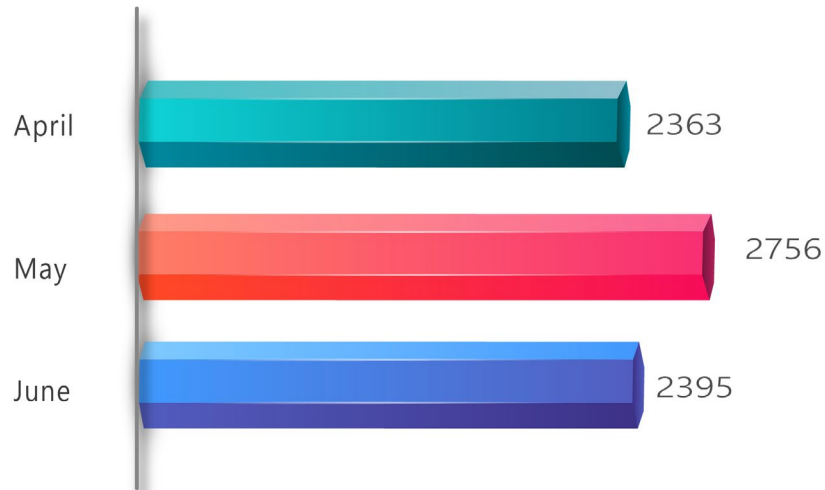
CVE - Q1 vs Q2 2023



CVE - Q1 2023



CVE - Q2 2023



It's noticeable that in May alone, 2,756 new CVEs related to vulnerabilities that could be exploited by attackers were published.

To effectively protect against the Reconnaissance phase, organizations must implement various security measures. This includes constant monitoring of dark web markets to track potential breaches of company data, the implementation of vulnerability detection solutions to identify and mitigate new CVEs, as well as user training and awareness to recognize and resist social engineering tactics.

Furthermore, it's important to keep systems and applications up to date with the latest security patches and adopt good cybersecurity practices such as using strong passwords and multi-factor authentication.

WEAPONIZATION



The weaponization phase is an important step within the Cyber Kill Chain, during which attackers transform a malicious payload into a weapon ready to be used against the target system. During this phase, various types of malware are often delivered, including botnets, info stealers, and RATs (Remote Access Trojans).

Botnets are networks of compromised computers remotely controlled by attackers. These bots can be used to carry out distributed denial of service (**DDoS**) attacks, send spam, or further propagate malware. The attacker leverages the botnet to send commands to the compromised bots and receive information collected by them.

Info stealers are types of **malware** designed to steal sensitive information from infected systems. These malware can collect data such as login credentials, banking information, credit card data, or other personal information. Once collected, the information is sent to the attacker's command and control (C2) for later exploitation or illicit use.

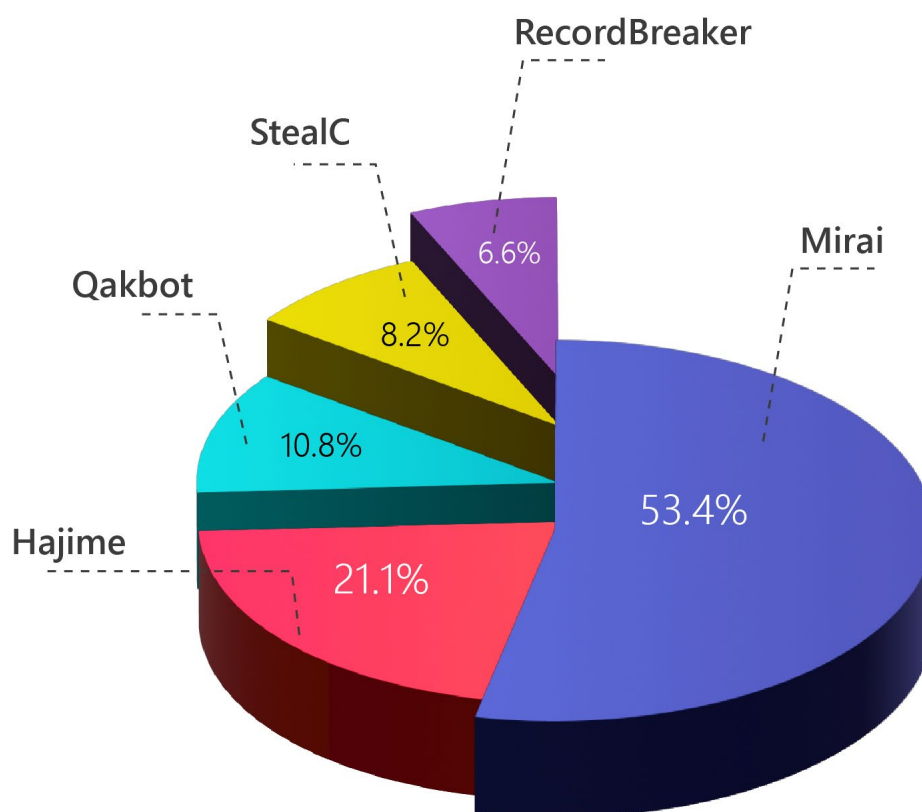
RATs, or Remote Access Trojans, allow attackers to take complete remote control of the compromised system. Attackers can access the system, execute commands, download and install additional malware, exfiltrate data, or perform other malicious actions. These tools provide attackers with stealthy and persistent control over the compromised system.

