GATEWATCHER

CYBER THREATS
SEMESTER REPORT

July-December 2022

SUMMARY

01 REPORT HIGHLIGHTS AND NOTES TO READER

For this second edition of the Semester Threat Report, Gatewatcher's Purple Team presents the threat trends identified each semester by Gatewatcher's CTI platform along with the active threat surveillance performed by the Purple Team's cyber analysts.

The aim of this report is to provide insight into the types of cyber threats observed between July and December 2022, how they evolved, and a perspective on future trends. The objective is to facilitate their detection and ultimately reduce the impact of future security incidents.

Each section features an explanatory ranking on each identified cyber threat topic. Thematic focuses focuses written by Purple Team analysts are also included to highlight established, emerging, or original new trends.

Within Gatewatcher, the Purple Team is dedicated to tracking and analysing the cyber threats facing our clients to ensure the constant updating and optimisation of the performance of our NDR, CTI, threat analysis, and qualified detection solutions.

The Purple Team boasts a diverse group of experts experienced in incident response, SoC analysis and integration, pentesting, CTI testing, and cyber security research.

The Cyber Threats Semester Report (#CTSR) is structured around five sections covering the following topics :

- The different file types used by cyber attackers and their evolving trends
- The malware most used by cyber attackers
- The most frequently used malicious techniques during the period
- The most active threat agents
- The activity sectors most targeted by cyberthreats

The aim is to report on the main trends in cyber threats over the period, for example during this half-year:

- Using HTML files for malicious purposes, as well as.
- The importance for an attacker to employ local system and information system discovery techniques for post-infection.
- The inclusion of the top malware- Qbot and the Threat actors SilverTerrier and Wizard Spider.

This report also highlights our interpretation of certain cyber developments such as:

- The decrease in the number of cyber threats targeting the cryptocurrency sectors;
- The targeting of authoritarian governments by hacktivists;
- The manipulation by cybercriminals of certain files for infection purposes, as part of the changes in the use of Microsoft Office.

The Purple Team was also keen to describe more anecdotal yet unusual cyber threats such as the use of Hangul files to compromise a workstation and an explanation of how Wannacry survived.

02 INFECTION VECTORS :

A STABLE PODIUM THAT HIDES A WIDE VARIETY OF FILE TYPES

In line with the beginning of 2021, the market is dominated by Linux (ELF) and Windows (PE) executables, with a strong prevalence of the latter taking the lead in the second half of the year.

This is because executables will invariably find their way into an infection chain, particularly in the final stages of its operation. The prevalence of Windows executables naturally reflects the overwhelming dominance of Microsoft's OS, most notably in the professional PC market. However, it is also a fact that the company has not managed to sufficiently reduce the attack surface on its flagship operating system. This is despite a number of initiatives concerning the MS Office suite.

MALDOCS, A CHANGING ECOSYSTEM

After some initial hesitation, the Redmond-based publisher finally came to the decision at the end of July to block macros by default on its Office suite. The departure of the Microsoft Office files from our top 3 was, therefore to be expected.

Until now, these files formed part of a predominant mode of infection initiated by a professional-looking phishing email[1], containing a Word, Excel, or PowerPoint file as an attachment. As this type of file is commonly shared within the business community, the target was inclined to be unsuspecting enough to open the attachment. The latter contained a macro[1], i.e. code written in Microsoft Visual Basic, executing a PowerShell command when opening the file[1] in order to deliver and execute a malicious payload, usually a Windows executable (PE) file.

Microsoft's decision significantly distances the potential victim from the malware payload by increasing the number of operations that must be performed before the malicious macro can be activated. This in turn reduces the incentive for threat actors to attack files in the Office suite.

Through an almost automated process, we noticed that cybercriminals are changing their techniques, tactics, and procedures (TTPs) and moving on to other types of files. Among the relevant actors are Mummy Spider (Emotet), Mallard Spider (Qbot), Maze Team (IcedID), and Agga (Agent Tesla).

As a sign these players are still feeling their way through the development of an infection chain that would replace those in which the Office suite files were operating at the time, we are seeing each of them flitting between different TTPs, each of which involves different file types. Among the latter are LNKs, archives and disk images that remain very much present over the half-year but also, in a more scattered and unexpected way, HTA, CHM, MSI, and XLL file types.

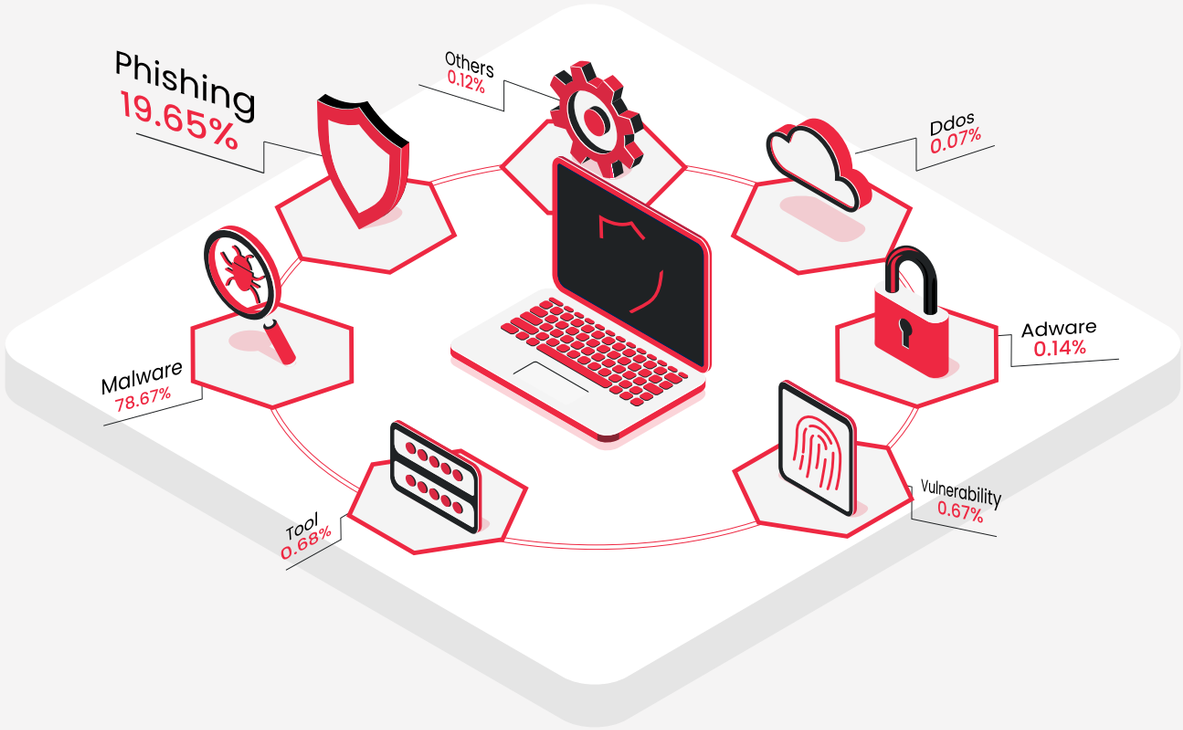
The biggest breakthrough in the second half of the year involved PDF files. As with MS Office files, PDFs are generally perceived as being secure, making them an effective entry point for a phishing email. In particular, they can be used to attack a vulnerability in the Adobe Acrobat reader in order to execute arbitrary code, or to embed potentially malicious JavaScript code. PDFs may also contain hyperlinks to malicious sites or servers that can, among other things, initiate a stealth download. For example, this was observed in the IcedID campaign in January 2023.

MALICIOUS FILE TYPES :

MALICIOUS FILES :
THE FISHING IS GOOD...

Absent from the last report, HyperText Markup Language (HTML) files took second place this semester. This type of file, comprising the extensions .htm, .hta and, overwhelmingly, .html, is so prevalent in the cybercrime ecosystem that it should remain at the top of the podium in the coming six months.

