GATEWATCHER

CYBER THREATS
SEMESTER REPORT

January– June 2022

SUMMARY

01 REPORT HIGHLIGHTS AND GUIDANCE FOR READERS

For this first edition of the Semester Threat Report, Gatewatcher's Purple Team presents the threat trends detected each semester by Gatewatcher's CTI platform and the active monitoring of the Purple Team's cyber analysts.

This report aims to shed light on the cyber threats observed between January and June 2022, the evolution of these threats as well as a perspective on future trends to facilitate their detection and ultimately reduce the impact of future security incidents.

Each section presents an explanatory classification of the identified cyberattacks as well as thematic focuses edited by the Purple Team analysts in order to highlight the different trends, established and emerging.

At Gatewatcher, the Purple Team's mission is to track and analyze threats targeting our customers in order to ensure the constant updating and optimization of the per-formances of our various NDR, CTI, Sandboxing or qualified detection offers. The Purple Team is characterized by the diversity of profile of its experts, with experiences in the fields of the response to incident, the analysis and integration SoC, the pentesting, the analysis CTI, and the research in cyber security..

As with any report on cyber threat trends, there are some unavoidable themes, such as the massive use of Office application vulnerabilities to infect a desktop. However, we must never forget that cyber attackers know how to evolve and find new techniques to achieve their goals, for example, using legitimate sites to store malicious payloads in order to act more discreetly on an information system.

This document is structured around 5 sections dealing with the following topics[1] :

- → Types of files used by cyber attackers
- → The malwares used
- → Techniques used by cyber attackers
- → Vulnerabilities being exploited
- → Most targeted industries

02 GLOSSARY AND TECHNICAL DETAILS

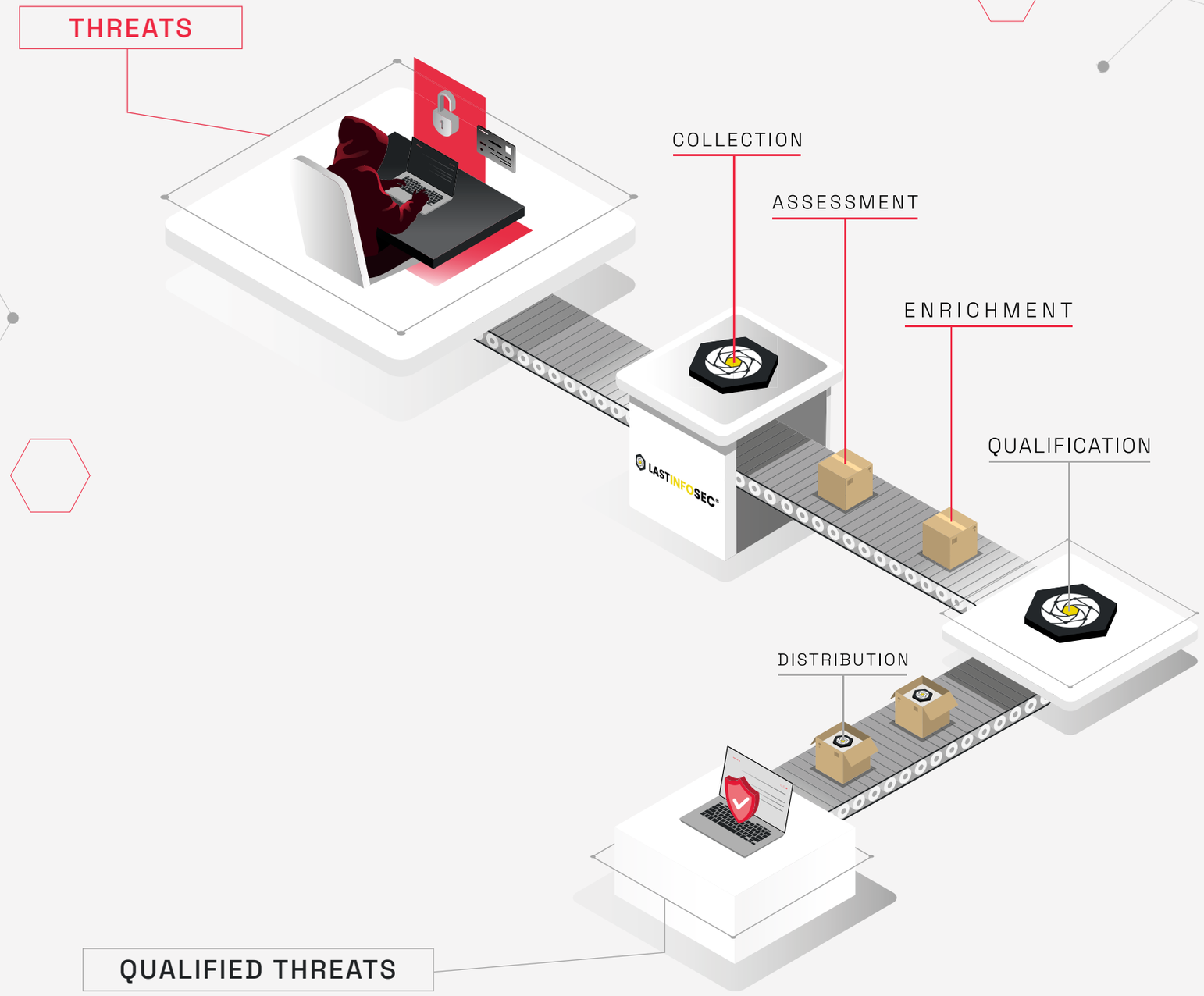
To better understand the nature of this data, it is necessary to explain how our LastInfoSec platform works.

LastInfoSec® is our Cyber Threat Intelligence (CTI) platform designed to facilitate the detection of internal and external threats that may target the information system and to track new techniques, vulnerabilities, tools, used by attackers.

LastInfoSec's automated collection, analysis and correlation engines are continuously fed with more than 3,000 data sources from multiple channels: social networks, specialized sites, darknet, deep web as well as telemetry from Gatewatcher's detection infrastructure. This allows LastInfoSec to generate more than 5,000 qualified markers per day, in near real time, and provide several types of high-value threat intelligence.

The LastInfoSec® infrastructure provides multiple types of threat intelligence :

- → Enriched, industry-contextualized indicators of compromise to reduce the time it takes to analyze a threat when detected
- → Tactical reports on new techniques, tools, application breaches, etc. used by attackers
- → Reports on vulnerabilities



5500

is the average number of contextualized IoCs per day

+150

is the total number of malware families actively tracked

+3000

is the number of data sources feeding LastInfoSec CTI infrastructure

03 MALICIOUS FILES

BETWEEN LONGSTANDING AND NEW INFECTION VECTORS

Windows and Linux platforms are the most targeted by cyber-threat authors, with ELF and PE malicious files at the top of the list.

There are several reasons for this, many companies have chosen to use Windows as their desktop operating system. As for Linux, the growth of the cloud and connected objects makes it a prime target for attackers. The question remains: How do these malicious files get onto the network ?

