



CYBERSECURITY ANNUAL REPORT
2021

Index of contents

Introduction	3
Company profile	4
Data	7
Section 1: Malware	8
Zero Day Malware	9
Impacted Industries	11
Propagation & Lateral Movement	14
Malware Operations in Italy	15
Section 2: Blocked Threats	18
Botnets and Opportunistic Activities	20
Section 3: The Email Threat	21
Section 4: Attack Techniques Trends	24
New Threats form the Supply-Chain	24
Sunburst Backdoor	24
Deep Web and Security Breaches	27

Introduction

Yoroi defends companies and organizations in the digital space from the very beginning of its life by improving its technology day by day and its analysis capabilities. Tracking threats, threat-actors and the way they change over time gets a central role in the continuous learning lifecycle; it would help technology and cybersecurity analysts to have a better feeling on threat management. We believe in information sharing as one of the main defensive weapons belonging to humanity. Every year we invest time in extracting, collecting and describing what we have learned in the past twelve months. This year we decided to improve our Yoroi Cybersecurity Report by balancing qualitative analyses and quantitative analyses in a single short document accessible to everybody who needs it. From this purpose we are pleased to introduce Yoroi Cybersecurity Report 2021.

A new decade approached our history and something new is hiding in new cyberattack while consolidated threats actions persist in targeting organizations all over the world. The current report is built to highlight what is new compared to what is consolidated over the past months, we decided to focus 2021 report on the following sections

Section 1: Malware. The authors describe the continuously increasing malware chain sophistication with a special focus on targeted malware. Yoroi's characterized section on Zero-days malware is improved by adopting a broad view on what is covered and what is not covered by common antivirus systems. A dedicated chapter on impacted industries is provided to map Malware to hit industries. That section would help CISO in being ready on the most common attacks related to his business vertical.

Propagation and lateral movement chapter describes how these artifacts move from one company to another. This section ends by describing threats in Italy as one of our most active countries.

Section 2: Blocked Threats. This section performs a deep dive into blocked cyber threats providing details on involved top level domains and describing the botnet/opportunistic attacks influenced in daily cyber activity. Since E-Mails is one of the most favourite attack vectors as reported in Yoroi Cybersecurity report 2019 and in Yoroi Cybersecurity report 2018, this year we decided to provide a dedicated section and comparing trends over the past few years.

Section 3: The E-Mail Threat. This section is fully dedicated to E-Mail vectors. Analysis of malware carriers and common subjects are described to highlight common patterns exploited by a clustered discussion. Studying E-Mail vector would enable defenders to improve their capabilities to improve the feeling of malicious E-Mail themes.

Section 4: Attack Techniques. Trends. This section is introduced to visualize new attack trends according to the MITRE ATT&CK matrix. Understanding the attack trends is an initial step to provide blocking solutions and detection mechanisms. Two dedicated chapters are focused New Threats from the Supply-Chain and Sunburst Backdoor.

We hope to provide a nice reading to everybody interested in studying cyber threat trends by giving an overview to what has happened in the past months.

Company profile

YOROI is a company that develops and manages Integrated Adaptive and Dynamic Cyber Defense Systems and aims to play a leading role in the Italian cyber defense sector.

YOROI combines on one side the most significant experience in the Italian market thanks to the recent incorporation of Cybaze S.p.A. (formerly Emaze S.p.A.) and @Mediaservice.net s.r.l two pioneering companies of the cyber security market in Italy with more than 20 years of existence, and on the other hand the vocation to the most advanced technological innovation of Yoroi s.r.l., a reality that since 2015 has rapidly imposed itself to the national attention and has developed proprietary technologies that have obtained significant recognition also on the international market.

The last step related to the growth and affirmation of YOROI as a reference point of Cyber Security in Italy was, in January 2021, the acquisition of the majority of YOROI share capital by TINEXTA S.p.A.

On this occasion Yoroi was chosen to integrate all the existing components of the Cybaze group: YOROI is now a company formed by more than 140 people and important infrastructures among which we recall:

- 4 Defense Centers (Trieste, Milan, Cesena and Benevento);
- One of the main CERT organizations in Europe, Trusted Introducer certified: YOROI is the first Italian company to have had the recognition of the third level "certified". This structure is composed of more than 10 specialized analysts operating from the CERT offices of Cesena and Benevento (YOROI CERT & Z-Lab).

In YOROI there are:

- More than 40 qualified cyber analysts,
- More than 50 developers,
- One of the most important ethical hacking team formed by more than 20 specialists among the most qualified and recognized both at national and international level.

All this, together with the acquisitions of the projects, solutions and R&D division of Corvallis and Swascan, will allow TINEXTA to create a national hub specialized in digital identity and digital security services. For more details see the press release: <https://www.tinexta.com/file/1760>.

YOROI's motto is **"Defense Belongs to Humans."**

This phrase summarizes what in YOROI experience and skills have led to recognize as a fundamental approach to significantly reduce the risk of damage caused by cyber attacks and be ready to react immediately in case they occur. It is necessary to move away from a logic of protection, with the consequent multiplication of tools and services, towards a logic of dynamic defense, which integrates those products and services in an integrated and reactive system, where the human component is inseparable from the technological component.

A cyber security system is composed of services and products that belong to the following main families:

- Cyber Defense Services: Cyber Security Defense Center (CSDC),
- Enterprise Security Analysis Services,
- Certification Services,
- Training Services,
- Proprietary Software.

General Attitude towards Customers and the Market and Posture of the Defense Service

YOROI would like to highlight among the differentiating arguments with respect to the majority of the market, the following factors:

- YOROI's attitude is not critical of the choices made by the Client company in terms of the deployment of the defensive arsenal against cyber threats; the main purpose is to give that arsenal, integrating it where necessary, system dignity to help achieve an effective level of defense, the highest possible resilience to attacks and the mitigation of any threats encountered in the shortest possible time, also by virtue of compliance with applicable regulations.
- It is YOROI's responsibility to point out, as a content of the final reports of the services rendered, any inadequacy and lack of effectiveness of the defenses put in place to protect the company.
- YOROI has internally developed proprietary technologies which use advanced Artificial Intelligence and Machine Learning tools and does not base its activity on the sale of "conventional" security solutions such as, for example, firewalls, antivirus, antispam, proxy, SIEM etc.

From the point of view of strategic consultancy, YOROI will verify the adequacy and effectiveness of the tools present at the Client's premises and will supply a complete report of what has been found accompanied by ideas and reflections always aimed at mitigation.

The defense service proposed by YOROI is able to interface its systems (at various levels) with the main solutions available on the market, both open source and proprietary of the main brands. The different level of integration depends on the dialogue capabilities offered by third party tools (via API, presence and availability of security LOG (SysLOG), etc.).

Services are provided through private cloud and are based on the following components and functionalities:

- search and collection of alarm reports from the proprietary probe that will be placed at the different Internet access points of the Customer's infrastructure. The probe is normally installed in a virtualized environment but is also available in an appliance version.
- Pre-processing of the information collected by the probe from all the components present at the Customer in terms of Firewall, Anti-Spam and Proxy Solutions and other security tools.
- Correlation of the security events detected and collected through integration of solutions already in the field.
- Further analysis, also by passing potentially dangerous components into the YOROI Multi-SandBox solution.
- Presentation of collected information and network status through a complete information dashboard.

Analysis and innovation capabilities aimed at the Security of Customers and their assets

Thanks to the integration with Mediaservice.net, a Turin-based company with a great and renowned experience in the provision of analysis and audit services of infrastructures and corporate application perimeter, YOROI has created a Security Audit service that combines in a single activity the disciplines of Penetration Test and Risk Assessment.

The discriminating characteristic of this service is the strong interaction between the two types of verification, which mainly allow to:

- optimize penetration testing activities, rationalizing the efforts on verification activities and weighing vulnerabilities in the best way;
- improve the accuracy of risk detection and subsequent mitigation, including a level of technical detail.

The Risk Assessment activities foresee the application of consolidated international methodologies, in compliance with ISO/IEC 27001:2005 and ISO/IEC 27005:2008 standards, with the possibility of qualitative or quantitative (in euros) valuation of the risks.

The OSSTMM methodology, a ten-year reference point in the field and widely requested at national and international level, is the methodology used for Penetration Test activities. Its application is performed on each of the five channels provided (TLC, data networks, wireless, physical access and personal) according to the security needs detected.

Great R&D capabilities put at the service of major Service Providers

The merging of Cybaze into YOROI has brought as a dowry one of the most important Research and Development groups in Italy, author of software solutions designed according to Customers' needs to solve specific problems strictly related to security.

In particular, it is possible to mention the DCS (Device Check and Support) project through which our Customers can, through a single interface, check and modify the configuration files of the routers of their network, of tens of thousands of devices of different models and manufacturers. Over the years, the Research and Development team has been the author of many other solutions that have become a must for large providers and, among these, we can remember the "Secure Network" service offered by Vodafone. In addition, other solutions such as DeCo, Rectify, Discover and ConCreTo have been released over time.

The portfolio of solutions developed by the YOROI Research and Development center is completed by customizations based on specific customer requirements in terms of provisioning, assurance, KPI collection, monitoring and predictive analysis.

Valuable skills in Training

Thanks to the solid skills gained over time, the experience in the field and the continuous activity of defense on one side and analysis on the other, YOROI is one of the few companies in the market able to offer a high level training program. The training offer is mainly composed of the following modules: Information Security, Corporate Fallout of GDPR, Risk Management (Security Compliance), Centrality of D. Lgs.231/01, Information Security Awareness and OSSTMM Professional Security Tester (OPST).

Certifications



Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University



TF-CSIRT
Trusted Introducer

[LINK](#)

Data

One of the most important characteristics in Yoroi Cybersecurity Annual Report is about data. The used raw data does not belong to open source intelligence (OSINT) or to external network detections but rather to real incidents that needed to be managed by human analysts. Indeed OSINT could have a lot of false positives or can't be representative for a geographic area while external network detections could be easily blocked by perimetral protections such as: NG-x, Proxyes, Antivirus, Anti-Spam etc. the used data belongs to real happened incidents.

While reporting statistics on general trends by using networking data and OSINT is interesting in having a general overview of cyberattacks, having stats on real incidents would help the final decision maker to better evaluate his business impact. The used data have been extracted from managed incidents in order to better fit the reality of real cybersecurity attacks and how they hit the analyzed business verticals.

Section 1:

Malware

The Double Extortion Practice

The violence of the Double Extortion attacks, which literally catapult the company into a Cyber Crisis, just in few hours

Many of the high-profile malware attacks emerged in 2020 were what security community calls Double Extortion attacks. In the same way the digitalization acceleration in was fundamental to most of the companies to ensure the business operation survival through the harsh of pandemic's lockdowns, it enabled the wide diffusion of such kind of advanced malware-based attacks. In fact, due to the weakening of the network perimeter and the massive and sudden number of changes in the IT infrastructure, may IT Departments struggled to keep up with the security controls.

We often hear about these attacks as Ransomware attacks. However, talking about ransomware is extremely reductive. The modus operandi of these attacks is different. The term ransomware, in fact, is circulating even earlier the birth of the double-extortion phenomenon: originally, ransomware attacks mostly hit private individuals, encrypting the data inside their pc. Instead, the dynamics of the Double Extortion attacks involves whole enterprises and even the national productive fabric.