The weaponization phase is crucial for attackers because it represents the moment when the malicious payload is turned into a functional attack tool. Attackers leverage these forms of malware, such as botnets, info stealers, and RATs, to gain and maintain unauthorized access to the target system and carry out further stages of the cyberattack.

Malware

We have identified the most prevalent malware during this period: **Mirai** ranked first, representing **53.4%** of the distributed malware, while **Hajime** and **Qakbot** took second and third place with **21.1%** and **10.8%** respectively.

Malware - Q2 2023



It's noteworthy that Qakbot is widely used to date, especially by ransomware gangs in the Weaponization phase, to execute malicious payloads that often lead to the execution of ransomware itself.

DELIVERY



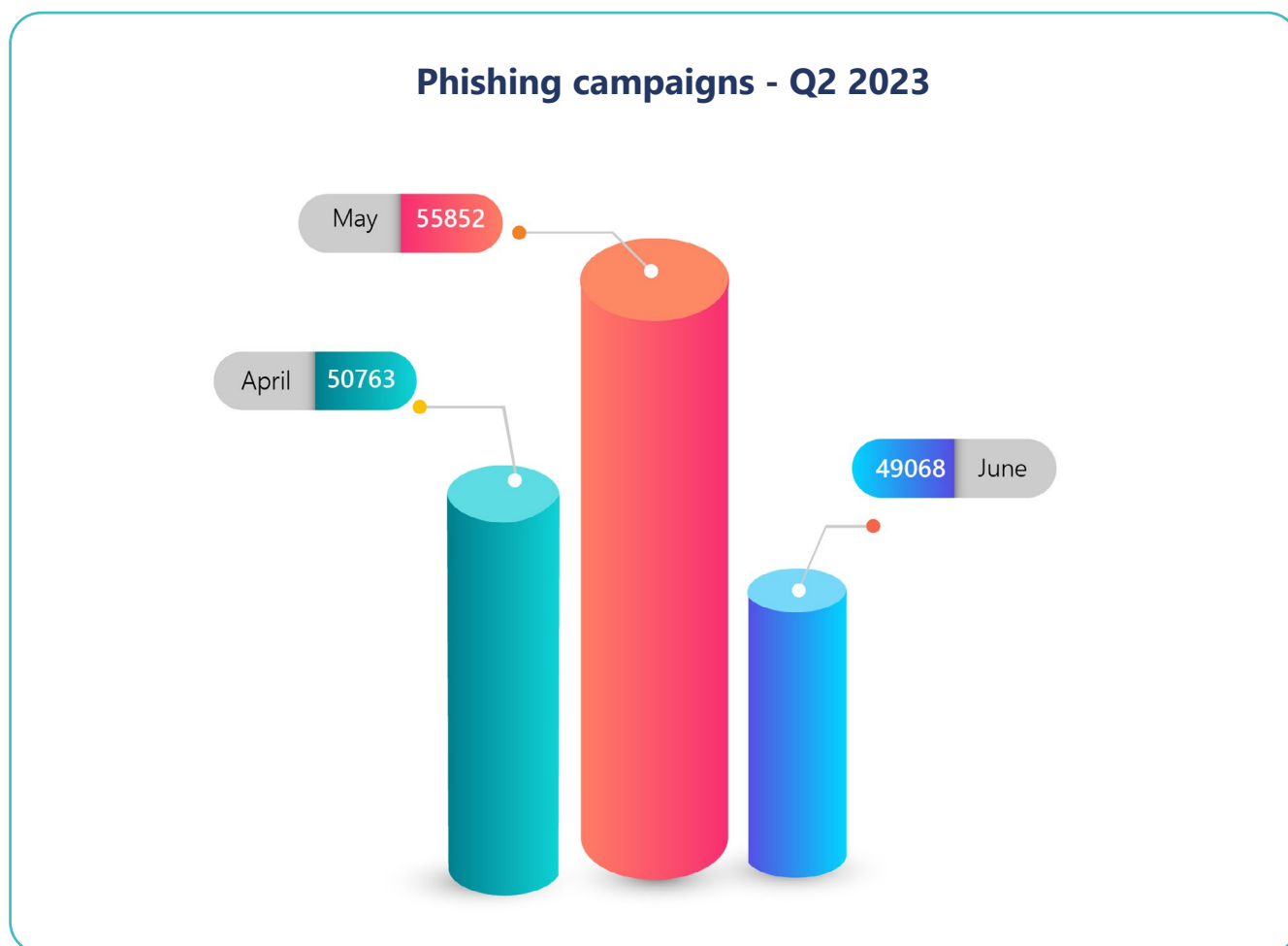
One of the most widespread and damaging threats detected in Q2 is phishing, a cyberattack that aims to deceive users and gain unauthorized access to their information.