OLD TECHNIQUES STILL PRESENT

As shown in the CVE ranking, Microsoft Office files are widely used by attackers to execute arbitrary code. This office software suite is widely used in companies, with Word, Excel and Powerpoint files, and is a good entry point into their infrastructure. Often sent as email attachments in phishing attacks with file names such as «Invoice-XXX.docx, Balance Sheet-2021.xlsx», they represent a significant source of attack.

Another common file type used in phishing attacks is PDF. Similar to Microsoft Office files, PDF files are «disguised» as normal files with labels that entice the victim to open it (invoice, refund, pay slip, etc.). Once opened, a malicious payload is executed in order to distribute other malware (e.g. a keylogger)

TOP MALICIOUS FILES

ELF → 45.434%
PE → 34.673%
MS-OFFICE → 9.611%
OTHERS → 6.149%
ARCHIVE → 2.691%
SCRIPT → 0.467%
PDF → 0.309%
RTF → 0.265%
ISO → 0.214%
INK → 0.186%

Webshells, a technique regularly used by cybercriminals, allow to have permanent access to web servers and facilitate the execution of arbitrary code remotely. They are written in programming languages such as PHP, Python, ASP.NET, JSP, and many more. At the end of June, a new vulnerability targeted the Confluence solution, published by Atlassian (CVE-2022-26134) via a webshell.

TOWARDS NEW INFECTION VECTORS...

At the end of May a new CVE has been released under the name of Follina (see Part 4). Through a Microsoft Word or RTF (Rich Text Format) file, it allowed an attacker to execute arbitrary code by exploiting the ms-msdt URI scheme. Due to its simplicity of use and its critical impact on a machine, it was quickly and massively exploited by malware such as Emotet or Qbot, which explains its position in our ranking.

We have noticed a «new» attack vector during this first semester: it consists of an ISO file with a Windows shortcut file (.lnk) that will often load a library (.dll) or execute a PowerShell command. We noticed that this method has been used to distribute malware such as Qbot, Emotet, IcedID, etc. It follows Microsoft's statements inducing a major change in the execution of macros in files marked as coming from the Internet (by default these files will have their macros disabled) which has resulted in attackers considering other means of infection. The advantage of choosing the ISO format is that it can be «mounted» directly if the victim double-clicks on the file, making its contents easily accessible. It also allows to bypass Mark-Of-The-Web, a marker that identifies that a file comes from the Internet, which allows Windows to adapt its security features (e.g. blocking Office macros).

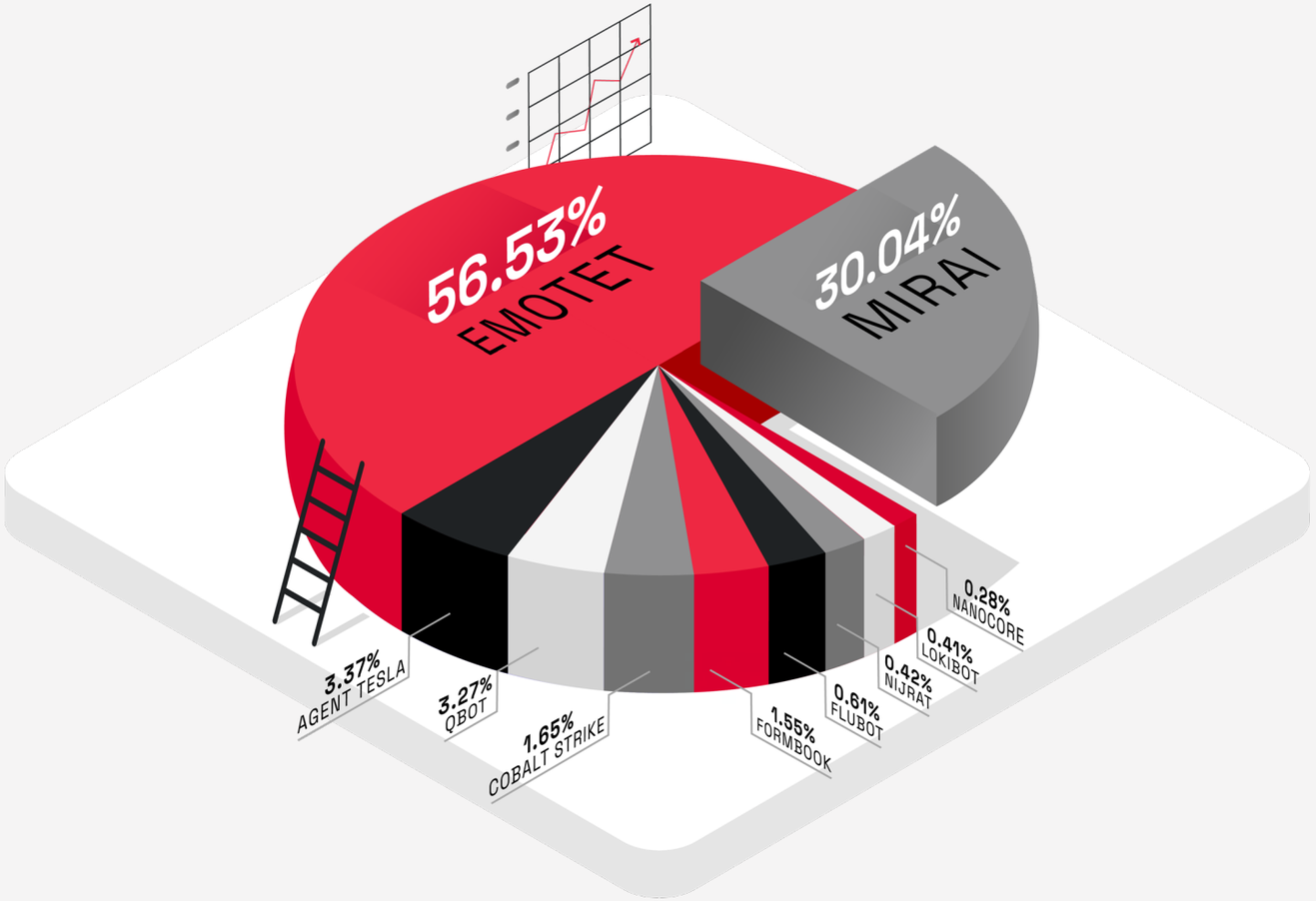
More and more malicious groups are using archives to distribute their malware. Compressing a file and password-protecting it allows to bypass some primary security on a network. If an archive is sent as an email attachment with a password, its contents will not be scanned most of the time. In archives we find mainly .zip, .rar, .gzip, .7z files, which are very well known by the general public and are present both in Linux and Windows.

04 THE GROWING USE OF ADAPTIVE MALWARES

With over 150 families of malware monitored during the first half of the year, we now present with the top 10 of our observations.

This first half of the year we have mainly tracked two already well-known malwares: Emotet and Mirai. Indeed, after an interruption of its activities in January 2021 following the arrest of some of its members and the closure of its infrastructure by Europol[1], Emotet Emotet made its comeback in November 2021.