Of course, the classic role in which this type of file is involved is in phishing[1]. In such cases, it is simply a matter of imitating a legitimate web page, such as a bank, a social network, a government service, and the like, in order to induce the victim to enter confidential information (Credentials[1]) or to download a malicious program. The task is made even easier by the widespread availability of phishing kits in public or semi-public access on the Internet. These «toolkits» greatly contributed to reducing the cost, both technical and operational, as well as increasing the quality of phishing campaigns. In this context, it is particularly relevant to highlight a variant of phishing called Spear phishing[1] that adds social engineering techniques to phishing in order to personalise the attack, thus making it much more effective.



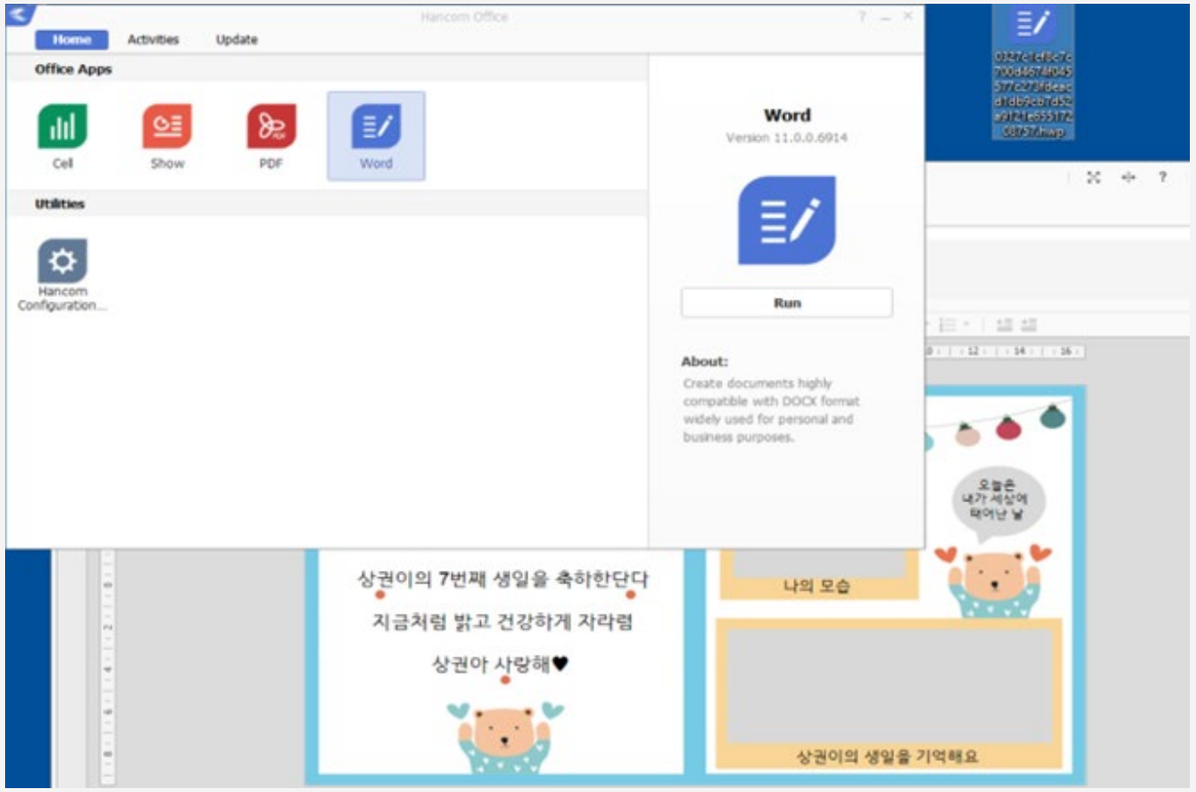
... BUT ALSO

HTML files can also be used for the purpose of bypassing email gateways. These usually provide some level of security to the user by filtering potentially malicious or unwanted emails from the inbox, using the so-called «HTML smuggling» technique[1].

This technique entails hiding a malicious payload inside an apparently benign HTML file. The malicious file will then be reconstructed when the page is loaded by the browser and downloaded to the victim's computer. In particular, this is the intrusion technique employed by the Qbot[1] malware discussed later in this report.

HANGUL FILES, A KOREAN SPECIALTY

In the results of our file collection, we found an unusual extension designated .hwp. HWP files, or Hangul files, derive their name from the «Hangul Word Processor» software, which became Hancom Office, commonly used in South Korea. Developed by Hancom Inc, this software has been widely adopted by national organisations and government agencies in the context of an IT independence policy initiated in the 1990s.



Consequently, it is often these institutional targets who find themselves the focus of campaigns by North Korean actors, based on this type of file.

If in the past[1], we witnessed campaigns relying on vulnerabilities intrinsic to software designed to process HWP files (e.g. CVE-2015-1774, CVE-2018-0360) or even abusing the ability of these files to execute code written in PostScript, the campaigns during our period in question are mainly based on exploiting the Object Linking and Embedding (OLE) protocol.

Under Windows, the OLE protocol enables applications working in different formats to communicate with each other. It is then possible to integrate or link objects generated or managed by other applications, such as images, videos, and spreadsheets, into a text document.

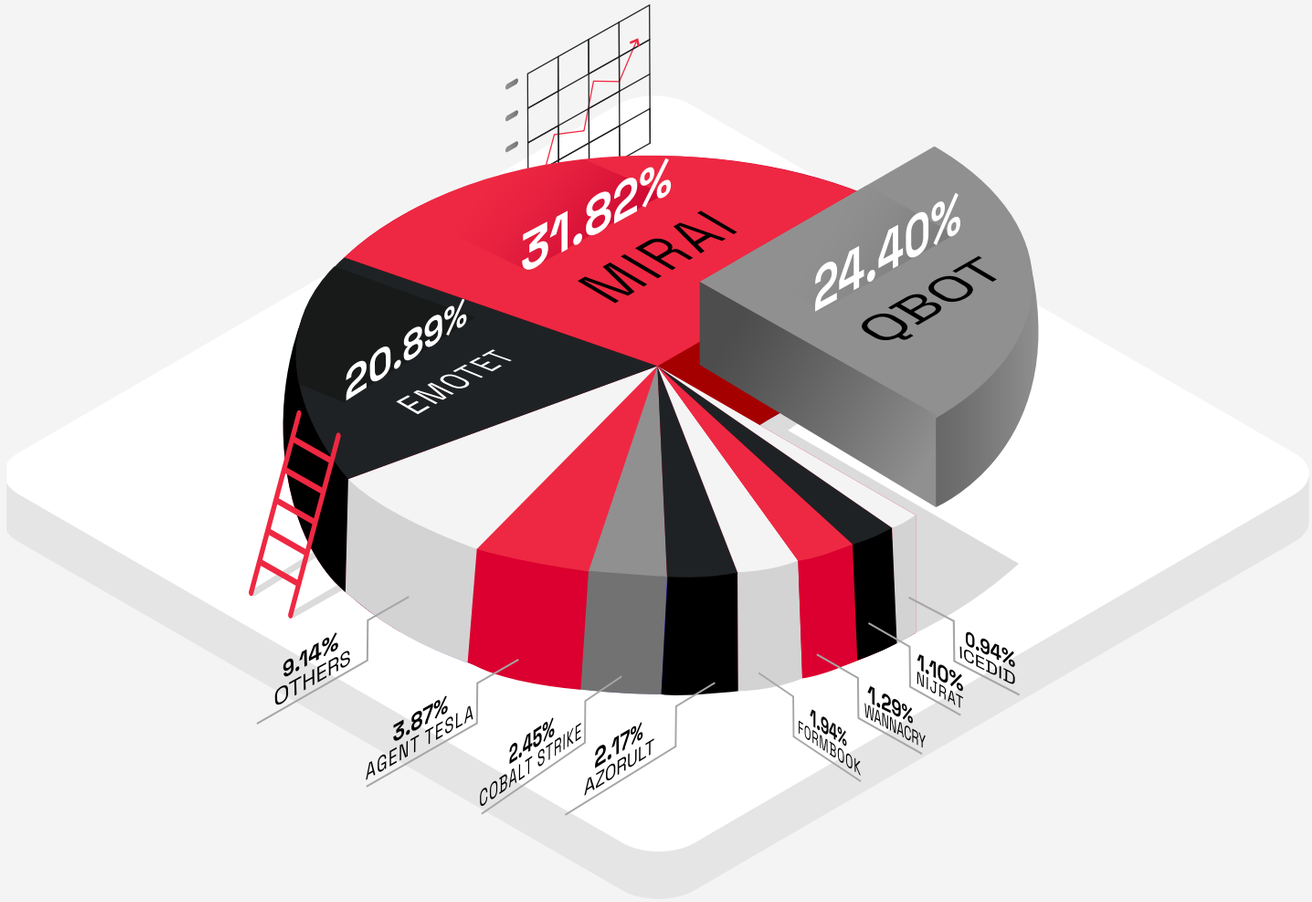
In the present Hangul file-based campaigns, various malicious scripts (PowerShell and VBS) and executables (PE) become embedded in the file via the OLE protocol. All they require is a simple click from the victim to deliver their malicious payload. The document's entire purpose is to entice the victim to click on the OLE link by disguising it as an email window, for example, or any other legitimate-looking link.