In the context of the Cyber Kill Chain, phishing falls within the “Delivery” phase. The delivery phase represents the moment when the attacker delivers a payload or attack mechanism to the chosen user. Phishing, in particular, uses sophisticated techniques to send deceptive emails, text messages, or communications that appear to come from trustworthy or legitimate sources. Attackers attempt to deceive users by persuading them to click on malicious links, download infected attachments, or disclose sensitive information.

Phishing

The trend of phishing is continually evolving and adapting to new technologies and defense strategies implemented by security experts. Attackers employ increasingly sophisticated methods, such as the use of targeted social engineering techniques and accurate imitation of websites and authentic communications, in order to deceive victims and induce them to take actions that could compromise their security.

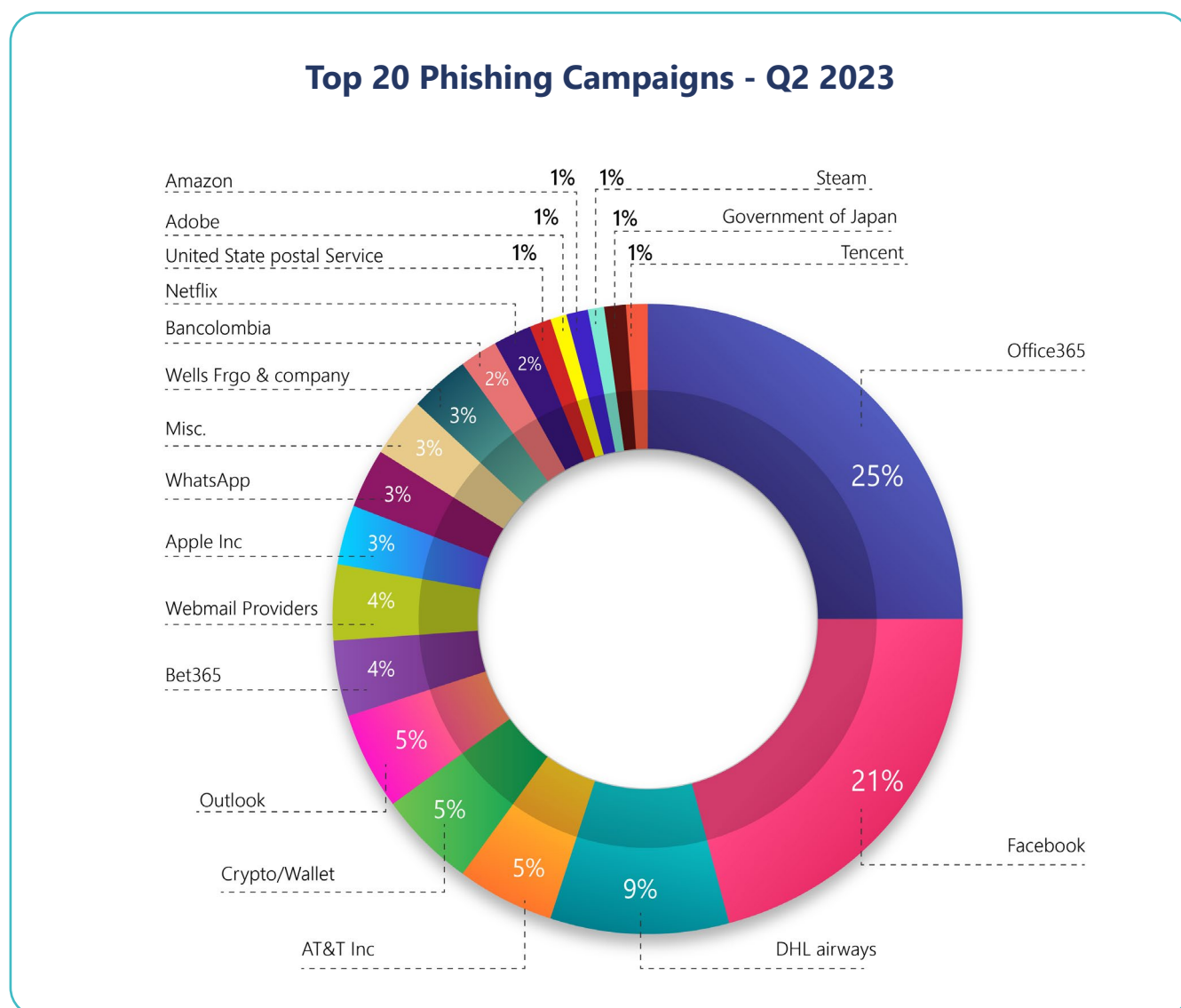
In the second quarter, a total of 155,683 phishing campaigns were detected and distributed as follows:



From the three months under analysis, the top 20 phishing campaigns were extrapolated with the relevant campaign theme.

