GLOBAL CYBER SECURITY CENTER

Newsletter

2019 January

Cyber Security is our mission

editorial

Security is not a cost!

Thanks to the provision of the Italian Data Protection Authority we know that a bank, relevant for the country system, has suffered an attack on infrastructure where the data of some account holder have been violated.
The attack was masked through a Tor network, consisted of trying out a huge number of logins with sequential codes and a static password. The interesting point was that this attempt in itself clumsy and technologically stupid has incredibly had a margin of success. Moreover, reading in the news we discover also that many customers adopt a weak password that the attackers have identified. Once again, the human factor plays a significant part in the logic of a cyber-attack.
Information security is a basic requirement for business success. For succeeding in business, we have to increase security awareness among all the employees, but the key factor is to raise the awareness level of senior management. In other words, we need a strong corporate cultures and organizational commitment on enhancing information security. The reason is that more organizations rely on data to survive in competitive markets, the more increasing becomes the need to maintain the confidentiality, availability, integrity and authenticity of information. Today again the prevailing view is that security produces costs, not profit. If we are not changing this way of thinking, we will realize soon that the cost of doing nothing will be very high. In many surveys, we are seeing that there are great deficiencies in the management of cyber-security, in particular often there is not enough commitment of the C levels.

We have to face with the reality that business today is based on networking. In the today's world we are not island, we are connected and soon always connected, if we are negligent on the information security management we risk failing in our business. All the activities related to information security issue have to be in line with the organization's business and the results imposed by them. C-level management must take commitment of these actions and provide the full support. This means that they have to understand the seriousness of the threat that information risks represent for the corporate assets. On top of that C-level have to control and ensure that all the middle management realizes the importance of this issue. Bear in mind that Information security policy represents, in the company, the position of senior management toward information security. Regarding that matter is really important that information security policy should be in the responsibility of some member of C-level.
So, information security is effective when there is a strong support and engagement of the C-level. They have to be involved and committed allocating the necessary funding to information security and responding without delay to new situations.

Enjoy your reading!

Nicola Sotira
General Manager GCSEC

events

Forum Software Industriale
Location: Milan, Italy
Date: February 6th, 2019
https://forumsoftwareindustriale.it/mostra-convengo/programma/

The first edition of Forum Software Industriale organized by Messe Frankfurt Italia and promoted by ANIE Automazione Gruppo Software will be held in Milan at the National Museum of Science and Technology "Leonardo da Vinci". Dedicated to industrial software technologies, it will deepen the benefits deriving from IT infrastructures in the process of digitizing companies. Forum Software Industriale will offer visitors the opportunity to update on the topics of convergence between Operational Technologies (OT) and Information Technology (IT), through conferences on Smart manufacturing, Virtual Manufacturing and Augmented Reality, Intelligent and Connected Product, and Industrial Cyber Security.

ITASEC19 – Italian Conference on Cybersecurity
Location: Pisa, Italy
Date: February 12-15, 2019
https://www.itasec.it/

The 2019 edition will take place in *Pisa;* it will gather Italian researchers and professionals working in the field of cybersecurity, from both private and public sectors and include academia, industries, research institutions, and government.

Global Cyber Security Summit
Location: London, UK
Date: February 27, 2019
https://skytopstrategies.com/global-cyber-security-summit-2018-uk/

The focus for this full-day program will be centered around strategic innovation in the war against cyber attacks — specifically addressing how cyber resilience will require an integrated approach across organizational

in this issue

The main cyber threats of 2018. A forecast trend in continuous and unstoppable growth
by Marco Fiore – GCSEC

The main cyber threats of 2018. A forecast trend in continuous and unstoppable growth

by Marco Fiore – GCSEC

Although two years ago, 2017, many have talked about the worst year for cybersecurity, 2018 confirmed the fear that many had. The past year has been even worse than the previous one and it has been called as "The black year" for cybersecurity.