In fact, the Double Extortion attacks trend has heavily grown during 2020 and its characteristic tailored fashion need to be accurately considered. These malware attacks are operated by organized teams, security specialists that operate like the **Red Teams** companies use to test their defenses: high-level cyber intrusion specialists, but with no ethics at all. In 2019 we observed the raising of this cyber-criminal trend, referencing these groups as **Dark Teams**. But at that time, they were focused to a single objective: install ransomware malware company wide. Instead, during 2020 many of these operators switched to the Double Extortion practice starting to steal valuable data from the victim's network and demanding money to "guarantee" the deletion of their criminal loot.

Also, the dynamics of Double Extortion attacks are reminiscent of the modus-operandi of advanced threat actors, the so-called Advanced Persistent Threat (APT). This fact is far more than a trivial detail. Such advanced cyber intrusion are many times **initiated through malware infected hosts** to step in the company network. Then, the criminal cyber-specialists leverage their toolset and implants to move around across the corporate network, to steal sensitive data and eventually to completely take over the IT infrastructure, cutting off the system administrators and massively deploying ransomware on any company asset.

Dealing with such threats was, until a few years ago, only a concern of organizations operating in strategic sectors or in heavily targeted verticals such as Banking, Finance, Defense or Critical Infrastructures. **After the acceleration of the covid19 pandemics in 2020, the same malicious operational methodologies are now threatening sectors much less cyber mature and even lesser cyber resilient**, slamming the cyber security issue right in front of many company boards.

This breaking point is impossible to ignore. The belief that many companies operating in less cyber matures sectors have - i.e. old strategies are still enough - shatters against the violence of the Double Extortion attacks, which literally catapult the company into a Cyber Crisis, just in few hours. A chaotic situation that brings in front of Senior Management a series of high severity issues having immediate impact on business operations, civil and criminal liability, brand reputation and long-term competitiveness.

So, how is possible to adapt the company cyber security strategy to tackle these threats?

There are many ways to do so. In complex business environments adopting the best-practices could result only in costly aesthetic exercises, it is much better to focus on good practices and principles. One principle a CISO could use as compass is **balance**. For instance, balancing the resources and the investment between prevention and detection and response. Answering to question such as: "How much the company invested in preventive security controls?" - or - "Is the company investing in detection and response?" or also "when is the last time the company deeply reviewed its security strategy?" may help to a lot in the decision-making process.

With this in mind, cyber-security strategies can be evolved empowering companywide **Cyber Crisis** readiness and emergency contingency plans. Investing in Security Operations, detection and response technologies like the Yoroi's **Cyber Security Defense Center** and **Kanwa Agents**, leveraging mature **Cyber Threat Intelligence** operations and services brings new risk-reduction opportunities to the business.

Zero-Day Malware

75.6% of malicious files used to attack the organization are zero-day malware and barely known malware, and have non-eligible chance to bypass the traditional security perimeter

The volume of the malicious code produced and disseminated in the wild is constantly increasing. Technical advantages and software engineering techniques not only empower companies to transform and digitalize their businesses, but also help cyber criminals in the systematic development of attack infrastructures.

With over a billion of samples produced in 2020 [<https://www.av-test.org/en/statistics/malware/>], malware can be seen - with no doubt - as an Industry characterized by production processes, engineering, supply chains and delivery. Year after year, this aspect is constantly growing and no matter how many actors and malware operators get arrested by law enforcement agencies, they are easily replaced with new emergent gangs. This is a side effect of the ongoing digitalization process that is involving our economy and its growth could potentially last for many other decades.

In this environment, such huge malware production represents a threat for companies and enterprises operating in the digitalized economy. Especially because many of the malwares out there are new.

New malware, or Zero-day malware, is incredibly dangerous for companies relying on traditional security systems, because it breaks one of the foundational assumptions behind the legacy anti-virus approach, which is based on stopping known pieces of malicious code. Therefore, we track Zero-Day malware in our telemetry.

In fact, Yoroi's technology captures and collects samples spread during cyber-attacks and automatically analyze them just when they approach the company network perimeter. During this process, as part of the automatic analysis pipeline, **Yomi Sandbox** checks and reports if the malicious files are potentially detected by Anti-Virus technologies in the specific time the malware is spread to the target organization. This give us a precious insight on how Zero-Day malware evolves in time and how critical is for companies, because well-known threats are much easier to be intercepted, unknown ones definely not.

We call Zero-Day malware every sample that turns out to be an unknown variant of arbitrary malware families. The following image (Fig:X) shows **the 58 % of the analyzed malware files in 2020 were unknown from common anti-virus solutions in the moment they crossed the company perimeter**.

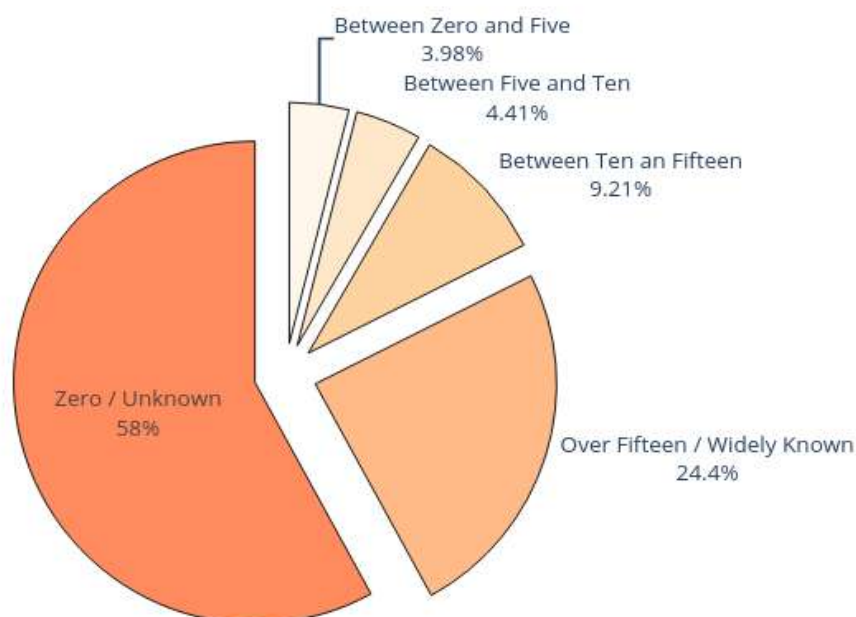


Figure 1. Zero Day malware delivered to organizations.

The reported data are collected during the first malicious files propagation attempts across organizations. This means companies are heavily exposed to a relevant Zero-Day malware risk. Detecting such kind of malware quickly plays a vital role in well-established cyber security strategies because it will sensibly lower the risk of major security issues, data breach or cyber crisis situations.

Along with the Zero-Day malware observation, a good part of the known malware samples are not so well detected by anti-virus solutions: the 41.8 % of the samples known were only barely recognized. In fact, over a third of the known malware were detectable by less than 15 antivirus engines at time of attack.

If we sum up these two categories, the zero-day malware and the barely known ones, we end up that **75.6 % of the malicious files used to attack the organization have a non-negligible chance to bypass the traditional security perimeter.**

A reasonable interpretation of these data conforms the sophistication of the malware industry. In fact, dissecting the Zero-Day malware category, many of the intercepted malware belongs to two distinct classes: the 66% of the unknown samples shows typical trojan behaviors, granting the attackers further, persistent access to the compromised workstation, and the 28% download and execute other malicious artifacts, behaving as a part of a more complex, multi-stage infection chain.

Summing up the findings, business organizations nowadays are facing extremely dangerous risk scenarios due to the current malware threat landscape, which is characterized by three main facts:

1. The extremely high volumes of malware samples produced and disseminated by the cyber-criminal operators.
2. Over two third of the incoming malicious files are unknown, or at least barely known, at time of attack.
3. Most of the malicious files are designed to drop and install further implants or provide direct access to the compromised machines.

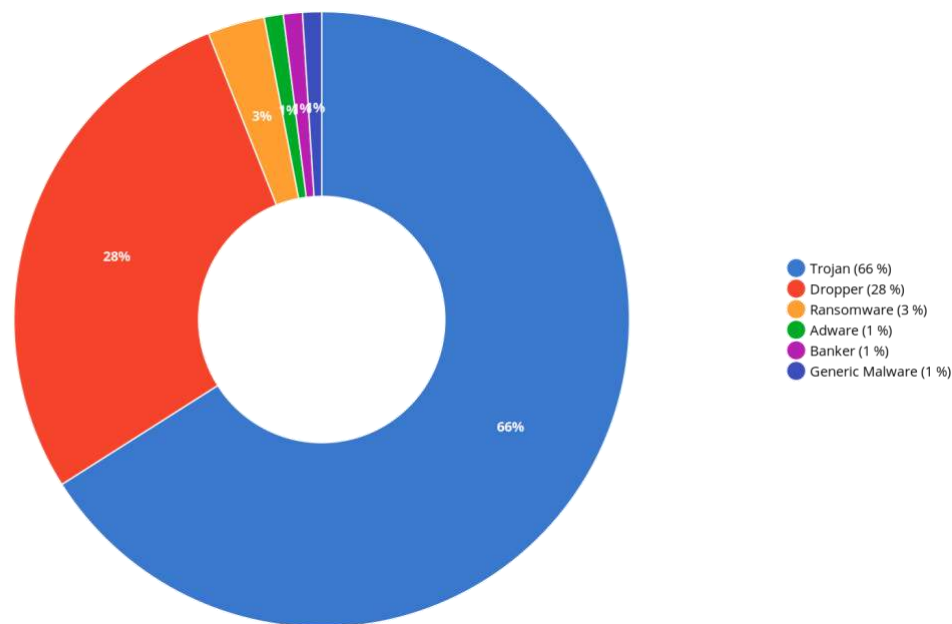


Figure 2. Zero-Day malware intercepted by CSDC technologies with no AV matches at time of detection.

Impacted Industries

The distribution of cyber attacks across sectors is not uniform

Understanding how malwares hits industries is a valuable source of knowledge which helps in the assessment of the real security exposure for each Industry and in the identification of most valuable business for attackers. In fact, there are business most vulnerable to cyber-attacks or to specific attack vector.

Moreover, such analysis, can act as a driver for the implementation of a tailored Defense strategy which takes into account attack vectors and time distributions of targeted attacks. For industries most vulnerable to cyber-attacks, the right security controls must be in place along with a good Vulnerability Management program and employee training in order to narrow down the security gap.