03 MALWARE : OLD BUT NOT **OBSOLETE THREATS**

In the report covering the first half of 2022, the top of our malware list was largely held by Emotet, which we reported on in our march[2] and december[3] 2022 barometers.

Emotet alone accounted for more than half of the observations, however, it was dethroned in the second half of the year. This sudden drop in the rankings can be explained by the news that the Conti Group, an intensive Emotet user, ceased its operations in mid-2022 shortly after the «Contileaks».

As a reminder, this event follows the Conti Group's position regarding the conflict between Russia and the Ukraine, where the group declared its «full support» for Russia.



MIRAI: A BOTNET AT THE FOREFRONT

In the second semester of the year, the top of the ranking was held by Mirai and its variants representing a little less than a third of the observations. These botnets are still very active. A special focus was already devoted to it in our June Cyber Threat Barometer[4].

The popularity of Mirai's targets and its behaviour ensures that, like WannaCry, it will occupy a prominent place in our top list, obviously for many years to come. Unsurprisingly, Emotet's successor in this ranking is the Qbot malware (also known as QuakBot, Pinkslipbot...) already present in the threat landscape since 2007.

National Cybersecurity Agency of France (ANSSI) in its 2020 report[5] already reported that Qbot was being circulated by Emotet since 2017 and that it had become the most distributed malware payload since August 2020. The same report also states that the relationship between Emotet and Qbot was probably more than just a client/service provider relationship.

Despite the long existence of Qbot, it continues to evolve and adapt its delivery methods. At the end of 2022, for example, the use of DLL hijacking in various components of Microsoft Windows and the bypassing of the «Mark-of-the-Web» (MotW) was the subject of a focus in our January 2023 Cyber Threat Barometer[6].

> *"In light of these various elements, it is conceivable that the collaboration between the Emotet operators and those of Gozi ISFB and QakBot extends beyond the mere client/service provider relationship.*
>
> **ANSSI | Report CERTFR-2020-CTI-010 - p.9**

2017-2021 :
Strengthening its links with Emotet

From 2017 onwards, Qbot became an established member of the malware landscape with its first high profile campaigns of 2019/2020. During this period, Qbot developed a similar modus operandi to Emotet: the ability to hijack email conversation threads in a localised manner.

At this point, the relationship between Emotet and Qbot became stronger: While Emotet was the most distributed malware at the time, Qbot was the most frequently delivered post-infection malware. It was also at this time that an extensive campaign was launched with Egregor, supported by the resources obtained after Maze's shutdown.

2017 : Observation of AD account bruteforce attacks to propagate

2017 : Distribution by Emotet

2018 : FBI alert on USB drives preloaded with Qbot

2019 : MegaCortex campaign (ransomware)

2019 : PwndLocker campaign (ransomware)

March 2020 : ProLocker campaign (ransomware)

August 2020 : Most distributed payload by Emotet

August 2020 : Emergence of localized thread hijacking

November 2020 : Egregor campaign

January 2021 : Emotet takedown

September 2021 : Back to hostilities, main vector is macro VBA Excel

September 2021 : ProxyShell / Qbot / Cobalt Strike campaign

October 2021 : Lockean campaign using Emotet / Qbot / Cobalt Strike

November 2021 : Use of the ZeroLogon vulnerability

November 2021 : Emotet comeback

February 2022 : Microsoft announcement: disabling macros

April 2022 : Use of MSI

May 2022 : Use of LNK

June 2022 : Use of Follina (CVE-2022-30190)

June 2022 : QBot observation in a BlackBasta campaign

July 2022 : Use of HTML smuggling [2]/ISO / LNK combination

July 2022: Use of sideloading DLL in calc

September 2022 : Use of BruteRatel of localized threads

November 2022 : Microsoft announcement: motw propagation to ISO files

November 2022 : Use of CVE allowing MotW bypass

2021-2022 : A new era

The demise of Emotet in 2021 reshuffled the deck somewhat, naturally leading to an increase in the use of Qbot. Significant campaigns based on exploiting vulnerabilities as initial infection vectors also emerged.

Finally, despite a strong comeback of Emotet in late 2021-early 2022, we noted the rapid adaptations of Qbot in its delivery methods, following Microsoft's announcements. Whether it was by exploiting vulnerabilities such as ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021- 31207) or Follina (CVE-2022-30190) or by using alternative file types such as LNK or MSI files. These adaptations enabled Qbot to retain its position when Emotet was phased out in the second half of 2022.

WANNACRY IN 2022 : A MISTAKE IN THE RANKING ?

As if any further introduction is needed, Wannacry, also known as WannaCryptor, WannaCrypt, or WCry, is a ransomware attributed to the Lazarus group that emerged in a massive attack occurring in 2017 and affecting 150 countries.

As a means of replication, WannaCry used an SMB vulnerability (EternalBlue - CVE-2017-0144) and a tool (Double Pulsar) disclosed some time earlier in an NSA data leak published by the Shadow Broker group.

While most of the malware listed in the top may not be surprising, the presence of Wannacry in 2022 may seem rather anachronistic. Unfortunately, a simple SMB honeypot in place for a few days, or even a few hours, demonstrates that this malware is still very much present and still active. One might reasonably ask how a 2017 threat using long-patched vulnerabilities could still be active.

At the end of 2021, the software vendor ESET reported that 21% of its ransomware detections involved Wannacry. For Kaspersky, Wannacry still accounted for 12% of detections in third quarter of 2022[7].

Nevertheless, the explanation for this incongruity is relatively simple. As opposed to most current threats, Wannacry is a worm.

By definition, it replicates itself at every opportunity via the EternalBlue vulnerability or by exploiting Double Pulsar. Hence, as long as vulnerable machines remain present and accessible, this threat will never go away. A 2021 study estimated that 18-20% of Microsoft's clients continue using systems that are no longer being supported and that 1.5-2 million machines still have SMB vulnerabilities exposed on the Internet[8].

