CertIST

Industrie Services Tertiaire

Annual Report on Attacks and Vulnerabilities seen in 2018

Released on April 2019

Table of contents

1. Introduction

Every year the Cert-IST is producing an annual assessment of the past year to highlight the general tendencies and threat evolution, and help the community to enhance their protections.

The report will begin with a summary of 2018 major security events (chapter 2). From there we will then focus on the key trends and analyze them (chapter 3). Apart from these events we will remind the recurrent threats on which, ones should stay attentive to (chapter 4).

We will also explore the Cert-IST activity throughout 2018 (chapter 5).

Finally, we will conclude this report with a short summary of the current cyber-threat landscape and the future challenges companies will have to face.

- **Few words about Cert-IST**

Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam for **I**ndustry, **S**ervices and **T**ertiary sector) is a threat alert and response center for corporations. Created in 1999, it helps its members to identify potential threats by continually analyzing the last vulnerabilities, their according severity and the possible mitigations. In the event of a cyber crisis targeting its member, Cert-IST's role is to help during the incident investigations to allow a fast "back to normal" situation.

2. What happened in 2018?

The following table summarizes the key events of 2018. You will find events which were highly mediatized (sometime on controversial topics, like in October 2018 with the Supermicro hardware hacked case) or more generally because these events are considered as major indicators of the cyber threat evolution.

January 2018	**Spectre and Meltdown** public disclosure. During the following three months, many patches (for processors, OS, web browsers) will be released to fix these issues, showing the difficulty in the handling such low-level flaws. We will further develop this subject in chapter 3.3.
January 2018	The smartphone application **Strava** (a GPS cycling and running app) disclosed location of secret US army bases.
February 2018	GitLeaks (a search engine for exposed credentials on GitHub, Bitbucket…) & BuckHacker.com (a search tool letting users trawl through unsecure AWS buckets) are published: more and more tools are available to find **unprotected or misconfigured**

	Cloud infrastructures which keep growing in numbers. To counter this trend, Amazon gives free access to its "S3 Bucket Permissions Check tool".
February 2018	The **Olympic Destroyer** malware (slightly) disturbed the Winter Olympic Games opening ceremonies hosted in South Korea. This is the first malware containing **very sophisticated false flags** to lure the threat hunters during their investigation and attack attribution.
February 2018	New **DDoS amplification** attack vector taking advantage of unprotected **Memcached** servers peaked at 1.3 Tbps during attacks towards OVH and GitHub.
March 2018	**www.cert.org** (aka CERT/CC) it's over! Created in 1988 following the discovery of the Morris' worm. It was the very first CERT (created and managed by the SEI) and it started declining after US-CERT establishment in 2006.
March 2018	**Trustico**'s (SSL certificates provider) sinking after publicly revealing that it kept a copy of the customers' SSL certificates private keys.
March 2018	Taking advantage of the Spectre/Meltdown media hype, CTS-lab released an alarmist report (and created a dedicated website AMDflaws.com) regarding new **AMD processors vulnerabilities**. This communication has been deeply criticized by the Cybersecurity community.
March 2018	Multiplications of new techniques to **lure AI systems**.
March 2018	Revelation that the **Triton** malware (discovered in late 2017, and targeting secure automated Schneider Triconex industrial systems) has been created to cause an explosion of a petrochemical company based in Saudi Arabia. Initially attributed to Iran, this attack was later on (October 2018) attributed to Russia.
March 2018	**SamSam** ransomware demands $50,000 (6 bitcoins at that time) to the city of Atlanta. Ransomware are evolving: instead of randomly asking for a 0.1BTC ransom, cyber crooks are now targeting large companies and asking for higher ransoms. This trend intensified from mid-2018 with the appearance of **Ryuk** malware which a variant (**LockerGoga**) impacted Altran in the beginning of 2019.
March 2018	**Facebook** faced its first media scandal with **Cambridge Analytica** (about 2016 US electoral campaign). In September the **"View as" bug** could allow a data breach impacting almost 50 Million accounts, in December another bug exposed private photos of almost 6.8 million users. A more complete review of this difficult year that Facebook faced is available in this report.
April 2018	"Don't mess with our elections…": this is the message **American patriotic hackers** displayed on 200 000 unprotected Cisco devices, mostly in Iran and Russia. This vulnerability is probably linked with the one cited below about Cisco Smart Install (SMI).