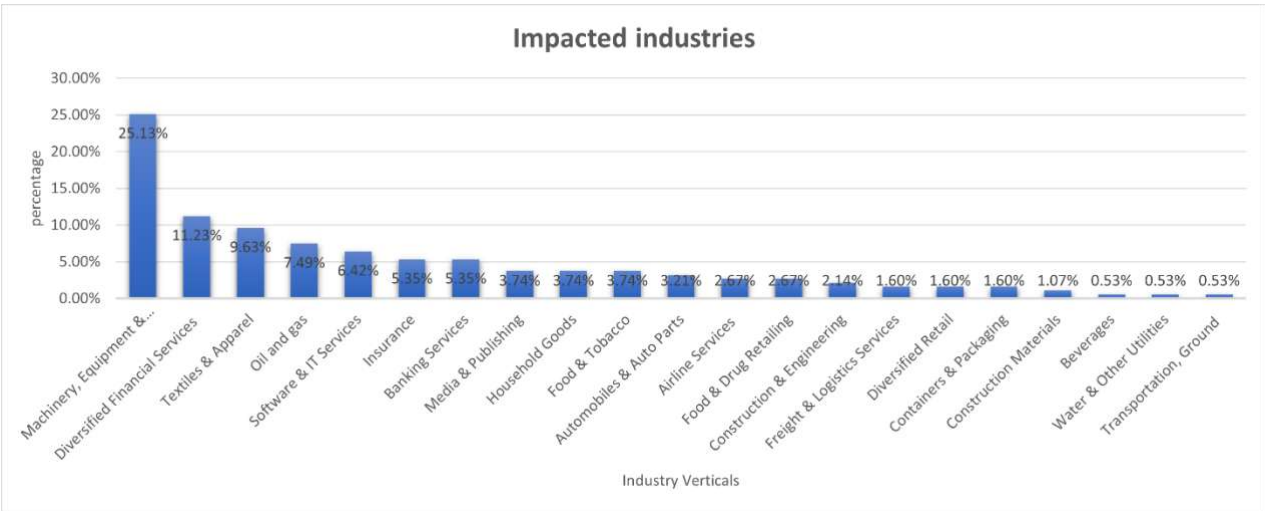


Figure 3. Impacted Industries

As shown by the distribution of cyber-attacks over the industries, the most impacted sectors for 2020 are *Machinery, Equipment & Components* with a share of 25.13%, followed by *Diversified Financial Services* with 11.23%, *Textiles & Apparel* with 9.63%, *Oil and Gas* with 7.49% followed by all the others. The last ones are *Beverages, Water & Other Utilities* and *Transportation* with 0.53%.

Comparing the distribution to the last year (2019) it is possible to notice that the most targeted sectors remain the same (*Machinery, Equipment & Components* and *Diversified Financial Services*). As shown in figure (Fig. X) email remains the primary attack vector used by cybercriminals. This underlines the opportunistic character of threats. From 2019 to 2020 email-based attacks increased from 89% to 92% and the trend is only getting worse.

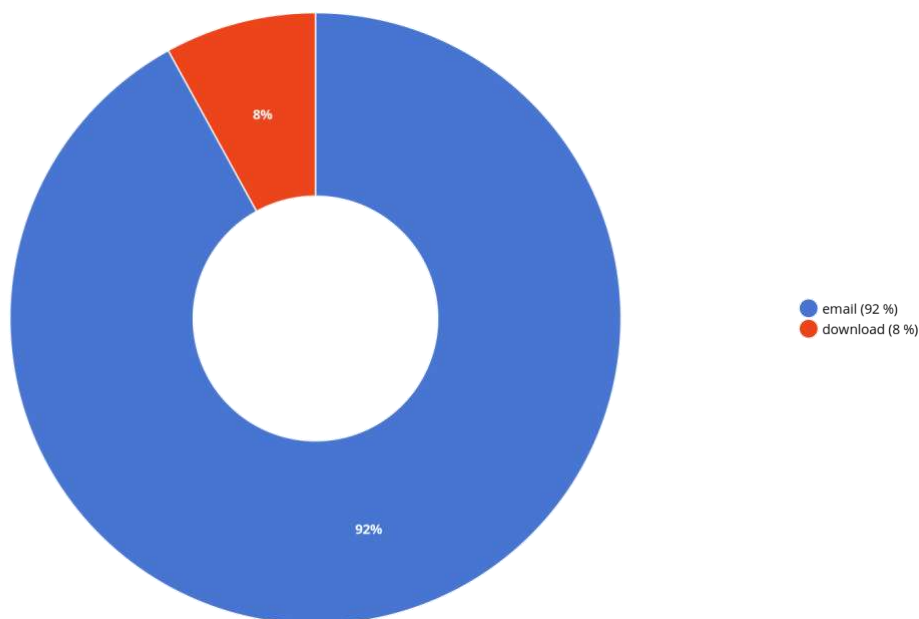


Figure 4. Attack Vectors

Phishing and Spear phishing are such a commonly used vehicle for subsequent attacks and affects all industries (as shown in Fig. X). Just a small portion (8%) of the attack's vectors is related to "downloaded files" i.e., file downloaded from any untrusted sources. Even if small as a percentage, it's worrying to see how, in many companies, employees still download malicious files from untrusted sources. This happened for several reasons, and it is a consequence of lack or inadequacy of security controls (perimeter firewalls and security gateways) which are not able to properly restrict the downloading of malicious files. Furthermore, this goes in conjunction with an ineffective or absent awareness program for employees which aim at the mitigation of risks deriving from an improper use of company assets.

In the following figure (Fig. X) it is possible to notice the distribution of attack vectors among industry verticals, such distribution is not uniform among industries. This trend does not indicate that one sector is more virtuous than the others, but in comparison to analyzed attacks, companies from one sector to other have strict policies periodically assessed than other with looser controls.

It is interesting to note that "*Banking Services*", "*Retail*" "*Logistic Services*" and "*Software and IT*" presents a high percentage of malicious downloaded files despite such services also have specific budgets to allocate for Security. This happened because such environments are more heterogeneous than others, and employees are more prone to download utilities for their daily work.

There are businesses which does not presents "*downloaded files*" at all, most probably because employees do not need to download additional software but just use their PCs with few programs needed for their mansion.

I.e. "Metals and Mining" or "Food and Drug retailing" or "Textiles and Apparel" are sectors in which employees must use equipment's or PC just in the production lines otherwise in this environment an attack could have a catastrophic impact.
In conclusion, email represent the main vector to deliver malware in today's business and the trend, respect the past years, keep growing.

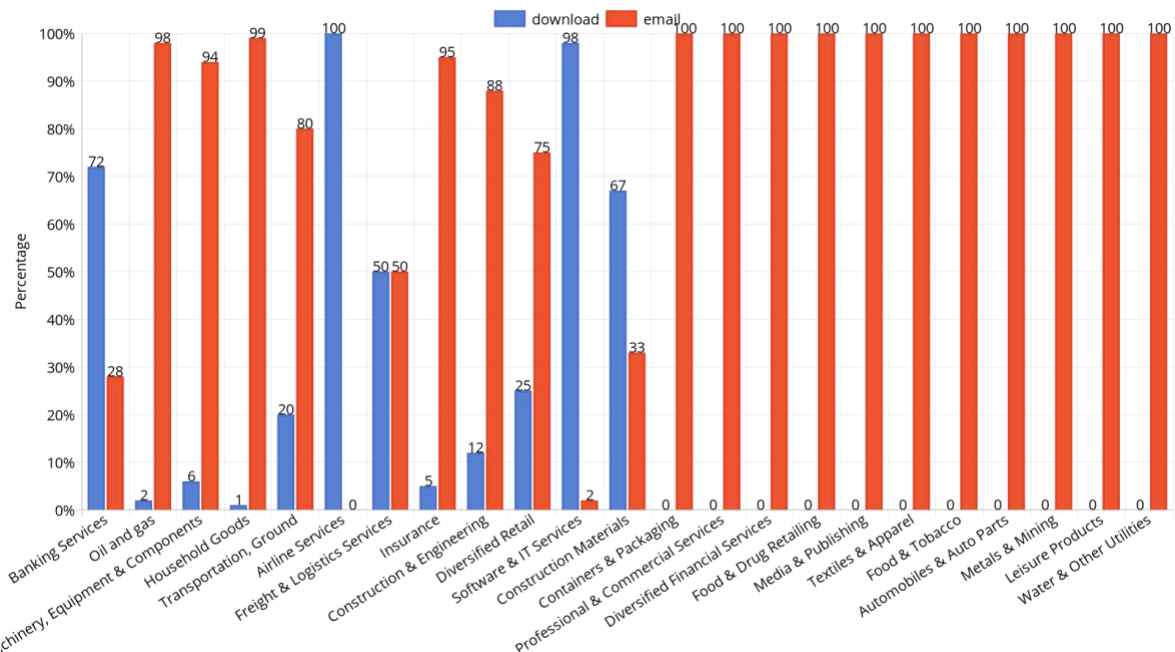


Figure 5. Impacted Industries by attack vector.

The time distribution of malware attacks shows us the attacker's opportunities expressed as relations in time and quantity:



Figure 6. Distribution of attack over the impacted industries

Attacks timing strongly depends on the business type. From the above diagram we spot that *"Household Goods"*, *"Oil and Gas"*, *"Banking Services"* and *"Containers and Packaging"* have been subject to cyber-attacks for long periods. Each business sector was impacted during the year.

Propagation & Lateral Movement

The ability of a cyber attack to spread laterally underlines the importance of a proactive strategy that allows to reduce incident resolution time before the propagation takes place

Often, cyber-attacks are duplicated among targets. Today's attacks are opportunistic and large-scale, this means they hit multiple business in a short time span. Know the propagation model is important in order to understand how fast attacks move from one business vertical to another. In a large-scale operation, the first targeted organization is called Patient Zero (PZero). In order to conduct such analysis, we processed data coming from our daily operations to find and isolate PZero. The following figure show us the propagation model of such attacks, it is possible to notice that the most prominent threat is related to malicious email campaign (Phishing, Spear Phishing, CEO Fraud etc.) which propagating in almost all industries in a shorten time span. A more uniform distribution than 2019.

This propagation behavior gives an indication of the character of threats which are not targeted but opportunistic in nature.

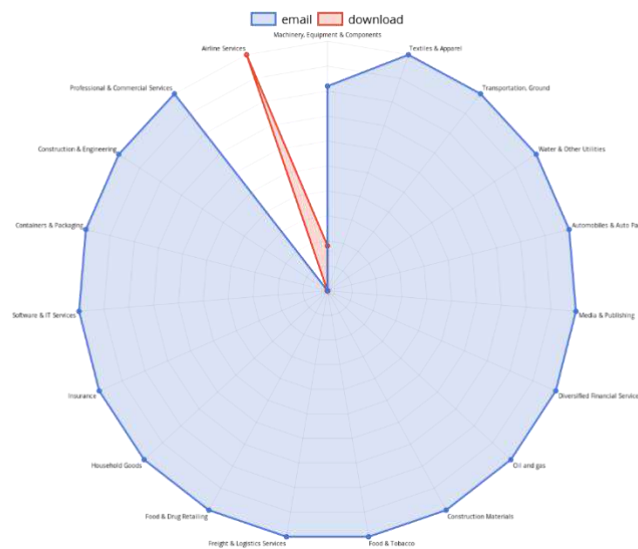


Figure 7. Patient-Zero sectors per attack vector

Cybercriminals don't care what area a business operates in or what size a company is. Each industry sector could be a potential PZero and the propagation towards other business it's just a matter of time. The adoption of a Proactive Security approach permits to tackle cyber threats and offer a high degree of control.

We collected data from multiple sources and record propagation attempts of malicious code, the analysis of such data showing interesting peculiarities and differences between industry verticals.

Once penetrated inside a boundary the malware can escalate and propagate all around the IT infrastructure. Compared to the last year we encountered an important increasing in the overall cyber-attack lateral propagation time (expressed in hours) mostly in several sectors like *Banking Services*, *Textiles & Apparel*, *Freight & Logistics Services*.