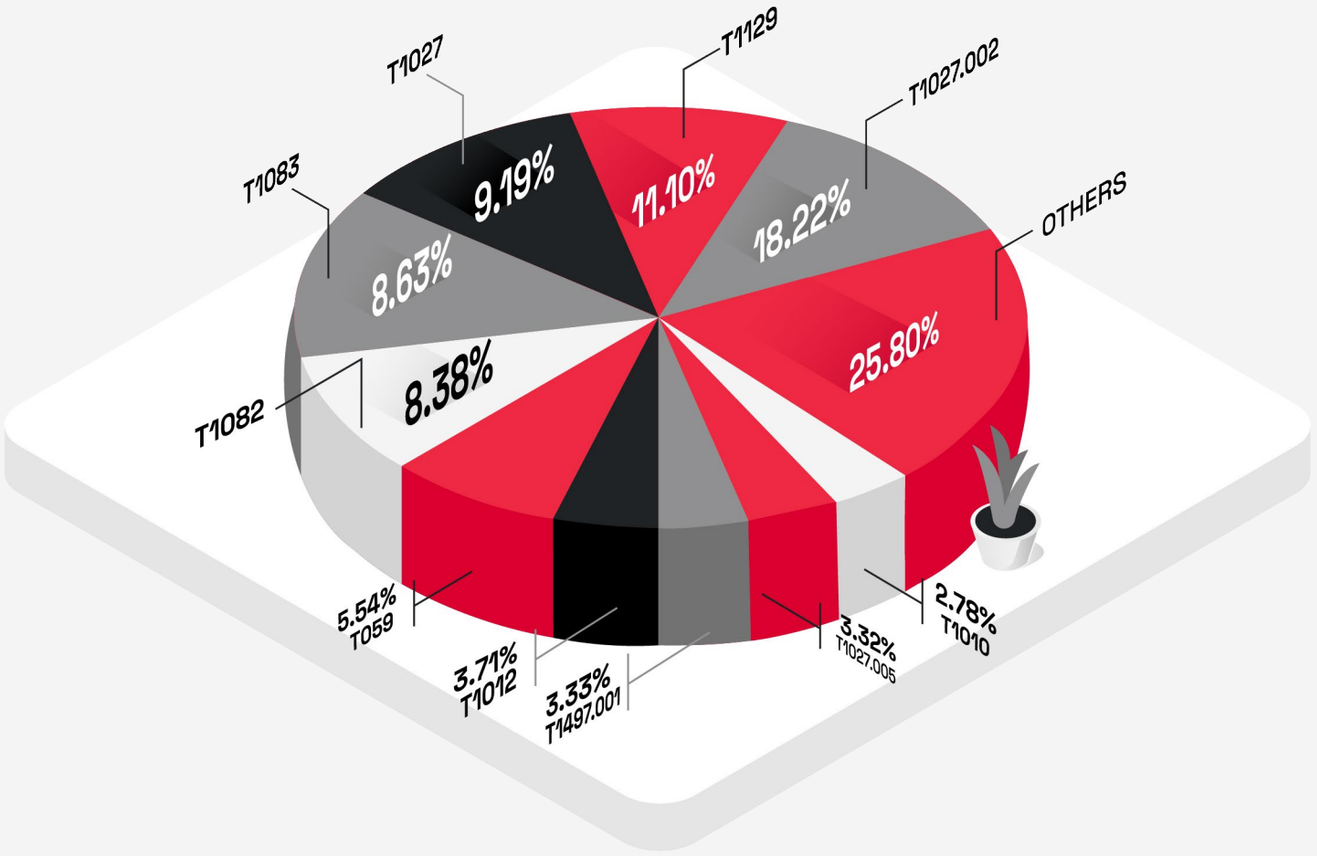
04 TTP : NEW ATTACKS, OLD TECHNIQUES

Our findings for the second half of 2022 have not revealed any significant changes in the behaviours and techniques employed by malicious actors, resulting in a top 10 that is essentially unchanged from the first half

The techniques outlined here are also typical of the methods employed by the malware we find on the podium of our top 10 malwares[1]. It should be noted that this is made possible due to the fact that these methods are generic enough to be used by many different types of malware.

Emotet alone accounted for more than half of the observations, but was dethroned in the second half of the year. This sudden drop in the top is, in our opinion, explained by the news of the Conti. group, an intensive user of Emotet, which stopped its activities in mid-2022 shortly after the «Contileaks».

As a reminder, this event follows the Conti Group's stance in the conflict between Russia and Ukraine, where the group displayed its «full support» for Russia.



A FOCUS ON QBOT

The upsurge in the number of Qbot[2] campaigns in the second half of 2022 confirms that this malware continues to be a reference tool for many attackers. One of the reasons for this success is due to its modularity, enabling the various groups of actors involved to easily adapt it to their needs. Yet, it is also being modernised as new techniques are regularly being used to avoid detections.

Un grand nombre de malwares sont distribués en tant que, ou font usage de DLLs (T1129). Il n'est pas rare que certaines étapes de packing fassent également intervenir une DLL, comme c'est le cas pour celui d'Agent Tesla analysé précédemment par nos équipes[6]. L'installation d'un service Windows se fait également avec une DLL.

Since its appearance in 2007 as a banking Trojan, Qakbot has thus become a versatile piece of malware offering attackers a wide range of capabilities: performing reconnaissance TA0043[1] and lateral movements , collecting and exfiltrating data TA0010[1], or provide other useful payloads on the assets concerned TA0002[1]. Qakbot mainly spreads through attachments and links in spearphishing attacks (T1566)[1].

According to information collected by LastInfoSec, our CTI knowledge base, initial access to Qakbot in Q3 and Q4 2022 was mainly via HTML Smuggling. This evasion technique, which relies on legitimate HTML5 and Javascript features, enables threat actors to deliver their malware via an attached HTML file, or directly via a website.

The malicious payload is directly read by the victim's browser enabling the creation of a password-protected archive in zip format. At the same time, a dialog box appears to save the file and displays the password. If the victim enters the password provided by the attacker and then opens the zip archive, then an .ISO file is extracted. This file enables the victim to become infected with the Qakbot malware. Once the patient zero is infected, Qakbot performs both a local and network reconnaissance to enable the threat actors to spread and achieve their goals.

As the initial attack vector involves phishing, end-users play a major role in combating this threat. In particular, they must be made aware of the risk of downloading encrypted archives (.zip, .7z...) using a password on the Internet. This method of sending malware has become widespread, enabling it to bypass any detection mechanisms present on the email server and even Endpoint Detection Investigation and Remediation (EDiR) or EDRs deployed on the terminals. It is also possible to look into the possibility of disabling the automatic mounting of disk image files, such as ISO files. This preventive action can be accomplished by changing the values in the Windows registry.

DISCOVERY : A CRUCIAL STEP

Our research revealed that system information discovery T1082[1] and file and directory discovery T1083[1] are among the most common techniques used by cybercriminals. They are in position 4 and 5 of our top.

Indeed, once an attacker has gained initial access to an infected system, they usually try to obtain information in order to make the most effective decisions for the next stage of their attack: privilege elevation, lateral movement, or even encrypting the information system. In concrete terms, this entails attempting to obtain detailed information about the operating system, patches, and service packs deployed as well as its architecture. Following this information gathering, the attacker will then be able to determine whether or not to completely infect the target, and by what means.

LOCAL DISCOVERY

Qakbot is no exception, as once the machine is infected and communication with the Command & Control server TA0011[1] its primary tactic is to automatically collect information about the infected system using a series of locally executed commands. To achieve this, the malicious program injected by Qakbot T1055[1] runs commands useful for its recognition by relying on command line tools natively integrated in Windows (T1082) / T1083 / T1087 / T1135 /etc.)[1] and therefore considered legitimate by the protection systems in place.

For example, the «net» command can collect information about users, groups, hosts, and files. The injected malicious process also extracts information from web browsers (Internet Explorer and Microsoft Edge) by abusing a built-in utility - the Esentutl binary. Browser data, including cookies and the browser history (T1539), are collected from the web cache. These can enable the spoofing of a user session to facilitate propagation.

EXPLORING THE INFORMATION SYSTEM

Querying the Active Directory (AD) is another common information gathering target. Attackers can harness the data extracted from the AD to gain information about the network and increase their privileges.

By this means, it is possible to identify the domain to which the infected machine belongs and to learn more about the users, groups, and assets of that domain. There are several tools designed for this purpose: PowerView, ADRecon, and also Bloodhound .

These tools may be used for legitimate purposes; however, they are also frequently used by cyber-attack groups.

AS AN EXEMPLE...

Recent incidents of Qakbot infections made it possible to highlight the deployment of the Brute Ratel framework[8] as a payload. Support for this framework enables easy integration of the SharpHound utility, the official data collector for BloundHound.