April 2018	US-CERT published TA18-106A alert regarding **attacks targeting unprotected routers conducted by Russia**. These attacks mostly used known vulnerabilities in Cisco Smart Install (SMI) and unprotected SNMP accesses.
April 2018	**Drupalgeddon2** (Drupal Armageddon 2) ahead!: two critical flaws corrected in Drupal CMS lead to massive attacks against unpatched Drupal servers during the following months.
May 2018	**EFAIL** vulnerabilities in **OpenPGP**, S/MIME and email clients.
May 2018	**MEWkit** (MyEtherWallet-Kit): a **BGP hijacking** attack leading up to traffic rerouting during many hours (traffic intended to Amazon Route 53 DNS servers).
May 2018	Early publication of Cisco TALOS regarding **VPNFilter** malware which infects unprotected networking devices. Cisco assumes that VPNFilter is originated from Russia and decided to release it now because they fear VPNFilter could soon be used in a large scale attack against Ukraine.
May 2018	**GDPR** comes into force in all EU countries. As of 10/16/2018, the French CNIL organization has received 742 GDPR notifications (in 7 months), an average of 7 notifications per day. In the meantime GDPR scams are emerging (see § 4.1).
June 2018	**Docker attacks:** malicious Docker images uploaded on Docker Hub are targeting vulnerable Docker environments. For more information, refers to our article on this subject. This type of attacks has been observed again in October.
June 2018	European Parliament suggests to exclude and ban programs like **Kaspersky** anti-virus. The concern is that Russian secret services may use Kaspersky for spying operations. USA already made similar recommendations in September 2017.
July 2018	"**Sextorsion**" scams: the attacker emails victims for a ransom, claiming to have taken videos while the victims visited a pornographic website. These scams will be seen several times over the second Half of 2018 (see the according Cisco Talos report).
July 2018	Increase of **"SIM swap"** (or "SIM hijack") attacks which allow hackers to steal existing (Instagram, Twitter…) accounts by taking the victim's phone number. This also highlights 2FA authentication bypass if this latter is based on received text message codes.
July 2018	**Massive Singapore SingHealth hospital hack** impacting 1.5 million patients, including the prime minister medical prescriptions. The attack sophistication suggests it is state-sponsored. The final report has been release on January 2019.
September 2018	**British Airways** has been the victim of a MageCart's attack which infected their payment website system leading to 380,000 victims in 2 weeks (from August 21th to September 5th). For several months "MageCart" attacks multiply. Some of them are targeting software suppliers to infect all E-commerce websites which rely on these supplier software; It was the case for TicketMaster in July 2018. This news illustrates

	two main trends of 2018: bank attacks (see Chapter 3.4) and attacks via suppliers (see Chapter 3.6).
September 2018	**LoJax:** the first-ever UEFI rootkit being used in the wild during a malware campaign conducted by APT28 Russian group (Sofacy).
September 2018	In the context of the **NIS European directive** France released its security rules to be applied by OES (Operators of Essential Services). A first list of 122 OES is established in early November. In the future this list should contains hundreds of French organisms.
October 2018	Bloomberg newspaper published an article about **tiny spying chips** added by **China to Supermicro motherboards** to infiltrate U.S companies like Apple or Amazon. Everyone denied this assumption. The idea of adding a spying chip does not seem to be technically difficult. However, a large-scale trapping of electronic components would be a first.
October 2018	US-CERT published a note to warn about **APT attacks targeting IT Service Provider customers**. In a webinar entitled "Chinese Cyber Activity Targeting Managed Service Provider" US-CERT reveals that these **Cloud Hopper** dubbed attacks appeared in 2014, rocketed up in 2016 and are still active.
November 2018	More than 50,000 vulnerable printers are hacked to print out flyers telling people to subscribe to **PewDiePie**'s YouTube channel. According to the author of this joke, over 800,000 printers are vulnerable and could have been used to spread these flyers.
November 2018	**Moscow's new cable car system** interrupted due to a ransomware infection.
November 2018	**Marriott hotels** revealed a massive data breach on their **Starwood hotels** reservation databases: 500 million guest booking and unauthorized access to the Starwood network since 2014.
December 2018	**Shamoon,** a destructive malware discovered in 2012 in Saudi Arabia (Saudi Aramco incident) re-appeared in Europe with V3: in Italy (Saipem incident), Netherlands and France.
December 2018	Amnesty International published an article describing for the first time, real attacks bypassing 2FA (using MiTM – Man In The Middle technique). These attacks **bypass common forms of two-factor authentication** (text message-based and OTP-based such as Google Authenticator, Authy, Duo…).
December 2018	Several reports about the Russian IRA (**Internet Research Agency**, also called the "troll factory" of Russian government) describe Russian disinformation campaigns taking advantage of social networks to influence 2016 US election.