The growing trends, year by year, in terms of cyberattacks reflect the technological evolution that nowadays represents an inevitable step towards a very necessary future. Following the lead of 2018, the considerable "Collection # 1" attack made it clear that 2019 will not be better. The violation has, in fact, affected 773 million accounts.

The main concern therefore is given by the increasing number of attacks and by the impacts on companies, private or public, clear signals of an unpreparedness or serious inattentions. The paradigm of the "Risk = 0", utopistically pursued and continuously sought to innovation and prevention, is a condition that currently dominates the IT security sector.

Clusit[1], the Italian Association for Information Security, in its annual report claims that in the first half of the year (2018) "cyber-attacks in Italy have increased by 31% compared to last year" (2017).

The statistical growth of attacks certainly has been influenced by important regulatory measures implemented by Member States of the EU. The most relevant example is certainly the GDPR regulation, specifically at articles 33 and 34 in reference to "data breaches" and the obligation to notify them to nationals Supervisory Authorities and data subjects.

In the Art.4 the GDPR, defines that in case of personal data breach, defines as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"[2], "the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent"[3], articles 33 and 34 build a very strict legal framework.

However, even if limited to personal data, notifications and its consequent communications have undergone an important change: the introduction of an obligatory and timely communication that imposes to all the victims of a breach, an explicit "statement" of the nature of the cyber-attack, the number of interested parties, categories and approximate the volume of data subjects, possible consequences of the violation of personal data as well as measures taken to mitigate any negative effects. This particular legal process has certainly contribute to increase the known statistic number of explicit violation of IT systems in the past few months.

According to the activity conducted against the cyber threat by the CNAIPIC, the Italian National Anti-Crime Center for the Protection of Critical Infrastructure of the Postal Police, the 2018 cyber- alerts to the critical national infrastructures doubled. The Center, numerically, handled 442 cyber-attacks on institutional sites and critical functions, along with addressing the role of public-private partnerships in bolstering cyber defenses across sectors.

[1] Italian Association for Information Security - Clusit - Report – Sept. 2018 – available at https://clusit.it/rapporto-clusit

[2] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 – Art. 4 - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 – Art. 33 - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

news

The first cyber threat to the #EU are the #malware for credential theft #CyberSecurity

https://www.difesaesicurezza.com/en/defence-and-security/the-first-cyber-threat-to-the-eu-are-the-malware-for-credential-theft/

FireEye cyber security expert Jens Monrad: The most dangerous cyber threat to the EU are malware for credential theft. In 2018, nearly 50 percent of all detected threats in Europe were within this category

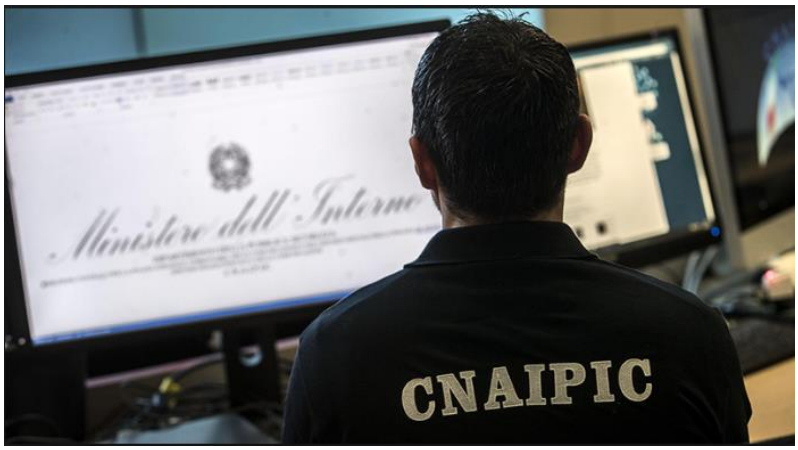
The most dangerous cyber threat in Europe are the malware for credential theft. It was highlighted by the FireEye cyber security expert, Jens Monrad. In a blog post on the company he explained that from 1 January to 31 December 2018 almost 50% of cyber threats detected, linked to the Old Continent, are part of the credential theft malware category. According to the expert, this is a global problem, but the organizations most at risk are those in the EU. This is due to a number of reasons, among which the constant long-term focus of the European Union on digitization. The initiatives in this sense focus on a variety of categories, ranging from ensuring high-speed connectivity for EU citizens to the way they interact with their governments, as well as the possibilities for European businesses and citizens to do business online.