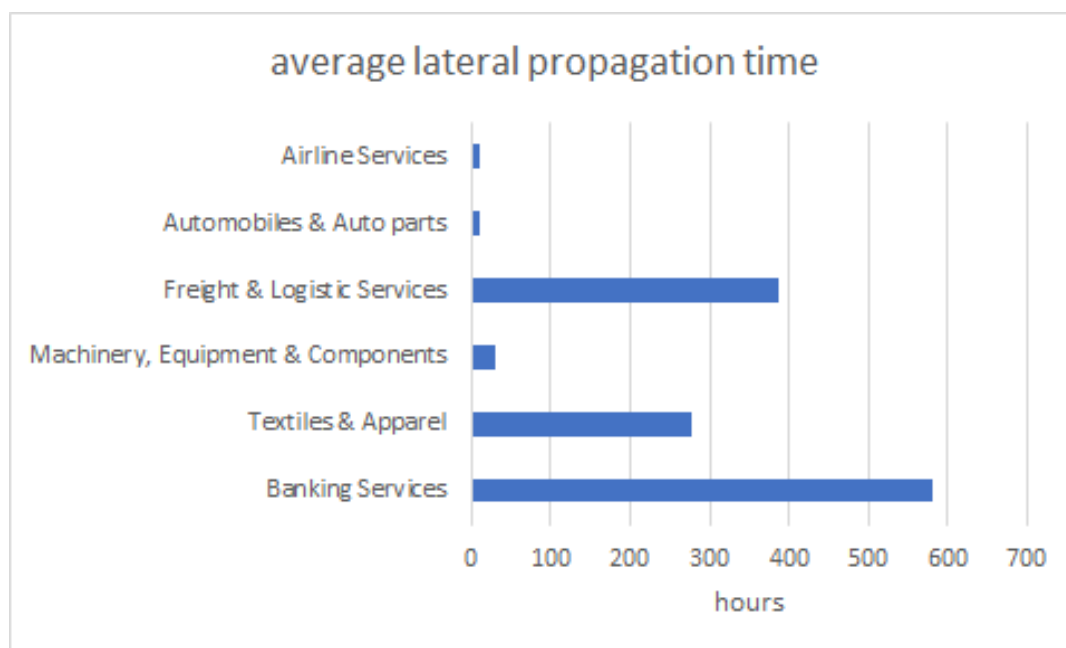


Figure 8. Average lateral movement propagation times

The fast lateral movements happen in *Food&Drug Retailing*, *Diversified Financial Services* and *Construct Engineering* scoring a time ranging from few minutes to few hours, also *Automobiles & Auto parts* and *Airline Services* score a lateral propagation time of few hours (10/12 hours). Services like *Banking*, *Textiles & Apparel* and *Logistics* score an averagely long propagation time which is a sign of difficulties in the resolution of incidents.

Considering the pervasiveness of today's threats, the ability to moving from one business to another in few or dozens of hours, and the ability to propagate laterally once inside a perimeter underline the importance of a proactive strategy which permit to reduce the time related to the resolution of incidents jointly with the consolidation of containment and eradication procedures.

Malware Operations in Italy

More than half of the malware attacks in Italy are banking Trojan malware, with 40% from the Ursnif family, which is confirmed to be the most severe threat that persists in the Italian IT landscape

Nowadays threat actors have built up consistent mechanisms able to constantly deliver malicious code through the construction of the so-called infection chains. Indeed, in this chapter, we focus on our geographical area, Italy, and we analyze the results obtained thanks to our telemetry gathered from our Cyber Security Defense Center and our Cyber Threat Intelligence operations.

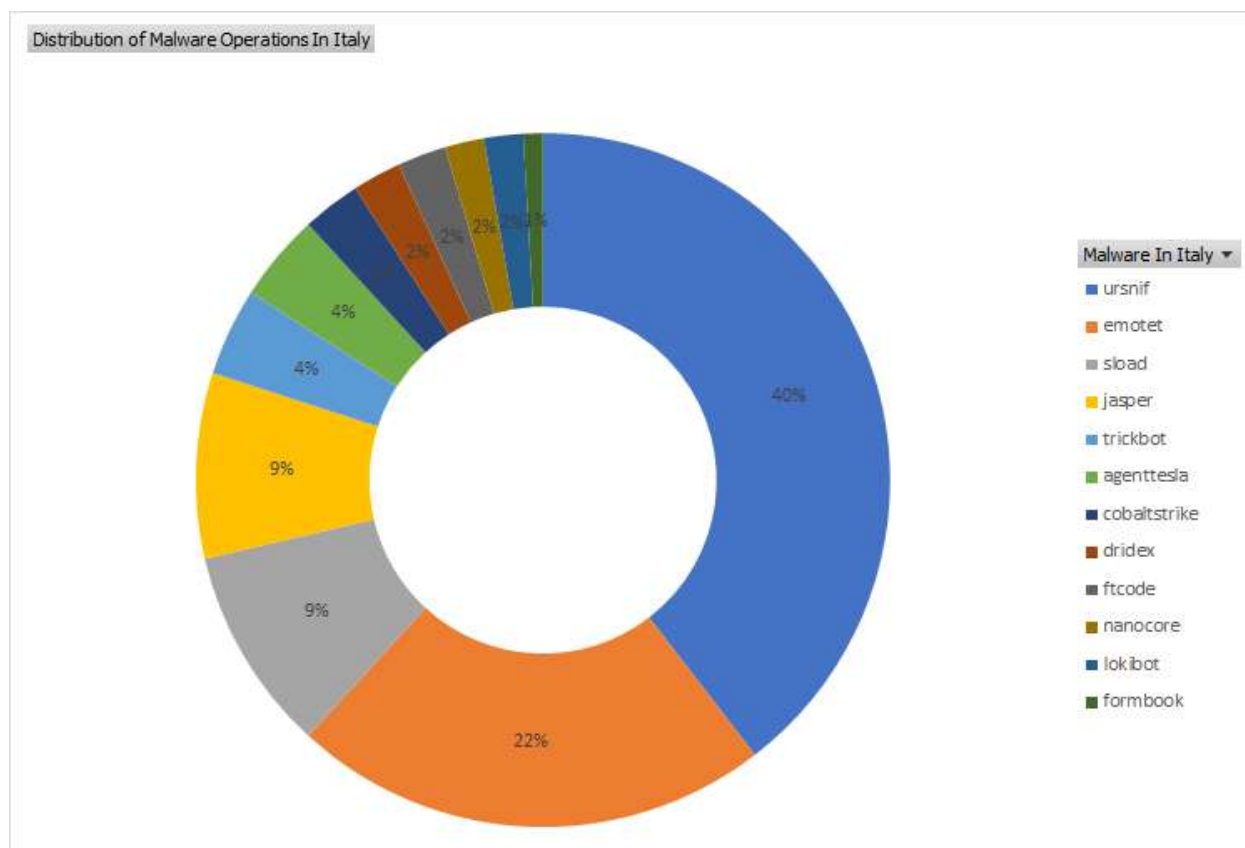


Figure 9. Distribution of principal threat families across malware attack waves in 2020

The figure shows that more than a half of the malware delivery attacks in Italy deliver banking trojan malware, with the lead of the 40% for the Ursnif family and the 22% with Emotet samples. This trend not only remarks what we saw the previous years, but it also shows an increased relevance of this class of malware.

Ursnif confirms to be most pounding threat insisting in the Italian cyber landscape. During the years, it constantly upgraded the payload delivering techniques, thanks to a fascinating creativity in its phishing emails, starting from word or spreadsheets and arriving to the final payload abusing PowerShell, XLM macros, steganography, and so on.

Emotet has been largely distributed on the final part of the year with massive campaigns. Unlike Ursnif, Emotet adopted a more uniform delivery schema: usually, the infection arrives either via malicious script or macro-enabled document files. The malicious emails typically contain familiar branding, with "Microsoft Office 365" logo, designed to look like a legitimate email and they try to persuade users to click the malicious files by using tempting language about "Your Invoice", "Payment Details", or possibly an upcoming shipment from the most common parcel companies. After enabling the macros, a PowerShell script starts to download the malicious component: a DLL from previously compromised websites, with custom URLs specifically built-up for the attack wave. However, in January of 2021, a coordinated international action conducted by [Europol and EuroJust](#) allowed the disruption of the entire malicious infrastructure.

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

27 January 2021

Press Release



Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

Figure 10. Emotet botnet disruption January 2021

sLoad and Jasper loader are responsible of the 18% of the malware distribution attempts. They are malware loaders, with information stealing capabilities, giving their operators a foothold on target network and persistence on the victim machine, enabling them to distribute the arbitrary malware payloads. The trend shows their increasing importance in malware distribution. They give adversaries the ability to gain an initial foothold on a system and are typically used to deliver various malware payloads following successful compromise.

In detail, we decided to deep dive into sLoad because it leverages the PEC mail, the Italian certified mail technology. sLoad is one of the few malware families heavily leveraging PEC communications to infect sensitive workstations. The victim believes that the mail has been validated by the PEC certification authority, anyway the mail often contains a nasty zip archive containing a malicious Visual Basic Script file, which releases further Powershell scripts. The peculiarity of sLoad is the initial foothold phase, where the Powershell script gathers information about the victim machine and only after that reconnaissance phase, the real malicious payload is downloaded and executed.

Trickbot and Cobalstrike have a percentage lower than the previous two but threat actors use them in more sophisticated operations such as in the Double Extortion attacks, described in Section 1, the evolution of ransomware attacks. In this case, adversaries perform actual Red Team operations in order to achieve the highest level of privileges and release the malware. These two malwares are a sort of "swiss army knife" for many groups operating under this threat paradigm. In detail, we observed that Trickbot is related to Ryuk/Conti ransomware activities and Cobalt Strike is a sort of jolly for most cyber intrusion operations, as we saw in many critical incidents along the past year.

Other constant threats in the Italian landscape are the info stealer malwares, like Lokibot, AgentTesla and Nanocore. This kind of malware can be used either as an tool for opportunistic attack, but also for targeted attack. In the first case, the cyber-criminal groups leverage these tools in order to create knowledge bases to perform frauds or other types of attacks like credential stuffing and similar ones. These malware families have been used also during targeted attack operations, where the info stealer capabilities were useful to perform reconnaissance on the target systems, where the act of stealing credentials is fundamental.

In the end, we noticed the fading of the Gootkit banking trojan in the Italian landscape. Over the past years, it represented a constant threat especially due to its Main-in-the-Browser capabilities. But in the last year, our telemetry in Italy didn't observe any massive operation leveraging this malware, which was still active in Europe and Germany in November 2020.

Section 2:

Blocked Threats

Most malware uses DNS protocol to communicate with their C&C in order to receive commands or download payloads but also to conduct malicious activities like network reconnaissance and enumeration. In fact, DNS is a reliable protocol which permits to decouple the malware from its own infrastructure and build a more flexible communication channel. For instance, DNS is a key enabler for the implementation of DGA mechanism, historically adopted by various botnet or also by the Sunburst backdoor. DGA permit the dynamic implementation of some Rendez-vous endpoint that point to the real C2, this mechanism permit to slow down identification and tracking by analysts and law enforcement. For these reasons, DNS represent a valuable source of information for threat intelligence operators. Monitoring inbound and outbound DNS requests permit to spot and block such malicious activity making the difference in protecting and defending the perimeter. The Yoroi DNS Defense Technology blocked 11.297 malicious domains related to different kind of threats.

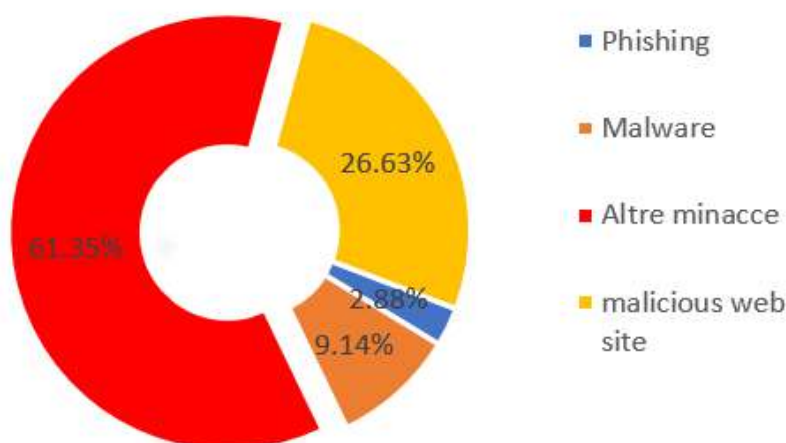


Figure 11. Distribution of the attack blocked by Yoroi's DNS Defense technology

The chart (Fig XX) shows the blocked threats distribution in 2020: 26.63% belongs to malicious web sites which includes compromised web sites, malvertising, adware, click-fraud, and illegit website set up with the sole purpose of inject malware. 9.14% are related to malware threats and their infrastructure such as communications with Command and Control, URL used for payload delivery, malware modules repository. 2.88% of the blocked domains are related to phishing domain. In this category fall domains used in targeted phishing campaign with the purpose of stealing credentials or PII in order to plan further sophisticated attacks. 61.35% are classified as "Other Threats", where we find all those domains that are not attributable to one of the previous categories.

These blocked threats are distributed among business verticals and the analysis of such distribution give us another interesting pieces of information. It's interesting to start analyzing the distribution of blocked phishing attempts per industry sector:

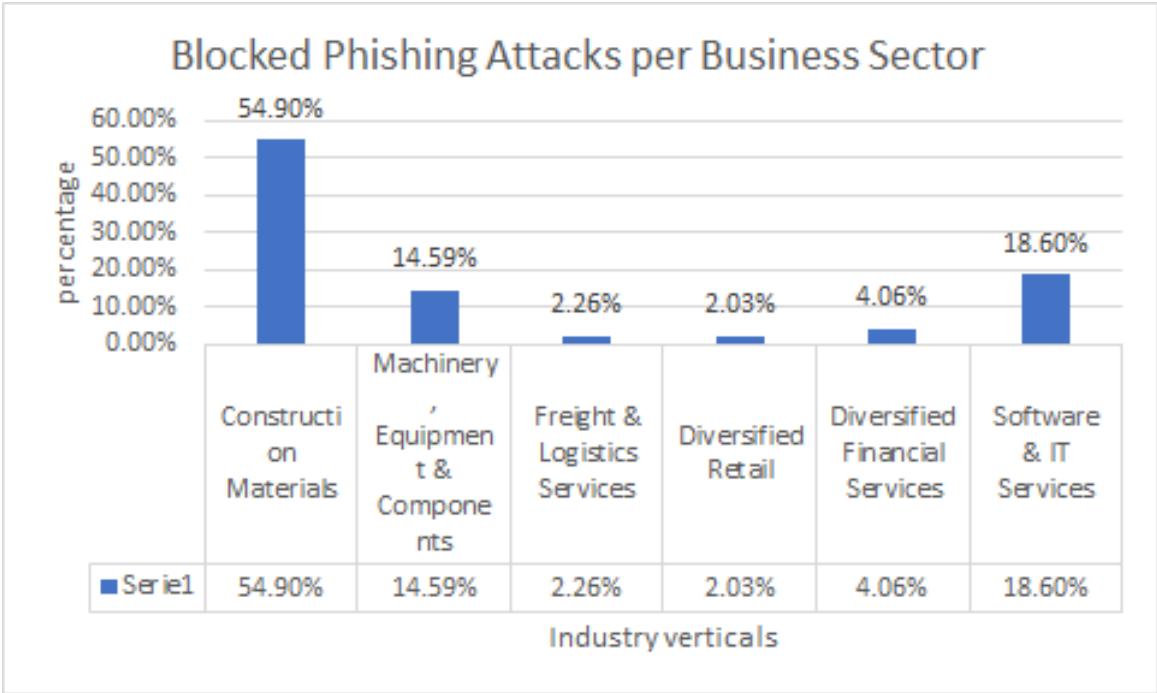


Figure 12. Blocked phishing attacks distributed on top 6 sectors

Almost any type of a data breach begins with phishing attack. The trend of the last year does not differ too much from the 2019. More than 50% of phishing attempts were recorded on *Construction Materials* sector which is composed by manufacturers of plaster, cement, steel, wood, glass, and clay industries and represent an important business for Italy.

It is followed by *Machinery, Equipements and Components* Then we found *Software & IT Services (18.60%)* which represent another important industry, very sensitive for the stealing of intellectual properties, also Financial Services are a valuable target for cybercriminals.

Phishing, in all its forms, remains one of the most active and insidious threat today. This because it is delivered through email and use sophisticated social engineering techniques leverages on human weaknesses, it also able to bypass spam mail filters and EDR. The impact of a successful attack could be tremendous, ranging from the stealing of intellectual properties, loss of image, fraud and sabotage. The Risk increases in critical sectors such as Water and Other Utilities in which the steal of employee credential can have harmful consequences.

Regarding the blocked malware attacks distribution per industrial sectors, it is possible to notice that most of such attacks belongs to 3 different groups: *Construction Materials* with 73.21% followed by *Textiles & Apparel* with 19.84% and *Food & Tobacco* with a score of 5.61%.

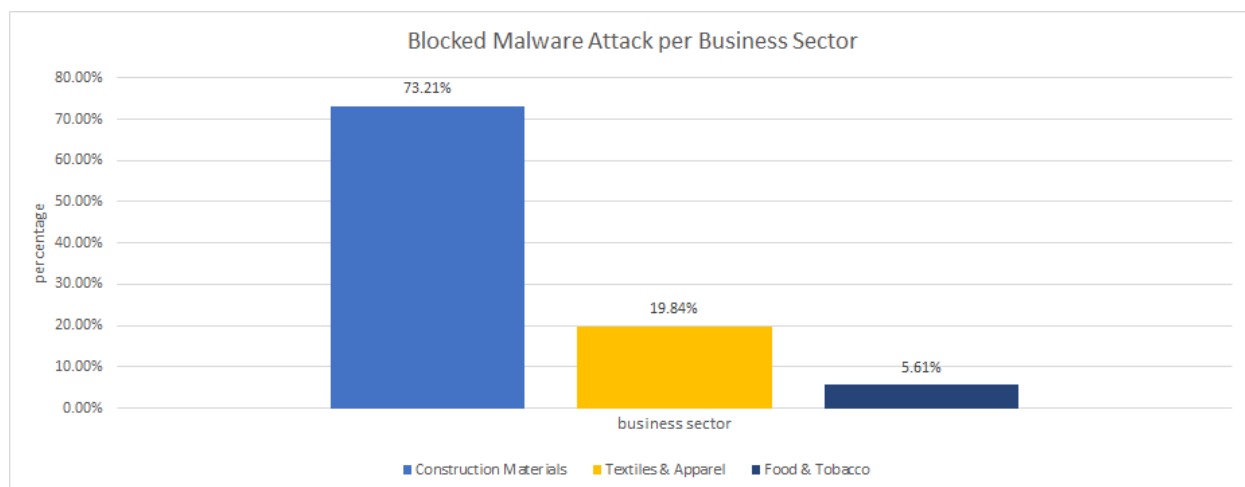


Figure 13. Blocked malware attacks distributed on top 3 sectors

Botnets and Opportunistic Activities

Data related to opportunistic attacks are useful for understanding the importance of a geofenced IP reputation strategy that must block all inbound connections from high-risk countries.

Network signature change over time while malware constantly evolve its behavior, so IP and address reputations is a key factor for proactively blocking opportunistic attacks.

Yoroi's technology also block and record external malicious IPs attempting to infiltrate or exploit exposed or internal assets. From these IPs are conducting large scale, opportunistic and geographically distributed attacks.

In most cases, the origin of IPs does not reflect the real origin of the attack which are perpetrated by distributed botnet. Some Botnets use free DNS hosting services such as *DynDns.org*, *No-IP.com* or IP Fluxing to masking the real source using network of compromised hosts that acts as a proxy.

The observation and analysis of the origin of these malicious activities provide useful insights for the protection of the perimeter.

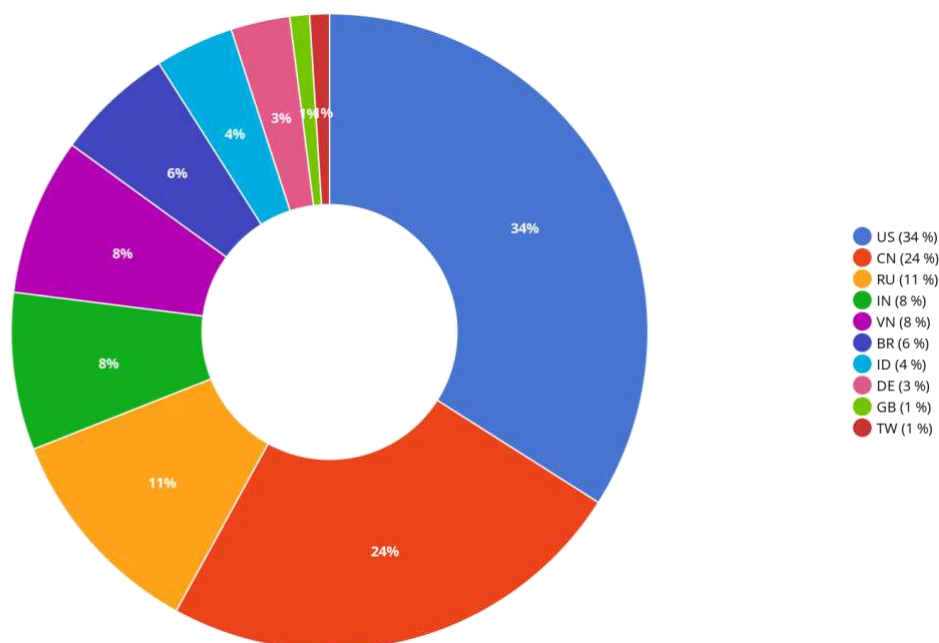


Figure 14. Most active countries in opportunistic attacks

Observing the distribution (pie chart image), US takes the top spots with the 34% of the share which are increased compared the year 2019 (12%). Moreover, attempts coming from China (CN) dropped from the 31% of the 2019 to 24%, as it is possible to see in the below histogram (Fig. X).

The attempts coming from Russia (RU) are increased from 9% to 11% while India (IN), Vietnam (VN), Brazil (BR), Taiwan (TW) and Indonesia (ID) share the 26% of total distribution compared to a total of 41% in 2019. For the 2020 we have two new entries: Germany (DE) with 3% and United Kingdom (1%) which became appreciable in absolute value.