3. Analysis of 2018 key trends

3.1. Few events that stand out this year

In this first section, like in an award ceremony, we will reveal the TOP vulnerabilities and most active malware of 2018.

- **Novelty of the year: Meltdown & Spectre**

We will further develop this in chapter 3.3, Meltdown and Spectre vulnerabilities discovery is one of the major event of this year.

- **Botnet of the year: Emotet**

Emotet (also known as Geodo or Feodo) has been the most active botnet in 2018. This malware exists since 2014 and was at the beginning a banking malware ("banker") which infects personal computer to steal banking credentials. Emotet has since evolved to become a "downloader" (aka MDS: "Malware Distribution System" or sometime "Malware Delivery Service"). Cybercriminals who control Emotet-infected computers are selling to other crooks a service to spread certain malwares (by creating spam campaigns spreading malicious e-mails) or to even install a certain malware directly on botnet machines.

- **Payload of the year: Cryptominer**

To get money a cyber crook needs to define his business-model: he can either sell his services to other crooks, e.g. with an MDS service as described above, or he can decide to steal the money from infected users, like in 2016 with several crypto-ransomware attacks where the attacker encrypts user data and request a ransom for the decryption. In 2018 however, the most seen model is cryptominers we will further detail in chapter 3.8.

- **Vulnerability of the year: Java deserialization**

Deserialization is the process of importing a Java object into an application. In the case of an application vulnerable to a deserialization flaw, a malicious Java object could force the deserialization engine to execute arbitrary code. This type of vulnerability has been discovered in 2006 but became especially active in 2017 and 2018. Deserialization is rank n°8 in the TOP-10 OWASP and listed CWE-502 in MITRE's dictionary. This vulnerability does not only affects Java: PHP, .NET and Ruby are also concerned.

Following is a list of web applications which have been affected this year; almost all the major JAVA web frameworks are listed!: CVE-2018-15957 (**ColdFusion**), CVE-2018-1567 (**WebSphere**), CVE-2018-3245 (**WebLogic**), CVE-2018-14667 (**JBoss**), CVE-2018-8421 (**SharePoint**).

3.2. Could GDPR be THE solution to the numerous data leaks?

Since many years the number of attacks and amount of data-leaks are constantly increasing. To such an extent where these types of incidents are not surprising anymore, except when a new leak exceed by numbers all the previous ones.

If we take a closer look at these data leaks (caused accidentally or due to a cyberattack) we can classify them into three different categories:

- Inefficient data protection,
- Protected data, but a new flaw has been discovered in the protection mechanism,

- Sophisticated attack bypassing the protection mechanisms.

In some cases data could also be unprotected. Nevertheless, the most common situation is when the protection have been set up in the beginning and finally became vulnerable few years later. Maintaining a constant level of security is crucial and is a key objective. It must take into account:

- New vulnerabilities discovered (are we up to date in terms of security patches?)
- The evolution of technologies and attack techniques (e.g.: Are our Amazon S3 servers correctly configured?)

GDPR enforcement will surely improve the security level of applications processing personal data (almost all applications). Consequently this should decrease the number of data leaks, but it is still difficult to evaluate how long it will take to produce observable results.

3.3. Spectre and Meltdown: time to apply firmware patches

In January 2018, **Spectre** and **Meltdown** attacks have brought to light a new type of attacks: attack against the **speculative execution** mechanisms of micro-processors. This is a processor internal mechanism, thus requiring a firmware patch (an update of processor's micro-code) to be protected from these vulnerabilities.

It is not the first time that low level attacks are requiring this type of updates (e.g. Intel AMT in May 2017 or Row Hammer in 2015) however, this time targeted products are very common (Intel CPU). Firmware update is a complex operation for a company, because deployed tools are not designed for this kind of operations, hence firmware update is often an unusual operation.

Takeaway regarding Spectre and Meltdown crisis:

- **Complexity of patches** (3 different levels of patches have been published: patches for web-browsers, operating systems and processor firmware) and the instability induced by certain patches (incompatibility with particular antivirus software, lack of reliability of certain Intel patches, possible impacts on performances).
- **Difficulty to determine how urgent** it is to deploy these patches. At first, given the severity of the vulnerabilities, deploying those patches seemed critical. However, the absence of real attacks and the complexity of deploying those patches led to reconsiderations.

Vulnerability management remains a complex activity where you have to deal with incomplete patches and risks of attacks which are difficult to evaluate and often over-mediatized. It is then important to gather the most factual pieces of information available and this is what we aim to provide through Cert-IST's publications. In the Spectre and Meltdown case, we assessed the vulnerabilities at medium risk (because the impact was "only" stolen data) and the risk of an attack remained at a "yellow level" (the lowest of the three possible alert levels). These are simply metrics which may be far from perfect but they are based on rational criteria and must be taken into account to moderate the media boom that cyber events now tend to produce.

3.4. New attacks targeting banks

Between 2010 to 2016 new techniques targeting banks or payment terminals emerged. Below, is an excerpt of our December 2018 monthly bulletin which describes these new techniques. 2018 is for us a turning point for bank attacks, because:

- The number of these new attacks increased significantly,
- There is a gradual geographical expansion of the targets. Initially, the attacks mostly targeted Russian satellite countries, Southeast Asia and South America; today, they seem to be spreading to the rest of the world and especially in Europe and the United States.

Extract from the article published in Cert-IST bulletin of December 2018

- **Jackspotting:**

This is a technique for attacking ATMs in order to make them flush their cash reserve. A typical scenario is when an attacker comes in front of the cash dispenser, drills a hole in the front panel, and plugs a malicious USB key into the PC that drives the cash dispenser. He can then use this USB key to take control of the PC (e.g. using a Rubber Ducky attack) and have the cash ejected.

This technique has been known since 2010 when it was demonstrated at the BackHat USA security conference by Barnaby Jack. The actual attacks appeared few years later. There are now kits available on the underground market, called "**black boxes**", to carry out this type of attack. According to Europol (see this May 2017 announcement), 15 blackbox incidents were counted in 2015 in Europe and 58 in 2016, which shows a significant increase in these attacks. The mainstream media (see this French article from LCI TV media) indicate that the phenomenon has also been affecting France since 2017. And in January 2018, the US Secret Service issued a public warning about possible attacks in preparation in the United States. There is therefore a clear shift in attacks from their countries of origin (e. g. Romania, Moldova, Russia and Ukraine) to Western Europe and the United States.

- **Advanced intrusions (APT)**

These are "cyber-robberies" against banks: hackers illegally infiltrate the bank's internal IT systems (typically with a spear-phishing attack), silently stay there (to monitor internal activity, collect information and wait for the most appropriate time), and perform the robbery typically by issuing illegal interbank money transfers (typically via SWIFT). This type of attack is totally equivalent to the APT attacks seen since 2010 in other industry sectors (industrial espionage). It appeared in the banking world in 2014 with **Carbanak** and became really significant in 2016 with the attack against the Bangladesh Central Bank. In 2018 we have seen the attack against the PIR bank in Russia (in July 2018, attributed to isolated cyber criminals) and the attack against the Cosmos bank in India (August 2018, now attributed to North Korea).

Up to now, these attacks seem to affect smaller financial institutions, in which security measures on computer systems are probably less exhaustive than in larger institutions. But the attackers are obviously very experienced, both in the internal operation of banks (knowledge of the bank procedures) and in computer attack techniques.

- **Form-jacking (aka Software Skimmers)**

This is an attack against e-commerce websites. If there is vulnerability on an e-commerce site, a hacker can use it to install a small invisible JavaScript code that waits for the user to reach to the site's payment page and collects all the payment information entered on that page (payment card number, CVV code, etc.). These attacks are generally named server side "Form-jacking", "Form grabbing", or even "software skimmer". They have existed since at least 2015 (but client side form-jacking has existed since at least 2007), and they increased sharply in 2018, with in particular the attack against the **TicketMaster** ticketing site (from February to June 2018) and the attack against **British Airways** (380 000 bank card data stolen in 2 weeks in August 2018).

- **Conclusion**

Banks have always been prime targets for cyber criminals. But in recent years new types of attacks have emerged. The first response that comes in mind to prevent these attacks is to strengthen security:

- The PCs that control ATMs seem insufficiently protected (against the plugging in of external devices, the attacks at OS level, and the attacks that bypass the security software running on these PCs).
- The banks attacked by APT seems to have a limited level of IT security (and monitoring), too low compared to recommended best practices.
- Websites should more strictly isolate payment forms from the rest of the code (included third party codes hosted on supplier servers) to avoid the installation of skimmers, invisibly dropped by attack in the mass of codes.

It can also be noted that the attackers are becoming more and more experienced. Some knowledge of the banks' businesses and banks' IT systems is required to carry out the first 2 attacks. Some of the attacks could probably be performed by very small teams (one developer and one pen-tester), but it is likely that they also often include people who worked in the banking sector. It is often said that the insider threat is the most dangerous (because of the damage it can cause by an attack), but, as attackers are now also expert in bank business, this changes the perspective.

3.5. Governments became the most visible actors in the threat landscape

Cyber-defense (as a generic term to cover all the cyber activities of a State) is omnipresent in the news. Media usually cover this topic to inform when a hacker group, supported by a foreign State, attacked a company or a State (e.g. Chinese attacks against industrials or Russian attacks to influence an election…). Therefore, it's the offensive aspect that prevails. However, States are also working to enhance their defenses through in-depth actions (such as enforcing new requirements for Critical Infrastructure, or adopting European NIS directive) but also through communication campaigns: you must let your enemy know that you can detect him and will fight back.

On this matter, **in 2018 the USA publicly named their main cyber-enemies ("Name to Shame" policy)**:

- **North Korea** (very first nation cited by the US) which they refer to as Hidden Cobra. Up to 2014 North Korea was seen as a "minor" threat group (with for example the attack against Sony Picture Entertainment in 2014), but US changed his speech in 2017 and named North Korea as a major cyber attacker (believed to be the authors behind Wannacry). In 2017 and 2018 North Korea has been mainly accused for financial attacks.
- **Russia**, known as Grizzly Steppe. Russia has been the most frequently cited threat actor in 2018 by the US, in particular with attacks against network infrastructure (TA18-106A alert on Cisco Smart Install - SMI) and attacks targeting American energy companies (TA18-074A alert).

- And more recently **China** (see this US-CERT web page). China has been largely implicated in 2010 for cyber-spying attacks against companies but has almost disappeared from the threat landscape by the end of 2015 when the non-aggression agreement between China and the USA was signed. In 2018 China is therefore making a comeback with attacks through the supply chain: see for example the TA18-276B alert on attacks through outsourced services.

In terms of attacks, the 2 most important events in 2018 are:

- **VPNFilter:** a Russian attack infecting poorly protected networks and turning them into sleeping bots which can be used later on for other attacks.
- **TRITON:** the most alarming industrial attack since Stuxnet. This attack targeted the Schneider Triconex safety systems at an industrial plant in Saudi Arabia. By chance this attack failed; however, if it had been successful, it would have probably caused an industrial disaster. The TRITON attack (also known as the Trisis or Hatman) was revealed in late 2017 but the details and incident scope remained unknown until 2018 (see the "March 2018" section, in Chapter 2).

3.6. Attacks through the suppliers or partners

The supply-chain attacks have been a concern for several years. They have 3 distinct variants:

- Bounce attacks via partners
- Trapping third-party software
- Hardware trapping

• Bounce attacks via partners

In the industrial world, the first publicly known case is the cyber-attack against RSA Security in 2011 (the goal was to collect there information to attack US defense contractors). Today, attack against an industrial plant usually starts by sending trapped emails (spear-phishing attacks) **from a trusted partner known by the victim**. This partner (a supplier for example) was in fact first infected by the attacker who then used the partner infrastructure to send malicious email that look trustworthy. In 2018, a NCCIC webinar (NCCIC is the US agency on top of both US-CERT and ICS-CERT) about **Russian attacks against American industrial infrastructures in 2017** (attacks dubbed **Dragonfly** by Symantec) presented these bounced attacks (see this article from the ARC advisory group): NCCIC calls the intermediate victims "staging targets", as opposed to "intended targets" which are the final targets.