SmokeLoader malware downloader enters list of most wanted malware

https://www.helpnetsecurity.com/2019/01/15/smokeloader-malware-downloader/

Check Point has published its latest Global Threat Index for December 2018. The index reveals that SmokeLoader, a second-stage downloader known to researchers since 2011, rose 11 places in December to enter the Index's top 10 at ninth place. After a surge of activity in the Ukraine and Japan, its global impact grew by 20. SmokeLoader is mainly used to load other malware, such as Trickbot Banker, AZORult Infostealer and Panda Banker. Cryptomining malware continues to lead the Index, with Coinhive retaining its number one position for the 13th month in a

IT infrastructures and 97 requests for cooperation within the "High Tech Crime Emergency" for a total of 68 investigations initiated and 15 people referred to prosecutor's offices.



According to the *Clusit "cybercrimes have increased in percentage terms in the first six months of this year"*:

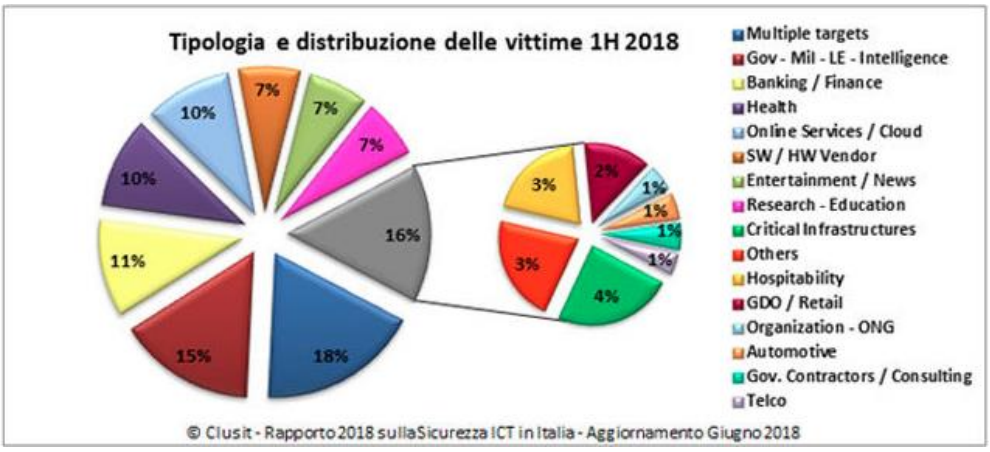
- + 200% in the" Automotive "sector,
- + 128% in "Research / Education" area,
- + 69% in "Hospitability" such as hotels, restaurants and residences suffered

Others relevant statistics:

- Healthcare sector (+ 62%)
- Institutions (+ 52%)
- Online services / Cloud (+ 52%)
- Consultancy sector (+ 50%)

The most significant change relates to the methods of attack is reklated to "*Multiple Targets attack*" with + 18% of the total global attacks. These serious attacks are carried out in parallel by the same group of attackers against numerous organizations, highlighting the "new industrial" methodology and the behaviour of cybercriminals.

"*More and more attacks* - commented Andrea Zapparoli Manzoni, member of the Clusit Steering Committee - *depends both from territorial constraints and type of targets. The increase of these attacks, perpetrated against a heterogeneous and geographically dispersed target on a global scale, demonstrates the ability, determination and organization of the attackers, who goal to maximize the economic result with a typical approach of organized crime*" indicating a new economic "*cyber-philosophy": "maximum result with minimum effort".*



Focusing on the international situation, it is interesting to report some of the most important attacks that marked 2018 on the international and national scene.

International Cyber-attacks:

1) **Panera.** An attack that has seen 37 million victims or all PaneraBread.com customer accounts. Names, e-mails, dates and the last four digits of customers' credit cards were in fact exposed and revealed in April 2018. The event was particularly singular. At first an expert noted irregularities in the system, warning the company of an important data leakage (presumably from August 2017). Despite the warning,

row and impacting 12% of organizations worldwide. XMRig was the second most prevalent malware with a global reach of 8%, closely followed by the JSEcoin miner in third with a global impact of 7%. Organizations continue to be targeted by cryptominers, despite an overall drop in value across all cryptocurrencies in 2018.

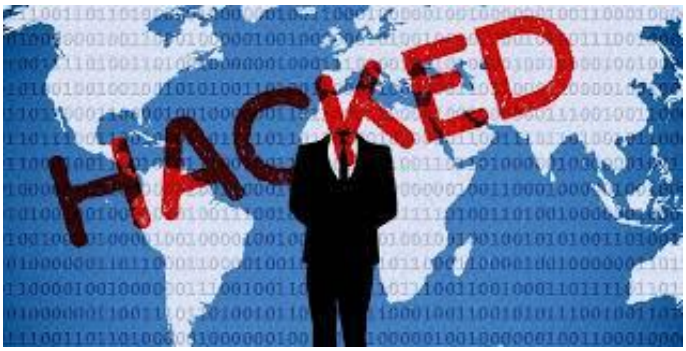
A flaw in vCard processing could allow hackers to compromise a Win PC
https://securityaffairs.co/wordpress/79907/hacking/vcard-win-hack.html
A security expert discovered a zero-day flaw in the processing of VCard files that could be exploited by a remote attacker to compromise a Windows PC
The security expert John Page (@hyp3rlinx), discovered a zero-day vulnerability in the processing of VCard files that could be exploited by a remote attacker, under certain conditions, to hack Windows PC. The expert reported the flaw to Microsoft via the Trend Micro's Zero Day Initiative (ZDI).
"This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Microsoft Windows. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file." reads the security advisory on ZDI.

The 773 Million Record "Collection #1" Data Breach
https://www.troyhunt.com/the-773-million-record-collection-1-data-reach
Many people will land on this page after learning that their email address has appeared in a data breach I've called "Collection #1". Most of them won't have a tech background or be familiar with the concept of credential stuffing so I'm going to write this post for the masses and link out to more detailed material for those who want to go deeper.
Let's start with the raw numbers because that's the headline, then I'll drill down into where it's from and what it's composed of. Collection #1 is a set of email addresses and passwords totalling 2,692,818,238 rows. It's made up of many different individual data breaches from literally thousands of different sources. (And yes, fellow techies, that's a sizeable amount more than a 32-bit integer can hold.)
In total, there are 1,160,253,228 unique combinations of email addresses and passwords. This is when treating the password as case sensitive but the email address as not case sensitive.

How Web Apps Can Turn Browser Extensions Into Backdoors
https://threatpost.com/web-apps-browser-extensions-backdoors/141061/
Researchers show how rogue web applications can be used to attack vulnerable browser extensions in a hack that gives adversaries access to private user data.

Panera did not take any countermeasures and 8 months later announced the massive subtraction of data by interrupting the service on its own site with obvious economic consequences for the company.

2) **Facebook - Cambridge Analytica.** Probably the most famous attacks but certainly not less serious than the others. About 87 million users have been exposed to a data theft. Lots of personal information has been making experts suppose, that this "attack" was used as an instrument to manipulate markets and international elections. In September 2018 personal profile information, political beliefs, networks of friends, private messages were acquired by Cambridge Analytica who illegally collected users' information without their permission. The violation took place a couple of years ago and only today we know the scope of the event.



3) **Newegg.** The attack has affected 50 million credit cards between August and September 2018. The Newegg is an e-commerce company whose site was hacked by cybergang Magecart. The hacker company injected a malicious code for credit cards in Newegg site and every time something was purchased, online attackers obtained all the payment information re-locating them directly to the Magecart control and command center (C&C).

4) **Elasticsearch.** This violation has had a good international resonance since it has affected many companies. 57 million consumers, 26 million companies for a total of 82 million victims. Lots of individual user data: names, email and physical addresses, phone numbers, IP addresses, employers and job titles were subtracted. From companies: names, company details, postal codes, carrier routes, customer geolocalization, census data, phone numbers, web addresses, e-mail addresses, number of employees, NAICS codes, SIC codes and many more. As in the case of Panera, the system vulnerability was detected by a researcher who highlighted some suspicious registrations. It is not known how long the databases have been exposed and left unattended. From the investigations carried out, it is thought that the liability is of a third company that collaborated with the owner. (In this case has not applied the appropriate security protocols to ensure adequate protection).

5) **MyHeritage.** 92 million victims. In the June 2018 account, email addresses and password hashes have been the subject of a real "password massacre". The company has communicated to its users that account holders who registered at portal before 26 October 2017 have been exposed to an important attack and therefore suggested to change their passwords.

6) **Quora.** 100 million victims. Names, email addresses, password hashes, profile data, public and non-public actions were under attack. Discovered in December 2018, the company maintained a decidedly vague reserve, limiting itself to declaring that a third party obtained unauthorized access to one of its systems.

7) **British Airways.** By the media, one of the most important events. The British Airways airline has suffered the theft of 380 thousand customers data: name, phone number, address and payment details. The customers involved have been contacted directly by the company.

8) **Cathay Pacific.** The number of compromised accounts rises to 9.6 million in the last 25th of October. identification data have been stolen, as well as information on the trips made by costumers. Credit cards should have remained safe, but to date there is still no assurance.

9) **Google+** has been talking about itself on two separate events. The first for the exposure of 500 thousand accounts, the second much more serious for a total of 52.5 million accounts exposed. In both cases it was a bug whose negative effects seem to be only potential, but the company has reported, in both cases, that it has not found signs of abuse. Google has decided to close the social network.

10) **Marriott Hotel.** 500 million people data were stolen including sensitive data and credit cards numbers. According to the New York Times it is an operation sponsored by the Chinese government.

Researchers have added another reason to be suspicious of web browser extensions. According to a recently published academic report, various Chrome, Firefox and Opera browser extensions can be compromised by an adversary that can steal sensitive browser data and plant arbitrary files on targeted systems.

"We identified a good number of extensions that can be exploited by web applications to benefit from their privileged capabilities," wrote Université Côte d'Azur researcher Dolière Francis Somé, in an academic paper titled Empowering Web Applications with Browser Extensions (PDF).

Phobos, the new ransomware of Dharma Group, infects hundreds of organizations

https://www.securitynewspaper.com/2019/01/22/phobos-the-new-ransomware-of-dharma-group-infects-hundreds-of-organizations/

A new ransomware called Phobos is infecting devices and networks in a massive way

A group of hackers is finding remote access to networks of different organizations to distribute new variants of ransomware. According network security and ethical hacking experts from the International Institute of Cyber Security, attackers are also infecting sites that share cracked versions of commercial software to spread the ransomware. Hackers have been remotely accessing enterprise networks to infect PCs, shared networks and virtual infrastructure with a ransomware called Phobos, as commented by network security specialists. In addition, attackers continue to distribute variants of STOP ransomware through adware embedded in some "cracked software" sites.

Although many hackers abandoned the use of ransomware attacks to engage themselves in other malicious activities, such as the cryptojacking, some cybercriminals gangs continue to dedicate themselves to distributing encryption software.

New malware campaign distributing Ursnif banking trojan uses fileless technique

https://cyware.com/news/new-malware-campaign-distributing-ursnif-banking-trojan-uses-fileless-technique-15e7b5ff

The new malware campaign distributing Ursnif banking Trojan uses PowerShell to achieve fileless persistence to avoid detection.

This malware campaign uses an already well-known payload delivery method which employs Microsoft Word documents containing a malicious VBA macro.

Cisco's Advanced Malware Protection (AMP) Exploit Prevention engine detected a new malware campaign distributing the Ursnif banking Trojan. It uncovered that the malware campaign uses Powershell to achieve fileless persistence to avoid detection from antimalware solutions.

Ursnif trojan also known as Gozi ISFB, is a variant of the original Gozi banking Trojan, which leaked its source code online in 2014.

11) **Under Armor.** 150 million victims of the MyFitnessPal app in the period between February and March 2018. The theft involved the company's food and nutrition app, opening up sensitive information to but not payment information.

12) **Exactis.** In June 2018, 230 million consumers and 110 million businesses were victims of an important attack. 2 terabytes of Exactis company data collection, including phone number data, e-mail addresses and physical addresses, interests, ages, religions, pet ownership, etc., has been transferred on a public site. It is not known who or how many people had access to this information before the attack was discovered.

13) **Starwood.** 500 million. The number of victims would be enough to make people talk about. Discovered on 10 September 2018, the attack may have continued since 2014. Names, email addresses and physical, telephone numbers, passport numbers, account information, dates of birth, sex orientation, travel information and accommodation information were stolen by hackers. Some of the violated information also included credit card information with hashes.

14) **Aadhaar**. 1.1 billion accounts violated. From 2017 and January 2018 private information on Indian residents, including names, their 12-digit ID numbers and others information such as bank accounts have been subtracted. the ID database of the Indian government, which stores citizens' identities and biometric information, had "a data leak on a system operated by a state service company called Indane". Indane had not protected efficiently its own application programming interface (API), which is used to access the general database giving to anyone the possibility to access to Aadhaar's database.

15) The **773 Million Record "Collection #1"** Data Breach is a set of email addresses and passwords totaling 2,692,818,238 rows. It's made up of many different individual data breaches from literally thousands of different sources. In total, there are 1,160,253,228 unique combinations of email addresses and passwords, 772,904,991 unique email addresses and 21,222,975 unique passwords. The first massive 2019 attack is projected in the first position of the most important data leaks ever completed.

Italy does not seem to have been otherwise immune to cyber-attacks.

Here are some of the most important and well-known cases that have affected Italian authorities and some Italian companies.

However, it is worth mentioning the valuable work of some of these companies that have taken important preventive countermeasures to mitigate the damage, making attacks not completely effective.

Only in May 2018 Cyber-attacks in Italy have touched the threshold of 140-per-day.

1) In March 2018 and October, a hacker group called **LulzSecITA** and **AntiSecurityITA** published thousands of e-mail addresses for schools and teachers on its portal. Ministry of Education, University and Research, specified: "The published data are not related to components of the IT systems of the MIUR. In particular no data has been stolen from the systems that manage access to the domains of @formazione.it. The published data of the other server @istruzione.it, shows that of 6,163 email addresses, 4,565 are not active and 1,598 are active ".
2) **AnonymousIT**. According to experts the attacks, divided, published and claimed in the first week of November (when Guy Fawkes is celebrated in the UK and iconized as a cult movie character "*V for Vendetta*"), are probably the result of a huge planned and operated work. The activists(as they define themselves) have put online: data, names, surnames, emails, passwords and telephone numbers of employees of various CNR institutes, some databases of the Ministry of Economic Development (Equitalia), data from the State Archives and personal data of members of italian political parties like "Lega Nord"," Fratelli d'Italia" and "Partito Democratico" data from Archivio di Stato di Palermo and Associazione Polizia di Stato Association (Assopolizia), personal data of Universities and training centers and data of an important multinational bottled water company.
3) The same hacker group, **Anonymous**, has targeted public institutions and research institutes. Probably the most impressive and important attack that the entire national infrastructure has ever suffered. On November 22, the newspapers titled: "*A vulnerability in the Telecom servers that handle thousands of certified electronic emails of judges and the telematic services of Italian courts has brought the entire Italian civil justice to its knees*". 500 thousand certified electronic mails were violated.

   98,000 users 'pec identification have been the subject of a very serious cyber-attack in particular among magistrates, military and CISR officials, the Interministerial Committee for the Security of the Republic (which includes the Department of Justice, Department of Interior, the Defense, the Foreign Affairs, Department of Economy and Economic Development, the Presidency of the Council of Ministers and the Delegated Authority.
4) **Italian Healthcare** has had as many problems as well. Many healthcare institutions suffered a very important cyber-attack that exposed millions of data. Among the victims: the ASL of Rieti and Viterbo, (on whose sites appeared a photo that depicts a "*political revisiting*" of Christian nativity scene), the Higher Institute of Healthcare, the National Agency for Regional Health Services (Agenas), Federfarma, San Giovanni Hospital in Rome, Difarma (a company of pharmaceutical products), the ASL of Caserta, the Azienda Agricola Lariana (Lake Como) and the local Healthcare unit of Legnano (Milan). In economic terms no damage estimates have been made but it is assumed that this attack brings about several million-euro damages.
5) **Saipem**. More than 400 servers were assaulted by unknown hackers. The attack through a variant of malware called "*Shamoon*", hit servers based in the Middle East:United Arab Emirates and Saudi Arabia and India, Aberdeen and Italy. The company announced in a public statement that the affected servers did not suffer any data loss due to the attack

allowing Saipem to proceed with restoring backups of its compromised systems.

6) **Automotive Company**. Two cybersecurity companies were charged as analysts to study and prevent an attack called ROMA225. Despite the unusual malware's name, the event was going to ruin the Christmas holidays to the two important automotive Italian companies. Fortunately, the malware has been unmasked before it could infect all the company's computers systems.
7) The famous Company **Unicredit** have been data attacked by unknown on October 21, 2018. Hackers tried to force the home banking online system and breached 6.859 user (customer identification code) and REB (identification code for access to the Multi-channel Bank service). The attack was promptly intercepted and blocked and the incident was closed and terminated. The event was notified to the Italian Privacy Authority that "*ordered to Unicredit to contact all interested parties*". Few days ago, the deadline of 30 days for notifying interested parties has expired and the company assures that currently "*a mechanism is being implemented to force the use of complex passwords*"**.**

The McAfee™ report helps us define exponentially growing trends; in particular in December 2018 the company has reported a constant increase in cryptomining. After growing by about 400,000 units in the fourth quarter of 2017, the new cryptomining malware increased by an astonishing 629%, settling at over 2.9 million samples in the first quarter of 2018 and "*recorded a boom growth of +86% in the second quarter of 2018. Among the most aggressive threats, moreover, are the malware designed to exploit the vulnerabilities to be patched, at + 151%, and the attacks on mobile devices, which recorded a + 27, growing for the second quarter in a row* ".

In 2018 phishing attacks are grown exploiting all the possible channels, from e-mails, to social networks, to instant messaging, manipulating the new social engineering techniques simultaneously and more effectively.

The Italian **Clusit** report (Association for Italian Cyber Security) defines 2018 as "*the year of the triumph of Malware, of the industrialized attacks carried out on a planetary scale against multiple targets and of the definitive descent into the field of States as threatening actors*". From this small declaration, there is an important change.

Attacks are increasing and there are treacherous protagonists: individual states with their economic and political interests. Nations, indeed, understood that information and intelligence moved on a more "*immaterial*" level. These new protagonists have turned from the condition of passive subjects into real active threat actors. Examples are the continuous intrusion, destabilization and surveillance of intelligence departments of specific states against others.