Then, the malicious process can run this tool to map the Active Directory domain and learn more about the structure of the targeted information system: Active Directory organisational units (T1087.002), group strategies (T1615) , inter/intra-domain trust relationships (T1482), privileged accounts and groups (T1615).

All harvested files are then compressed into a ZIP file for subsequent exfiltration.

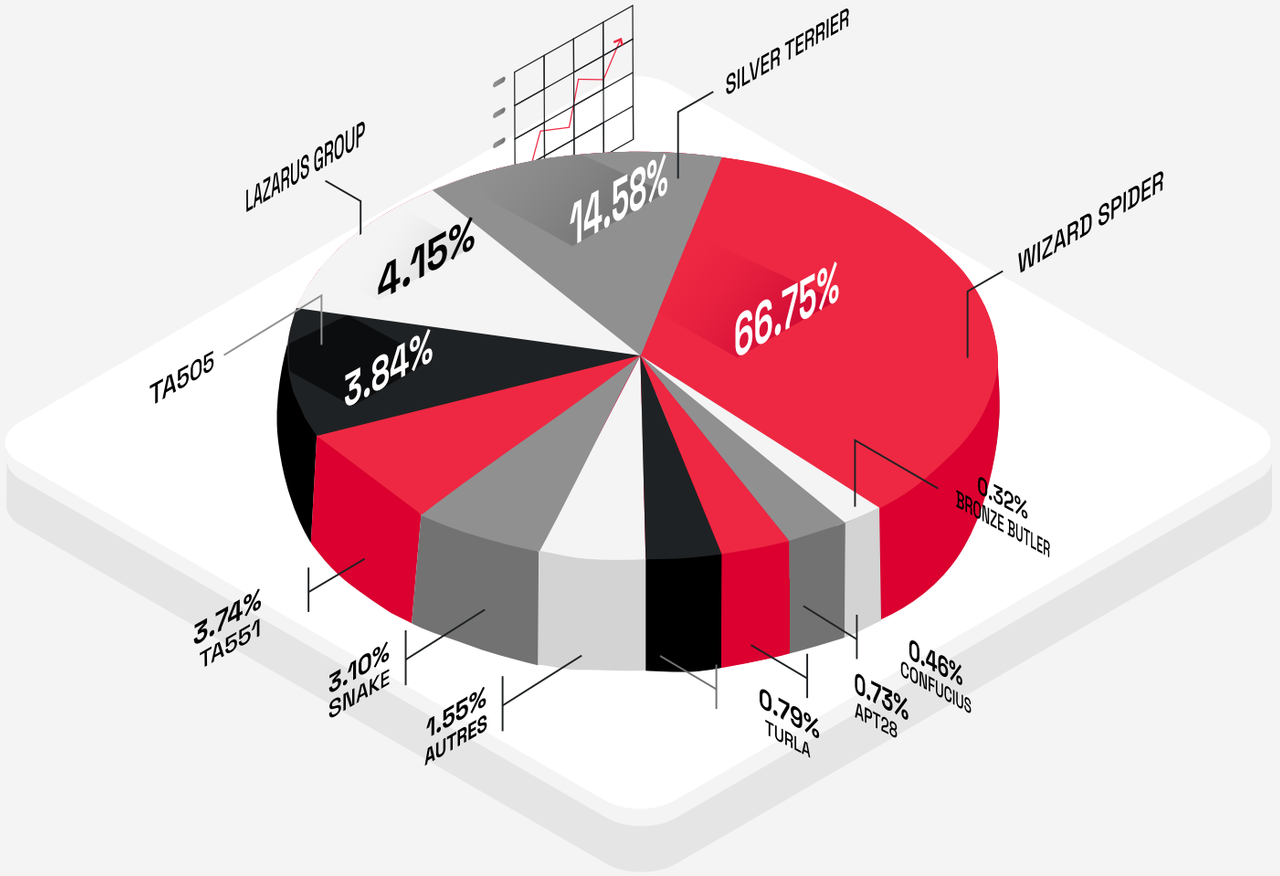
Similarly, in recent Emotet[2], malware campaigns, it was noted that a propagation module was added via the SMB protocol[9]. Once this module is loaded on the infected machine, a reconnaissance is launched listing the network resources (T1135) to build a list of servers. Subsequently, the module scans the freshly established list attempting to connect to the IPC$ sharing using lists of hard-coded common usernames and passwords (T1110.001).

If no connection can be made with the available credentials, the SMB module may also attempt to search the Windows API NetUserEnum function for additional usernames from the targeted server. Each new potential username found will be subject to a brute force attack with the previously used hard-coded list. If a connection succeeds, the module finally attempts to connect to the ADMIN$ and C$ sharing by copying the Emotet loader to the said sharing and then executes it: a lateral movement is then performed.

05 THREAT ACTOR : AN EASTERLY WIND IS BLOWING ACROSS THE LANDSCAPE

With approximately 100 threat actors tracked during the second half of 2022, we are presenting for the first time a listing of the 10 most actively observed cybercriminal groups.

Unsurprisingly, our ranking is mainly made up of Russian and Chinese groups. These two geographical regions are known to have a substantial pool of cyber attackers. First of all, we should note that these groups have been operating for more than a decade. They are driven by two motives: financial gain and cyber espionage.



WIZARD SPIDER

At the top of the list is the Wizard Spider group. This threat actor, most likely affiliated with Russian cybercrime networks, is also identified as UNC1878 or Team9.

It is mainly renowned for the multitude of malware that its members developed since 2017 such as Emotet, Conti, TrickBot, BazarLoader, and Ryuk. This organisation is well equipped to carry out large-scale cyber-attack campaigns, from reconnaissance and intrusion phases to payment and laundering of extorted money. Wizard Spider has perpetrated millions of spam, ransomware, and data theft attacks, enabling them to fraudulently disclose private information.

The group targets public sector, government, and healthcare organisations, a wide range of large private companies, the defence sector, and many others. Despite having a reduced presence in the second half of the year, Emotet remains third in our ranking. This explains why Wizard Spider, the cyber group behind this trojan, sits in first place.

SILVER TERRIER

It is followed by SilverTerrier, a consortium of several Nigerian attackers specialising in Business Email Compromise (BEC) scams. A BEC scam entails sending an email mimicking the origin of a known source making a legitimate request. This group has been operating since 2014, primarily targeting companies in the high-tech, higher education, and manufacturing sectors. Silver Terrier's position in our ranking is consistent with the FBI Internet Crime Complaint Center (IC3)[10] 2021 report where it has held the top spot for six consecutive years. Over the past few months, the Agent Tesla and Lokibot malware were being used extensively in campaigns. The latter are listed in 4th and 12th place respectively in our malware ranking.

LAZARUS GROUP

The Lazarus group rounds off the podium. Also known as APT38, this group, active since 2009, is sponsored by the North Korean government and is known worldwide for carrying out ideologically motivated attacks. Its prime objectives include extortion, information theft, sabotage, and espionage. Throughout its long history, it has attacked the banking sector, the defence industry, software companies, pharmaceutical groups, crypto-currency platforms, as well as industries in manufacturing and energy. It conducts its attacks by relying on social engineering and deception through the use of phishing campaigns as a primary infection vector.

Its goal was to steal private keys and to leverage vulnerabilities to engage in fraudulent transactions. In recent years, the group has reportedly stolen approximately $2 billion in crypto-currency. At the bottom of the podium comes TA505, a Russian group best known for creating the Dridex banking trojan, which is discussed later in this report.

This group attracted our attention this year owing to the diversity of tools used and their determination to improve the malicious code they were able to experiment with over the past few years. Since 2018, TA505 introduced Azorult to its arsenal of home-grown malware. The latter was spotted in several campaigns at the end of the year, occupying the 6th place in our top malware list.

Occupying the middle of this top is TA551/Shathak, a group distributing its malware via email, targeting mainly Europe and Japan. In the numerous campaigns attributed to it, the IcedID malware, listed 10th in our malware ranking, was used with an attack chain that has become a regular occurrence this year. It relies on a ZIP archive attachment containing an ISO file with a Windows shortcut (.lnk) that, through a PowerShell command, loads a Windows library (.dll).