- » In the month of **April**, **50,763** campaigns were detected, of which 14,507 were identified as Spear Phishing, and 24,117 were related to the top 20 imitated brands.
- » In **May**, **55,852** campaigns were detected, with 15,778 identified as Spear Phishing, and 28,170 related to the top 20 imitated brands.
- » Meanwhile, in **June**, a total of **49,068** campaigns were detected. Among these, 12,141 were identified as Spear Phishing, and 25,842 were related to the top 20 imitated brands.

Below is the percentage breakdown of campaign themes in the second quarter:



In the first place, there's **Office365**, accounting for **25% of phishing attacks**, in second place **Facebook** with **21%**. These campaigns are often used as bait to capture credentials and steal social media accounts.

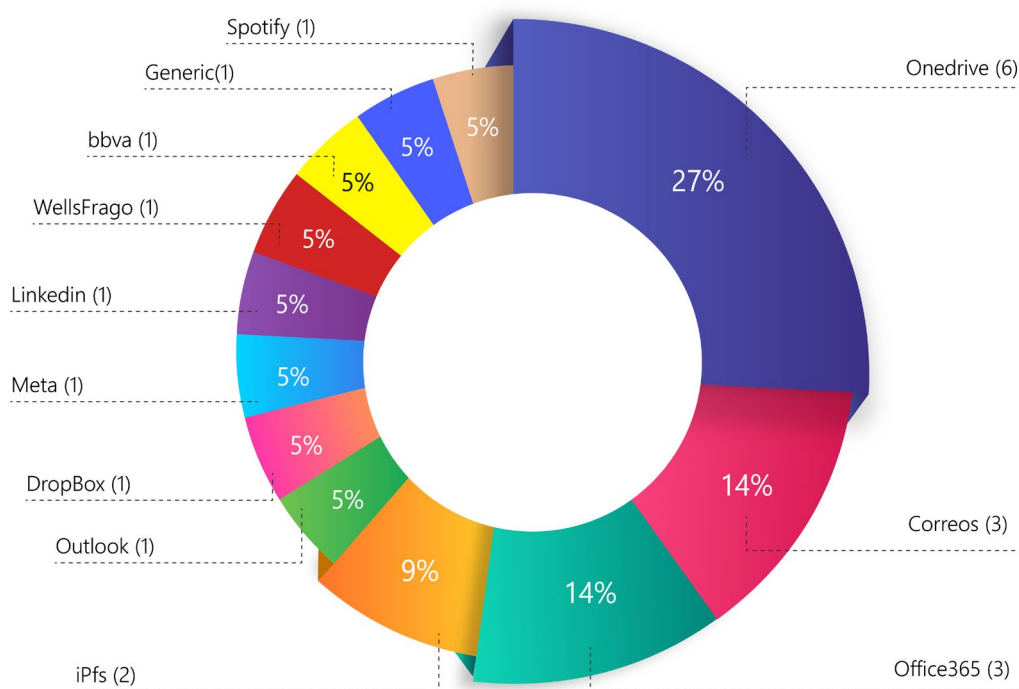
In the third place, there's **DHL** with **9%**, often exploited by hackers to create counterfeit emails that appear legitimate, convincing victims to provide their personal information.

The rest of the list includes AT&T Inc. (5%), Crypto/Wallet (5%), Outlook (5%), Bet365 (4%), Webmail Providers (4%), Apple Inc. (3%), WhatsApp (3%), Wells Fargo & Company (3%), Credit Agricole S.A. (3%), Bancolombia (2%), Netflix (2%), United States Postal Service (1%), Adobe Inc. (1%), Amazon (1%), Steam (1%), Government of Japan (1%), and Tencent (1%).

It shall be noticed that the banking sector is the most targeted by attackers with the aim of exfiltrating login credentials and payment information.

