Swascan
TINEXTA GROUP

Threatland Report H2 2023

www.swascan.com
info@swascan.com

CONTENTS

Disclaimer

The research conducted by Swascan is based on OSINT and CLOSINT data obtained through Threat Intelligence. This publication does not necessarily represent the state of the art – given the transient nature of the sources - and Swascan reserves the prerogative to update periodically. Third-party sources are cited as appropriate. Swascan is not responsible for the content of exter-nal sources, including external websites referred to in this publication. This publication is for in-formational purposes only. It is intended to be accessible free of charge. Neither Swascan nor any person acting on its behalf is responsible for the use that may be made of the information con-tained in this publication.

About us

Swascan

Swascan is a Cyber Security Company born from an idea of Pierguido Iezzi and Raoul Chiesa. The first Italian Cyber Security company owning a Cyber Security Testing and Threat Intelligence platform, as well as a Cyber Security Research center of excellence; a center awarded with numerous national and international awards by the most important players in the IT market and beyond. Since October 2020, Swascan has been an integral part of Tinexta Cyber (Tinexta S.P.A), becoming an active player in the first national Cyber Security hub: not just a company, but an Italian group, a new national hub specialized in digital identity and digital security services.

Tinexta

Tinexta is an Industrial Group that offers innovative solutions for digital transformation and growth of businesses, professionals and institutions. Listed on Euronext STAR Milan (MIC: MTAA), it is included in the European Tech Leader index as a high-growth tech company. Based in Italy and present in 12 countries across Europe and Latin America with more than 2,500 employees, Tinexta is active in the strategic sectors of Digital Trust, Cyber Security and Business Innovation. As of December 31, 2022, the Group reported consolidated revenues of € 357.2 mil-lion, Adjusted EBITDA of € 94.8 million and Net Income of € 78.1 million. Through its Group companies, Tinexta promotes an integrated offering of advanced services for digital identity and certification, cybersecurity, digital marketing, access to financing for innovation and interna-tionalization. It manages complex digital transformation projects and implements targeted de-velopment strategies to support the innovation plans of small and medium-sized companies, large groups and institutions. A widespread territorial presence and a vocation international, a high degree of operational agility and solid institutional oversight, a wealth of resources of high professionalism and the enhancement of skills are the distinctive features of the Group. Thanks to them, Tinexta today continues to grow in domestic and foreign markets, anticipating chal-lenges and trends, innovating processes and growing the business.

Data collection notice

This report was compiled exclusively by Swascan's Security Operations Center (SOC) and Threat Intelligence Team, through the use of Open Source Intelligence (OSINT) and Closed Source Intelligence (CLOSINT) techniques, as well as Swascan's proprietary platform. The information collected and presented in this paper represents only the emerged part of the whole situation, as only companies affected by ransomware attacks that, having refused to pay the ransom, had their data published on data leak sites were considered.

It is emphasized that the number reported in this report reflects a general trend based on availa-ble information. However, it is crucial to understand that this figure represents only the tip of the iceberg, as the actual number of victims could be significantly higher, considering a multipli-cation factor n times larger.

Swascan cannot guarantee the accuracy or completeness of the information provided in the re-port, as this data is subject to change and may be influenced by various external factors. Users are therefore urged to carefully consider the context and complexity of the situation before draw-ing firm conclusions or making decisions based on this information.

No liability is accepted for any consequences arising from the use of the information contained in this report. Swascan is committed to maintaining the utmost confidentiality and professionalism in its analytical activities and provides this report for informational purposes without assuming any legal or other liability.

H2 2023 – a first look

The second half of 2023 saw a significant increase in cyber-attacks aimed at stealing data and demanding ransoms in exchange for restoring affected systems. Swascan's SOC and Threat Intelligence Team conducted an in-depth analysis on ransomware, malware and phishing scenarios, providing a detailed picture of emerging threats and evolving trends.

Numerous ransomware campaigns were observed during H2, characterized by the spread of ma-licious software that encrypts victims' data and then demands a ransom to repriransom them. These attacks have affected a wide range of industries, including financial, healthcare, and governmental, putting information security and business continuity at risk.

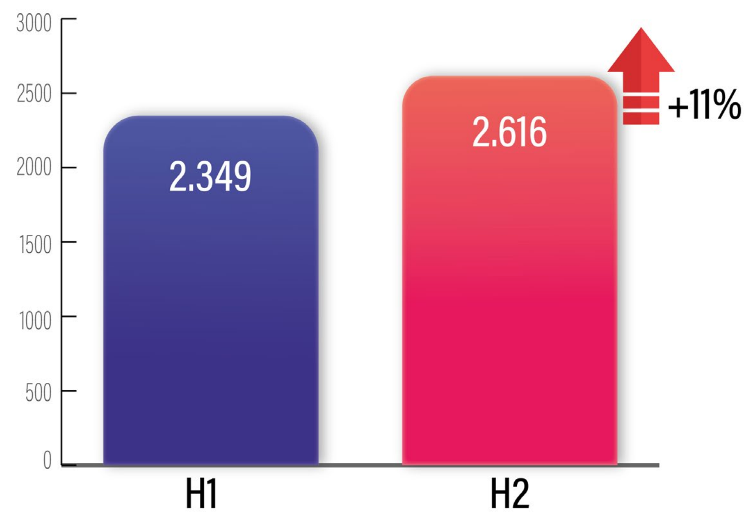
The evolution of tactics used by cybercriminals, especially in H2, has been particularly troubling. Ransomware has become increasingly sophisticated and targeted, and numerous new ransomware gangs have emerged.

Parallel to ransomware attacks, phishing has continued to pose a significant threat to cybersecurity. Attackers have used increasingly sophisticated methods to deceive users, creating deceptive emails, websites, and text messages that appear to come from legitimate sources. Through these techniques, attackers try to obtain sensitive information such as passwords, financial data, and login credentials in order to commit fraud and harm victims.

In this report, we will analyze the major recorded ransomware and phishing attacks, highlighting modes of operation, victims, affected regions, and emerging trends, and examine recommended security measures to mitigate the risk of these threats.

H1 e H2 what has changed – Ransomware

Ransomware Attacks



Affected countries

H1

89

H2

94

Active groups

H1

43

H2

52

H2 in detail - Ransomware

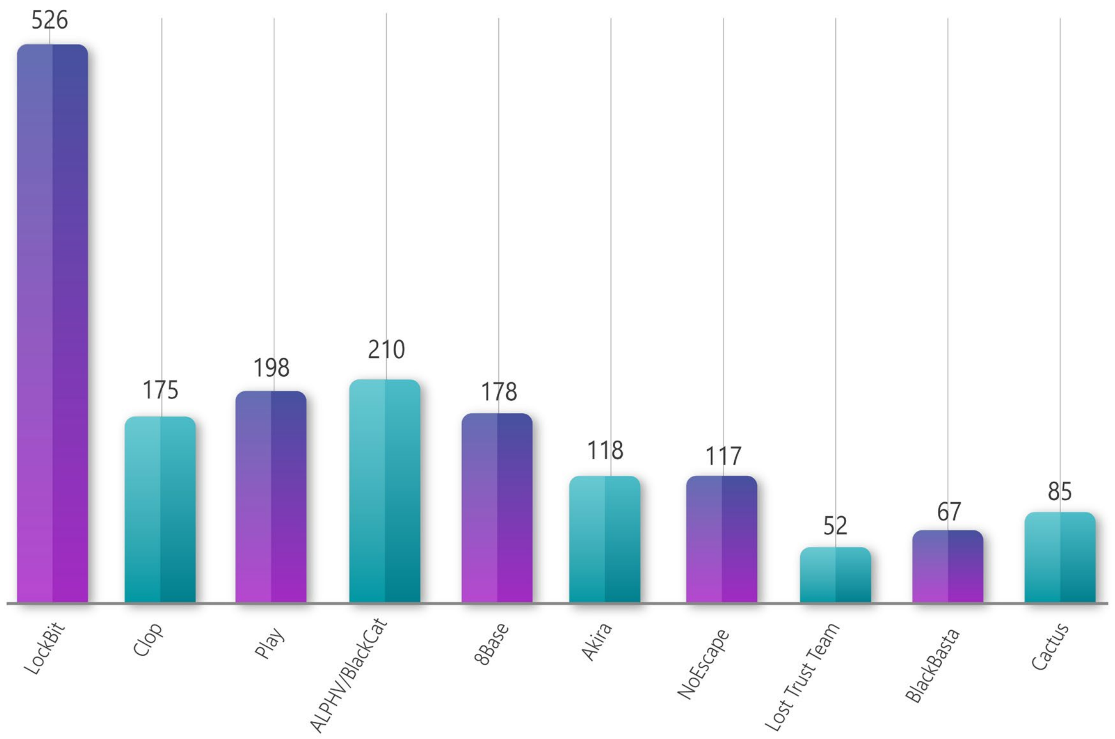
H2 - 2023

2.616 Total victims

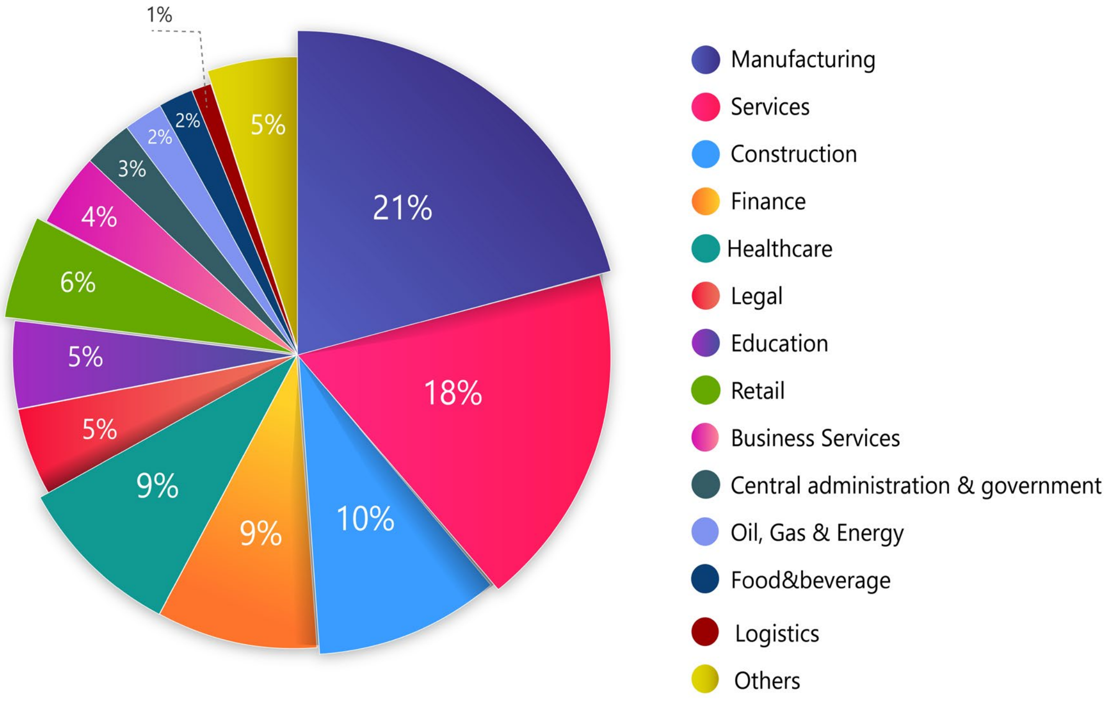
94 Attacked countries

52 Active gangs

Numbers of victims H2 - 2023



Attacks by sectors H2 - 2023



What numbers says?