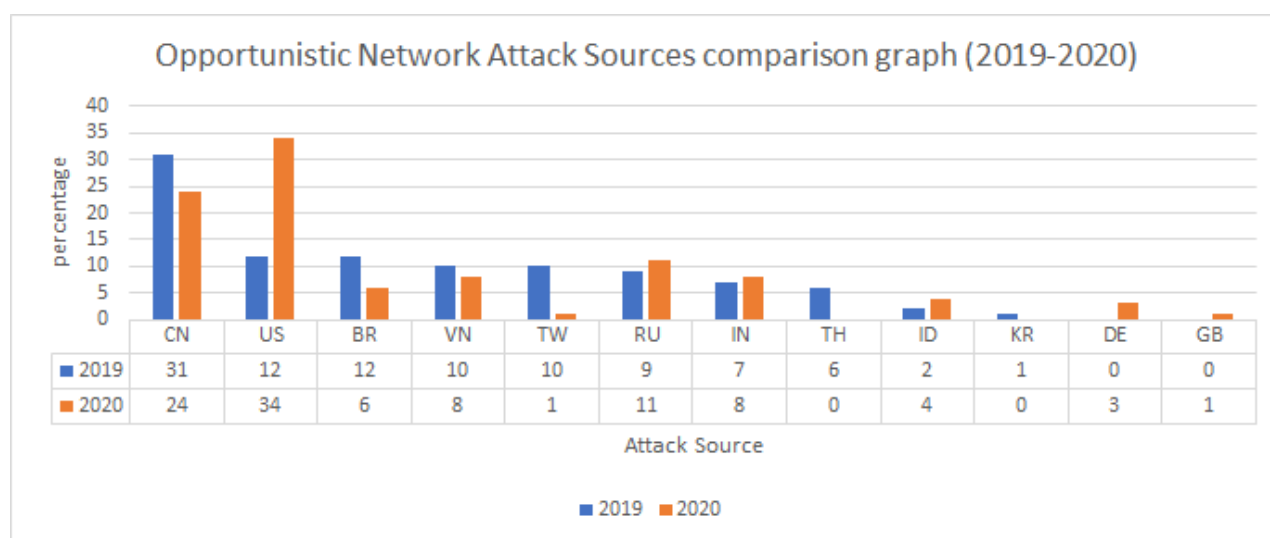


Figure 15. Comparison between principal opportunistic attack's sources

Changes in the last year distribution compared to the 2019 are to be considered "normal" since the attacks are opportunistic in nature so, the networks involved in such attempts are very often previously compromised network of zombies. US, CN and RU are the largest countries, and this is the reason why most Botnet network originating from there. Moreover, for this year we registered also some European country.

This data could be useful to understand the importance of a geofenced IP reputation strategy which have to consider the countries with which business relations exists. In fact, if the company has its own business in US and not in china for example, block all inbound connection from CN would be recommended. In this way in fact, it is possible to mitigate many opportunistic attacks.

Blocking specific sources for inbound connections could be a good proactive defense strategy jointly to other mitigations such as the DNS reputation and network signature solution.

Section 3:

The Email Threat

Adversaries continue to prefer emails as principal malware spreading vector. For the fourth year in a row, malicious mails represent a relevant part of the cyber-attacks. Criminals are free to adopt two different strategies to develop a malicious spam - i.e. "malspam" - campaign.

The first one is to build a resilient exploit kit or leveraging botnets to spread general-purpose campaigns to hit private citizen and small companies. An example could be an invoice mail with a malicious Office document asking the enabling of the macros to view the full content of the document. Then, targeting high value victims and preparing email leveraging specific themes and access to trusted mailboxes.

Also, 2020 year will be remembered by the history due the COVID-19 pandemic, even by cyber criminals. In fact, they leveraged the pandemics in order to make the malicious mails look more impacting on the emotional sphere of their targets. Moreover, the pandemic situation constricted companies to adopt immediate changes, such as smart, remote or full remote working. The consequences impacted in a negative way the security of the users that, in many cases, were operating out of the security perimeter.

Reviewing the telemetry collected by the Cyber Scurity Defence Center monitoring infrastructure, we can confirm Microsoft Office documents are the most relevant malware delivery vector, representing the most common way to spread the first stage of malware infection chain. In fact, **Microsoft Word documents (35%) and Excel spreadsheets (33.2%) collectively represent the 68.2% of all the malicious attachments intercepted by Yoroi's eMail Protection services.**

FileTypes Distribution

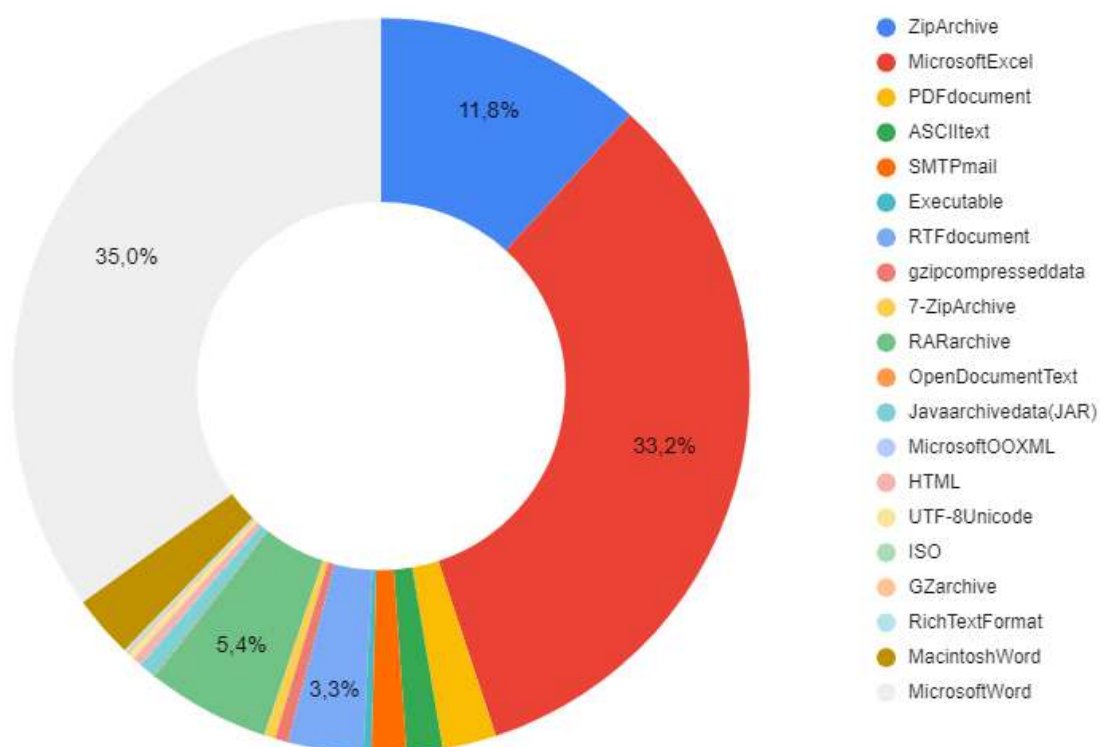


Figure 16. Malicious attachments distribution

The percentage of malicious documents in general is even higher. In fact, one of the latest tactics adopted by the cyber criminals is to compress the attachments inside an archive file (zip, gzip or rar, 7zip) and encrypt them with a password mentioned inside the body of the mail. It is a quite simple method, but it was very effective during the past year.

Another technique widely used in 2020 was the abuse of XLM Macro 4.0. XLM Macro 4.0 is a legacy technology still supported in modern Office suites, that have been abused to evade anti-virus and anti-spam detection of the classic antivirus signatures and allow the second stage of malware infection chain.

However, our sandbox technology, Yomi, can analyze this type of techniques and detect the malicious behavior attachments and we are constantly updating it to detect the new anti-detection tricks.

The group composed by ISO images, RTF documents, as-is executable, JAR archives etc. represent the smaller slice of the pie. In the past, these file format types covered a more important role inside the threat landscape. However, the improvement of exploit detection and code introspection implemented inside perimetral boundaries and endpoint protection systems make harder the growing up of directly delivering these threats. On the other side, threat actors, in order to bypass that countermeasures, created a longer infection chain, through implementing much more complex multistage attack basing on sophisticated DropURL and C2 infrastructures. We are playing a sort "cat and mouse" game with adversaries.

Other interesting point to analyze is the social engineering tricks used by attackers to lure the user into click the malicious link or attachment. Even this year, we performed several studies onto machine learning clustering algorithms to detect how many are the **mail subject** and **attachment name** clusters, referring to a different malspam campaign.

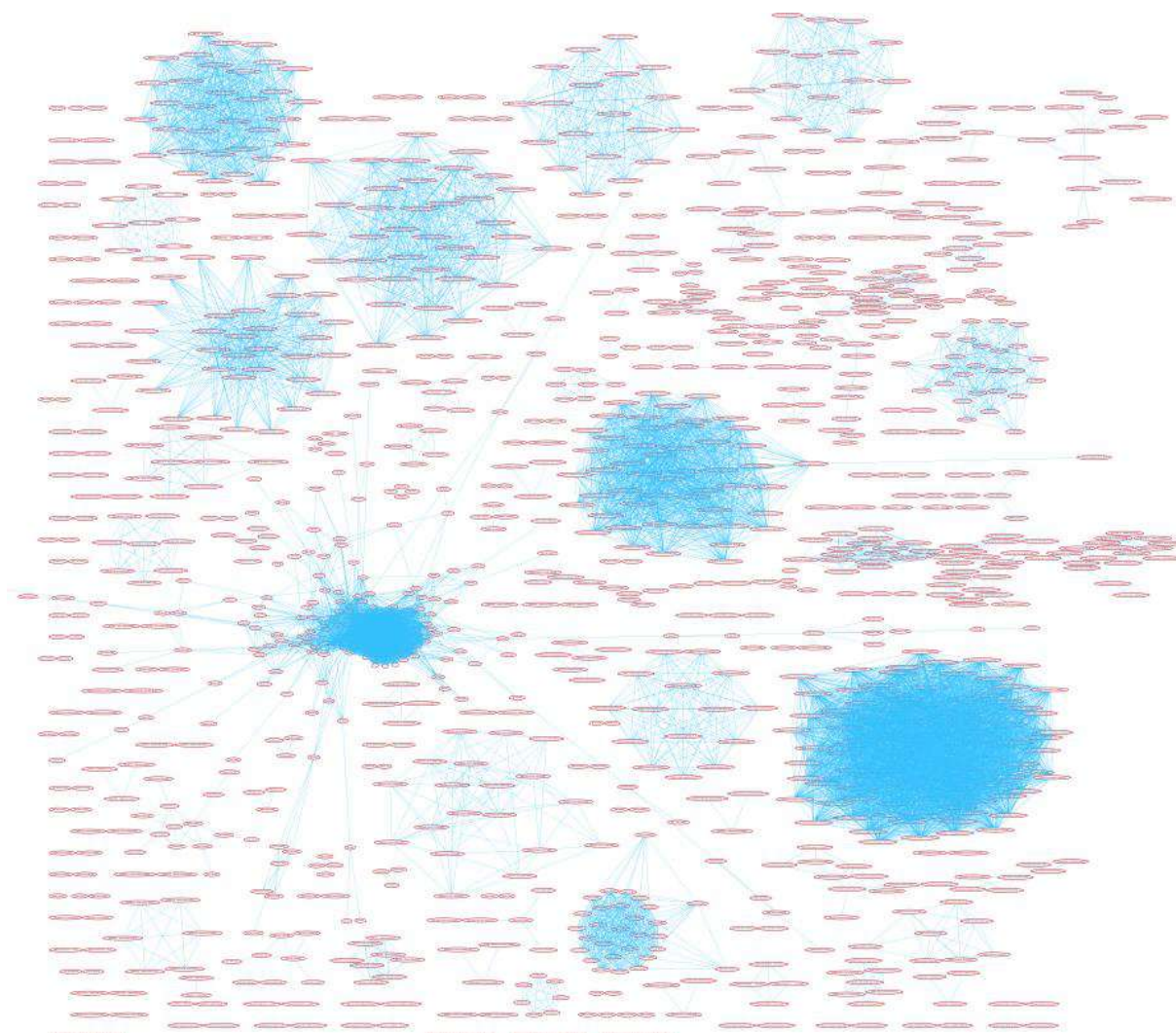


Figure 17. Clusters of malicious spam themes

Our natural language processing analysis revealed that this year we have at least twelve different major malspam campaigns: the double than the past year!

The topics are practically the same of the past Annual Report results, the topics are the following:

- Invoices and Orders
- Packages Delivery and Tracking
- Taxes modules
- Medical Certificates
- Curriculum vitae
- Replies to previous threads
- Generic messages like
 - “Hello, I hope you are doing well”
 - “For the attention of”
 - “Office work”
 - Etc..

Besides them, we want to keep your attention on the 2020 emerging plague, Covid-19 pandemic. As previously mentioned, this topic hits not only the professional sphere of the user, but also the emotional one. Cyber criminals know that and use this flaw into their advantage.

They created specific malspam campaigns leveraging this topic, we were able to intercept and identify them. We found thousands of mails with that topic and main mail subjects' category grossly are:

- Invoices and orders about covid-19
- Information, instructions or procedures about covid 19 precautions
- Refurbish campaigns
- Cashback campaigns
- Delayed payments

Concluding, this last phenomenon let us think how much the link between safety and security is getting thinner, in these century. An event happening inside into the real world has significant consequences inside the cyber world and vice-versa. We in Yoroi believe in digital education and cyber security awareness to make both the worlds safer.

Section 4:

Attack Techniques Trends

New Threats form the Supply-Chain

Supply Chain attacks are motivated by espionage end sabotage of specific targets and can impact any hardware or software component in production

Supply Chain attacks ([T1195.001](#)) are considered the most sophisticated form of threats, posing a significant risk for modern organizations. Historically such threats are perpetrated by APT exploiting and infiltrating the production pipeline in order to implant malware or for disruption.

As stated by MITRE “*Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise*”.

Supply Chain attacks can impact any hardware or software component in production, while the main motivations behinds are espionage end sabotage of specific targets, threat actors may move on to additional tactics and target a broad set of consumers.

The 2020 is also the year of the *SolarWinds* Supply Chain attack. SolarWinds produce the *Orion suite* a Network monitoring and management software used by organizations all over the world. The attack consists in compromising the Orion DevOps pipeline and inserting a malicious DLL backdoor dubbed **Sunburst**, firstly reported on December 2020.

The incident hit multiple entities across the world including governments, Intelligence agencies, big tech companies, telco etc. Due to the spread and the popularity of the Orion software, the related Risk and impact of this incident is considered catastrophic.

Sunburst Backdoor

The backdoored component is the SolarWinds.Orion.Core.BusinessLayer.dll plugin of the Orion suite, digitally signed by SolarWinds which communicate to a third part server (C2) via HTTP protocol.

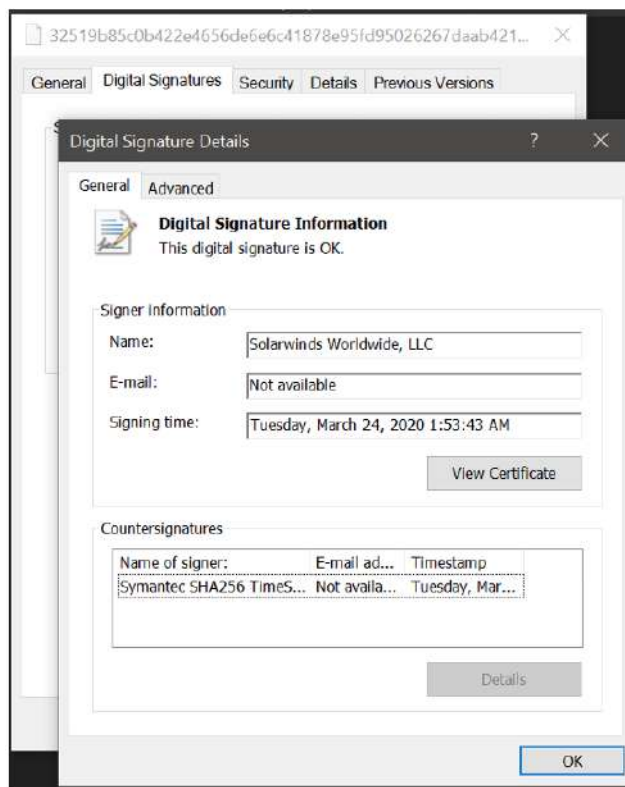


Figure 18. Sunburst backdoor signed by SolarWinds

Once the backdoored component was installed on the system, it permits the deploy of different post exploitation activities adopting techniques with a light footprint on system. In fact, sunburst backdoor permit the delivering of different malicious payload and memory-only dropper (TEARDROP) and the installation of Cobal Strike beacons. Once the backdoor start it's execution, it sleeps for two weeks, then start and execute "jobs" which are responsible for profiling the system, execute files and disable forensic and antivirus tools. The Threat Actor uses different tactics to avoid suspicion and evade detection, following are summarized:

- Lateral movement using different credentials.
- Memory-only dropper and malleable beacons.
- IP addresses located in different countries.
- Attacker hostnames match victim environment.
- Use a DGA algorithm and intermediary C2.

Moreover, the backdoor behavior is masqueraded inside the legit SolarWinds activity as the *Orion Improvement Program (OIP)*. The Threat Actor compartmentalize their operations limiting the exposure of infrastructure to each victim. Following is summarized the communication flow. The intermediate C2 (coordinator) instruct backdoor and redirect SUNBURST to the real C2 via DNS CNAME records. The intermediate C2 acts as the authoritative DNS server for the domain avsvmcloud[.]com, so, to communicate with the C2 coordinator, SUNBURST uses a DGA to construct

subdomains and resolve them. This malicious campaign was conducted with a high level of operational security and could be detected only with the implementation of a persistent defense strategy.

The effort to stay undetected by the threat actor is impressive, in addition they write the backdoor with the SolarWinds coding style and avoid infecting their internal network with specific checks on domain names found inside the .NET backdoor

```
private static readonly ulong[] patternHashes = new ulong[]
{
    //      HASH              CRACKED              ASSUMPTIONS
    // -----
    1109067043404435916UL, // 'dev.local' -> SolarWinds Dev local
    15267980678929160412UL, // 'swdev.dmz' -> SolarWinds Development DMZ
    8381292265993977266UL, // 'lab.local' -> Local lab
    3796405623695665524UL, // 'lab.na' -> SolarWinds North America office
    4578480846255629462UL, // 'lab.bрно' -> SolarWinds Brno office
    8727477769544302060UL,
    10734127004244879770UL, // 'cork.lab' -> SolarWinds Cork office
    11073283311104541690UL, // 'dev.local' -> Development
    4030236413975199654UL, // 'dmz.local' -> Demilitarized Zone
    7701683279824397773UL,
    5132256620104998637UL, // 'saas.swi' -> maybe: SaaS SolarWinds
    5942282052525294911UL, // 'lab.rio' -> maybe: SolarWinds Rio Office
    16858955978146406642UL, // 'apac.lab' -> SolarWinds APAC offices
};
```

Figure 19. Sunburst backdoor preliminary check

All these elements give us an idea of the level of sophistication of this campaign, the goal is clear: stealing data from strategic organizations and intelligence entities around the world so the Orion suite is just a mean and not the real target. SolarWinds has over 300,000 customers including (based on the company website):

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military, the US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

This list is not exhaustive at all but give us the perception and the magnitude of the campaign. Another element of its success is that SolarWinds Orion operates at the highest access privileges, for this reason, any access-based security control is ineffective.

Based on shared telemetry we can confirm that the prominence of the impacted organization is from US followed by UK and scattered among other countries. Italy unfortunately was also affected, and due to the prevalence of such operation, since the early stages of discovery Italy activated the *Cyber Security Nucleus (Nucleo Tecnico per la sicurezza cibernetica)*, this structure was created by the *Presidency of the Council of Ministers* in 2017 which is responsible for coordinating the response to any cyberattack that could have a potential impact on national security.

The Nucleus, for all these organizations that uses the Orion platform, recommend examining the problem with the utmost and attention, and making use of the [special section](#) created on the Italian CSIRT website for this purpose, containing advice, updates and possible accident mitigation measures.

In a [joint statements](#) FBI, CISA and NSA attribute the responsibility of the intrusions to an APT, most likely Russian. On Dec. 17th, DHS's Cybersecurity and Infrastructure Security Agency (CISA) released a [sobering alert](#) on the SolarWinds attack, noting that CISA had evidence of additional access vectors other than the SolarWinds Orion platform. CISA's advisory specifically noted that "one of the principal ways the adversary is accomplishing this objective is by compromising the Security Assertion Markup Language (SAML) signing"; SAML-based authentication is used also by SolarWinds and relies on Microsoft's Active Directory Federated Services.

As stated on the alert, CISA has evidence that there are other initial access vectors [TA0001] than the SolarWinds Orion platform. In fact, CISA has identified some compromises where victims do not use Orion platform or where not active exploitation of Orion was observed.

The other initial access vectors consist of password abuse [T1101.001], password spraying [T1101.003], external remote access services [T1133] and by compromising the SAML signing certificate using their escalated Active Directory privileges: TTPs consistent with the ones used in the SolarWinds Orion supply chain compromise.

Deep Web and Security Breaches

The impact of the data leak related to Fortinet VPN gateways is tremendous, since the data was related from a 2-year-old vulnerability and in such leak there are IPs related to important companies, banks and government organizations worldwide including Italian ones

Another major incident characterized the 2020: The publication of a data leak related to the **CVE 2018-13379** about *Fortinet VPN gateways*. On November 19th, 2020 in fact, the leak of a about 49.000 IPs of Vulnerable Fortinet VPN Gateways has been released on a popular hack forum.