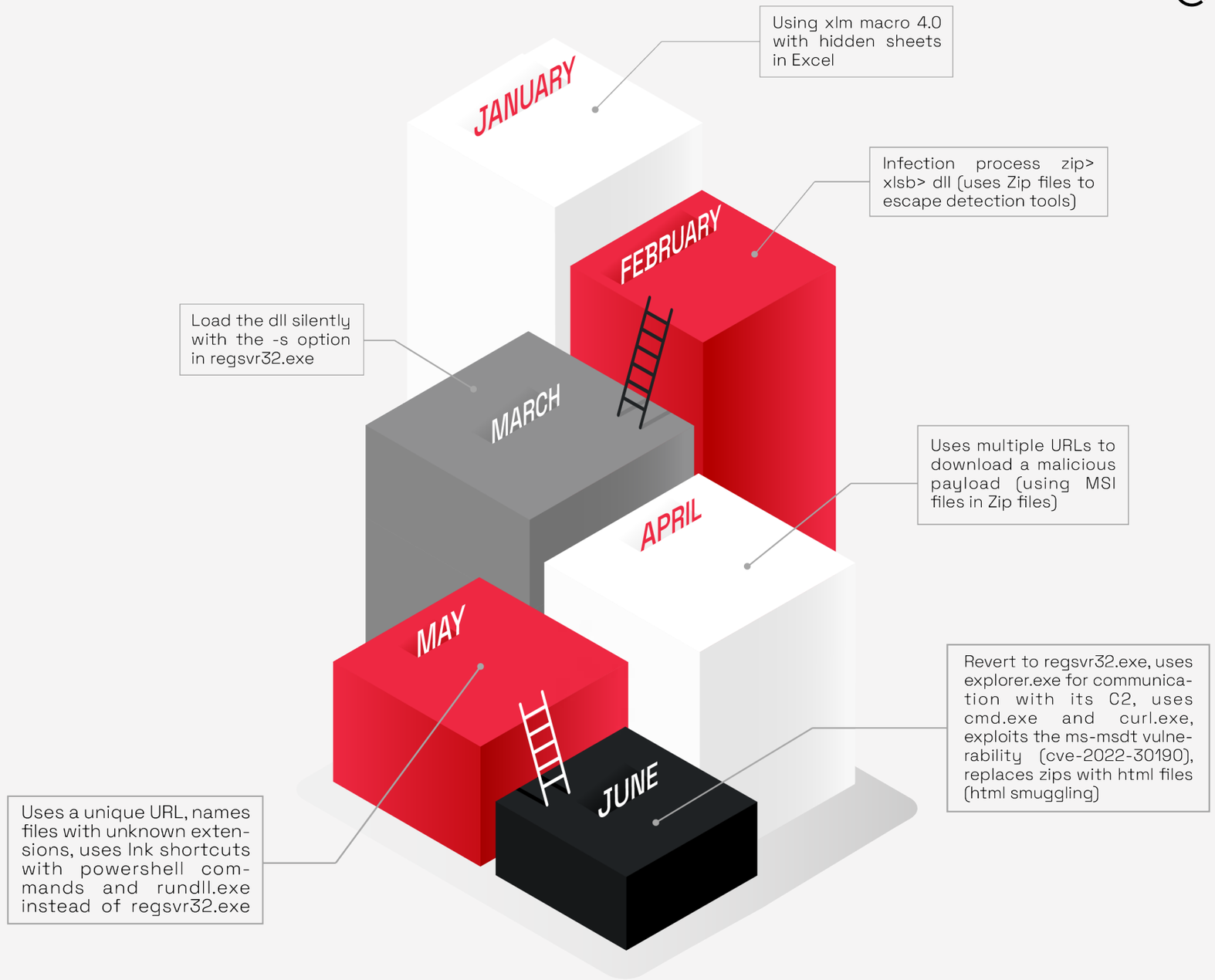
Mirai, on the other hand, has been around since 2016. Thanks to the publication of its source code, many variants have been produced[2].



MONITORING OF MALWARES WITH A HIGH EVOLUTION PATH

Some malwares stands out this semester by theirs particularly dynamic evolvment over the period.

Qbot, also known as Qakbot, is a very modular information thief. It has distinguished itself by the rapid adaptation of its infection techniques, moving from Macros to MSI files, then more recently to LNK files and phishing URLs from legitimate sites (Onedrive, Google Drive) as shown in the timeline below.



A second malware grabbed our attention during this period: Flubot, an Android malware targeting mainly the banking system since 2 years in Europe, Asia and Oceania. This malware, whose primary objective is to steal its victim's banking credentials, also stands out for its increased ability to evolve rapidly. Finally, in third place is Agent Tesla, a trojan written in .NET that our team analyzed last March. This Trojan focuses on the banking, energy and transportation sectors. We found that it exploits vulnerabilities present in our top 10 CVEs (e.g. CVE-2017-11882, CVE-2018-0802).

Here is the evolution of Flubot over the last six months :

LATE 2021

Ability to receive URLs in addition to html and javascript web injections (allowing injection codes to be saved in memory).

Added TLD to generate new domains using DGA, offers the user a fake Flash Player application.

JANUARY 2022

Use of the message support (SMS) for smishing attacks.

Targeting new countries (Japan, Hong Kong, South Korea, Singapore, Thailand).

Interception of received notifications and automatic response with a message configured by C2 and use of the Flubot botnet to distribute Medusa.

FEBR - APRIL 2022

Cookies snatching.

MAY 2022

Use of message support (MMS) for smishing attacks.

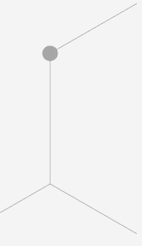
JUNE 2022

Dismantling of the Flubot infrastructure by Europol on June 1. However, the police do not seem to have recovered the private RSA keys.

TOOLS AND TECHNIQUES COMMON TO MALWARES

During these first six months, we have noticed the use of Cobalt Strike, fifth in our ranking, by Qbot and Emotet among others. This Command & Control tool (a system we presented in August) is one of the most used by attackers to communicate with their malware.

Some tools are, for example, reused by attackers to communicate with their malware. We have identified the use of Cobalt Strike by the Emotet and Qbot malware, which is now one of the most used Command & Control (C2) ltools by attackers (in fifth place in our ranking).[3]