The ranking of ransomware victims by industry provides a significant overview of the areas most affected by this rapidly growing cyber threat. We carefully analyze the data to understand emerging trends and possible implications for cybersecurity in different industries.

Manufacturing: 21%

The dominance of the manufacturing sector could be attributed to its increasing digital intercon-nection, with the presence of complex infrastructure and dependence on automated systems. The manufacturing industry should further focus on cybersecurity to mitigate future risks.

Services: 18%

The service sector, being large and diverse, presents a wide range of targets for ransomware at-tacks. Companies in the industry should implement advanced defense strategies, considering the diversity of services offered.

Construction: 10%

Despite the common perception that the construction sector may be less vulnerable, 10 percent indicate a significant presence of ransomware. This could be due to increasing digitalization in the industry and dependence on data management systems.

Finance: 9%

Financial institutions have traditionally been prime targets. Despite efforts to implement ad-vanced security measures, the financial sector remains vulnerable due to the high value of the information it handles.

Healthcare: 9%

The presence of ransomware in the healthcare sector is alarming, considering the sensitivity of personal and healthcare data. The need to implement robust security measures is imperative to ensure continuity of care and protect patient privacy.

Legal: 5%

Even the legal sector is not immune to ransomware attacks, with 5% of victims. Access to sensi-tive and confidential information makes it an attractive target for attackers.

Education: 5%

Education, with 5%, may be targeted due to the increasing digitization of academic institutions. Protection of student data and academic information is essential.

Retail: 6%

The retail sector, at 6%, may be vulnerable due to its large online presence and financial transac-tions. Companies need to focus on security solutions to protect both customer data and business operations.

Business Services: 4%

The variety of business services contributes 4%. Companies must implement advanced security measures to ensure the protection of corporate and customer data.

Central Administration and Government 3%

The presence of ransomware in the government sector underscores the importance of ensuring the security of sensitive information and public services.

Oil, Gas and Energy: 2%

The energy sector is also involved, highlighting the need to protect critical infrastructure against cyber-attacks.

Food and Beverage: 2%

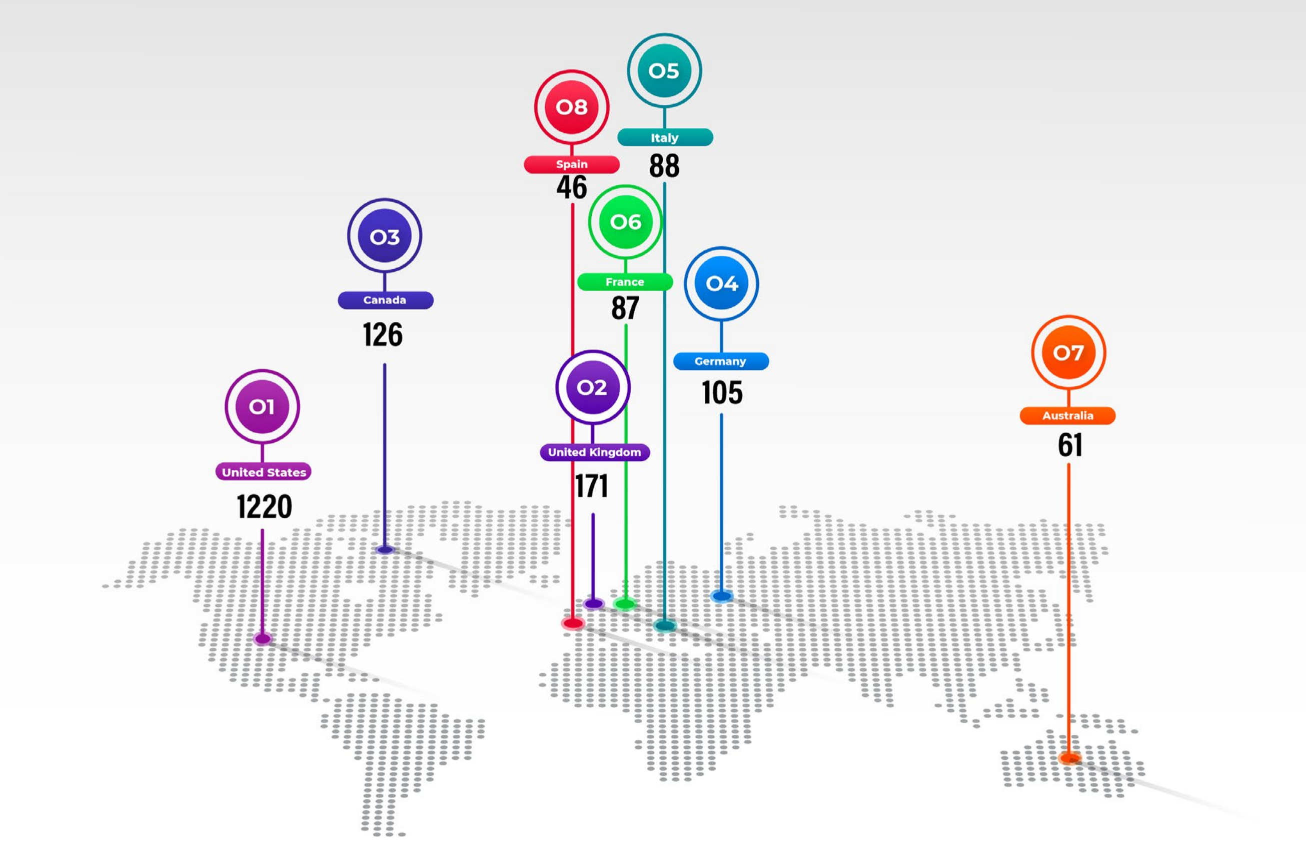
Despite the relatively low percentage, the food and beverage sector is an attractive target be-cause of the complex supply chain and the data sensitivity.

Logistics: 1%

Although the logistics sector accounts for only 1%, its importance in supply chain management makes it a significant target.