Next is Turla/Snake, a Russian group that carried out various attacks using keyloggers such as Agent Tesla and NjRAT. The remainder of the ranking consists of groups conducting cyber-espionage such as APT 28 (7th), Confucius (8th), Bronze Butler (9th), and Dragonfly (10th). These perpetrators mainly target critical sectors such as defence, government, and energy. The war in Ukraine, which broke out in February 2022, leading to an energy crisis and a volatile geopolitical context explains the strong presence of these cyber attackers over the period.

...FOCUS 1 : TA505

TA505 is a Russian cyber-criminal group operating since 2014, known to be behind the Dridex banking Trojan and the Locky ransomware. In its early days the group relied heavily on third-party services and tools to conduct its fraudulent activities. Over the years, it matured to become an independent force in the entire kill chain.

Also commonly known as Grateful Spider, Evil Corp, Gold Drake, ATK103, and Dudear, Indrik Spider TA505 has a history of launching massive phishing campaigns with a high success rate, exploiting vulnerable systems, and enticing users to download their malware.

Financial gain is the prime motive of this actor, obtained through the theft of sensitive data and holding it for ransom. The group has also extorted many millions of dollars from its victims. Graceful Spider maintains a high level of technical sophistication by constantly evolving its tactics to evade detection. Running the Necurs botnet, the group originally started its core business by selling access to compromised networks to other malware operators, through which it was able to operate some of the most notorious spam campaigns.

TA505 TIMELINE :

2014 - 2017 :

Limited activity apart from distributing Trojans and ransomware. Running the Dridex malware, the cybercriminal group favoured the Locky ransomware in 2016 before re-launching campaigns in 2017. TA505 employed the TrickBot malware in attacks in 2017.

2018 to the present :

Shift in intrusion method from trojan and ransomware to backdoor. TA505 offered access to hacked information systems, yet kept some of them in order to launch malicious payloads on the victims' machines. In the first phase, the group used various downloaders including malware enabling the delivery of an offensive payload such as Quant Loader, Marap, Amadey, and Gelup.

These enabled the group to gain access to their victims' machines via backdoor entries such as FlawedAmmyy, tRat, ServHelper, FlawedGrace, FlowerPippi, or SDBot. We observed that some of these malwares were still being used by the group in 2022.

Other families of malware are believed to be linked to this group, such as FlawedAmmyy, the Neutrino botnet, and the ServHelper backdoor, a variable of which enables the FlawedGrace remote access trojan[3], to be downloaded, as well as the Clop ransomware, which is believed to have infected numerous companies. The threat actor has a history of implementing remote access tools via RDP (T1572, Protocol Tunneling). We noted that the online banking and e-commerce sectors fell victim to this backdoor at the beginning of the second half of the year.

Since 2019, the cyberattacker began using a backdoor dubbed ServHelper to hijack victims' accounts and issue commands enabling keystroke logging (T1056.001, Input Capture: Keylogging) and theft of sensitive data.

Since August 2022, a vulnerability (CVE-2022-31199) in the Netwrix Auditor solution was exploited to enable the distribution of Truebot malware. As of October 2022, the Truebot malware was distributed via Raspberry Robin. Two botnets were involved in the infections, one targeting Mexico, Brazil, and Pakistan while a second one later in November targeted the USA. This second botnet took advantage of Windows machines with open Internet services such as SMB and RDP.

BY THE END OF 2022 :

These attacks could have been carried out for the purpose of using the Clop dual extortion ransomware. At the end of 2022 we witnessed an increase in the presence of the Truebot malware, also known as the Silence Downloader, responsible for major attacks on financial organisations.

This malware enabled the delivery of the Grace malware also known as FlawedGrace or GraceWire. The TA505 group broke new ground by switching from a traditional method of transmission via malicious emails to an older technique via USB sticks.

...FOCUS 2 : APT41

APT41(G0096) is a sophisticated cyber-espionage actor, probably backed by the Chinese government, operating since at least 2012. This threat group has been targeting organisations around the world in vertical sectors such as high-tech, telecommunications, and healthcare.

In the last six months, APT41 made headlines in the United States following some revelations by the US Secret Service[15]. The latter publicly reported the group's involvement in what they denounced as the first case of pandemic fraud supported by a foreign government. Through its scheme, the group allegedly managed to steal at least $20 million in Covid-19 benefits, including loans and unemployment insurance funds from more than a dozen different governments.

In addition, on 22 September, the Health Cybersecurity Coordinating Center (H3C), part of the US Department of Health and Human Services, issued a memo regarding the Chinese cybercriminal group APT41 calling for increased vigilance. Although this threat actor may not be present in our top 10, statements from the US government indicate that this group remains active, warranting continued attention.

The group stands out for its distinctive pattern of engaging in financial operations. This is rather unusual among known threat groups that are sponsored by the Chinese government. This last point also raises the suspicion among cybersecurity researchers that the group operates as a company with several teams, each of which pursues distinct objectives.

In the past, APT41 repeatedly perpetrated abuses of software supply chains. The group hacked into the development environments of several software vendors, injecting malicious code into signed tools thus enabling them to distribute malware on a large scale. An example is the 2017 attack on CCleaner, which resulted in compromised copies of the utility[11] being distributed to 2.2 million users.

In recent years the group also demonstrated a strong ability to take advantage of publicly disclosed vulnerabilities, enabling it to gain access to many networks. As an example, in early 2020, the group was tied to a global intrusion campaign exploiting devices and applications from major vendors such as Cisco, Citrix, and Zoho. This enabled it to gain access to dozens of entities, across all sectors, in over 20 countries. It should be noted that unlike their traditional campaigns, where initial access was gained through phishing or malware dissemination, in this instance the attacks were primarily targeted at vulnerable systems and devices directly exposed on the Internet.

Similarly, in December 2021, just hours after the Apache Foundation issued its security bulletin addressing the Log4j vulnerability[12], the group exploited the same vulnerability to compromise two state governments, as well as more traditional targets in the telecommunications sector.

These ongoing attacks prompted the US government to issue two indictments against five alleged members of the group between 2019 and 2020. To date, these individuals remain at large and their names have been added to the FBI's most wanted list[13].