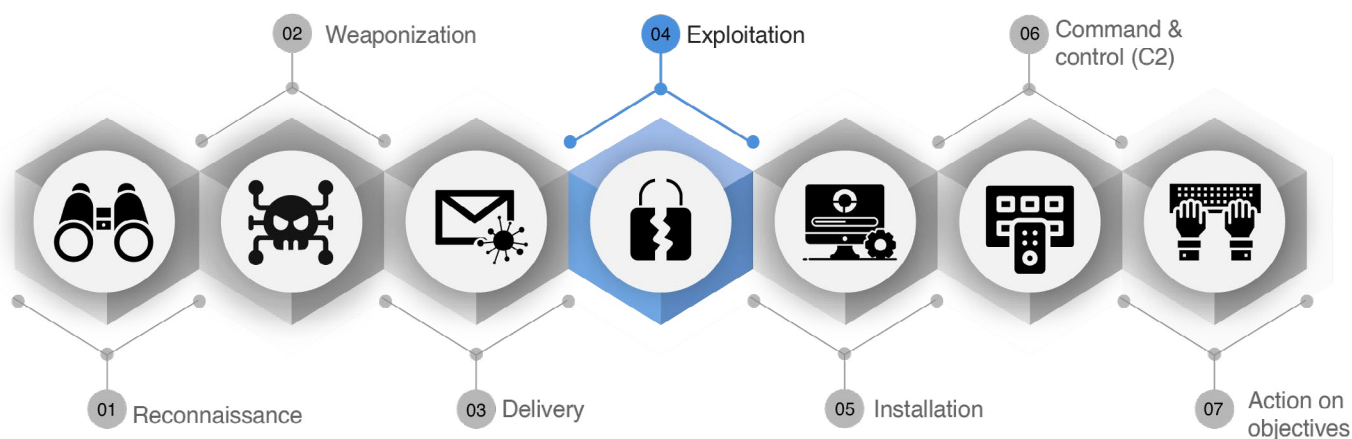
Additionally, **22 phishing kits** were detected in the analysed quarter, where the main themes often revolved around Microsoft services (OneDrive, Outlook, Office365), banking, and social media.

Phishing Kits - Q2 2023



The Phishing kits are often used on a mass scale for campaigns aimed at capturing sensitive information (credentials, credit cards) or for the deployment of malware that can range from Information Stealer to Remote Access Trojan, with the latter then proving to be the initial attack vector for ransomware campaigns.

EXPLOITATION



In the second quarter of 2023, we further identified the CVEs related to the quarter that, given their severity, could allow an attacker to enter infrastructure and execute arbitrary code.

Within the context of the Cyber Kill Chain, a model used to understand, and address cyberattacks, and the exploitation of CVEs falls within the “Exploitation” phase.

The Exploitation phase represents one of the crucial moments within the Cyber Kill Chain, during which attackers seek to exploit a vulnerability or flaw in the target system to gain unauthorized access. It is the next step after the delivery phase, where the malicious payload is delivered to the user or target environment.

During the Exploitation phase, attackers use a range of sophisticated techniques to take advantage of vulnerabilities in software, operating systems, or network configurations. These vulnerabilities can result from programming errors, missing patches, or inadequate configurations, providing opportunities for attacker entry.

Attackers can employ various methodologies to carry out the exploit. For example, they may use “zero-day” exploits that target previously unknown vulnerabilities not yet patched by software providers. Alternatively, they can use known exploits that have not yet been corrected by users or organizations.

Specifically, these vulnerabilities could be used to deliver ransomware or infect devices en masse with malware (e.g., Information Stealer, RAT).

CVE

Below are the CVEs most discussed and exploited by Threat Actors and related to Q2 2023:

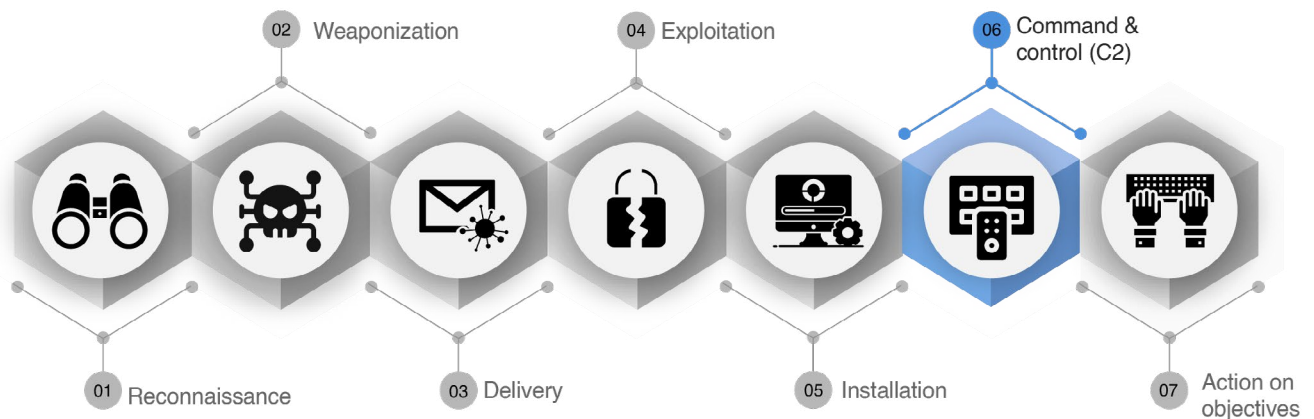
CVE ID	Summary	CVSScore
CVE-2023-34362	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions.	9.8
CVE-2023-27997	A heap-based buffer overflow vulnerability [CWE-122] in FortiOS version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, version 1.2 all versions, version 1.1 all versions SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.	9.2
CVE-2023-2868	A remote command injection vulnerability exists in the Barracuda Email Security Gateway (appliance form factor only) product affecting versions 5.1.3.001-9.2.0.006. The vulnerability arises out of a failure to comprehensively sanitize the processing of .tar file (tape archives). The vulnerability stems from incomplete input validation of a user-supplied .tar file as it pertains to the names of the files contained within the archive. As a consequence, a remote attacker can specifically format these file names in a particular manner that will result in remotely executing a system command through Perl's qx operator with the privileges of the Email Security Gateway product. This issue was fixed as part of BNSF-36456 patch. This patch was automatically applied to all customer appliances.	9.8