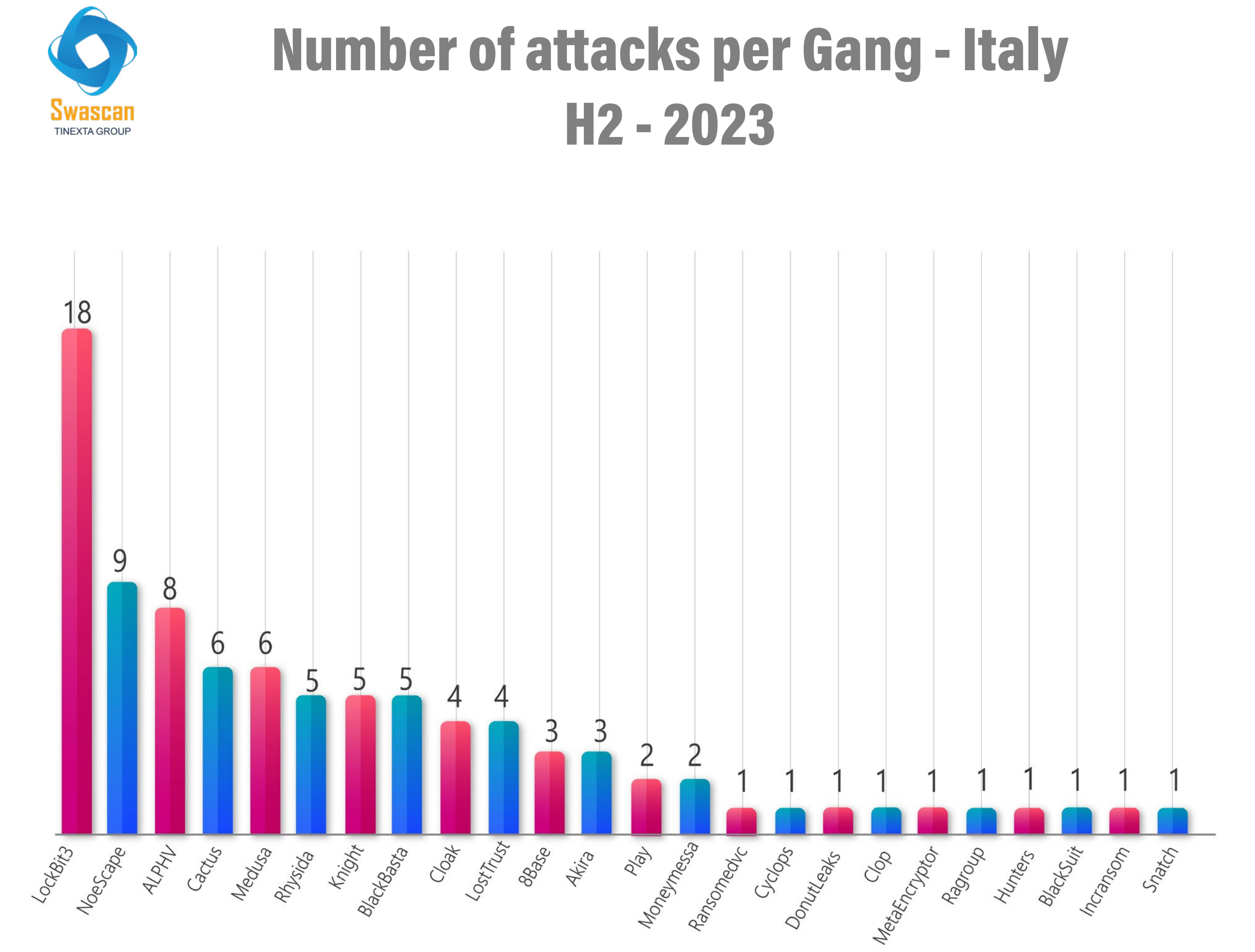
The geography of the victims

Top 8 attacked countries H2 - 2023

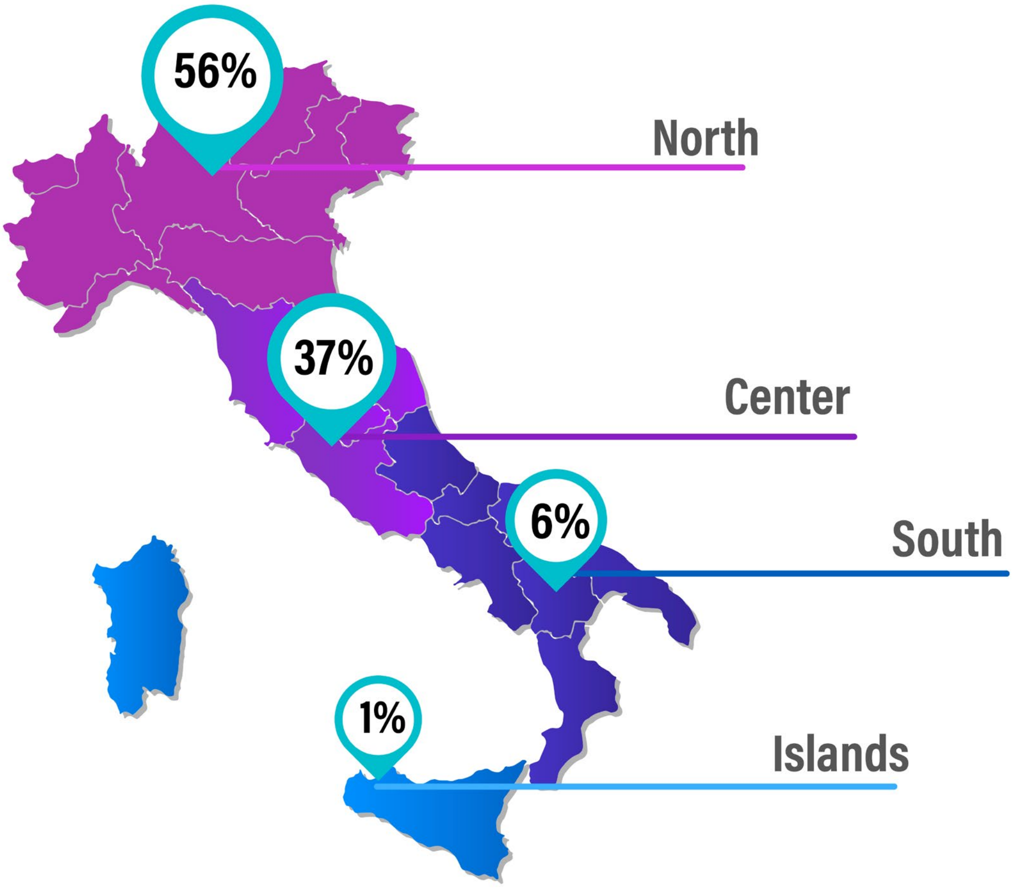


01	United States	1220
02	United Kingdom	171
03	Canada	126
04	Germany	105
05	Italy	88
06	France	87
07	Australia	61
08	Spain	46

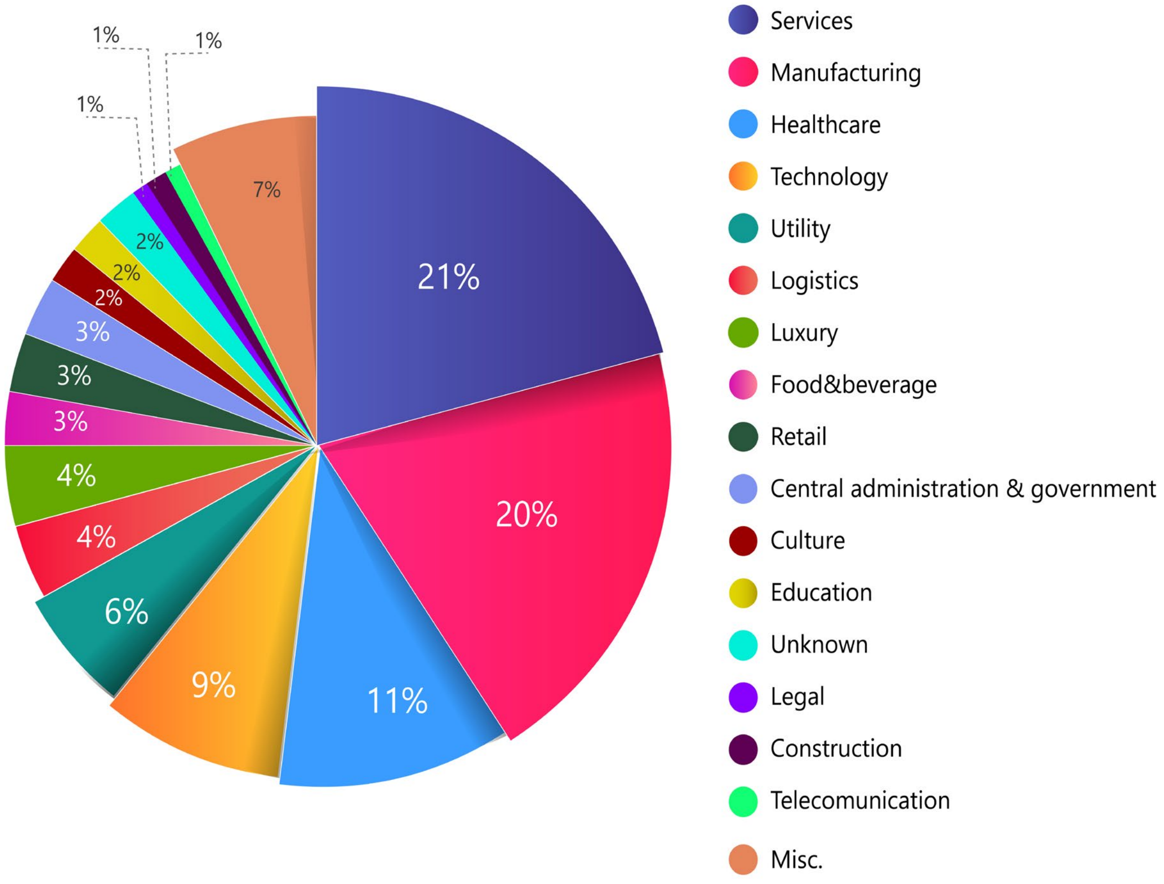
H2 Italy – Ransomware



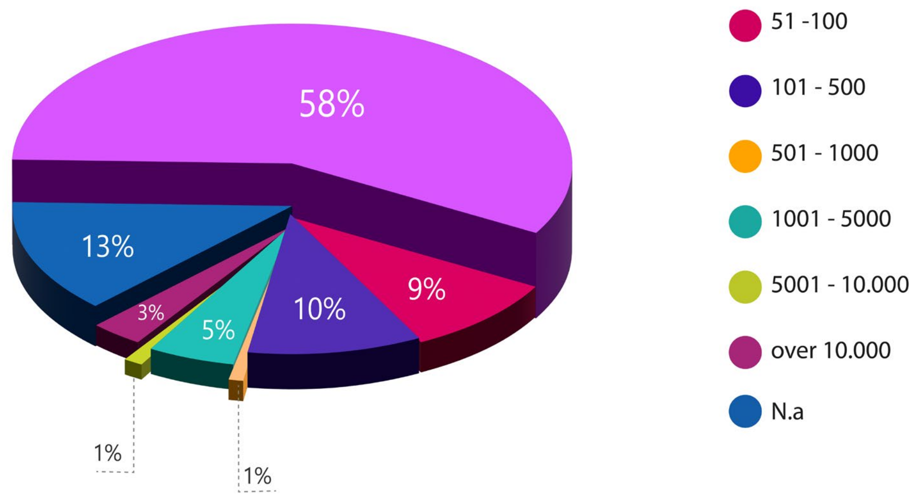
Attacks by regions - Italy
H2 - 2023



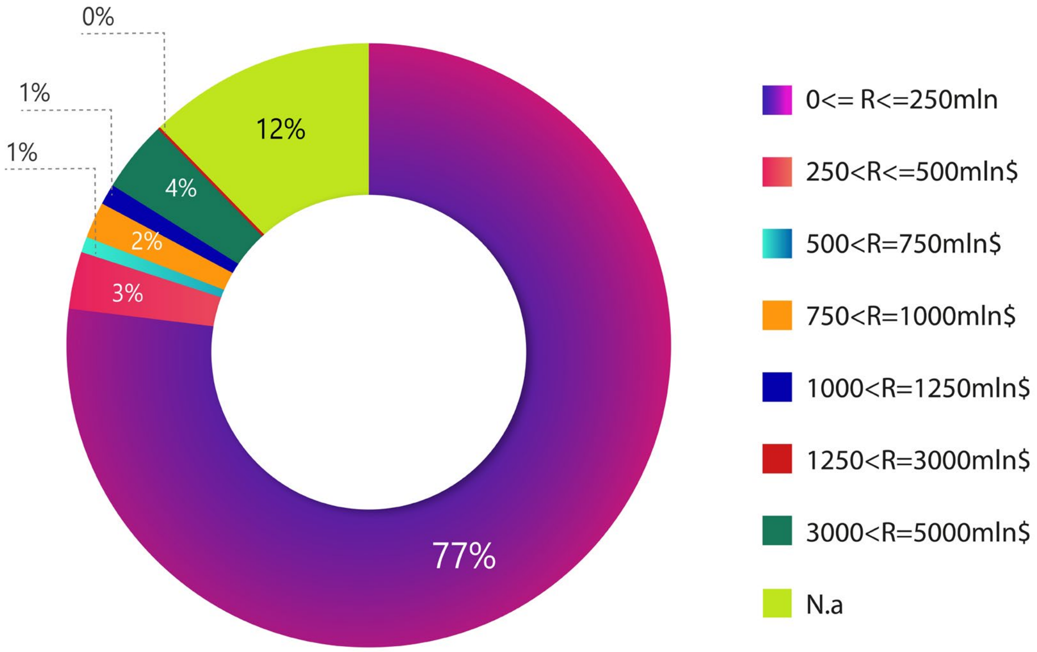
Attacks by sectors - Italy
H2 - 2023



Number of Employees of Affected Companies Italy - H2 2023



Affected Companies Based on Turnover- Italiy - H2 2023



Key Take aways

An analysis of data on ransomware attacks in Italy in the second half (H2) of the year offers a detailed look at the situation, including the gangs involved, the sectors affected, the dimensions of the companies involved, and the turnover of victims. Here is a scrutinized and eloquent examination:

Gangs involved

During the reporting period, Italy experienced a total of **88 ransomware attacks**. The gangs involved show a variety of actors, with **Lockbit3** leading the way, recording 18 attacks. **Alphv** and **NoEscape** follow with 8 and 9 attacks, respectively. The diversity of gangs reflects a growing and articulated mini attack by malicious actors with increasingly sophisticated tactics.