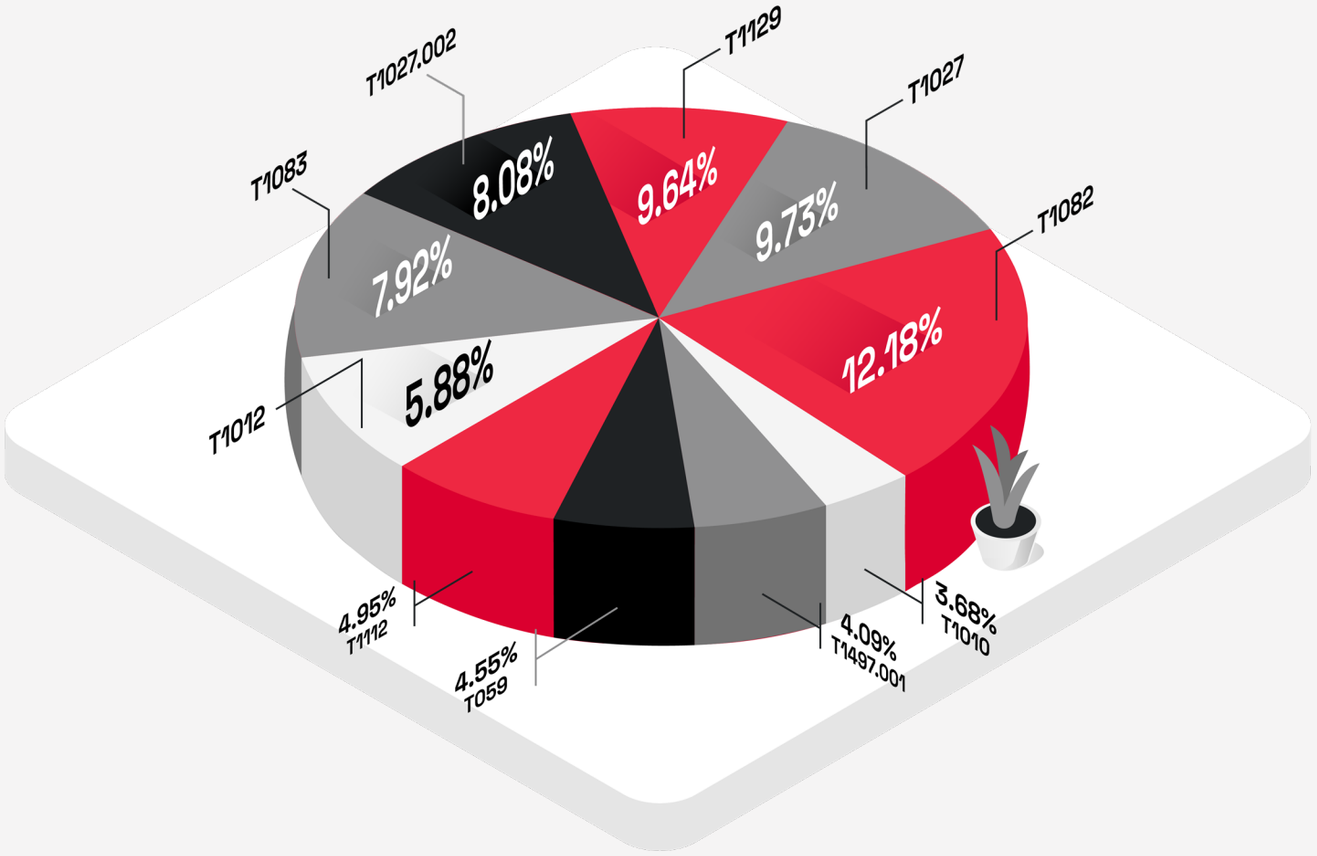


Attackers also use email phishing techniques to deliver their malware. Email phishing is a social engineering technique that aims to provoke an action from the victim, such as clicking on a link, opening an attachment, etc. The goal is to get information from the victim. The objective is to retrieve personal information and/or exploit the machine through the executed attachment. This is the case for most of the malware present in our top 10 malware, and distributed denial of service (DDoS) attacks are still very present. The growing number of connected objects (IoT), the default configurations of various machines accessible to the general public, as well as the number of CVEs with a high CVSS (Common Vulnerability Scoring System) score, allow Mirai and its variants (Satori, Beastmode, RapperBot, etc.) to be one of the most present and impactful threats.

Among the most widespread malware today, we find mainly information thieves and ransomware. The information thief (infostealer) is a recurring type of malware at the beginning of this year. Taking into account trojans and RATs (Remote Access Trojans), which have information stealing capabilities, infostealer makes up almost all of our ranking. Ransomware is a threat that has been growing rapidly since the COVID-19 health crisis. It aims to encrypt a victim's data and restore access to it in exchange for a ransom payment. However, we notice a decrease in the frequency of use of this type of malware over the first two quarters of 2022.

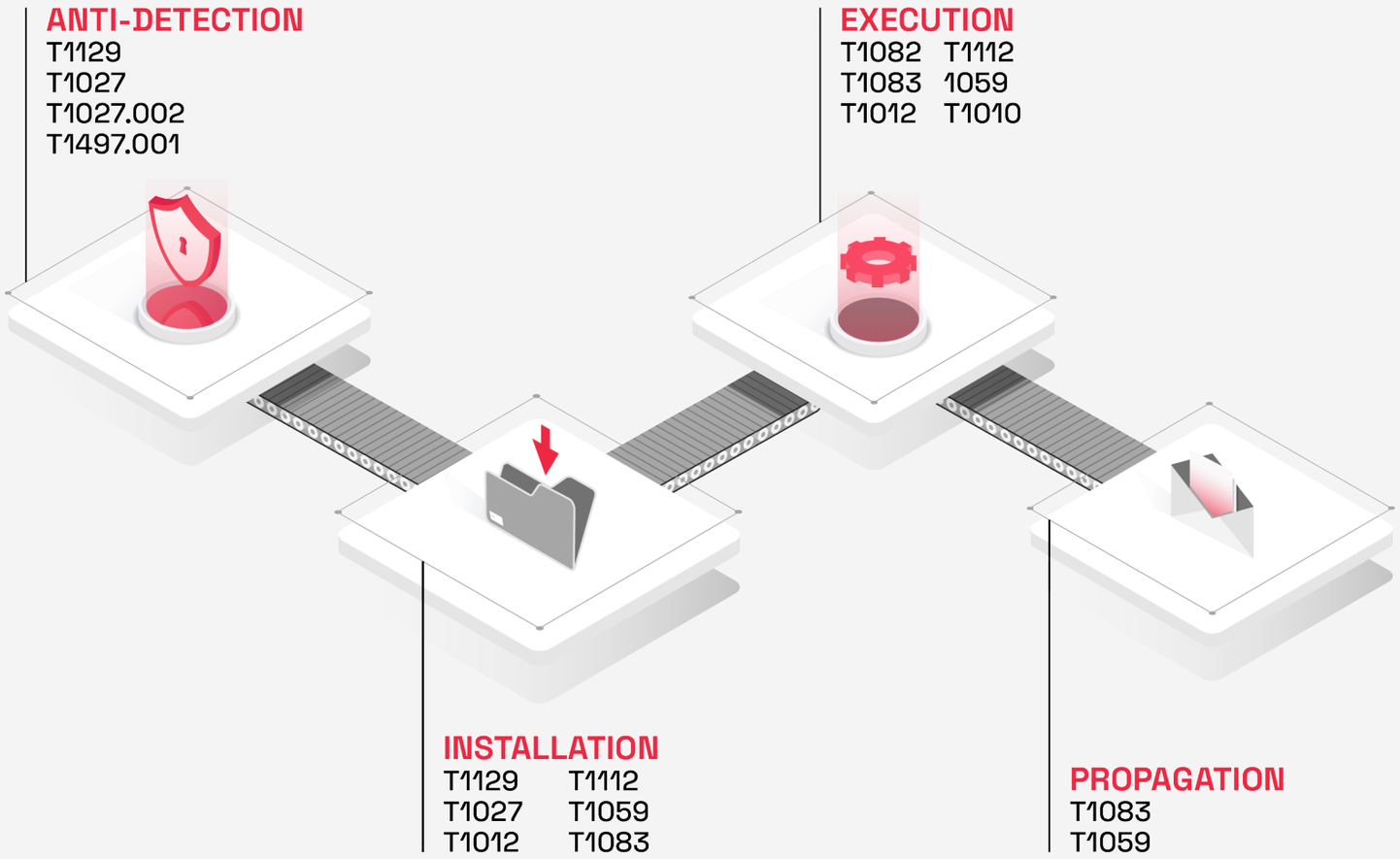
05 TRENDS IN TTP

TTPs (Tactics, Techniques and Procedures) are a set of behaviors and techniques used by malicious actors, published by the MITRE[4]. Specifically, they are generic malware behaviors, with many ways to implement each of these TTPs. This top 10 allows us to see the most commonly used malicious behaviors.



T1129 → Shared Modules
T1027 → Obfuscated Files or Information
T1082 → System Information Discovery
T1027.002 → Obfuscated Files or Information Software Packing
T1083 → File and Directory Discovery
T1012 → Query Registry
T1112 → Modify Registry
T1059 → Command and Scripting Interpreter
T1497.001 → Virtualization/Sandbox Evasion System Checks
T1010 → Application Windows Discover

These TTPs can be classified in different stages of the kill chain of a malware infection [5] :



A large number of malware are distributed as, or make use of, DLLs (T1129). It is not uncommon that some packing steps also involve a DLL, as it is the case for Agent Tesla analyzed previously by our teams[6]. The installation of a Windows service is also done with a DLL.

The obfuscation of a malicious payload is an essential step of a malware, which allows it to avoid detection and to be able to carry out its operations (T1027). This step is usually handled by the packer[7] used (T1027.002). More advanced packers can be used to detect a Sandboxing environment for example, and limit the risks of automatic detection (T1497.001). Information discovery appears to be an essential step (T1082, T1083, T1012, T1010). It is about the attacker obtaining information about the infected system in order to prepare further attacks, lateral moves, or simply encrypting the disk for ransomware. It can also help to spread to other machines (e.g. searching for shared folders).

Writing to the Windows registry (T1112) is often used to ensure the persistence of the malware (creation of a service, addition to the automatic startup, deactivation of protections). Execution of shell commands (T1059) can also be used for these operations, in addition to allowing remote control of a machine in the case of a Trojan Horse like Lyceum[8].

PACKING

Several previous TTPs (T1129, T1027, T1027.002, T1112, T1059, T1497.001) are usually directly or indirectly related to the use of a packer. About 80% of the malware distributed today is packaged. There are legitimate packers that are commonly used to protect proprietary software, or to facilitate its distribution. The Firefox installer for example is packaged with UPX to reduce the size of the final file. However, these legitimate packers are regularly used or even hijacked by malicious actors, as we have seen with NSIS[9]. For instance, there are many modified versions of UPX, or malware packaged with MPRESS, Enigma VMProtect, etc...

Malicious packers can become more complex to include data obfuscation (in a JPG file for example for Lyceum[10]), and implement protections against payload analysis (anti-debug, anti-virtual machine, anti-sandboxing...).

The development of new packers is still relevant because it is often easier for a malicious actor to «repackage» its payload in a new packer than to modify it. Estimates tend to show that 50% of new samples come from old malware «repackaged» in another packer. Packer detection, and especially automatic unpacking (and obtaining the final payload), is therefore an essential objective, although it remains a complex research topic. Several tracks are explored by Gatewatcher, notably based on emulation.

Many malwares are nowadays transmitted via Offices documents, and the macros they contain. It is often a matter of writing a file on the disk, then executing it (either a PE directly, or most often a shell script that extracts or downloads a payload and executes it). Several of the previous TTPs can therefore be applied to macros, which themselves constitute TTP 1137.

As mentioned earlier, TTPs are generic behaviors. Thus, sandbox detection or evasion (T1497.001) can take many forms, from simple techniques to more advanced ones. A simple «Sleep» with a long duration can be considered a sandbox evasion technique, as the malware only starts its execution after the maximum scan time of the sandbox. A slightly more advanced sandbox will simulate the expected delay instantly by hooking the relevant calls.

More advanced sandbox detection techniques also exist, such as hardware enumeration to detect virtual devices, searching for connected USB devices, detecting user interaction (does the mouse move?), etc....

THREATS STORAGE ON LEGITIMATE SITES :

A TTP not mentioned before appears to be used more and more. This is T1102.003[11]. An increasing number of malware use legitimate services as a means to store data on the Internet. First of all Pastebin, Google Drive, Dropbox, whose access is more and more frequently blocked in companies, and then Twitter. More recently with the use of instant messengers like Telegram or Discord.

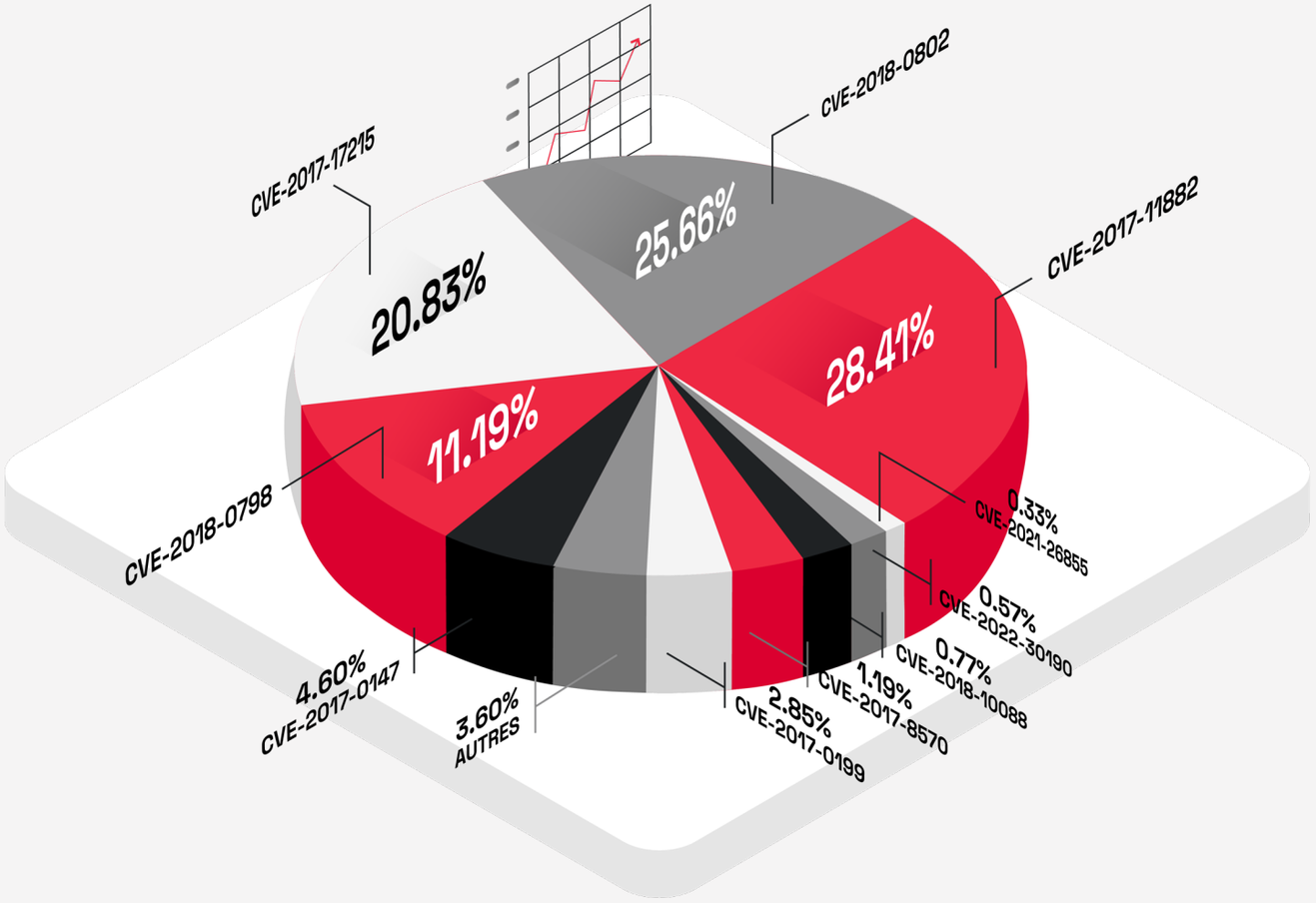
Thus, during a classic infection, the first payload executed simply downloads a more advanced one from one of these services. Some families go as far as to implement the C2 completely in one of these messengers, such as Telegram which was used by the ToxicEye and Racoon Stealer malware for example.

This method has many advantages for an attacker as it is very easy to implement, as these services are free and anonymous, and it remains more complex to detect. If they are not blocked by the company's internal policy, a connection to one of these services will not be unusual or malicious a priori because none of the usual indicators of a connection to a C2 will be present (connection on an IP without DNS, self-signed certificate, known malware IOC). These services can also be replicated across multiple geographies, allowing attackers to leverage the Content Delivery Network (CDN) for better performance, resiliency, and multiple IPs virtually associated with their C2.

06 CVE - A STABLE TREND BUT NOT FROZEN HOWEVER

It is important to note that the nature of the vulnerabilities exploited will differ greatly depending on whether it is an industrial or web environment. Although the amalgam is sometimes made, it is important to distinguish malware from vulnerabilities. Our observation here will focus on the 10 most exploited vulnerabilities (CVEs) by different malware.

These vulnerabilities are usually used to obtain higher permissions (privilege escalation), to enter and move laterally within the information system or, more simply, to execute arbitrary code. It should be noted that other vulnerabilities can be used by attackers at different stages of the kill chain. We can see here that almost all of the top 10 vulnerabilities are used during the first infection stage and are of the RCE (Remote Code Execution) type).

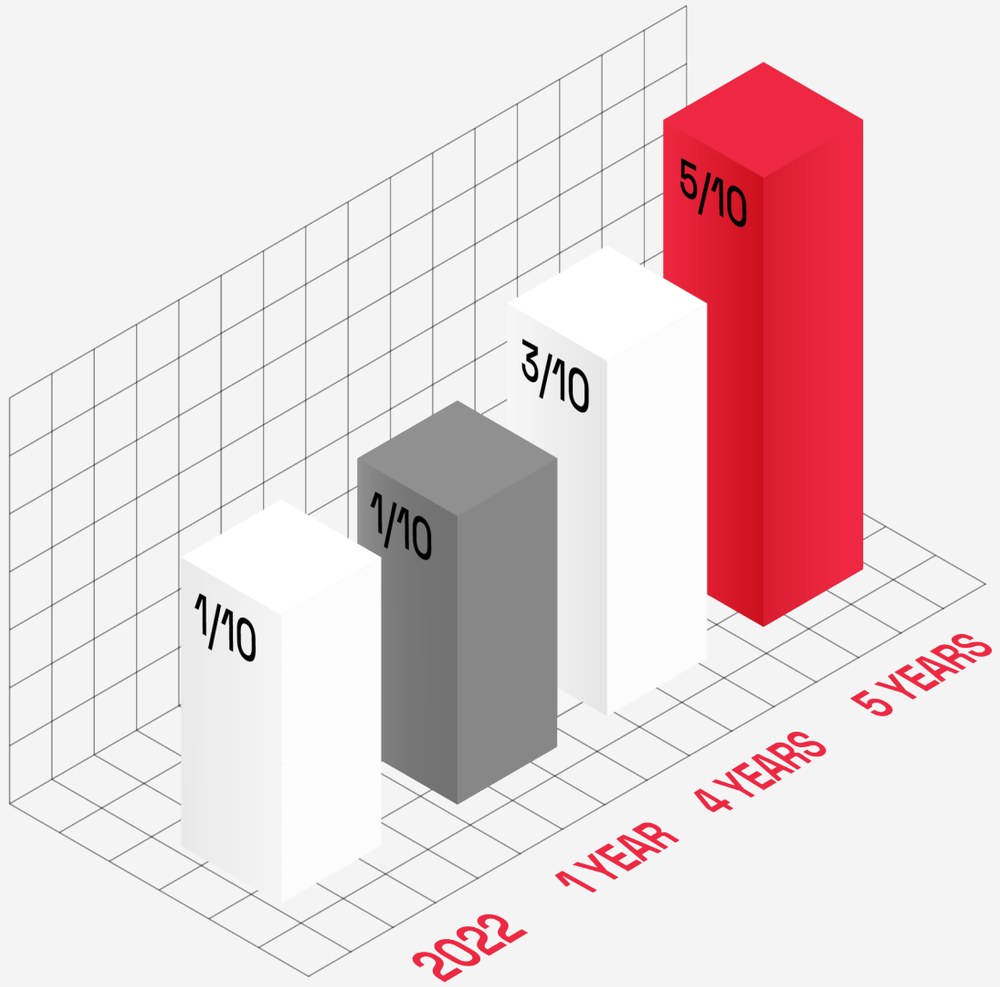


Although it may be surprising, the overwhelming majority of the used vulnerabilities have been around for more than three years and target, not surprisingly, the Microsoft Office suite.

However, we can distinguish CVE-2017-17215 and CVE-2018-10088 affecting respectively Huawei routers and the XiongMai uc-httpd HTTP server, devices represented here by their use in the now famous Mirai botnet (and its variants such as Satori) targeting IoT devices and networks exposed on the Internet.

A STABLE TREND EVIDENCED BY THE OFFICE VULNERABILITY

The Office suite and maldocs have been a preferred infection vector for several years now. Although the vast majority of malware simply uses macros to infect the unwary user, some use vulnerabilities to infect even a wary user. Thus, malware tends to use the same vulnerabilities and not change them as long as they remain exploitables.



CVE-2017-11882, a memory corruption allowing arbitrary code execution in Microsoft Office, has held the top spot for several years nows.

Barely a week after its fix by Microsoft, this vulnerability was seen exploited by APT34. Since then, its popularity remains until it is mentioned in the 2020 CISA alert[12] about the most regularly used vulnerabilities. This CVE is still relevant today, having been used recently by malware such as Loki, Formbook, Zbot or Agent Tesla.

While these vulnerabilities are nowadays detected by security solutions (a special mention for CVE-2017-0199 which has no less than 12 dedicated detection rules, in addition to those included in anti-virus engines), we can legitimately wonder why these old vulnerabilities are still so much exploited.