CVE-2023-2982	The WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 7.6.4. This is due to insufficient encryption on the user being supplied during a login validated through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they know the email address associated with that user. This was partially patched in version 7.6.4 and fully patched in version 7.6.5.	9.8
CVE-2023-33299	A deserialization of untrusted data in Fortinet FortiNAC below 7.2.1, below 9.4.3, below 9.2.8 and all earlier versions of 8.x allows attacker to execute unauthorized code or commands via specifically crafted request on inter-server communication port. Note FortiNAC versions 8.x will not be fixed.	9.8
CVE-2023-28424	Soko if the code that powers packages.gentoo.org. Prior to version 1.0.2, the two package search handlers, `Search` and `SearchFeed`, implemented in `pkg/app/handler/packages/search.go`, are affected by a SQL injection via the `q` parameter. As a result, unauthenticated attackers can execute arbitrary SQL queries on `https://packages.gentoo.org/`. It was also demonstrated that primitive was enough to gain code execution in the context of the PostgreSQL container. The issue was addressed in commit `4fa6e4b619c0362728955b6ec56eab0e0cbf1e23y` of version 1.0.2 using prepared statements to interpolate user-controlled data in SQL queries.	9.8
CVE-2023-32434	An integer overflow was addressed with improved input validation. This issue is fixed in watchOS 8.8.1, iOS 16.5.1 and iPadOS 16.5.1, iOS 15.7.7 and iPadOS 15.7.7, macOS Big Sur 11.7.8, macOS Monterey 12.6.7, macOS Ventura 13.4.1, watchOS 9.5.2. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.	7.8
CVE-2023-32435	A memory corruption issue was addressed with improved state management. This issue is fixed in Safari 16.4, iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3, iOS 15.7.7 and iPadOS 15.7.7. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.	8.8

CVE-2023-20887	Aria Operations for Networks contains a command injection vulnerability. A malicious actor with network access to VMware Aria Operations for Networks may be able to perform a command injection attack resulting in remote code execution.	9.8
CVE-2023-32031	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8

The 0-Day relating to CVE-2023-34362, for instance, was actively exploited by the Ransomware Cl0p gang, leading the group to compromise more than 150 organisations, including companies in the consulting, technology, and energy sectors, and leading to the estimated compromise of personal data of more than 16 million people.

COMMAND & CONTROL



In the second quarter of 2023, malware continues to pose a threat to the security of companies and individuals worldwide.