Sectors Affected

The sectors most affected by ransomware attacks are **services (21%)** and **manufacturing (20%**). Growing digital dependence in critical sectors such as **healthcare (11%)** and **technology (9%)** demonstrates the pervasiveness of the threat. Other affected sectors include utilities, logistics, luxury, and food, revealing a diversification of victims.

Corporate Size

Most of the affected companies have between 1 and 50 employees **(58%)**. This suggests that ransomware attacks not only affect large enterprises, but also SMEs. The involvement of companies of various sizes underscores the need for universal security measures.

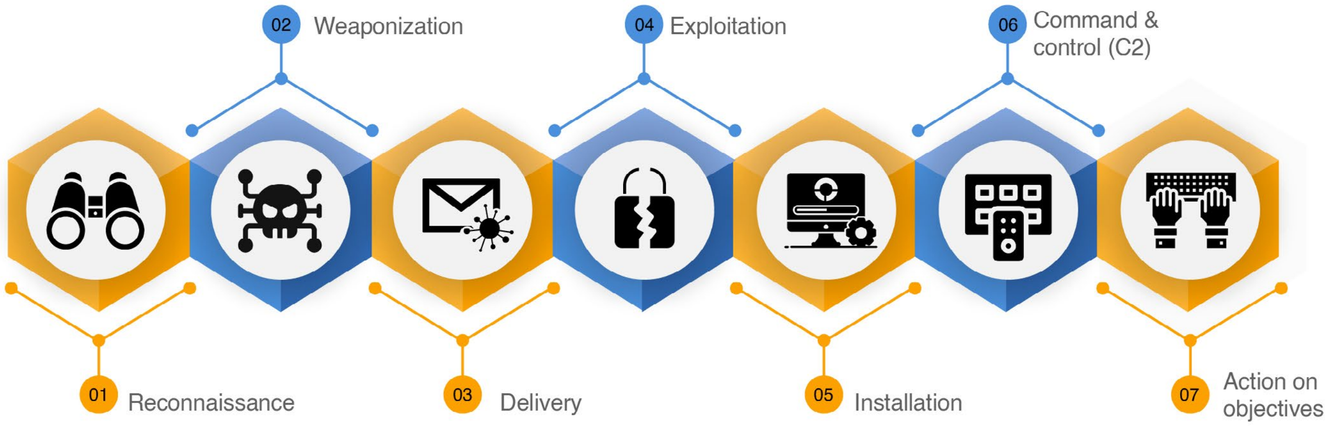
Corporate Turnover

Analysis of the turnover of affected companies shows that the vast majority **(77%)** have revenues between $0 and $250 million. This finding underscores that even companies with relatively modest revenues are vulnerable to ransomware attacks. The diversity of victimes, from an economic perspective, highlights the need for security solutions at all business sizes.

The cyber kill chain: a strategic approach to defending against cyber attacks

After looking at the most significant numbers for ransomware attacks, let's take a step back and take a look at how people come to suffer an attack.

In the increasingly complex and frequent landscape of cyber attacks, the Cyber Kill Chain emerges as a key tool for identifying and countering threats from criminal hackers. This defense methodology, inspired by the Kill Chain concept used in the military field, has been adopted in the cyber security sector in order to identify the stages through which an attack develops and to prepare an appropriate defensive strategy, and consists of seven well-defined phases. These phas-es represent the steps that a potential criminal hacker would have to take to carry out an attack and allow one to understand the attackers' modus operandi, identifying the signs of attack and putting in place the necessary coutermeasures.



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

1. **Reconnaissance:** at this stage, the criminal hacker identifies the target and conducts extensive research to identify vulnerabilities present in the target's security system. This phase is of fundamental im-portance because it determines the success of the subsequent phases.

2. **Weaponization:** in the second step, the attacker uses the information gathered in the previous step to select the most suitable tools to create remote access to the target system.

3. **Delivery:** at this stage, the created malware is delivered to the target through various vectors, such as phishing emails or links found 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.

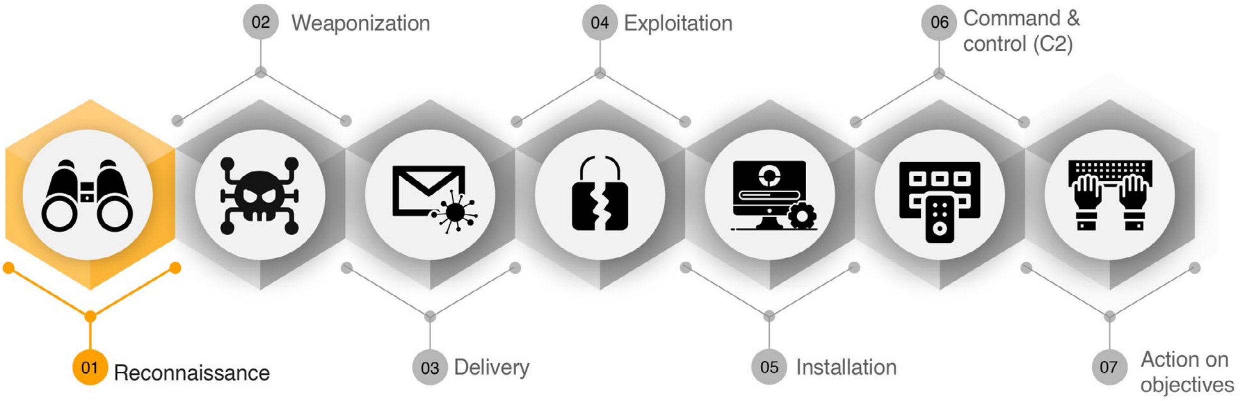
5. **Installation:** during the installation phase, the attacker makes sure to install and execute the malware in the target system. This allows it to bypass security controls and maintain access to the system. The installation of the malware occurs through the exploit selected during the weaponization 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 last link in the chain, attackers carry out the attack by hitting the intended target, and this can lead to data manipulation, exfiltration of sensitive information, data destruction, or un-authorized access to confidential resources.

The Cyber Kill Chain provides a strategic framework for understanding cyber-attacks and acting accordingly. There is no one-size-fits-all approach to dealing with an attack, but this model allows you to put yourself in the attacker's shoes and take a similar approach to prevent or mitigate the intrusion. In the analysis below we will look at the different stages of the Cyber Kill Chain in detail.

Reconnaissance



The reconnaissance phase is the first important stage within the Cyber Kill Chain, during which attackers gather valuable information to plan a targeted attack. During this stage, several strategies are adopted, including, for example, collecting credentials from dark web markets, identifying new vulnerabilities (CVEs), and using social engineering campaigns.

Attackers can acquire sensitive credentials from marketplaces in the Deep and Dark Web, where stolen information such as usernames, passwords, and access details to online systems or ac-counts are illegally exchanged. These credentials can come from previous data breaches or phishing techniques and can be used to gain unauthorized access to si-systems or to impersonate a legitimate user.

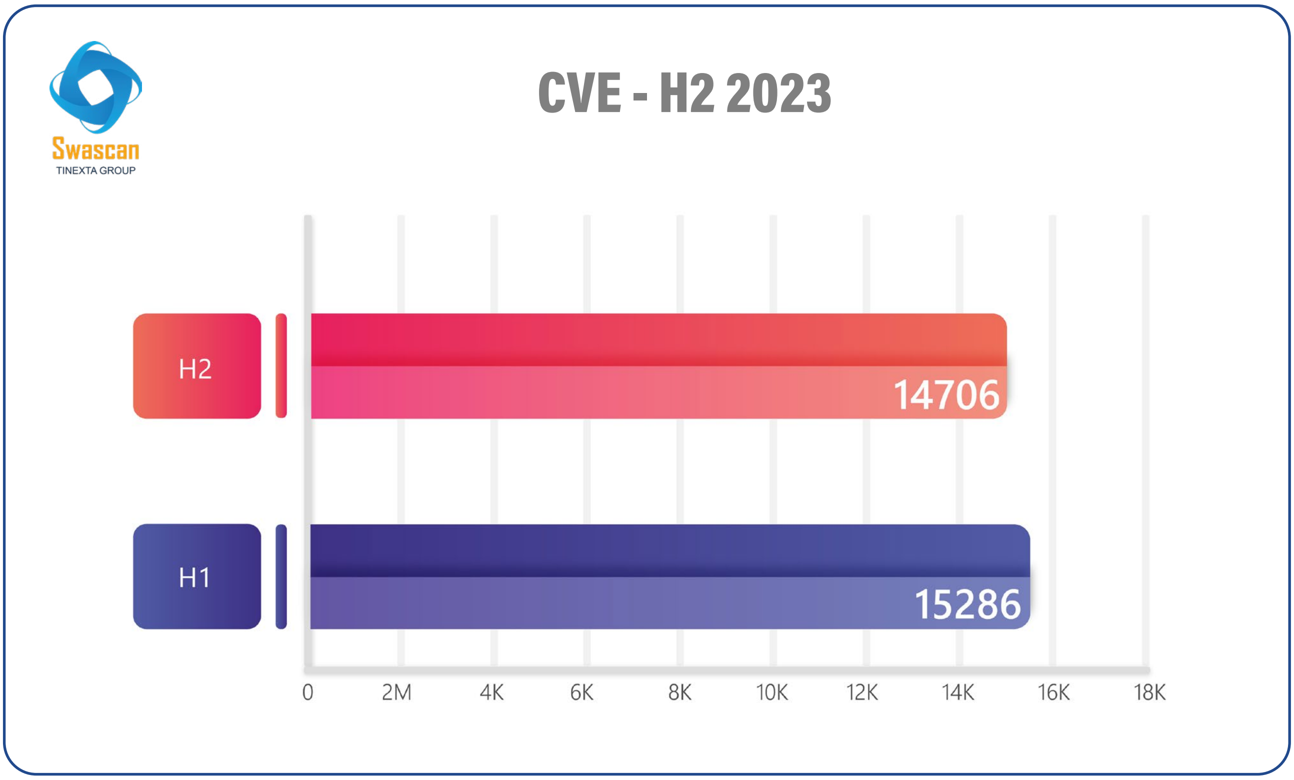
Social engineering campaigns constitute another common tactic in the Reconnaissance phase. Attackers seek to gather valuable information about users or organizations through deception and psychological manipulation. This may involve sending fraudulent e-mails or text messages re-questing sensitive information or inducing users to click on malicious links. For example, **155,683 phishing** campaigns were indeed observed in Q2. Through these tactics, attackers try to gain access to confidential information or deceive users to facilitate later stages of the attack.

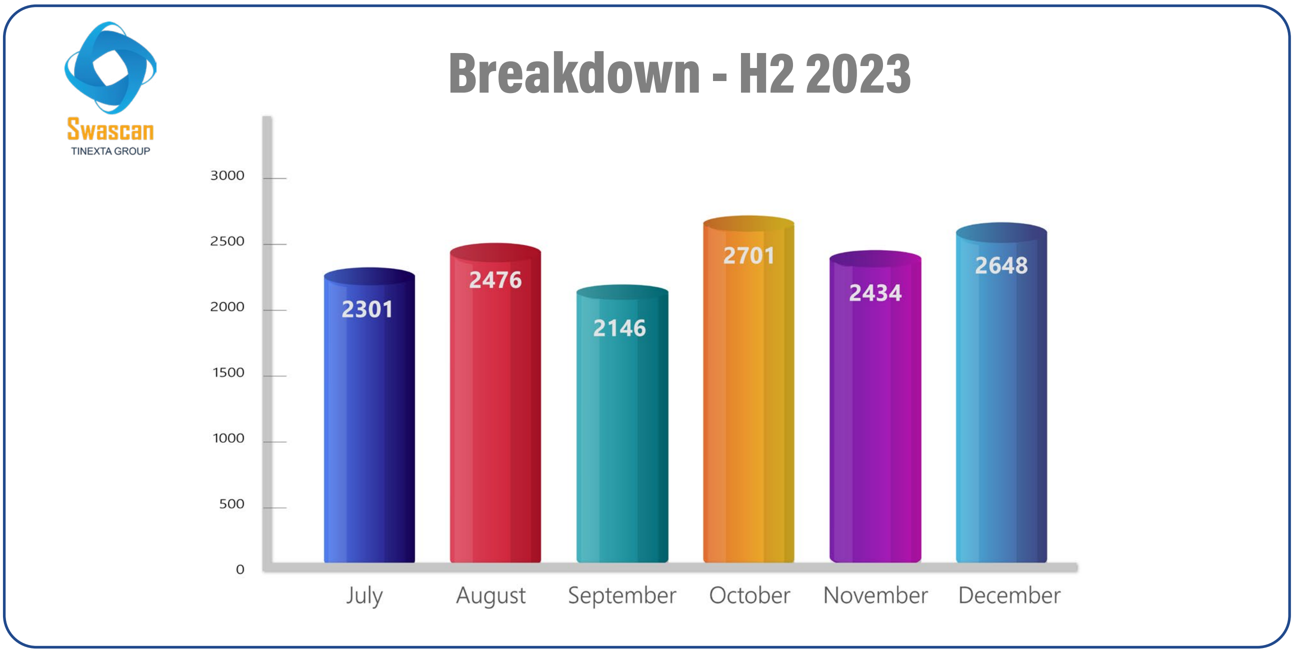
Among the analyzed campaigns, it is possible to note some examples where an attempt is made to deceive the victim by pretending to be real products or services:

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 costantly monitor new vulnerabilities that are discovered in software, operating systems, or applications. This al-lows them to identify weaknesses in target systems and exploit them later during the attack.

In H1 for 2023, **15286 new CVEs** had been published compared to 14706 published in H2:





How to mitigate risk:

1. Constant monitoring:

Maintain regular monitoring of sources of vulnerability information, such as NIST National Vulnerability Database (NVD), to be timely in identifying new rilevant CVEs for their systems.

2. Impact assessment:

Classify vulnerabilities based on the impact they could have on systems and data. This helps to prioritize actions and focus on the most critical vulnerabilities.

3. Rapid patch application:

Update and Patch systems in a timely manner, following the guidance of CVEs. Timely imple-mentation reduces the window of exposure to threats.

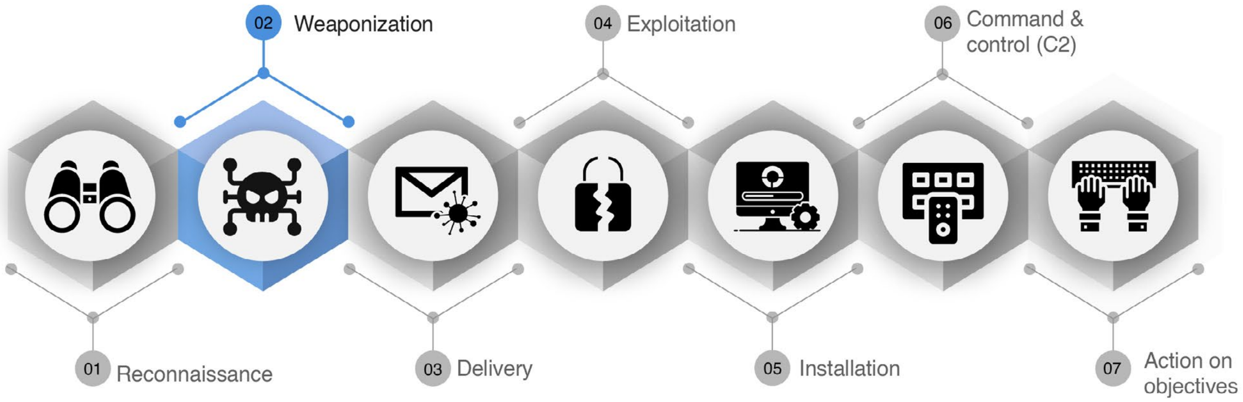
4. Configuration management:

Ensure that systems are properly configured, and security measures are adequate. Proper con-figuration can mitigate many vulnerabilities.

5. Network monitoring:

Utilizzare strumenti di monitoraggio delle reti per rilevare attività sospette o tentativi di sfruttare vulnerabilità noti. La tempestiva identificazione può prevenire potenziali danni.

Weaponization



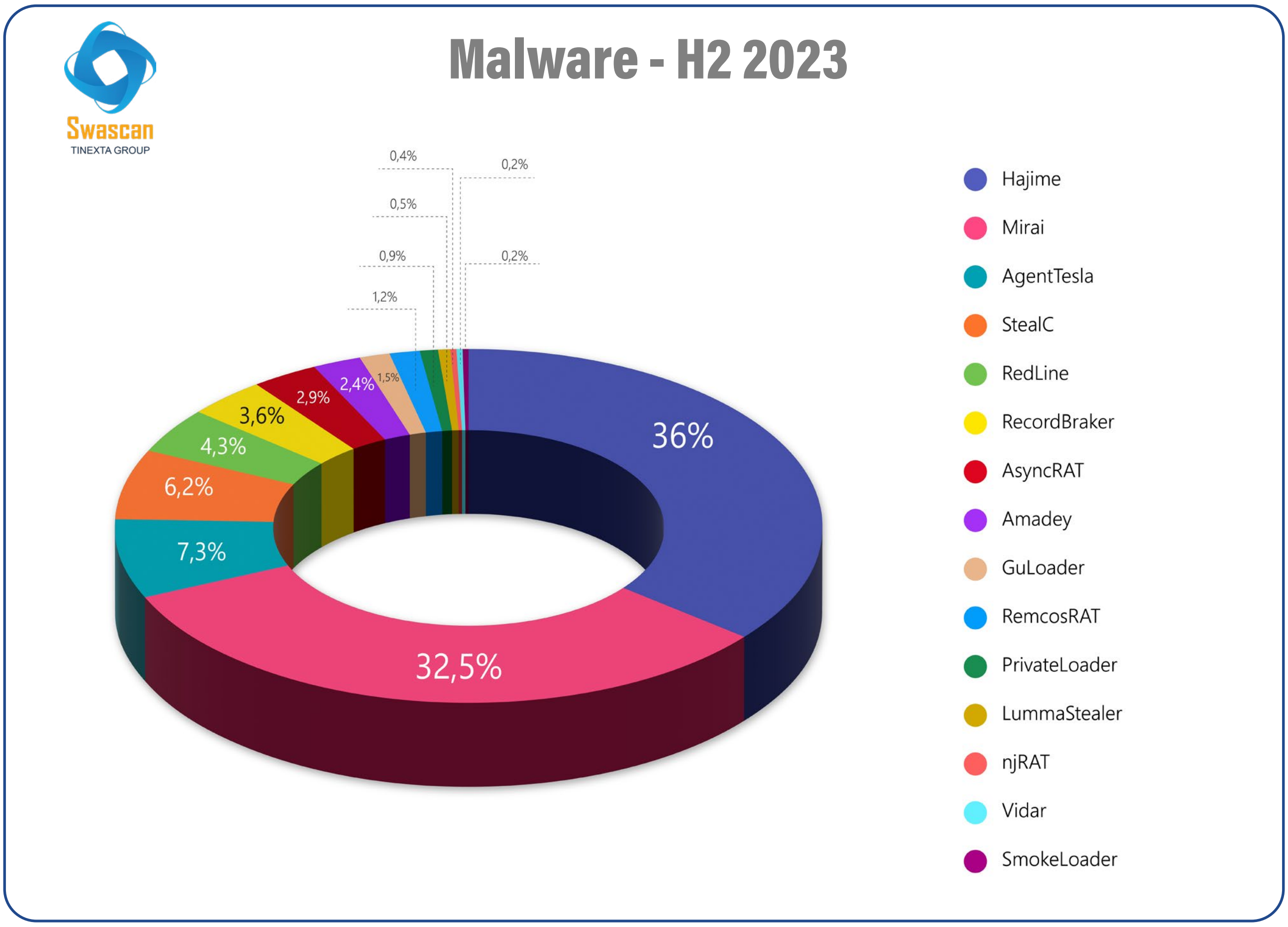
The weaponization phase is an important stage within the Cyber Kill Chain, in which attackers transform a malicious payload into a weapon ready to be used against the target system. During this stage, different types of malwares are often carried, including botnets, infostealers, and RATs.

Botnets are networks of compromised computers remotely controlled by attackers. These bots can be used to conduct distributed denial of service (DDoS) attacks, send spam, or further propagate malware. The attacker exploits the botnet to send commands to the compromised bots and to re-ceive information gathered from them.

Infostealers are types of malwares designed to steal sensitive information from infected systems. They can in fact collect data such as login credentials, banking information, credit card details, or other personal information. Once collected, the information is sent to the attacker's C2 for lat-er exploitation or use for illicit purposes.

RATs, or remote access Trojans, allow attackers to take complete control of the compromised system remotely. Attackers can access the system, execute commands, download, and install addi-tional malware, exfiltrate data, or perform other malicious actions. These tools give attackers stealthy and persistent control over the compromised system.

The weaponization phase is crucial for attackers, as it represents the moment when the mali-cious payload is transformed into a functioning attack tool. Attackers exploit these forms of mal-ware, such as botnets, infostealers, and RATs, to gain and maintain unauthorized access to the target system and to conduct further phases of the cyber-attack.



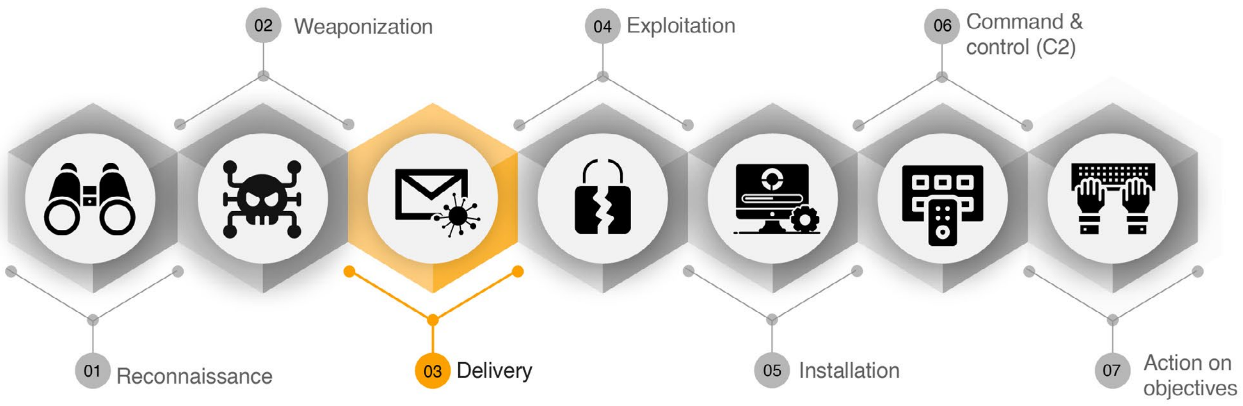
Key Takeaways

Hajime and **Mirai** are the most prevalent malware with **1127** and **1019** detections respectively. Both are known to attack Internet of Things (IoT) devices and can be related to botnets aimed at carrying out distributed DDoS-type attacks.

On the other hand, AgentTesla and StealC are more information theft oriented. Their presence may indicate a growing interest in stealing sensitive data or personal information.

As if this were not enough, the presence of different types of malwares such as RedLine, Record-Braker, Asyn-cRAT, Amadey, GuLoader, etc., suggests a diverse malware landscape. This diver-sity may indicate that attackers are exploiting different tactics and attack vectors, while some malware such as GuLoader, PrivateLoader, and LummaStealer are designed to upload and dis-tribute additional malicious loads. The presence of these malware may indicate a tendency to use specific payload loading techniques to carry out targeted attacks.

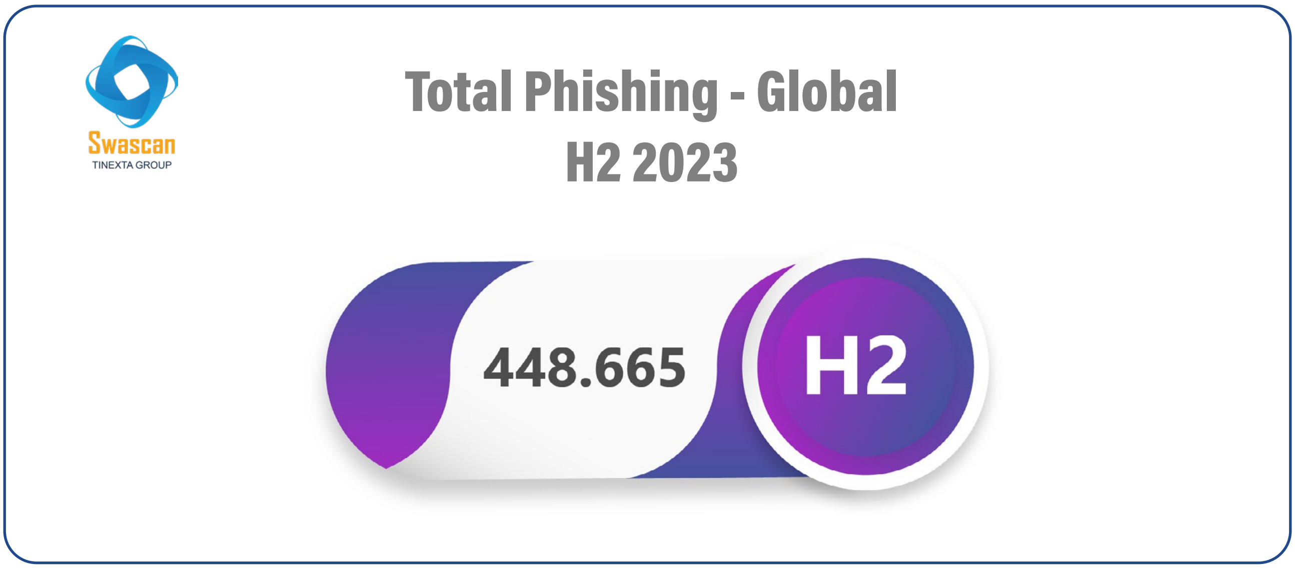
Delivery – Phishing



One of the most widespread and malicious threats detected in H1 is phishing, a cyber-attack that aims to deceive users and gain unauthorized access to their information.

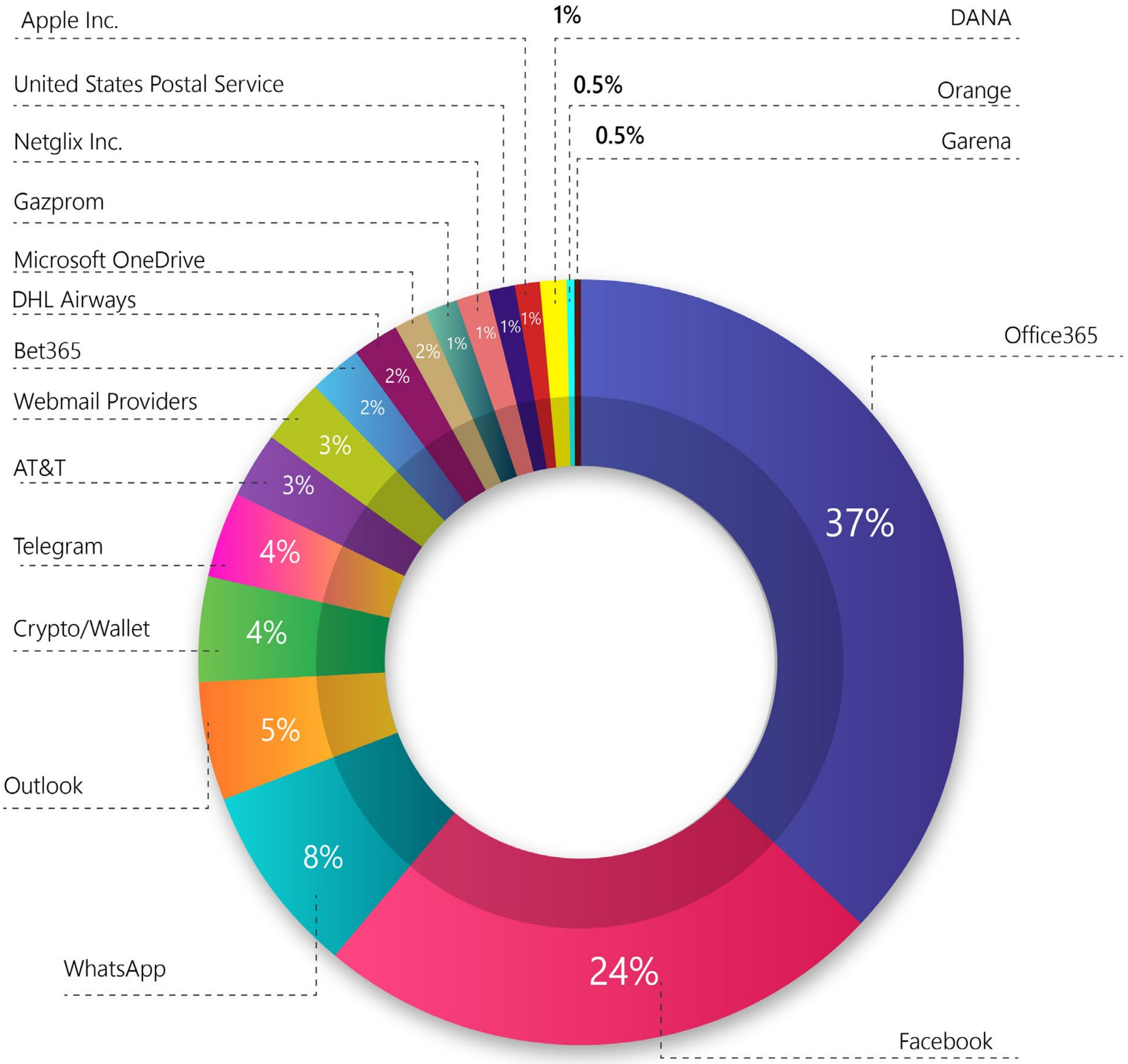
In the context of the Cyber Kill Chain, phishing is placed in the "Delivery" or delivery phase.

The delivery phase represents the moment when the attacker delivers a payload or attack mech-anism to the chosen user. Phishing, in particular, exploits sophisticated techniques to send de-ceptive e-mails, text messages, or communications that appear to come from trusted or legitimate sources. Attackers seek to deceive users by persuading them to click on malicious links, download infected attachments, or reveal confidential information.



Phishing is a constantly evolving threat, adapting to new technologies and defenses implemented by security experts. During the second half of 2023 (H2 2023), a total of **448,665 phishing attacks** were reported, with some particularly prominent campaigns involving different companies and sectors.

Top 18 brands imitated for phishing



The major phishing campaigns during H2 2023 used the following brands as bait:

1. Office365: with a total of **79,809 attack**s, Office365 has been widely used as bait to convince users to enter their login credentials into counterfeit websites, with the goal of stealing personal information and compromising security.

2. Facebook: with **51,698 attacks,** Facebook has been exploited to induce users to provide their credentials through fake websites, exploiting the popularity of the social network to lure.

3. Whatsapp: attackers exploited Whatsapp's popularity, with **17,556 attacks**, to trick users through fake mes-sages and counterfeit websites, aiming to obtain sensitive information.

4.Outlook: with **10,809 attacks**, Outlook has often been used as bait to send counterfeit e-mails, aiming to induce users to click on malicious links or provide confidential information.

5. Crypto/Wallet: With **9,417 attacks**, Crypto/Wallet-related phishing campaigns sought to exploit the growing in-terest in cryptocurrencies by trying to gain access to digital wallets and financial information.

6. Telegram: Telegram has also been involved in **7,701 attacks**, used to deceive victims through fraudulent messages, with the goal of obtaining personal information.

These data highlight how the brands mentioned have been exploited as bait in various phishing campaigns, demonstrating the versatility of attackers in targeting popular platforms and ser-vices to deceive victims. It is critical that users are aware of these threats and take appropriate security measures to protect their information personal and business.

Analyzing the brands involved in phishing campaigns during H2 2023, several considerations emerge. Attackers targeted widely used platforms such as **Office365**, **Facebook**, **Whatsapp**, and **Outlook,** exploiting users' familiarity with these services to deceive them. This highlights a strategy to maximize the number of victims by exploiting the popularity of online platforms

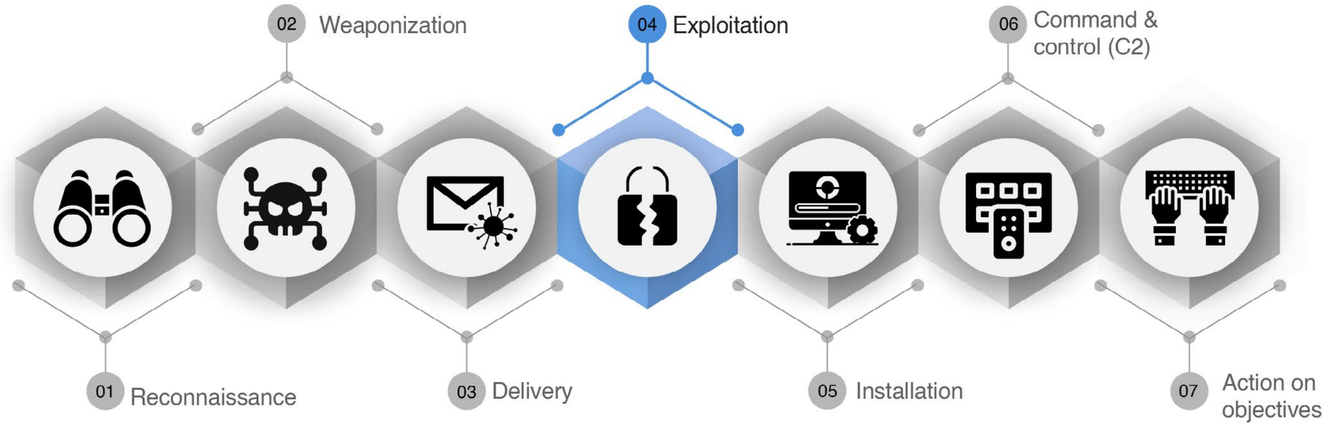
The presence of **Crypto/Wallet** among the targeted brands indicates a growing interest by attackers in cryptocurrencies. This can be linked to the goal of gaining access to digital wallets or financial information related to cryptocurrencies, reflecting evolving trends in the cybersecurity world. Telegram has been implicated in phishing attacks, suggesting that attackers are exploring the use of messaging platforms to spread fraudulent messages. This tactic could prove effec-tive given the prevalence of these communication applications.

In addition, the inclusion of **DHL** preys on the classic feeling of expectation for all those who use package shipping/delivery services. This approach aims to deceive victims by convincing them to provide personal information.

In addition to online services and communication platforms, specific sectors such as online betting (**Bet365**) and energy (**Gazprom**) have been implicated.

This indicates a diversification of attackers' targets, who seek to exploit the popularity and trust associated with specific brands in various sectors. The changing nature of phishing threats during H2 2023 reflects a continuous adaptation of attackers to user habits and trends of the mo-ment. User awareness and implementation of advanced security practices are critical to mitigating these risks in a constantly evolving threat environment.

Exploitation



“Exploitation” is the phase that follows delivery (delivery) and deployment (weaponization). In the Cyber Kill Chain, during the exploitation phase, attackers exploit vulnerabilities discovered in the previous phases to further infiltrate a target’s network and achieve their goals. In this process, cybercriminals often move laterally through a network to reach their targets.

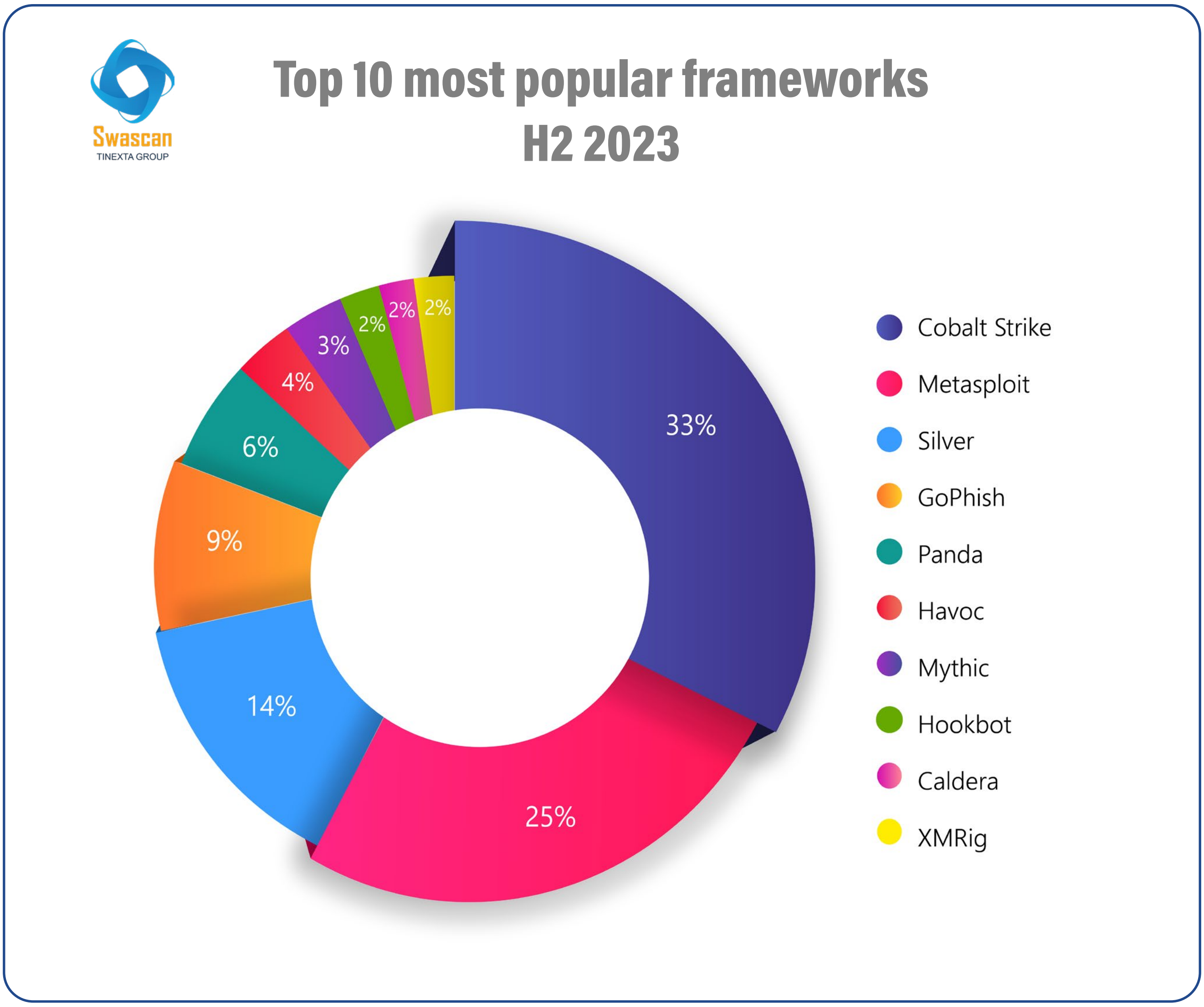
Exploitation can sometimes lead attackers to their targets if those responsible for the network have not implemented sufficient measures. In essence, this phase is the next step after attackers have delivered and deployed their malware or malicious code. In this phase, they try to exploit system vulnerabilities to gain deeper and more persistent control over the network or target device.

Command&Control

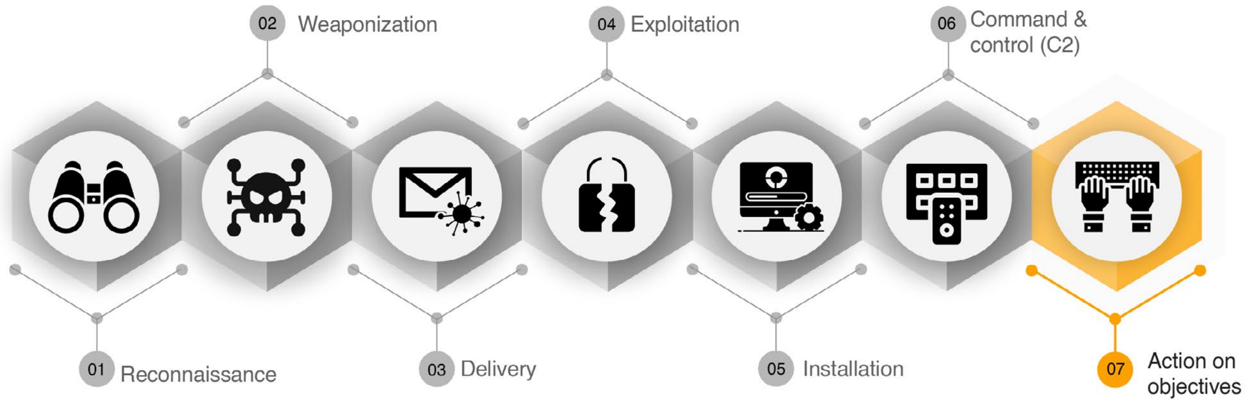
In the second quarter of 2023, malware continues to pose a threat to the cybersecurity of busi-nesses and individuals worldwide. In the context of the Cyber Kill Chain, the installation of Malware for communication with a remote server is in the "Command&Control" phase.

The Command & Control ("C2") phase is crucial for attackers, as it allows them to maintain con-trol over compromised machines and continue to perform malicious operations undetected. It is essential that organizations 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 con- trol over and interact with the compromised system. This involves the use of sophisticated malware and Command & Control frameworks.



Actions On Objectives



As reported at the outset, there was a significant increase in the number of victims affected by ransomware attacks in H2 2023, with a total of more than 2,600 incidents reported around the globe. This is the last phase of the Cyber Kill Chain, known as "Actions on Objectives," which is the climax of an attack. Once the attacker has successfully infiltrated the target system, he is able to act to achieve his initial objective. The actions taken at this stage can take many forms, ranging from extracting sensitive data to completely destroying it.

Victims of ransomware in the second quarter came from a wide range of countries and islands, reaching a total of 94 countries involved. This shows how ransomware is a global problem that knows no geographic boundaries: organizations and individuals around the world have been tar-geted by attacks, putting data security and business continuity at risk.

The comment of CEO, Pierguido Iezzi

Today we are faced with a digital reality that is evolving at an impressive rate, with the second half of 2023 bringing a significant increase in cyber-attacks around the world. The numbers speak for themselves: **2,616 ransomware incidents** affected **94 countries**, an increase **11.4 percent** over the first half of the year. Italy, unfortunately, was not immune, recording a **44.1 percent** increase in ransomware incidents. These attacks, orchestrated by ransomware gangs, have affected 88 companies in our country, creating significant disruptions in several sectors.

In short, the cyber-crime landscape continued its path of continuous evolution in 2023, demonstrating a more efficient and aggressive approach. Criminal hackers continue to innovate and adapt to regulatory changes and law enforcement actions. Despite cases such as the Hive seizure and the BlackCat disruption, ransomware has still seen significant growth.

The phenomenon, as the report's data show, is evolving toward an increasingly "commodity" dimension. This shift can be attributed to the increasing democratization of cyber-crime, made pos-sible by simplified access to new codes and vertical expertise. This democratization also trans-lates into increased accessibility, allowing a variety of actors, even less experts, to exploit these cyber-crime resources.

These numbers thus reflect an increasingly sophisticated and diverse threat. CobaltStrike and Metasploit dominate the command-and-control malware landscape, while phishing continues to be a pervasive problem, with more than **448,000 global attacks.**

In this digital age, cybersecurity has become an inescapable priority; companies must strengthen their security measures; they must remain vigilant. Italy has already strengthened its cyber resilience through the establishment of the Agency for National Cybersecurity (ACN) and the Nucleo per la CyberSecurity (NCS), demonstrating a tangible commitment to addressing emerging threats.

But their effort cannot be separated from the collaboration between the private sector, academic institutions and government, which is essential to meet this challenge. A concept echoed and em-phasized, in Italy, by Defense Minister Guido Crosetto himself, who has already stressed the importance of collaboration between entities public and private entities and the need for a system-atic approach to dealing with threats.

We must consider cybersecurity not only as a technological issue, but as an imperative necessity to protect our assets, economy and, above all, citizens.

Only through a predictive, preventive, and proactive defense strategy can we address the ever-emerging threats and preserve our digital security. Particularly today, a time when the cyber threat has become even more evident in relation to current international events.

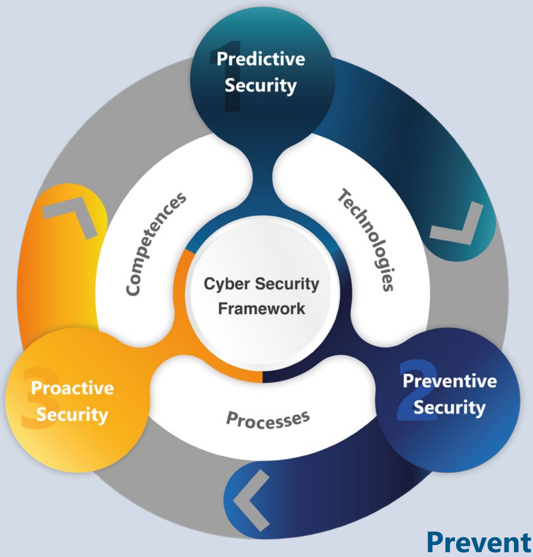
How to defend against ransomware
The cyber security framework

The best approach to increasing perimeter resilience goes through the three pillars of modern Cyber Modern Security. Therefore, the three canons of:

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

Predictive Security

1. Identify corporate threats outside the corporate perimeter operating at the web, DarkWeb and Deep Web level
2. Look for any emerging threats
3. Carry out Early Warning activities
4. Provides evidence to Preventive Safety
5. Indicates the areas of attention to Proactive Security



Proactive Security

1. Identify cyber threats operating within the corporate perimeter
2. Counter and block cyber attacks
3. Manages Cyber Incidents
4. Provides evidence to Preventive Safety
5. Indicates the areas of investigation for Predictive Security

Preventive Security

1. Verify and measure the Cyber Risk
2. Defines remediation plans
3. Indicates the Risk exposed to the Proactive Security Layer
4. Provides Predictive Security Investigation areas

Action Plan

In line with the best practices described in the Cyber Security Framwork, it is recommended to implement a Cyber Secuirty action plan based on the following Steps:

Predictive Security

Domain Threat Intelligence: Domain Threat Intelligence searches for public and semi-public related to domain vulnerabili-ties, subdomains, and compromised emails. The service does not perform any testing on the target. It operates solely on information available on the Web, darkweb and deepweb. It collects, analyzes and clusters available information at the OSINT level (Open Source Intelligence) and Closint (Close Source Intelligence) present on databases, forums, chat, newsgroups.

Specifically, based on the target domain of analysis, it identifies:

- Potential vulnerabilities
- Details of vulnerabilities in terms of CVEs, impacts, and severity
- GDPR Impacts (CIA)
- Number of subdomains
- Number of potential compromised emails (they are only counted and not collected or processed)
- Number of sources of compromised emails
- Typosquatting

Cyber Threat Intelligence: this is Swascan's advanced threat intelligence service. It performs a search, analysis and collec-tion activity of information present at the Web, Darkweb and Deepweb levels relative to the do-main/target of analysis.

Specifically:

- Data Leaks: credentials/source/data
- Identifies Forum/Chat ...
- Botnets related to customer, vendor and employee dispositions
- Botnets with credentials and related login page urls
- Typosquatting/Phishing
- Surface
- Top Manager Analysis

Preventive Security

Vulnerability Assessment: scans Web sites and applications to identify and proactively analyze security vulnerabilities.

Penetration Test: penetration testing activities are carried out by certified Penetration Testers and in line with in-ternational standards OWASP, PTES and OSSTMM.

Phishing/Smishing attack Simulation: allows companies to prevent damage from phishing/smishing attacks through real attack simulations. It is indeed possible, through a web interface send real simulated phishing / smishing campaigns that generate irreplaceable learning opportunities for employees. The latter, in fact, thanks to such simulated attacks will be able, in the future, to detect a real phishing e-mail or a smishing message and avoid it. An irreplaceable training and awareness of your employees through real simulated phishing/smishing attacks

Awareness (Cyber Academy): dedicated Cybersecurity training courses in the classroom or via webinars. Awareness activities for technical staff, employees and Top Managers.

Proactive Security:

SOC: designing, commissioning, and maintaining a Security Operation Center can be costly and com-plex. Swascan’s SOC as a Service is the most effective, efficient, consistent, and sustainable solu-tion for enterprise settings. Soc as a service with its Monitoring & Early Warning enables the identification, detection, analysis and reporting of attacks cyber before they can turn into a con-crete threat to the business.

A dedicated team in the business of reactive Monitoring & Early Warning of cyber threats on lo-cal networks, cloud environments, applications and enterprise endpoints. Our team of Security Analyst monitors data and assets wherever they reside within the enterprise. Regardless of whether the resources are stored in the cloud, locally, or both. The activity of monitoring and re-porting allows action to be taken only when a real threat is identified.

Incident Response Team: the Cyber Incident Response Team by Swascan is a 24-hour Cyber Emergency Response service with the aim and purpose of supporting companies in the activity of responding to and handling cyber security incidents and Ransomware attacks.
In line with the international NIST SP 800-61rev2 Computer Security Incident Handling Guide standard, following a cyber incident Swascan’s IRT aims to:

- Contain possible damage
- Determine the 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

Analysis by:

Riccardo Michetti
Riccardo D'Ambrosio
Martina Fonzo

Technical Contributors:

Soc Team Swascan

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