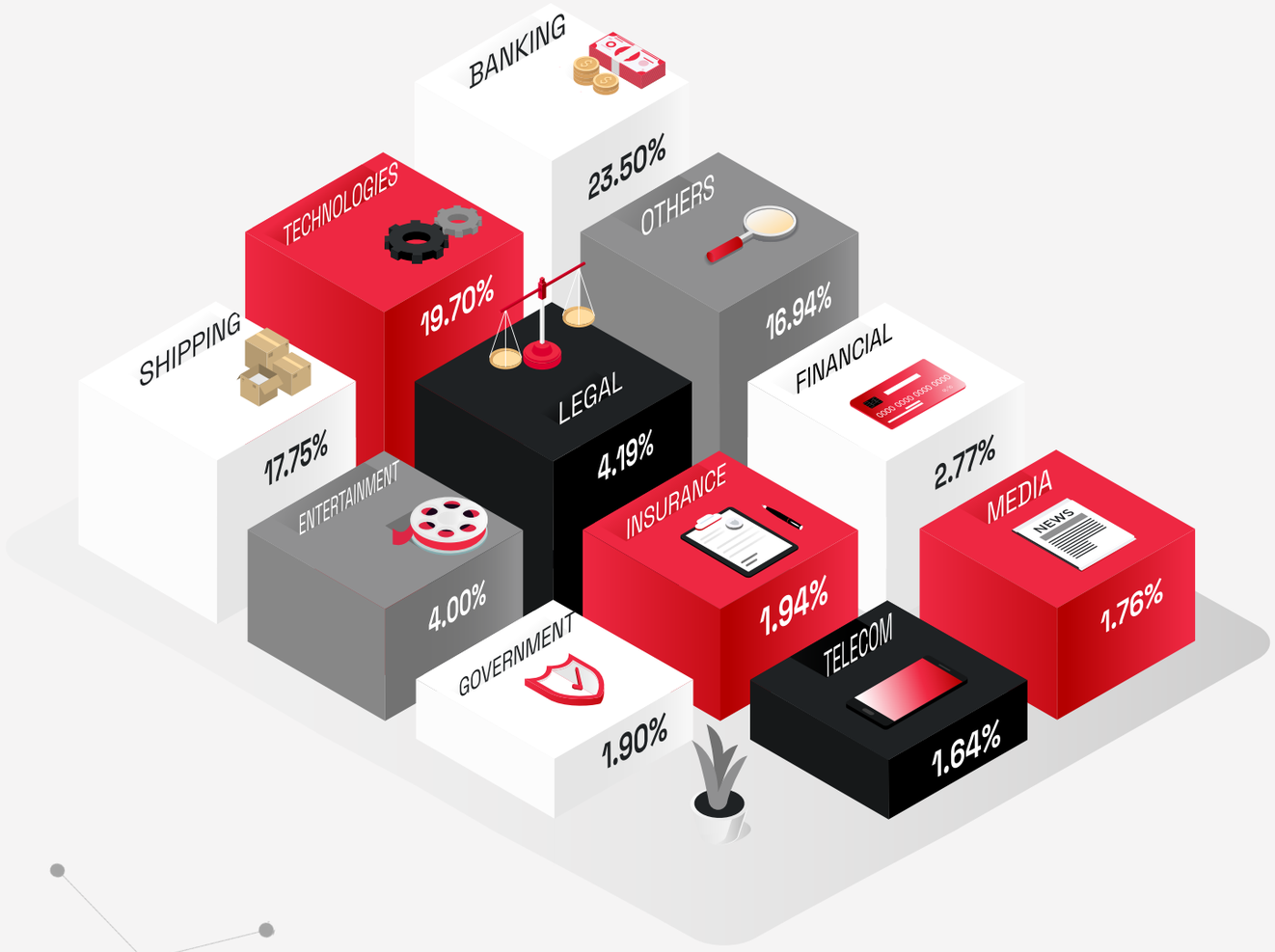
The group is notable for its advanced compromise tactics, including exploiting several zero-days[4] and implementing a number of obfuscation techniques to mask its activity[5]. Additionally, the group maintains an arsenal of tools to accomplish its missions, including mainstream utilities, malware shared with other Chinese spy operations, as well as its own specific tools.

APT41 exploits a variety of common techniques to gain initial access to its victims. These include the use of spear-phishing T1566[1], lateral movement from a trusted third party (1133)[1], exploitation of stolen credentials (T1078)[1] and others.

However, once inside a victim organisation, this threat actor can exploit more sophisticated TTPs and deploy additional malicious tools. For example, over the course of a nearly year-long campaign, APT41 compromised hundreds of systems, using nearly 150 unique pieces of malware, including backdoors (T1053.005, T1547.001, T1542.003)[1], identity information stealers nT1112[1], and keyloggers T1056[14].

This malicious group demonstrated in recent years that it knows how to adapt its initial access techniques to suit its target, and that it has sufficient means to quickly exploit a newly publicised vulnerability on a large scale. Furthermore, the indictments against a number of group members do not appear to have deterred them from their activities, which makes it all the more important to be vigilant with regard to the group's potential future activities.

06 WEALTHY INDUSTRIES MORE AT RISK ?
YES BUT NOT LIMITED TO...



Similar to the top sectors in the previous report (1st semester), the banking sector is again at the top of the list. It attracts a lot of attention because of the potential for fraudulent gains and the value of private information that can be converted into cash after extortion.

Other sectors that are currently experiencing attacks also make up the middle of the top, including the legal sector, the financial sector, and the entertainment sector, which includes gambling.

Insurance and telecommunications round out the bottom of the list, along with strategic sectors such as media and government, which we'll discuss later. To conclude, the cryptocurrency sector, which ranked last, has disappeared, possibly due to the sharp downward correction of this market.

CRYPTOCURRENCIES: A CASCADING COLLAPSE

With the value of crypto-currencies plummeting, NFTs no longer captivating, and a metaverse struggling to gain traction, the year 2022 was a turning point, for the worse, in the crypto-currency universe.

In particular, the successive crashes of the UST and LUNA currencies, of the hedge fund Three Arrows Capital, and above all the bankruptcy of the crypto-currency exchange FTX resulted in an extreme panic among small investors with a massive withdrawal of crypto-currencies from the exchange platforms.

Phishing attacks, the most widely used threat affecting the sector, were consequently side-lined by attackers. However, another threat gained in popularity: the malicious use of cryptominers (also called coinminers). Already in existence, these software programs employed in the mining of cryptocurrencies were extensively hijacked by attackers with a rising trend in the number of variants observed throughout the year 2022.

The idea is to infect the targeted machines with a cryptominer to harness its resources for the benefit of the attackers. A study conducted by Sysdig highlighted that every dollar mined amounts to a cost of $53 for the companies exploited [1] including the cost of energy and cloud resources that a botnet can generate.

The growing popularity of cryptominer infections can be explained by various factors :

- → No need to pay for electricity
- → No need for the infrastructure
- → Limited technical knowledge required
- → The ease of integrating them into a wider attack

Although deploying cryptominers is mainly done through phishing, downloading pirated content, malware disguised as legitimate resources, or by exploiting vulnerabilities, some attackers are showing even more resourcefulness.

We witnessed the misconfiguration of Docker container APIs, publicly exposed and exploited on a large scale, as well as the emergence of fake Docker images of Linux distributions, infected upstream. This latest method enabled the attackers to deploy a non-negligible volume of cryptominers, with no less than 20 million downloads of at least 30 images observed.

Info stealers make up the other threat affecting this sector. This category of Trojan is designed to gather information from a machine and forward it to the attacker. Most of this malware steals login credentials from the system or from browsers. They recently evolved to retrieve information from locally present digital wallets. As with cryptominers, this is a very inexpensive method, requiring only the right targeting to achieve significant gains.

FORGOTTEN ATTACKS, THOSE TARGETING GOVERNMENTS

The «during» and «post» crisis of Covid witnessed countless cases of ransomware infections, particularly against already overburdened health services. This follows the example of the attack on the Corbeil-Essonnes hospital, which we mentioned in a previous half-yearly report. The quest for financial gain, the primary motivation of threat actors, brought phishing and ransomware to the fore.

At the same time, we hear less regularly about state-sponsored attacks on government services and administrations. These are aimed at exposing activities, disrupting services, or stealing sensitive information on behalf of other governmental powers.

In general, three types of attackers can be distinguished :

- State-sponsored attacks, backed by a government, which enable them to carry out large-scale attacks, irrespective of the targets.
- Criminal organisations, whose main objective is the financial gain the attacks can generate.
- Hacktivists, whose goal is social and political change.

The latter category has become highly vocal, particularly through the group «Anonymous», whose activities have been in the media spotlight on numerous occasions in recent years. In September 2022, for example, this group of activists took part in developments in Iran by taking down several Iranian government websites and obtaining personal information from a parliamentary database.

Various Anonymous-affiliated groups also claim to have published data from ministerial and government departments, claiming responsibility for hacking the Iranian President. These various attacks provide moral support to the Iranian people, who have been plunged into an almost total Internet blackout for several months.

The Iranian government is not only being targeted for human rights abuses; it is also being subjected to cyber espionage by tThe Iranian The Iranian government is not only being targeted for human rights abuses; it is also being subjected to cyber espionage by the Chinese group APT15[2]. Active since 2010 and already renowned for its espionage campaigns against governments in North and South America, Africa and the Middle East, this time around the group targeted Iranian institutions from July to December 2022. During this period, several government infrastructures, including the Ministry of Foreign Affairs, established communications with a C2 server known to the APT15 group. This scheme would point to information theft rather than damage to infrastructure.

The campaign was reportedly launched because the group disagreed with a cooperation programme signed between China and Iran.

China was also thrust into the spotlight last July when a Shanghai police database was made available for sale. The database contained the private personal information of nearly one billion Chinese citizens as well as several billion police reports dating from 1995 to 2019.

The database contains the names, addresses, telephone numbers, and ID numbers of many Chinese citizens, not just residents of Shanghai. Even more unbelievable, the data was publicly accessible for over 14 months via a web interface linked to the database. The cause is believed to be a misconfiguration of the service, leaving it exposed on the internet. Anyone with the URL could access it freely, without having to login.

CONCLUSION

The Purple Team Gatewatcher's analysis of the intelligence provided by our CTI infrastructure between July and December 2022 indicates that cyber threats remained stable overall during this period. Indeed, the motivations behind threat actors remain mainly money, espionage, and hacktivism.

In addition, long-term effective techniques such as phishing, malware development, or information gathering prior to lateral moves continue to be widely used techniques in intrusions.

The report elaborates on how threat actors are able to respond quickly and effectively to changes in the market in the same way that a successful, agile start-up company would. As an illustration, we noted the sharp reduction in phishing targeting clients of cryptocurrency exchange platforms following the fall of FTX and the drop in the price of cryptocurrencies.

Furthermore, malware such as Qbot demonstrates that adaptability is the only way to survive in this constantly evolving technical ecosystem, where even the unrivalled maldocs, as a gateway to compromise, was undermined by a decision from Microsoft.

This increasing complexity of macro execution is forcing cyber attackers to find new solutions such as :

→ The use of disk images (ISO, UDF, ...)

→ The use of Windows shortcuts (LNK)

→ Bypassing security systems such as the Mark-of-the-Web.

In addition, intelligence analysis revealed surprising situations such as the survival of the Wannacry worm which, even after many years of existence, still enables new machines to be infected thanks to its automated search for new victims. On the other hand, the use of virtually unknown file types, such as Hangul in our analysis, illustrated the persistence of some threat actors in analysing the attack surface in advance in order to set up tailor-made attacks to reach their victims.

In conclusion, Stephen Hawking's words «Intelligence is the ability to adapt to change» remind us that cybercriminals continually adapt to their prey's attempts at defence and evolve masterfully in an increasingly complex digital hunting ground. Publishers and cybersecurity teams will constantly face new challenges from «Intelligence» using information, automation, machine learning, and increasingly powerful threat analysis systems.

08 GLOSSARY AND TECHNICAL DETAILS

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

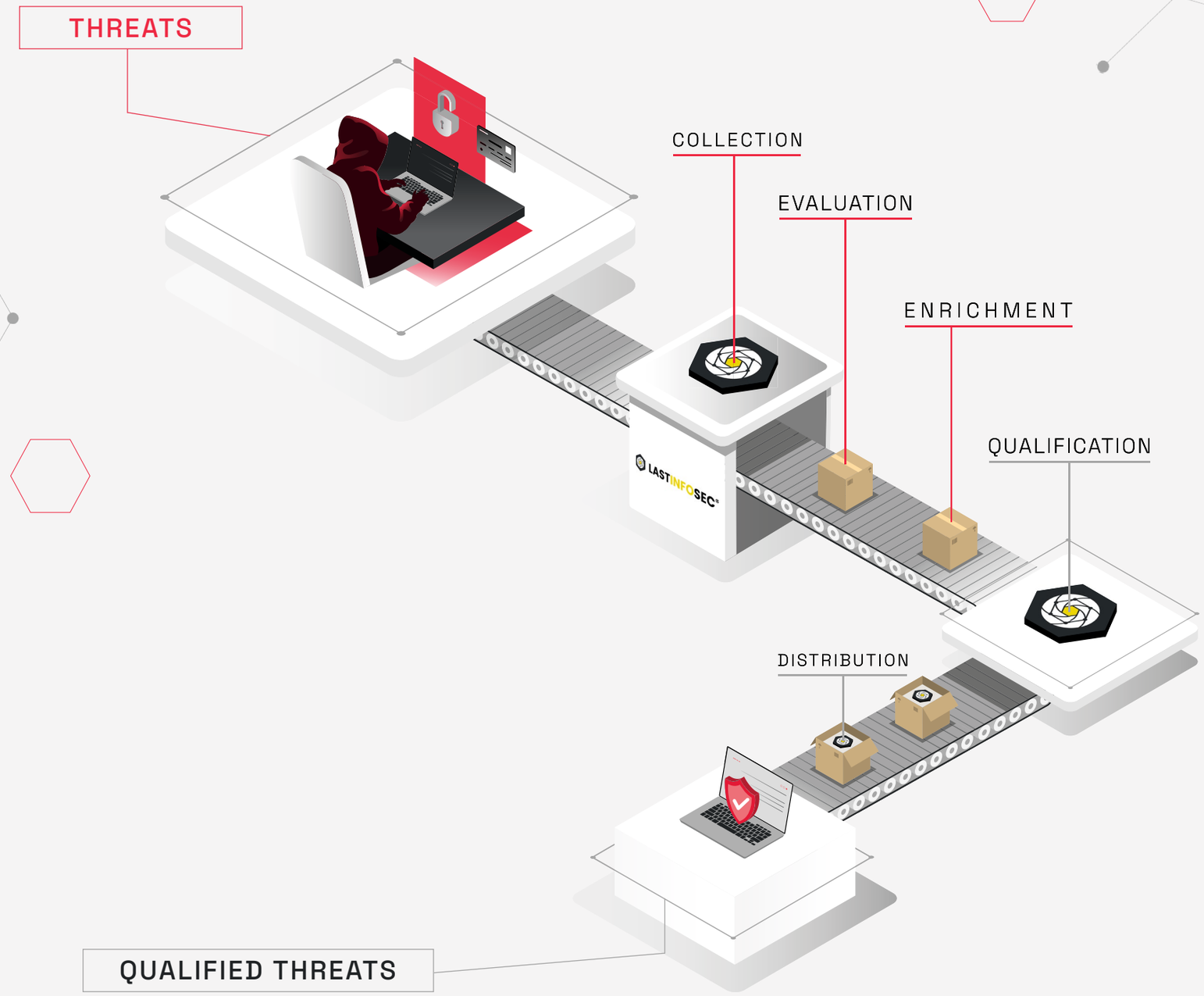
LastInfoSec® is our Cyber Threat Intelligence (CTI) platform designed to facilitate the detection of internal and external threats that may target the information system and to track new techniques, vulnerabilities, tools, used by attackers.

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 6,000 qualified markers per day, in near real time, and provide several types of high-value threat intelligencee.

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

LastInfoSec® integration is quick and easy with standardized quickly thanks to standardized exports to the latest standards (Stix v2, Stix v2.1, TAXII..) and integrated connectors available for the main analysis tools analysis tools on the market (TIP, SIEM, SOAR...).



6000

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

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 real-time view of cyber threats on the entire network, on premise as in the cloud.

All the threats mentioned in this report can be detected by an Network Detection and Response (NDR) solution such as Gatewatcher AIONIQ.

AIONIQ®

Natively linked to LastInfoSec's CTI feeds, AIONIQ can reliably identify malicious actions and suspicious behavior not covered by other detection tools by dynamically mapping all assets on the information system. Its innovative network flow analysis performance, even encrypted, allows a 360° modeling of the cyber risk level associated with each connection between assets and users, for an increased level of detection and visibility.

SOURCES

[1] Attack Mitre

[2] Édito du CyberThreats Barometer Mars 2022

[3] Édito du CyberThreats Barometer Décembre 2022

[4] Édito du CyberThreats Barometer Juin 2022

[5] Article Malware As a Service Emotet

[6] Édito du CyberThreats Barometer Janvier 2023

[7] Article IT threat evolution in Q3 2022

[8] Article Is WannaCry Still a Threat ?

[9] Article Emotet Returns With New Methods of Evasion

[10] Internet Crime Report 2021

[11] Article Recent findings from CCleaner APT investigation

[12] Bulletin d'alerte du CERT-FR

[13] APT 41 GROUP

[14] APT41 a dual espionage and cyber crime operation

[15] Article Hackers linked to Chinese government