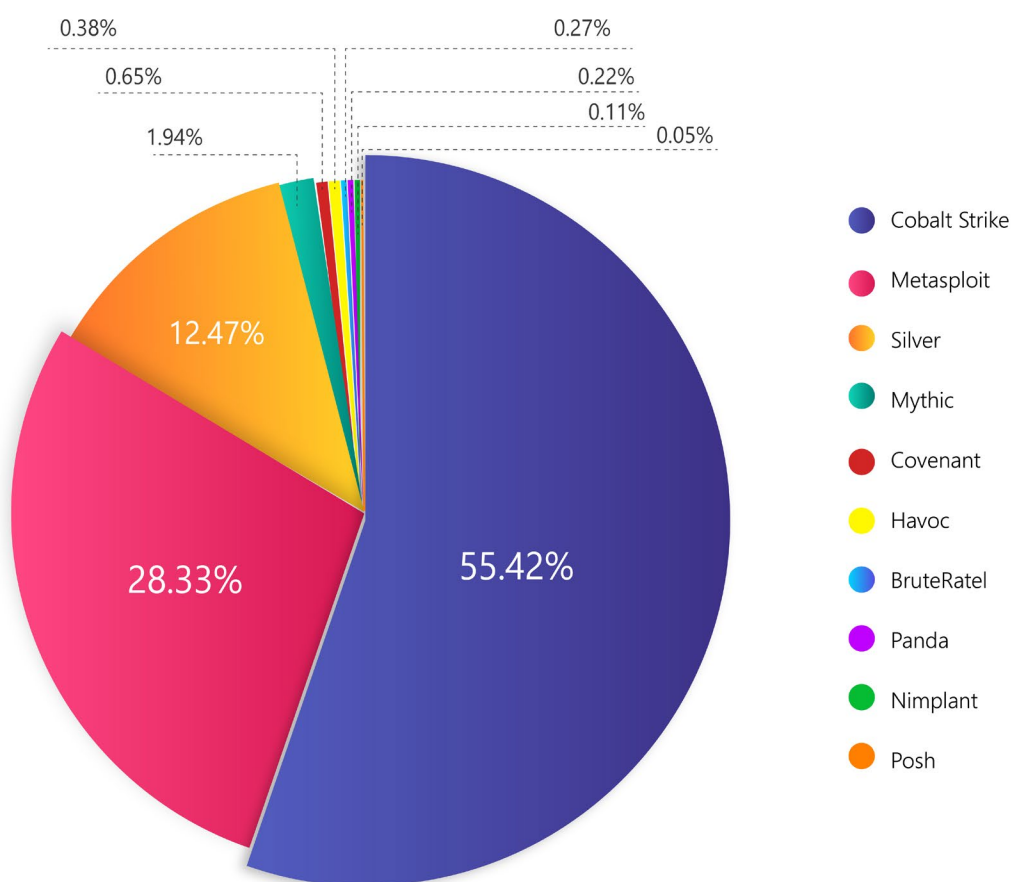
In the context of the Cyber Kill Chain, the installation of malware for communication with a remote server is in the 'Command & Control' phase.

The Command & Control ('C2') phase is crucial for attackers, as it allows them to maintain control over compromised machines and continue to perform malicious operations undetected. It is essential that organisations implement advanced threat detection solutions to identify and block communication between compromised systems and attackers.

During the C2 phase, attackers use a variety of techniques and tools to maintain control over and interact with the compromised system. This involves the use of sophisticated malware and Command & Control frameworks.

CobaltStrike came in first place, accounting for 55.42 per cent of the C2 frameworks used, while Metasploit and Silver came in second and third with 28.33 per cent and 12.47 per cent respectively.

The most popular frameworks - Q2 2023



CONCLUSIONS

During the first half of 2023, the ransomware threat continued to disrupt organizations worldwide significantly. Among the active ransomware groups, LockBit emerged as a particularly impactful actor, causing substantial damage to numerous organizations. The overall landscape for H1 2023 suggests a concerning uptick in the number of ransomware victims compared to previous periods.

Fortunately, authorities have not overlooked the criminal hacker community's focus on stolen credentials. International law enforcement's actions resulted in the closure of two major illicit marketplaces specializing in the trade of pilfered information. However, this shift has led cybercriminals to favour trojans and information stealers to access sensitive data, which is no longer as readily available.

The insights from this study provide glimpses into potential future cybercrime scenarios. To effectively counter the evolving threat landscape, proactive measures are essential. This involves anticipating potential attack vectors and proactively engaging with individual stages of the cyber kill chain before they reach fruition.

This proactive approach encompasses not only the implementation of technical security measures but also a comprehensive awareness campaign regarding these threats, both within the private and public sectors.

COME DIFENDERSI DAL RANSOMWARE: IL CYBER SECURITY FRAMEWORK

The most effective approach to bolster perimeter resilience entails adherence to the three fundamental pillars of modern Cyber Security. For this reason, it is imperative to consolidate and uphold these three tenets:

- **Predictive Security**
- **Preventive Security**
- **Proactive Security**

Predictive Security

1. Identify cyber threats beyond the corporate perimeter by operating at the web, Dark web, and Deep web levels.
2. Search for potential emerging threats.
3. Conduct early warning activities.
4. Provide evidence to pre-emptive security measures.
5. Highlight areas of concern for proactive security efforts



Proactive Security

1. Identify cyber threats operating within the corporate perimeter.
2. Counter and block cyberattack.
3. Manage cyber incidents.
4. Provide evidence to pre-emptive security measures.
5. Indicate investigation areas for predictive security.

Preventive Security

1. Verify and measure Cyber Risk.
2. Define remediation plans.
3. Identify the risk exposed at the Proactive Security Layer.
4. Provide areas of investigation for Predictive Security.