Without falling into conspiracy theories, it is good to analytically report some of statistic data that have affected the national scene and the main trends of future attacks.

Andrea Zapparoli Manzoni of the Clusit Steering Committee, reports in the work of the Association for Information Security that "*the use of vulnerabilities*" 0-day "*grows by 140% compared to the last six months of 2017 (and it is a figure obtained from the number of accidents known limited and therefore probably underestimated). The category of APT (Advanced Persistent Threat) increases instead of 48%.*"

However, the simple malware remains the most used attack vector, which is the cause of 40% of the total attacks. This technique marks an increase of 22% in the first six months of this year (2018 n.d.r.) compared to 2017. Ransomware and Cryptominers represent today 43% of "simple malware" used by cybercriminals. In particular, the Cryptominers, almost non-existent until 2016, were used in the first half of the year in 22% of the attacks carried out through malware (they were 7% in 2017), slightly exceeding the Ransomware (+ 21%), demonstration of the dynamism of the attackers, able to create new threats

and change "business model".

According to the Clusit Report 2018, also Phishing and Social Engineering techniques are increasing in number by 22% in the first six months of this year.

"*Given that in our sample we analyze particularly serious attacks against leading global organizations, it is staggering that the sum of the most trivial attack techniques, such as SQLi, DDoS, known vulnerabilities, phishing and simple malware, still accounts for 61% of the total. It means that the attackers succeed in making successful attacks against victims theoretically structured with relative simplicity and at very low costs, moreover decreasing. And this is one of the most worrying considerations among those that emerge from our research*".

Some others important derivations of phishing are the "*Business Email Compromise*" and the "*Spoofing*", two of the most used e-mail scams to carry all kinds of malware, including ransomwares. We can point out also an increase of *Cryptojacking*, the process by which a device is illegally exploited by criminals that statistically shows no sign of slowing down.

Vulnerabilities of new devices, in particular IoT and domotic device, would be subject to potential and specific cyber-attacks (I.e. Alexa,Google Mini). Creation of dedicated cryptomining networks will be another problem to deal with.

The picture outlined above is obviously surrounded by a constant connection with privacy and data protection concomitant with the new and strict rules on PSD2 payments, Blockchain strategy and Cloud Services.

It's now ever necessary ask if companies and the most important national and international infrastructures, administrations and governments are ready to implement effectively their security architectures to prevent those new threats.

Quoting the famous "*British Cicero*" Edmund Burke " *Early and provident fear is the mother of safety (1792) because in that state of things the mind is firm and collected, and the judgment unembarrassed. But when the fear and the evil feared come on together, and press at once upon us, deliberation itself is ruinous, which saves upon all other occasions; because, when perils are instant, it delays decision; the man is in a flutter, and in a hurry, and his judgment is gone* ";

the constant fear of the sudden progress made in cyberwar by hackers and activists, protagonists of an increasingly asymmetric war, should stimulate innovation and technological progress both in terms of system security and scientific research. It is therefore necessary for companies and entire Nations invest on Cybersecurity.

Technological progress in cyber world must become a fundamental priority and important investments must be made in order to prevent collateral damage that can bring the entire economy to its knees.

CERT STAR

PROGRAM

CERT STAR is a program of closed meetings dedicated to **CERTs and SOCs** aimed to enhance competences, improve cooperation and experiences exchange.

During the meetings, core security topics like threat hunting, incident prevention and response, intelligence and digital forensics are analysed at technical operational level. Meetings include practical exercises and use of tools and instruments.

2019 Calendar

04 April - Dark web intelligence
11 June - Threat intelligence and Digital forensics
12 September – Application Security
07 November - MISP: insert, classify and share IoC with other parties
03 December - Meeting with executive

Location

Hotel Radisson Blue – Via Filippo Turati, 171Roma

For more information send an email to info@gcsec.org