The reason lies in the fact that they still represent an efficient propagation vector for cybercriminals who are becoming more professional and are looking to make their actions profitable.

The teams in charge of information systems are often short of manpower to keep their systems up to date. This phenomenon has a direct consequence on the functioning of ransomware groups, which will use this situation to their advantage.

...BUT THAT REMAINS NOT STATIC (FOLLINA VULNERABILITY)

However, this weakness is known. As a result, more and more entities have improved their processes to reduce the time to fix this type of vulnerability. At the same time, there is an acceleration of the various groups for the express exploitation of vulnerabilities when a patch is released or a vulnerability is notified.

Let's take the example of one of the vulnerabilities that made a remarkable entry in the top this year: the CVE-2022-30190 also called «Follina» and for which a dedicated note has been written by Gatewatcher Purple Team.

05/27/2022 → Tweet (exploitation detected)

05/30/2022 → Assignment of a CVE to this vulnerability / beginning of press coverage / Use of the CVE by TA4133 group

05/31/2022 → Availability of the first detection rules / availability of a workaround by Microsoft

06/03/2022 → Communication to our customers detailing the vulnerability and providing other detection rules

06/06/2022 → Use in a phishing campaign targeting US local governments and European governments.

06/07/2022 → Use by TA570 group, affiliated to Qbot

06/13/2022 → Use by the Sandworm group in a campaign targeting Ukraine

06/14/2022 → Publication of a patch by Microsoft

06/21/2022 → Use credited to APT28 in a campaign targeting Ukraine

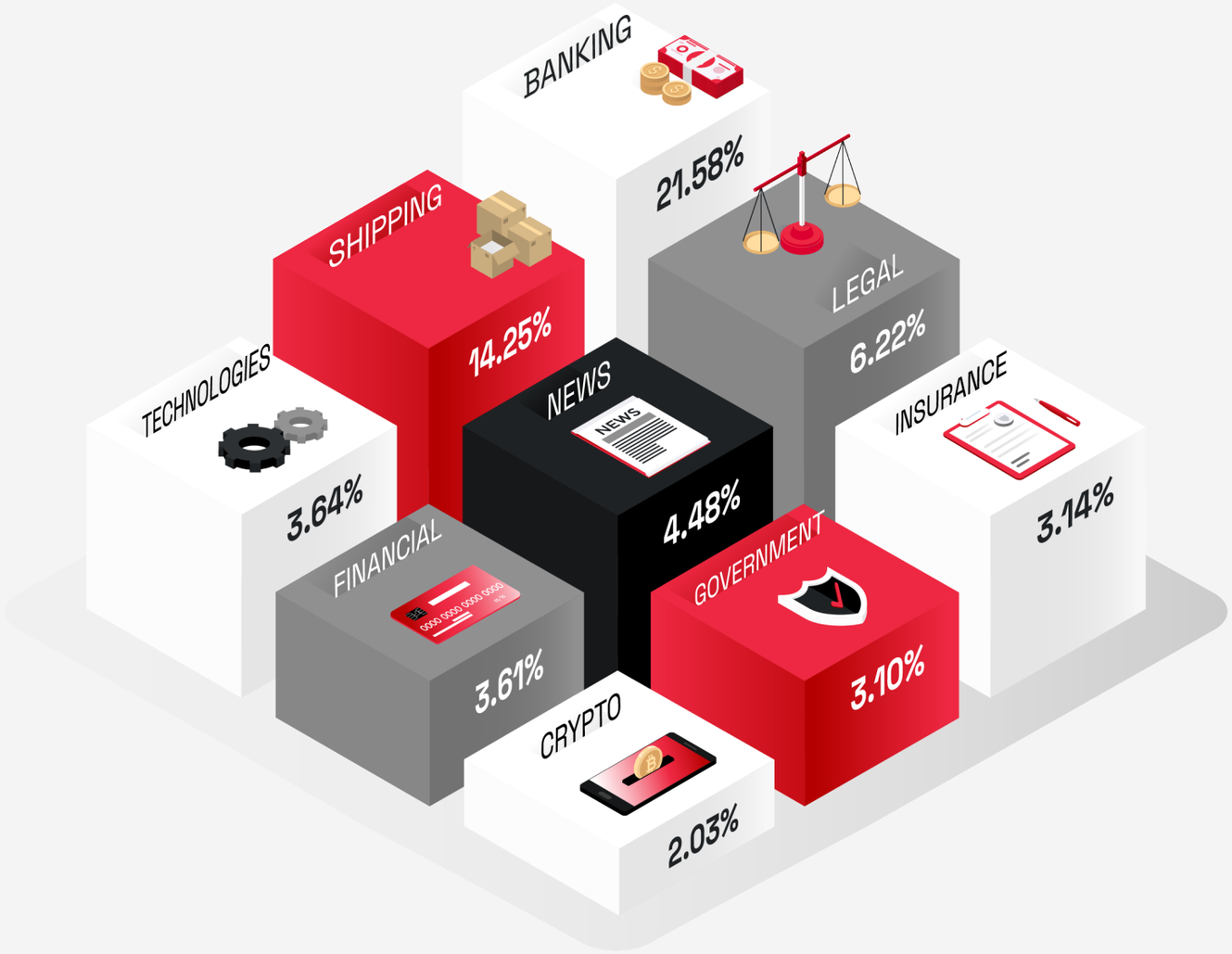
07/09/2022 → Use for the distribution of Rozena

EOT

Released at a time when Microsoft announced that they wanted to block macros in Office documents, this vulnerability has allowed to highlight the speed of reaction of the different malicious actors to include the exploitation of a vulnerability in their infection process. Let's recall that this vulnerability allowed, under certain conditions, to trigger the malicious load during a simple preview of the document. Moreover, as the chronology of events shows, the moments between the publication and the correction can be very different, underlining the importance of the reactivity of the systems on the detection of these events.

07 A MULTI-SECTORS THREAT

MARKED BY THE USE OF SMISHING



This ranking is not a surprise when we know that these are some of the most dynamic sectors, which are the preferred targets of ransomware attacks. This is obviously the case for the banking sector, the media, and technology in priority.

Although financial motivation is often the main reason for attacks, the temporary interruption of the media or a banking system, as well as access to confidential legal or government data are also very present objectives.

Note the freight sector (logistics expedition) which, although traditionally little impacted, is making a noticeable progression as a new target of choice for Threat Actors.

FOCUS 1 : LIVRAISON DE CYBERMENACES À TRAVERS LE SMISHING

Similar to the widespread frauds in France targeting the personal learning account (CPF) or health insurance, phishing through fake delivery emails or SMS is now rampant. This practice is becoming more and more widespread and is currently in second place in our ranking of business sectors that are victims of attacks.

There are two types of processes :

- → The attackers send SMS messages pretending to be legitimate delivery services, telling the customer that he has to pay various fees, such as customs fees, to have his package delivered. The small amount requested does not alert the victim.
- → The attackers ask the victim to fill in their credentials via a web interface similar to the delivery service.

This approach is particularly effective during holiday periods such as Christmas, when individuals are more likely to order products over the Internet and are waiting for their packages.