Action plan

In line with the best practices described in the cyber security framework, it is recommended to implement a cyber security action plan based on the following steps:

Predictive Security:



Domain Threat Intelligence: Domain Threat Intelligence research publicly and semi-publicly available information related to domain vulnerabilities, subdomains, and compromised emails. The service does not perform any testing on the target but solely operates on information available on the web, Dark web, and deep web. It gathers, analyses, and clusters information available through OSINT (Open-Source Intelligence) and Closint (Close Source Intelligence) from databases, forums, chats, newsgroups. Specifically, based on the target domain under analysis, it identifies:

- Potential Vulnerabilities
- Vulnerability details in terms of CVE, impacts, and severity
- GDPR impacts (CIA)
- Number of Subdomains
- Number of Potential compromised emails (counted but not collected or processed)
- Number of sources of compromised emails
- Typo squatting

Cyber Threat Intelligence: This is Swascan's advanced Threat Intelligence service. It conducts research, analysis, and collection of information available on the web, Dark web, and Deep web regarding the domain/target under analysis. Specifically:

- Data Leaks: credentials/sources/data
- Identifies Forums/Chats ...
- Botnets related to devices of Clients, Suppliers, and employees
- Botnets with credentials and related login page URLs
- Typo squatting/Phishing
- Surface
- Top Manager Analysis



Preventive Security:

Vulnerability Assessment: It performs scans of websites and web applications to proactively identify and analyse security vulnerabilities.

Penetration Test: Penetration Test activities are carried out by certified Penetration Testers and in line with international standards such as OWASP, PTES, and OSSTMM.

Phishing/Smishing attack Simulation: This allows companies to prevent damages caused by phishing/smishing attacks through actual attack simulations. Through a web interface, it is possible to send real phishing/smishing attack campaigns that create invaluable learning opportunities for employees. Thanks to these simulated attacks, employees will be able to identify and avoid real phishing emails or smishing messages in the future. This is an irreplaceable training and awareness activity for your employees through real phishing/smishing attack simulations.

Awareness (Cyber Academy): Dedicated cybersecurity training courses conducted in classrooms or via webinars. Awareness activities for technical personnel, employees, and top managers.



Sicurezza Proattiva:

SOC: Designing, implementing, and maintaining a Security Operation Centre (SOC) can be expensive and complex. Swascan's SOC as a Service is the most effective, efficient, consistent, and sustainable solution for business environments. The SOC as a Service, along with its Monitoring & Early Warning service, allows for the identification, detection, analysis, and reporting of cyberattacks before they can become a tangible threat to the company.

A dedicated team is engaged in the Monitoring & Early Warning of cybersecurity threats in local networks, cloud environments, applications, and corporate endpoints. Our team of Security Analysts monitors data and resources wherever they reside within the company, whether stored in the cloud, locally, or both. The monitoring and reporting activity enables action only when a real threat is identified.

Incident Response Team: Swascan's Cyber Incident Response Team is a 24/7 Cyber Emergency Response service aimed at supporting companies in the response and management of cybersecurity incidents and Ransomware attacks.

In line with the international standard NIST SP 800-61rev2 Computer Security Incident Handling Guide, following a cybersecurity incident, Swascan's Incident Response Team aims to:

- Contain potential damage.
- Determine possible damages and impacts.
- Ensure an effective and efficient response.
- Support the restoration of Business Continuity.
- Provide guidance and suggestions to prevent future incidents from occurring.

DISCLAIMER

In this analysis, when victim numbers are mentioned, only those entities were taken into account that not only suffered a ransomware attack but were also victims of Data Leak via double extortion.

ABOUT US



The European DIGITAL SME Alliance is the largest network of small and medium-sized ICT companies in Europe, representing over 45,000 businesses in total. SME Alliance is the collective effort of 30 national and regional associations of SMEs from EU member states and neighbouring countries to place digital SMEs at the centre of the EU's agenda.



Swascan is a Cyber Security Company born from an idea by Pierguido Iezzi and Raoul Chiesa.

The first Italian Cyber Security company that owns a Cyber Security Testing and Threat Intelligence platform, as well as an award-winning Cyber Competence Centre recognized by numerous national and international players in the IT and beyond. Since October 2020, Swascan has been an integral part of the Tinexta S.P.A. Group, a company listed on the STAR segment of Borsa Italiana.

Swascan has become an active protagonist in the first national cyber security hub: not just a company but an Italian group, a new national hub specializing in digital identity and digital security services.

Analysis by:

Swascan

Technical Contributors:

Swascan Cyber Threat Intelligence Team

Editing & Graphics:

Federico Giberti

Melissa Keysomi

Contact Info

Milano

+39 0278620700

www.swascan.com

info@swascan.com

Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI