YARIX
a vargroup company

YSOC
SECURITY REPORT

Q1 2019

Summary

Introduction

The document provides insight into data received and analyzed by Yarix SOC from January to March 2019

Who we are: Yarix, the Digital Security Division of Var Group

Yarix is a division of **Var Group**, a company working in the digital security sphere, and is a recognized leader in the cyber security sector. Its stated mission is to develop targeted solutions for companies and government agencies, health companies, schools and universities. It was the earliest private company in Italy to be admitted to FIRST, the global protection network that brings together key players such as NASA, Apple and Google with the aim of countering emerging threats.

The SOC

Yarix has one of the most advanced Cognitive Security Operation Centers (C SOC) in Italy: an IT bunker equipped with state-of-the-art physical and biometric security measures, based on predictive and cognitive computational models. It is active 24 hours a day, is manned by a team of 27 IT security experts and provides companies with access to security, business continuity and disaster recovery services, in a manner that responds effectively to the evolution of threats and risks. Just as the protection of the technological, informational and intellectual assets of an organization has become vitally important, so the SOC represents the most powerful tool to counter cyber threats, through its suite of advanced intelligence features and the adoption of a holistic approach to security.

The effectiveness of the SOC has been strengthened over time via integration of **Artificial Intelligence** tools – capable of performing predictive analyses - alongside **Cyber Threat Intelligence** solutions which are applied to open source data as well as a range of diverse sources, and which can anticipate potential cyber attacks.

The approach is multidisciplinary and multilevel: the synergy between security competences and legal and economic skills amplifies the ability to respond to cyber crime, including offering protection solutions for its legal and socio-economic implications.

The Report

The purpose of this document is to provide an overview of the landscape of cyber-threats that have affected Italy and make an assessment of the trends and mitigation actions necessary to reduce their impact. The report refers to **the first three months of 2019** and will be updated on a regular basis every three months, in order to construct a historical record of data for comparison purposes.

The Methodology

The document provides insight into data received and analyzed by Yarix SOC from January to March 2019. The data comes from the specific group of companies monitored by the SOC and corresponding to Yarix customer base, representing a broad cross section of businesses from all sectors of the national economy. The companies involved within the data analyzed comprise, on average, over a thousand employees, representing a total turnover of more than 50 million Euros. The data were statistically normalized and homogenized so that they yielded robust, useful quantitative output which could in turn provide support for qualitative decision-making. All data have been automatically anonymized and aggregated for privacy purposes, removing any link between the information collected and the companies involved.

The report is divided into two sections:

// **Quantitative section**
This section reports the number of security events recorded by the SOC, highlighting how many have evolved into real attacks that require management, and which sectors have been most affected. The report will respond to these questions through data collected and processed by Yarix analysts, starting from a representative panel of the various Italian economic sectors, which specifically includes the following:

- Financial
- Insurance
- Fashion
- Automotive
- Transportation
- Industrial/steel
- IT System Integrator
- Critical Infrastructures
- Gaming
- Health

// **Qualitative section**
This provides analysis of the data collected in the previous section in an objective and informed way, to identify trends and anomalies.

The **final section** will identify the main trends of the period analyzed and related countermeasures aimed at mitigating the problems identified. Furthermore, one of the most important cybersecurity events identified in the period under review will be reported, namely, ‘spear phishing’ attacks carried out via Certified emails (known as PEC in Italy), which affected many companies and public administrations.

1. Data analyzed

In the first quarter of 2019 the monitoring systems reported approximately 12 thousand security events

In the first quarter of 2019, the monitoring systems implemented by Yarix SOC reported approximately **12 thousand security events**.
Yarix analysts subsequently analyzed this database, collating it and correlating it with additional **Threat Intelligence information**, derived from internal sources and partnerships with institutions, public bodies and other companies. Last but not least, this analytical document takes into account the news coming from the **FIRST** network (Forum for Incident Response and Security Teams), the most extensive and authoritative international community, with over 470 teams registered in 91 countries, for joint prevention and management of security incidents. Yarix's Computer Emergency Response Team is among the few Italian companies admitted to this prestigious global forum.

2. Quantitative analysis

Quantitative data analysis was performed by analyzing the sample according to different aggregations

Quantitative data analysis was performed by analyzing the sample according to different aggregations. In some cases, it required the introduction of statistical bias removal methodologies, due to the presence of a greater number of companies or larger companies in one specific sector when compared to another.

2.1 Events and security incidents

The difference between event and security incident is subtle. For the sake of completeness, the definitions we have used for the two terms, which will be valid for the whole report, are as follows:

// Security Event
This is an occurrence, identified by the status of a system, a service or a computer network, which indicates a possible violation of defined computer security levels. It can also manifest itself as an unknown situation, which may be potentially relevant to the security of an organisation's information and corporate assets.

// Security incident
Event or chain of events resulting from an intentional or accidental action carried out within the controlled IT system. The security incident can cause the loss of confidentiality, integrity or availability of company data and services provided by protected IT assets. It can also compromise the use of assets, with the aim of committing offences or causing damage to third parties, in violation of corporate and/or legislative provisions.