Already in December 2021, the French Customs Department warned against this practice, which in some cases imitated customs emails. The German delivery service DHL reported on June 28, 2022 that it was the target of a global phishing attack of this type and is actively working to block these attacks and associated fraudulent sites worldwide.

FOCUS 2 : THE HEALTH OF HOSPITALS UNDER CYBER-THREAT

A second sector that is not in our top 10 but that we are hearing more and more about in the last two years is healthcare. From the start of the pandemic, this healthcare sector was quickly a target, with a 150% increase in the volume of cyberattacks in the first two months of 2020, particularly against hospitals. Other infrastructures that have been affected include national health organizations, vaccine companies, research institutes and also contact tracing applications.

Although this sector has historically been targeted for personal information, the targets and objectives have diversified. On the one hand, we have seen attacks against research institutes as well as disinformation campaigns, and on the other hand the appearance of purely financial motivations with the phenomenon of ransomware.

Focus on a recent attack : Corbeil-Essonnes Hospital Center in the south of Paris region

During the night of August 20-21, 2021, the Corbeil-Essonnes Hospital Center was the victim of a ransomware that encrypted the institution's data and some backups. The attack, which paralyzed its computer equipment, has since been stabilized. This is not an isolated case. Jean-Noël Barrot, Minister Delegate in charge of the digital transition, has indicated that healthcare institutions in France were victims of a cyber attack every two weeks on average over the first half of 2022. In the case of this attack, the management of the investigation by the specialized services of the national gendarmerie revealed the involvement of the Lockbit ransomware.

This is surprising because the Lockbit group clearly states in the rules for its affiliates that it is forbidden to encrypt institutions where the damage to files could lead to the endangerment of users. In any case, the group claimed responsibility for the attack in early September on their website.

It appears that the hijacking of a provider's support account was the initial intrusion, and that the cyber attackers infiltrated the hospital's network 10 days before launching the attack.

It appears that the cyberattacker group had initially demanded a $10 million ransom to decrypt the data, then reduced their demand to $2 million in exchange for the return and deletion of the stolen data after the hospital refused the first offer. The cyberattacker group also released a sample of the stolen data to pressure the hospital group, which included medical certificates, contracts with partners, account statements and other administrative documents and personal information about patients.

As a reminder, the ANSSI (french cyber security agency) has instructed hospitals and health care institutions not to respond to ransomware requests. The payment does not guarantee the decryption of the data and can encourage cyber attackers to reproduce their attacks. This was notably the case for Great-East Hospital Center and Epinal Hospital Center which saw their confidential data published.

This latest attack was clearly the one too many for the French government, which announced a 20 million euro budget for the ANSSI to specifically reinforce the support of health care institutions.

The different detection solutions against threats like Lockbit :

- DGA detection: the analysis of a domain name seen on the network indicates the associated risk level, provided that the connection is not encrypted.
- Sandboxing solution: the analysis of a file seen on the network indicates the level of associated risk.
- Behavioral observation: viruses often use lateral movements to propagate within a company's network. In our case, Lockbit propagates through the SMB protocol and tries to connect to servers using credentials it has managed to recover. It is possible to observe this behavior by paying attention to the failed connection alerts.
- C2 Beaconing detection: viruses usually communicate with a C2 server to receive instructions and send information.

WHY ARE HOSPITALS IN PARTICULAR SO VULNERABLES ?

First of all, their dependence on a connection to digital services (patient data, connected medical equipment) that cannot be interrupted makes them more likely to accept ransomware quickly. In addition, a lot of this comes down to human and digital assets. The lack of staff in hospitals and the temporary recruitment of less qualified personnel has accentuated cyber risks.

It is worth noting that hospital information systems, as is often the case among industrial IS, are not always updated because to do so would be to take the risk :

- to cause software and applications to malfunction and only work properly under a certain version of the operating system.
- of interrupting for a significant period of time an information system that caregivers need to be operational with a potential increase in the vital risk for patients.

CONCLUSION

During the first 6 months of 2022, the Purple team has highlighted the use by cyber attackers of methods that have already been tried and tested for many years: exploitation of old unpatched vulnerabilities (office, router...), packing techniques, malware family already identified as Mirai, etc.

The main reason for using these methods, which are already known, is that they are still as effective as ever, whether in their entirety, or for a victim who is not yet mature enough to put in place the appropriate protections.

Moreover, attackers are not necessarily looking for the most sophisticated attack if we take the example of VBA macros. These have been used maliciously for many years and still are today, even if we note that Microsoft has reduced their impact by limiting the default execution of macros.

Improvements in the areas of detection or limiting the effectiveness of an attack also show that attackers are always looking for new or innovative ways to achieve their goals :

→ Exploitation of new vulnerabilities (with the example of the Follina CVE)

→ Use of certain file types to destabilize our habits (ISO, LNK...)

→ Use of legitimate sites to hide an attack (Discord, Pastebin, google drive...)

As with the famous quote from Sun Tzu «Know your enemy and know yourself; if you have a hundred wars to fight, you will be victorious a hundred times over», an effective recommendation to limit cyber risks would be to really understand the threat as such, and to be able to observe it over time while having the appropriate tools to ensure efficient and reactive detection and thus quickly remedy their impacts.

ABOUT LASTINFOSEC CYBER THREAT INTELLIGENCE

LastInfoSec® is a Threat Intelligence platform designed to provide an immediate improvement in your level of protection. Its proprietary technology combines machine learning and Big Data processing to generate a high-quality stream of information on cyber threats in a very short time.

- → LastInfoSec® simplifies decision making for your operational security teams and significantly reduces their incident analysis and response time without changing their internal processes.
- → LastInfoSec®'s automated collection, analysis, and correlation engines make threat information available an average of 24 hours before the competition.
- → LastInfoSec® integration is quick and easy with standardized exports to the latest CTI standards (Stix v2, Stix v2.1, JSON, etc.) and available connectors to the leading analytics tools on the market (Splunk, OpenCTI, etc.)
- → LastInfoSec® 's platform continuously inventories and evaluates data sources accessible on multiple channels: social networks, specialized sites, dark and deep web...

ABOUT GATEWATCHER

Gatewatcher is a technological leader in cyber threat detection and has been protecting the critical networks of large companies and public institutions in France and abroad since 2015. Its offer combines AI with dynamic analysis techniques to provide a 360° and real-time view of cyber threats on the entire network, in the cloud and on premise.

Gatewatcher's NDR, CTI and Sandboxing solutions provide an immediate improvement to current and future cybersecurity challenges by addressing organizations' new detection needs. They are designed to be scalable and immediately operational for easy integration and use by our customers and partners.

SOURCES

[1] March 2022 CyberThreats Barometer monthly highlight

[2] June 2022 CyberThreats Barometer monthly highlight

[3] August 2022 CyberThreats Barometer monthly highlight

[4] May 2022 CyberThreats Barometer monthly highlight

[5] Lyceum malware analysis article

[6] Agent Tesla malware analysis report

[7] July 2022 CyberThreats Barometer monthly highlight

[8] Lyceum malware analysis article

[9] NSIS Packer malware analysis report

[10] Lyceum malware analysis article

[11] Web Service : One-Way Communication