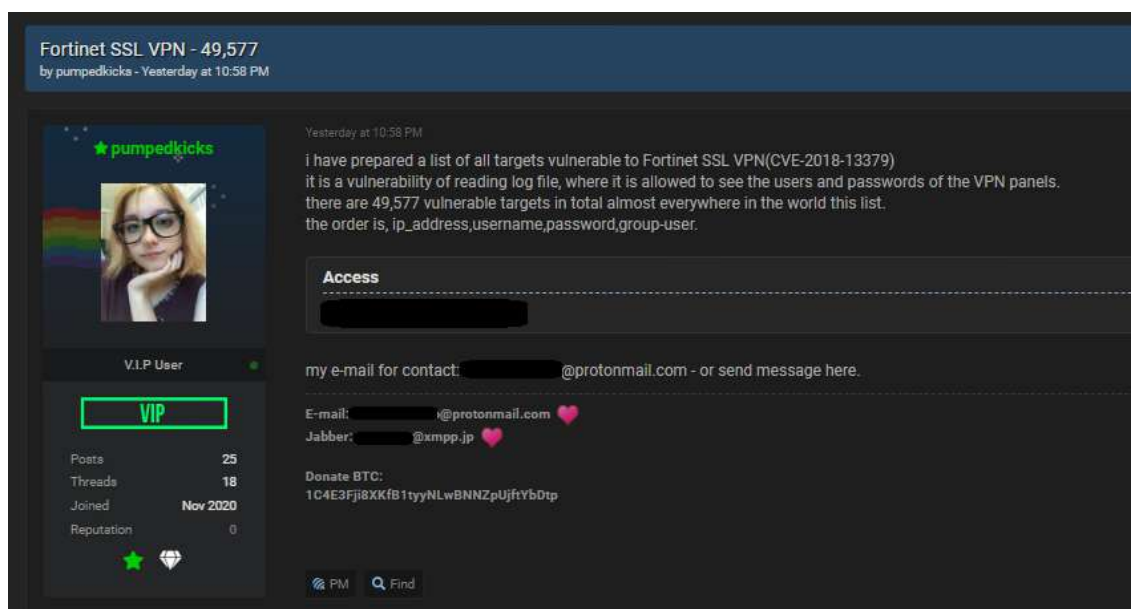
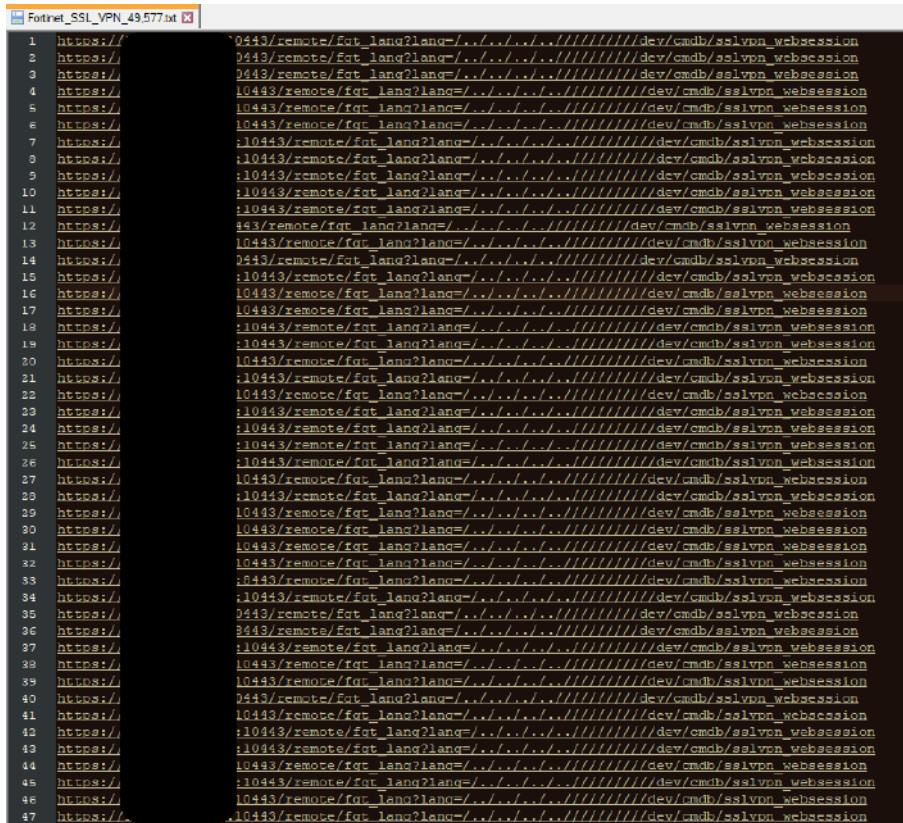


Figure 20. Fortinet VPN vulnerability list announcement

About 6 days later, on the same forum, another actor also published a list of plaintext credentials related to the same Fortinet IP list. The magnitude of the impact is tremendous, since the data was related from a 2-year-old vulnerability, in such leak there are IPs related to important companies, banks and government organizations worldwide including Italian ones and still not patched.



```

1 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
2 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
3 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
4 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
5 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
6 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
7 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
8 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
9 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
10 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
11 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
12 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
13 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
14 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
15 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
16 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
17 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
18 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
19 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
20 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
21 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
22 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
23 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
24 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
25 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
26 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
27 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
28 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
29 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
30 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
31 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
32 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
33 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
34 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
35 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
36 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
37 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
38 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
39 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
40 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
41 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
42 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
43 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
44 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
45 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
46 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession
47 https://10443/remote/fqt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession

```

Figure 21. Fortinet VPN vulnerability list

The CVE 2018-13379 is a Path traversal vulnerability in some versions of **FortiOS** (6.0.0 to 6.0.4, 5.6.3 to 5.6.7) due to an improper validation of a Pathname to a restricted Directory, it allows an unauthenticated attacker to download *sslvpn_websession* file (which contains credentials) via special crafted HTTP requests under SSL VPN web portal. The CVSSv3 Base Score of the CVE 2018-13379 is 9.8 with Severity defined as Critical.

In a [joint advisory](#) published on last October, CISA and FBI reported that the Russian Energetic Bear APT is also using this one and other exploits to carrying attacks against various U.S. critical targets.

These credentials are still circulating on the web so it could be simply accessed and abused by a malicious actor in order to infiltrate in an unauthorized manner inside infrastructures and steal data or implant malware for different malicious purposes. A quota of these exposed IPs belonging to Italian organizations: 1639 internet protocol number belonging to Italian organizations because are related to Italian providers, corresponding about the 3.3% of the exposed IPs. The Italian quota is composed by IPs related to the following sectors:

- ISP: 91%
- Education: 0.25%
- Business: 3.7%
- Hosting: 4.93%

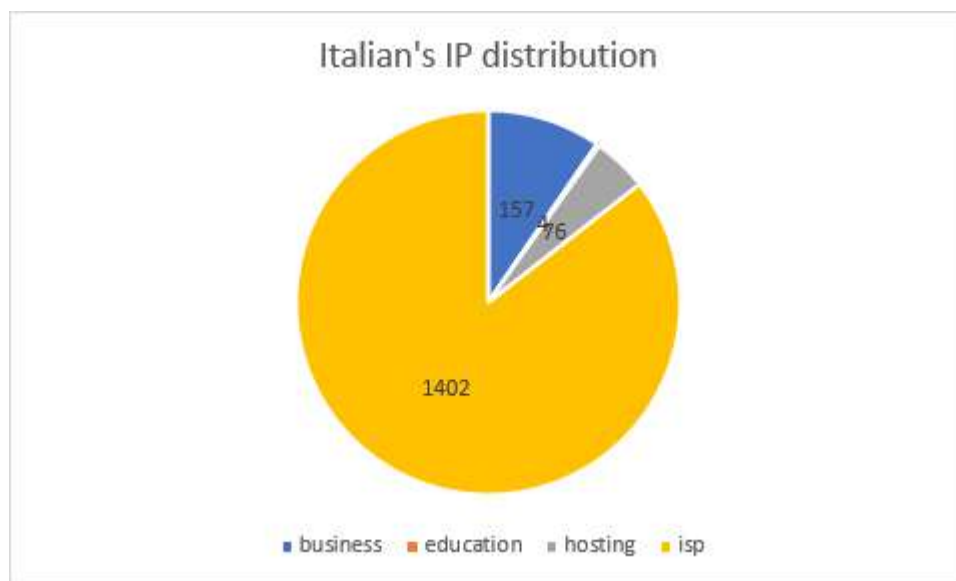


Figure 22. Distribution of Fortinet VPN vulnerability in Italy

It is possible to notice that most of these IPs belongs to ISP networks (91%), followed by Hosting (4.93%), Business (3.7%) and Education with just the 0.25% of the total share. However, these numbers do not give the real dimension of the attack surface, which is much bigger, because, most probably, there are a huge number of systems still publicly exposed and not already patched.

For a malicious actor it's not difficult to looking for vulnerable endpoints, considering that Fortinet Fabric is quite widespread in some environment. Today most organizations remain still vulnerable and have not patched this vulnerability yet, this because not all predispose and **implement a proper Vulnerability Management Program that is crucial for an effective cyber risk mitigation strategy.**

Conclusion

During the past 12 months the entire society radically changed. Covid-19 was able to slow down economies, to change the way -many of us- are working, to move market shares and drastically to force the way companies execute their digital space. The digital technology helped the entire society during the frequent and spread lockdowns by giving us a way to communicate, to share experiences and to keep working by home. Remote working enabled domestic routers or personal computers to be connected directed to company assets. Usually by opening-up VPN tunnels able to bypass perimetral boundaries landing road warrior connections directly on the internal LAN. Many companies found themselves having external connections coming from untrusted machines straight to their management networks or to their business ones, since IT admins needed to operate through VPN or workers needed to interact with internal CRM in order to move on business from remote homes. This was one of the most abused attacks path during the past months. Basically, attackers exploiting unprotected home devices waited for VPN connections and then started a lateral move from such a device to internal assets. Those assets were not designed to stand out internal attacks since before lockdowns they were protected by proxies, IDS, Firewalls, DNS solutions, and so forth. Quite often the company services have not been designed to have direct access to external and unprotected devices. As seen in previous chapters, emails are still one of the main favorite attack vectors as much instant messaging is, but attackers are quickly moving to use phishing lures, so that we bet in the near future Phishing Kits will play an interesting role in the next threats.

But 2020 and the beginning of 2021 is also a remarkable year because we experienced the Emotet takedown. One of the biggest cyber operation ever, which involved private and public sectors, international police forces and international private companies. We saw all this groups working together for make the digital space a better place to stay. Humongous operations very well synchronized destroyed the Emotet Command and Control Systems and deactivated the living implants by deploying a self-destructive Emotet payload to every infected device.

But unfortunately, if on one hand we had this big success we also experienced one of the most important supply chain attack in the history. SolarWinds was just a remarkable cyber attack performed by sophisticated groups affecting hundreds of thousands of companies all around the world. This attack highlighted a known topic about supply chain attacks and warning the entire cybercommunity that company suppliers would be the next thing to watch out for.

Nowadays like never before every company needs to enforce its cyber protections since its business success runs through its digital space which is constantly threaten by cyber attackers. Companies like Yoroi need to improve their attraction to Small Business helping them to succeed in their business protecting their digital assets as never before. We are here to increase the cybersecurity of the digital era.



Yoroi S.r.l.

www.yoroi.company - info@yoroi.company

Piazza Sallustio, 9

00187 – Roma (RM)

+39 (051) 0301005

Yoroi S.r.l. ® 2014-2021 – All rights reserved

Yoroi ® is a registered trademark



Registration N°: 016792947



Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University



TF-CSIRT
Trusted Introducer