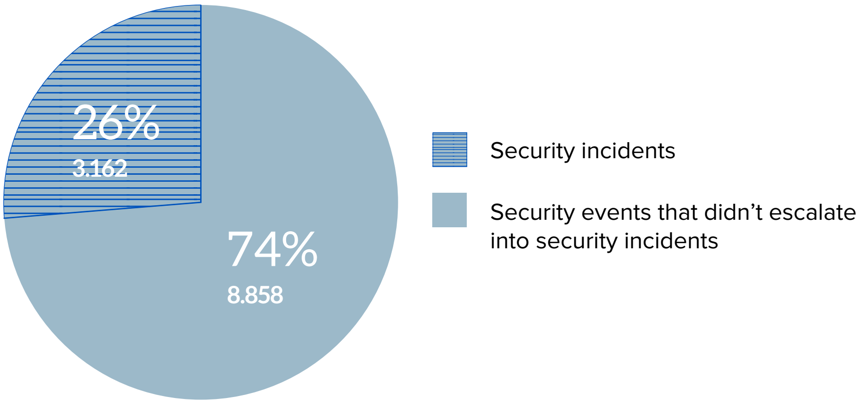
In order to provide a non-exhaustive list of examples, the security events analyzed include:

- events attributable to malicious codes/malware;
- exploitation of known vulnerabilities;
- presence of systems connected to Botnet;
- data exfiltration;
- intrusion;
- compromise of systems and/or applications and/or services;
- DoS/DDoS attacks;
- unauthorized modification or deletion of data;
- the sending of phishing emails;
- communication with IPs, domains, URLs attributable to malicious activity.

The events analyzed totalled 12.020, **3.162** of these **escalate into security incidents**, of differing degrees of severity.

Figurae 1

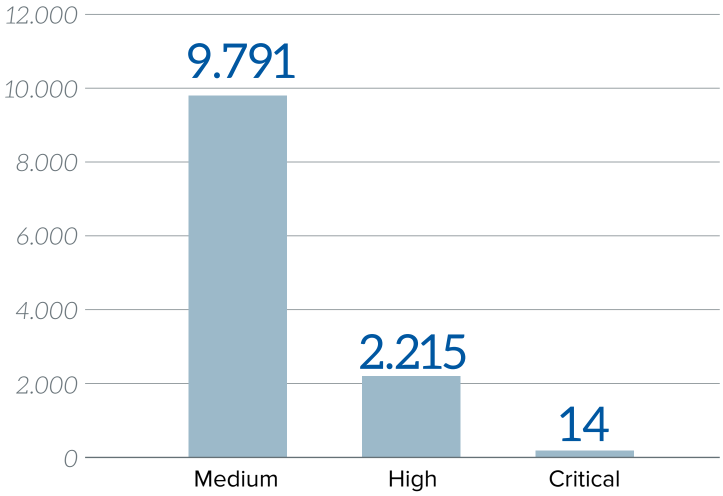
Total events analyzed



The severity of the events was calculated based on the details contained in the playbook of the individual companies monitored by the SOC, and defined according to the agreed metrics and procedures, based on **national and international standards**. This **classification makes it** possible to align the types and severities of the incidents detected for individual customers in the following infographic.

Figure 2

Events divided by severity



In particular, the events classified as 'critical' were supported with specific **Emergency Response** activities, implemented by the Yarix YCERT to ensure correct management, resolution and analysis of the incident. In these cases, the aim is to detect the origin of the compromise or attack, identify possible additional damage and prevent persistent activities carried out by the attacker.

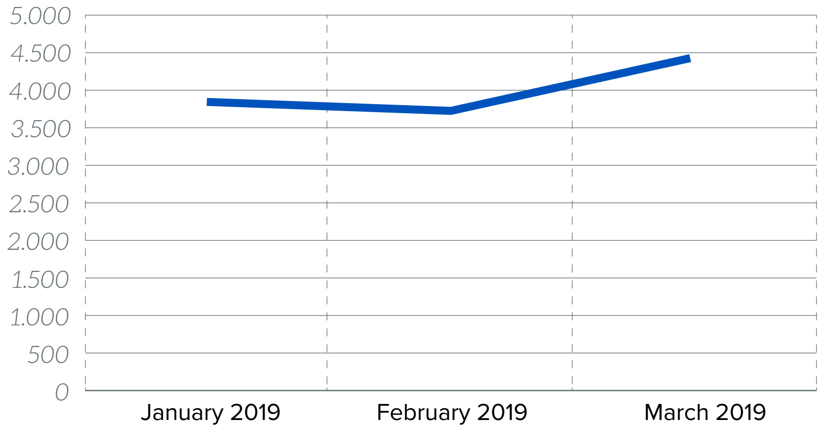
In the **14 critical incidents detected**, the Emergency Response action carried out was decisive not only to restore the normal operation of the systems and to guarantee access to subsequent detailed forensic analysis. Emergency Response management also made it possible to improve control systems, or "lessons learned", by defining strategies aimed at preventing and limiting consequences in the event that the same type of attack should happen again.

Following a Report of an IT Incident a series of actions are carried out, as below:
- **Assist** the subjects involved in the management of security incidents;
- **Respond** to incident reports, alerting those involved and following developments;
- **Disseminate** information on the most common vulnerabilities and security tools to be adopted;
- **Assist** those involved in the implementation of preventive measures deemed necessary for reducing the risk to acceptable levels;
- **Issue** directives on the minimum safety requirements for machines with network access, verifying compliance of same;
- **Manage** technical refresher courses, at all levels, and in particular for end users;
- **Keep** security tools and methodologies up-to-date;
- **Test** existing methodologies and tools, and develop new ones for specific needs.

With regard to the number of events detected in the months analysed, the trend observed remains almost constant, with no particular peaks in activity.

Figure 3

Distribution over time

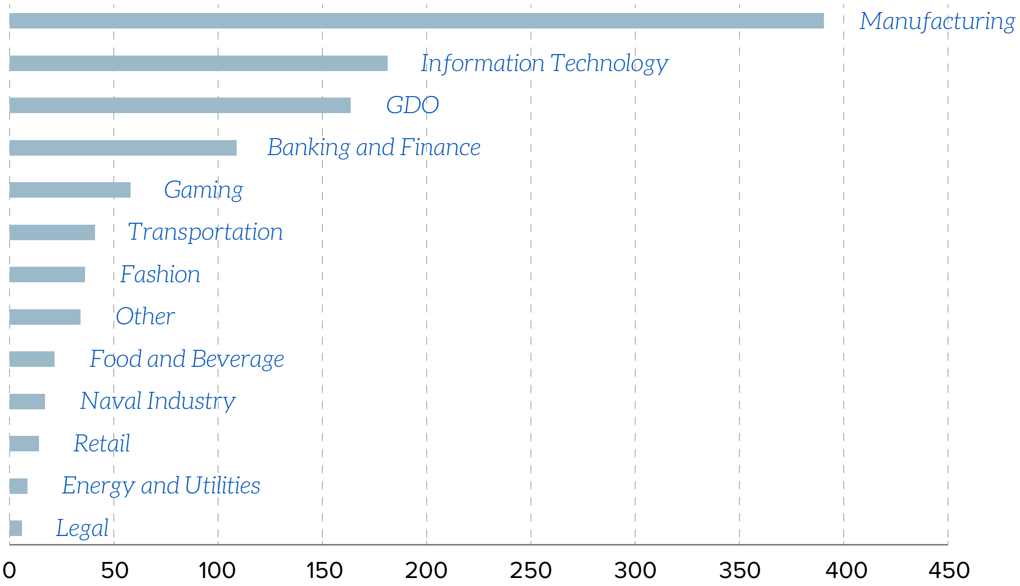


Clearly the above graph will take on greater significance when subsequent reports are released and the period analysed is longer.

The below graph shows analysis focused on the type of industrial sector impacted.

Figure 4

Events by industrial sector



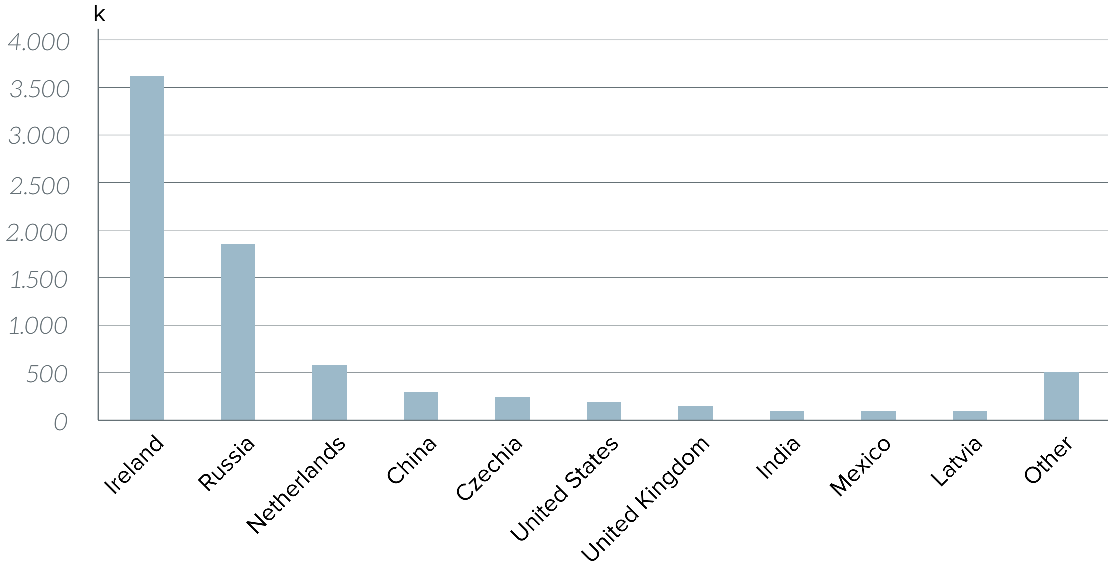
As can be seen from the graph the sector most affected is **Manufacturing**, which essentially had double the number of events recorded in the other sectors, including IT and large-scale retail channels.

2.2 Threat Intelligence

By using the network of honeypots (traps) that Yarix has positioned in various geographical areas around the world, the information gathered by the SOC starting from its customers' systems has been enhanced with **context information**: by analyzing artefacts left by attackers, it was thus possible to acquire indicators of compromise (IOC) and insights into additional risk scenarios.
The following graph provides information concerning the geolocation of the attacks.

Figure 5

Threats by country



As can be seen, of the approximately 7 million events recorded globally over the quarter, the largest number of attacks appears to come from Ireland, followed by Russia, the Netherlands and China. The reason lies in the fact that most of the online protocols used by companies and exploited by cybercrime are based in these countries. Specifically, cyber criminals use two systems to take advantage of these unprotected services:

- Exploitation of known vulnerabilities of the exposed protocols;
- Brute Force attacks, or repeated login attempts with standard users and common passwords.

Regarding the Yarix Honeypots, these are traps we have distributed intentionally. This is not the case with regard to corporate services and protocols, which are often used for remote connections to machines as in the case of SSH, RDP and SMB, which rather unwisely can often can be freely accessed without restrictions. In fact, these vulnerabilities can be detected quite simply by means of automatic tools that scan the network in search of potential entry points to the company's IT systems. It is clear that, if these connections have no safeguards, the risk of intrusion into the company system increases dramatically.

The main malware families released by attackers are:

- **75%** of the total is a variant of the "**Zusy Trojan**", which is banking malware that is typically spread through emails containing a malicious attachment. The goal of the malware, which can spread across the network through features similar to worms, is to gather information about the user's bank credentials;
- **20%** of the total is a variant of the "**Wanna Cry**" ransomware, widely reported malware that spread globally in 2017.

2.3 Email analysis

Because the trend of attacks is towards more targeted attacks, which use persistent methods and are aimed at specific objectives, it is not always possible to trace the original causes. However, it is possible to state that, in most cases, **the main attack vector is email**.

The types of malicious emails are many and various but this tool remains one of the most effective and efficient for attackers. In fact, by exploiting this communication channel, by far the most common in a business environment, it is relatively simple to **orchestrate attacks on an industrial level**. The attempt to breach computer systems takes place by sending out massive quantities of emails to a wide range of recipients, without specific objectives, with the aim of compromising the greatest number of assets. As an example:

- a phishing email, containing a link to a fake authentication portal, can jeopardize the user's credentials. The latter can then be used for targeted attacks;
- an email containing a malicious attachment can compromise the user's client, making it part of a botnet. Worse still, it can contain executables that can compromise the entire business system, such as ransomware or an APT.

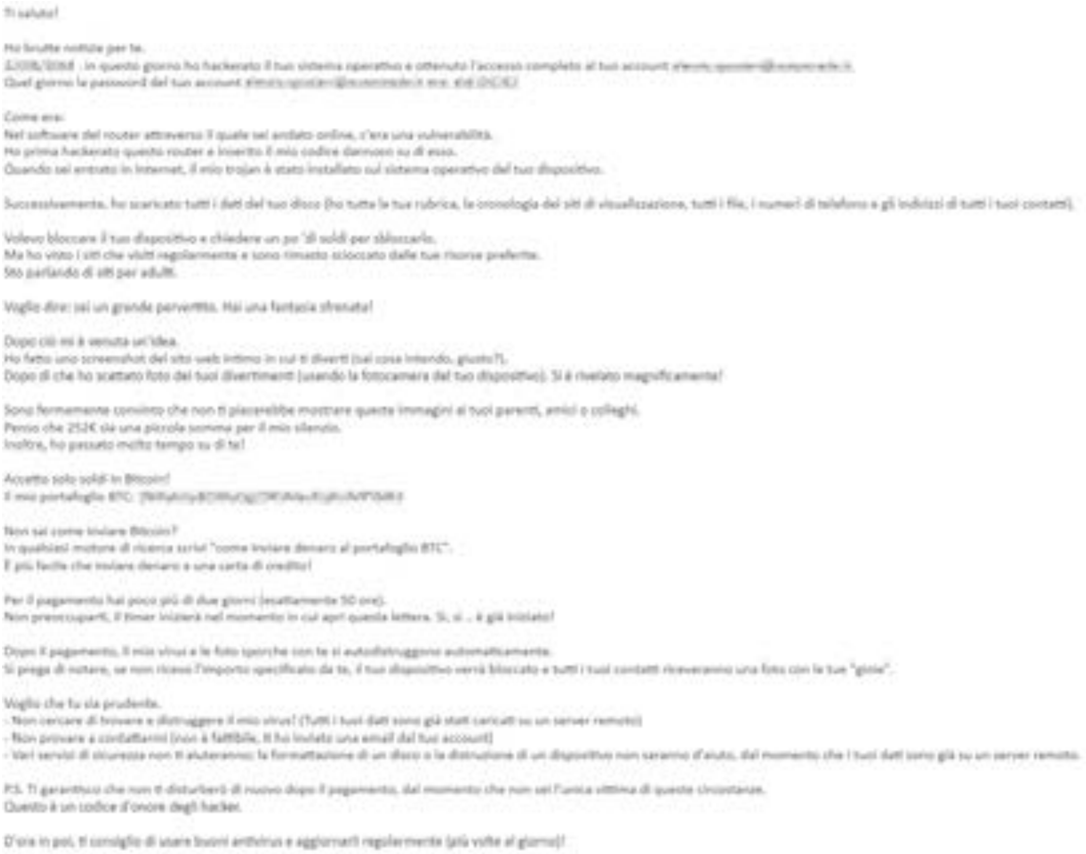
The main phishing campaigns reported in the 3-month period under review are reported below, with related circulation trends within the environments monitored.

// Sextortion

the campaign related to this type of blackmail peaked in January, and then continued to a lesser extent also during the following months. The attackers blackmail the victims, recovering small amounts of money from a large number of targets, through cryptocurrency payments.

Figure 6

Sextortion



Ti saluto!

Ho brutte notizie per te.
[redacted] - in questo giorno ho hackerato il tuo sistema operativo e ottenuto l'accesso completo al tuo account [redacted]
Quel giorno la password del tuo account [redacted]

Come era:
Nel software del router attraverso il quale sei andato online, c'era una vulnerabilità.
Ho prima hackerato questo router e inserito il mio codice dannoso su di esso.
Quando sei entrato in Internet, il mio trojan è stato installato sul sistema operativo del tuo dispositivo.

Successivamente, ho scaricato tutti i dati del tuo disco (ho tutta la tua rubrica, la cronologia dei siti di visualizzazione, tutti i file, i numeri di telefono e gli indirizzi di tutti i tuoi contatti).

Volevo bloccare il tuo dispositivo e chiedere un po' di soldi per sbloccarlo.
Ma ho visto i siti che visiti regolarmente e sono rimasto scioccato dalle tue risorse preferite.
Sto parlando di siti per adulti.

Voglio dire: sei un grande pervertito. Hai una fantasia sfrenata!

Dopo ciò mi è venuta un'idea.
Ho fatto uno screenshot del sito web intimo in cui ti diverti (sai cosa intendo, giusto?).
Dopo di che ho scattato foto dei tuoi divertimenti (usando la fotocamera del tuo dispositivo). Si è rivelato magnificamente!

Sono fermamente convinto che non ti piacerebbe mostrare queste immagini ai tuoi parenti, amici o colleghi.
Penso che 252€ sia una piccola somma per il mio silenzio.
Inoltre, ho passato molto tempo su di te!

Accetto solo soldi in Bitcoin!
Il mio portafoglio BTC: [redacted]

Non sai come inviare Bitcoin?
In qualsiasi motore di ricerca scrivi "come inviare denaro al portafoglio BTC".
È più facile che inviare denaro a una carta di credito!

Per il pagamento hai poco più di due giorni (esattamente 50 ore).
Non preoccuparti, il timer inizierà nel momento in cui apri questa lettera. Sì, sì ... è già iniziato!

Dopo il pagamento, il mio virus e le foto sporche con te si autodistruggono automaticamente.
Si prega di notare, se non ricevo l'importo specificato da te, il tuo dispositivo verrà bloccato e tutti i tuoi contatti riceveranno una foto con le tue "gioie".

Voglio che tu sia prudente.
- Non cercare di trovare e distruggere il mio virus! (Tutti i tuoi dati sono già stati caricati su un server remoto)
- Non provare a contattarmi (non è fattibile, ti ho inviato una email dal tuo account)
- Vari servizi di sicurezza non ti aiuteranno; la formattazione di un disco o la distruzione di un dispositivo non saranno d'aiuto, dal momento che i tuoi dati sono già su un server remoto.

P.S. Ti garantisco che non ti disturberò di nuovo dopo il pagamento, dal momento che non sei l'unica vittima di queste circostanze.
Questo è un codice d'onore degli hacker.

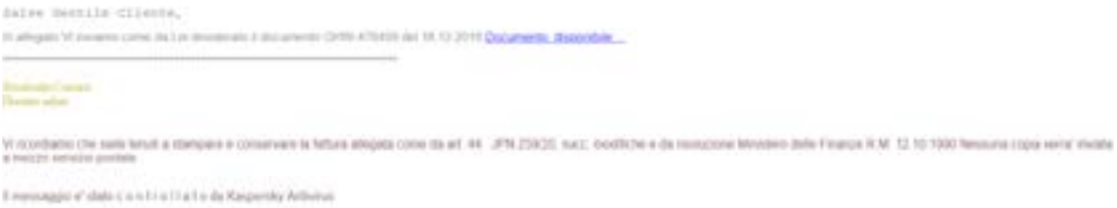
D'ora in poi, ti consiglio di usare buoni antivirus e aggiornarli regolarmente (più volte al giorno)!

// Suspended invoice

This type of campaign made its first appearance during 2018, and then continued to varying degrees during the course of the year. Even in early 2019, it has appeared on several occasions in the form of malicious emails, containing one or more links leading to the download of dangerous attachments. These attachments vary for each campaign and may belong to the family of banking malware, generic Trojans or ransomware.

Figure 7

Suspended invoice



Salve Gentile Cliente,

In allegato Vi inviamo come da Lei desiderato il documento [illegible] del [illegible] Documento disponibile ...

[illegible]
[illegible]

Vi ricordiamo che siete tenuti a stampare e conservare la fattura allegata come da art. 44 DPR [illegible] succ. modifiche e da risoluzione Ministero delle Finanze R.M. [illegible] Nessuna copia sara' inviata a mezzo servizio postale.

Il messaggio e' stato controllato da Kaspersky Antivirus

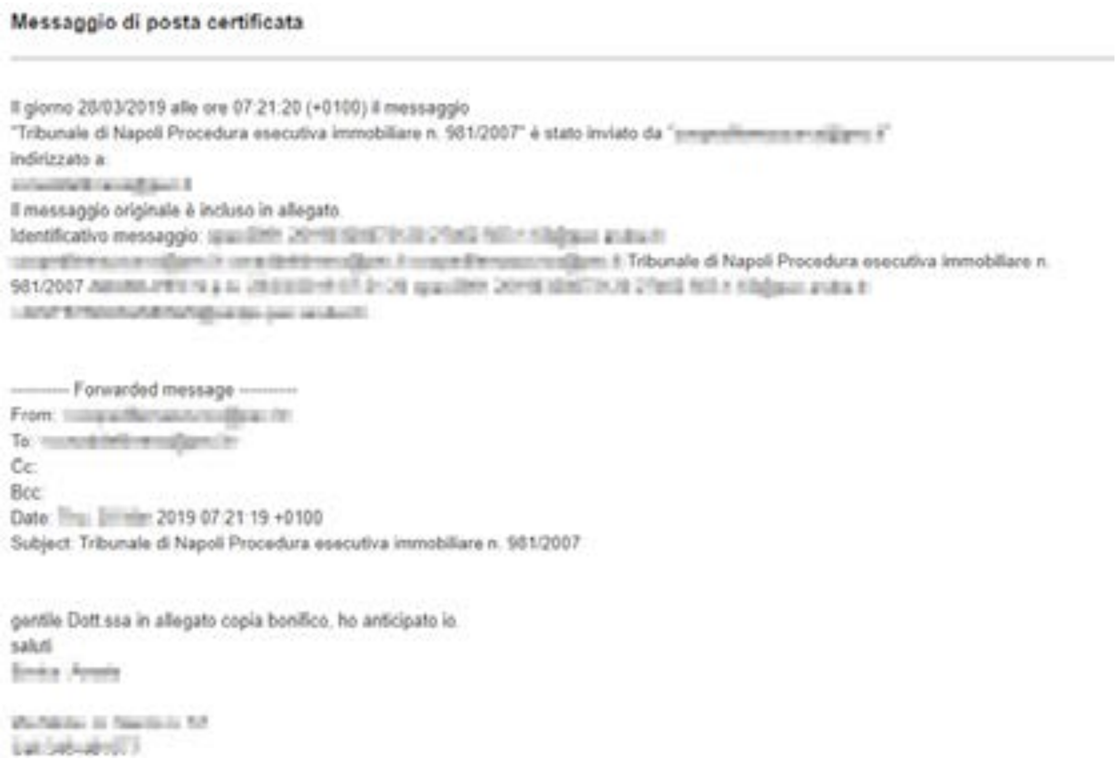
// Certified email campaigns

During the month of March, a phishing email campaign was carried out using Certified emails (known as PEC in Italy). The attack was carried out through a malicious attachment, whose purposes were twofold:

- to compromise the recipient's Certified email inbox, so as to be able to step up the attack by means of a new "clean" channel;
- to compromise the host on which the attachment is executed, so as to be able to launch a persistent attack and obtain further information on the attacked environment.

Figure 8

Certified emails campaigns



Messaggio di posta certificata

Il giorno 28/03/2019 alle ore 07:21:20 (+0100) il messaggio
"Tribunale di Napoli Procedura esecutiva immobiliare n. 981/2007" è stato inviato da "[redacted]"
indirizzato a:
[redacted]
Il messaggio originale è incluso in allegato.
Identificativo messaggio: [redacted]
[redacted] Tribunale di Napoli Procedura esecutiva immobiliare n.
981/2007 [redacted]
[redacted]

---------- Forwarded message ----------
From: [redacted]
To: [redacted]
Cc:
Bcc:
Date: [redacted] 2019 07:21:19 +0100
Subject: Tribunale di Napoli Procedura esecutiva immobiliare n. 981/2007

gentile Dott.ssa in allegato copia bonifico, ho anticipato io.
saluti
[redacted]

[redacted]

3. Qualitative analysis

Analytical framework of the attacks identified by Yarix SOC, based on the method illustrated

The information in this section traces the analytical framework of the attacks identified by the Yarix SOC, based on the method illustrated in the introduction.

3.1 Trend of the analyzed data

The first considerations regarding the three months analysed must take into account the limited time frame they refer to: as the analysis progresses and further quarterly reports are compiled by Yarix SOC, it will be possible to provide more in-depth information and include an overview covering the medium-long term.

The macro-trends identified by Yarix analysts are listed below.

// Trend 1

The number of events recorded from January to March 2019 does not show peaks or particular concentrations, and the curve is constant and continuous. The emergence of constant, uninterrupted cyber security events leads to the generally-accepted conclusion that cybercriminals no longer use impromptu attacks, neither in terms of the number nor method of attacks, but adopt a **systematic and industrialized** approach. The goal, in fact, is to reach a very large set of potential victims, with a minimum investment in terms of time and money.
This approach is exemplified by the large number of phishing campaigns that are very similar to each other: the same malicious email model can be used to convey different malware, with malicious executables that are can be easily found and utilised on the deep web. In other words, very often there is no need to “invent” anything and all the tools to perform a (potentially catastrophic) attack are available to anyone who is motivated enough.

// Trend 2

The second issue was identified using data collected by the Honeypot probes. They indicate that one of the potential points of entry to corporate networks resides in **vulnerable services which are not checked and regularly verified**. In particular, this can occur through services such as SSH or RDP, used respectively for authentication to Linux- and Windows-based machines.
The vulnerability represented by these types of services can be identified immediately by potential attackers, even using simple web indexing tools - such as Shodan - which perform continuous scans precisely to detect exposed services. Once these flaws are identified, the attackers have plenty of time to attempt brute force attacks or exploit known vulnerabilities of outdated protocols, in order to gain access to and compromise corporate systems.
Also the data related to the geolocation of the attacks support this analysis: Ireland appears to be in first place in terms of the number of security events due to there being one compromised

machine in this country which has then been incorporated into a botnet. This has resulted in a very high number of requests and subsequent drops of malicious executables.

// Trend 3

The third trend concerns the distribution of attacks on companies detected by the SOC, aggregated by production sector. The sector that suffers the most attacks is **manufacturing**, which represents an attractive target for cybercrime. The reasons are many:

- Despite the introduction of the GDPR protocols and the fact that some companies have started to tackle cybersecurity issues, the manufacturing sector continues to be somewhat insensitive to the institutionalized implementation of structured IT security management methods within the company. Even the widespread perception that this sector has lower budgets and resources when compared to companies operating in the financial or banking sector influences their tendency to be the focus of cybercrime;
- Production environments, typical of manufacturing, make extensive use of ICS/SCADA systems, which are often outdated, vulnerable and consequently attractive. For a cyber criminal, gaining access to one of these systems means being able to cause unimaginable damage to the company. A breach of this type, in fact, involves not only the theft of sensitive data and information but can even jeopardize the operation itself and force a company to interrupt its normal business activities.

Based on the findings of the Yarix SOC, the ranking of the most affected sectors includes **Information Technology** and **Large-scale Retail Channels**.

While for the former the trend is in line with national statistics, for the latter the same considerations made for the manufacturing sector are valid. In the case of Large-scale Retail Channels, hackers also act through phishing attacks perpetrated against customers, with the creation of fake prizes or loyalty card portals.

Despite not appearing among the most affected sectors in the Yarix ranking, it should be emphasized that one of the areas most subject to attacks is certainly **the public sector and the public administration**. The real-world case study presented in the next section focuses on this case history.

4. Real case

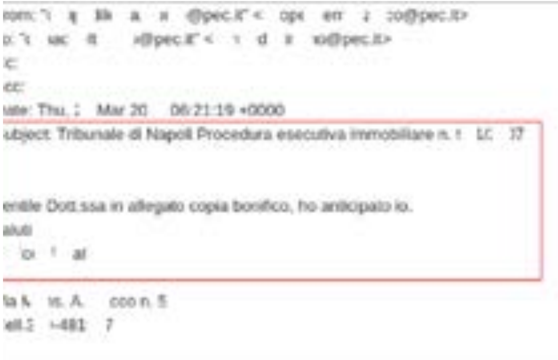
Towards the end of March, Public Administrations and businesses were subject to a major Spear Phishing attack

Towards the end of March, Public Administrations and businesses were subject to a major Spear Phishing attack: a new and more subtle version of the Gootkit malware which carried malicious content through Certified Electronic Mail (known as PEC in Italy).

The malware is spread through Spear Phishing emails sent via Certified Electronic Mail. By exploiting this communication channel, the attacker can trick the end user into trusting the message that is delivered to him, and he thus disregards the need to validate its authenticity. The email message delivered is similar to the one shown below. *(Fig 9)*

Figure 9

Email message using PEC (Certified email)



rom: [illegible] @pec.it" < [illegible] :o@pec.it>
o: [illegible] @pec.it" < [illegible] io@pec.it>
c:
cc:
ate: Thu, [illegible] Mar 20 06:21:19 +0000
ubject: Tribunale di Napoli Procedura esecutiva immobiliare n. [illegible]

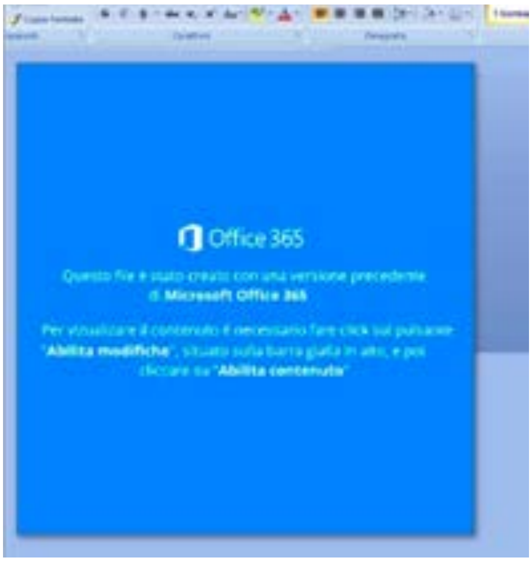
entile Dott.ssa in allegato copia bonifico, ho anticipato io.
aluti
[illegible]

[illegible] coo n. 5
ell.: +481 [illegible] 7

The email message informs the user of the payment, and the details for the bank transfer are attached to the email message. The attachment looks like a Word document, which in this case turns out to be "Tribunale_di_Napoli__Procedura_esecutiva_immobiliare_xxxx". Nested within the document there is active code (a macro), which is executed when the document is opened: the user is warned that in order to access the document itself it is necessary to enable the content for editing because of compatibility issues between different versions of Microsoft Word. The message the user sees is as as follows. *(Fig 10)*

Figure 10

Microsoft Office 365 alert



Office 365

Questo file è stato creato con una versione precedente di **Microsoft Office 365**

Per visualizzare il contenuto è necessario fare click sul pulsante "**Abilita modifiche**", situato sulla barra gialla in alto, e poi cliccare su "**Abilita contenuto**"

When the user clicks on *"Enable content",* Word immediately executes the code hidden within it.

This code, which is hidden and cannot be detected by classic antivirus software, has been analyzed by Yarix CERT. The technical details can be consulted in the report available here.

Of particular interest is the fact that the malware verifies the language that the user's user interface is set to, closing immediately when the detected language is "RU, UA, BY, CN", without further investigating further or conducting any further operations. This means that the devices of the nations mentioned above (Russia, Ukraine, Belarus and China) are immune to this type of compromise: it is likely that the origin of the executable is, therefore, to be traced back to one of these countries.

The purpose of the attack is to take complete control of the infected device via communication with the command and control centre (C&C). The compromised machine connects to the C&C to receive new code to execute or to send sensitive information entered by the user, such as passwords or sensitive data which can be used later for blackmail or targeted attacks.

5. Conclusions

The first quarterly report produced by the Yarix SOC provides details of constant and ongoing risk situation, in line with the threat landscape encountered nationally by Italian companies and institutions

The first quarterly report produced by the Yarix SOC provides details of constant and ongoing risk situation, in line with the threat landscape encountered nationally by Italian companies and institutions. The latter contribute indirectly to an increase in the overall vulnerability of systems nationally, because they do not erect adequate defensive barriers between their computer networks and cyber criminals.

The countermeasures to be adopted are many, ranging from increasing user awareness of the threats faced, and the choice of services used to support internal resources in the administration of threat detection activities and how they are managed. These are now indispensable tools for any public or private organization, regardless of the sector or size of the organisation.

The issue of **increasing user awareness** greatly enhances the level of protection of the corporate infrastructure, since, as highlighted in the report, emails remain the main vector of the attacks perpetrated. The ability of the recipient to recognize a malicious or phishing email and the provision of appropriate internal mailboxes for reporting suspicious emails can be the first step to increase the level of computer security.

Equally important is the ability to have a deeper understanding of the events that take place within an organisation and the recording of this information on a **dedicated, centralized platform**. These platforms (SIEM) are able to collect information from the various sources, but they can do more than this: they have a correlation engine, which is able to collate the collected data and provide alerts if abnormal activities are detected within the infrastructure. The management of such alerts can be complicated from the point of view of the number of events and the tuning that must be performed in order to maintain a low level of false positives. The outsourcing of services of this type to an **external SOC** greatly reduces the load on internal staff and allows 24-hour monitoring of detected events, with immediate interventions if these prove necessary. In this way, it is possible to minimize the exposure of a company's operating environment to attacks coming from both outside and inside.

YARIX
a vargroup company