• Trapping third-party software

These types of attacks were particularly covered by the media in 2017 (see for example chapter 3.2 of our last year's annual report) with attacks using trapped versions of MeDoc (NotPetya attack), NetSarang and CCleaner software. In 2018, we had another example of trapping third-party software with the MageCart attack on TicketMaster's website. This time, the malware has been inserted into the chat-bot service code sold by Inbenta.com and used on TicketMaster's website.

• Hardware trapping

This last category is different from the two previous ones, because it is of primary concern to governments rather than companies. It is the likelihood that some hardware devices would have been trapped during their fabrication so that they can spy on their future users. This risk has always existed for isolated attacks by spying services. On the other hand, in recent years, governments have been concerned that such attacks could be carried out on a large scale, especially by China, since they are the largest factory in the world for computer technologies. These matters were discussed several times in 2018, especially:

- The United States and Europe concerns about Huawei and ZTE manufacturers (see the US law project to forbid their devices in administrations). These fears are now focusing on the 5G technology,
- The possible trapping of SuperMicro motherboards which has since been denied (see the "October 2018" section in Chapter 2).

We can also add to this category Kaspersky's antivirus banning (in September 2017 by the USA, followed in June 2018 by the European Parliament).

3.7. Attackers' TTPs are evolving making attributions even more difficult

- **False flags to mislead investigators**

Once an attack is detected, one of the objectives of the incident response team is to identify who the attackers are. In 2010, the geographical location of an IP address, the language or the keyboard's layout were sometime seen as sufficient to attribute a malware to a country. Recently, a lot of attention has been paid to find similarities between malware binary codes (searching for possible common sections in 2 distinct malware source codes). However, the **"Olympic Destroyer" attack** (during the 2018 Olympic Winter Games in South Korea) marks the end of these approaches. This attack is considered to be the **most advanced example where "false flags"** (see this Kaspersky article) have been inserted into the malicious code to mislead investigators on the real origin of the attackers. First China (with rather weak evidences), then North Korea (with evidences, that later on, turned out to be lures) and finally Russia were suspected. As the attack was a lot less damaging than it could have been, some people think it was actually a demonstration to show to the worldwide secret services that attackers were able to strike hard and incriminate another country.

- **Remain under the radar by using common tools**

Another phenomenon in this area is the use of already available common tools in attacks, rather than specially crafted binaries (malware). These tools are usually standard administration tools (such as Power-Shell on Windows) or tools largely used by all attackers (regardless of their nationality). This strategy benefits the attacker in two ways:

- It is difficult to detect attacks if the tools used are also being used for legitimate platform administration tasks.
- It is hard to attribute the attack to a particular group if all threat groups are using the same tools.

Note: These attacks that do not use any specific binaries are often referred to "fileless attacks" (see Chapter 3.4 of last year's review on this subject). In 2018, Symantec invented the term "**Live off the land**" to describe this strategy.

- **Mapping attacker's tactics with ATT&CK framework**

In 2018, MITRE's ATT&CK project became a reference for classifying attackers. ATT&CK is a catalog that includes known attackers groups and the techniques they use. This framework offers two promising perspectives:

- It becomes theoretically possible to recognize an attacker by the techniques he uses, instead of relying only on the attack indicators (IOC),
- It allows companies to prioritize their protective measures on the most commonly used attack techniques.

3.8. A year of Cryptominers mania

In 2017, the cryptocurrency exchange rates (such as Bitcoin) rocketed and led to a massive increase of attacks called cryptojacking. These attacks consist in installing on a machine (without the owner's consent) a crypto-mining software running in the background, and generating cryptocurrency for the attacker benefit. It is therefore a diversion of CPU resources (hence the term "crypto-hijacking").

The most commonly used cryptocurrency for these types of attack (and more generally for all illegal activities) is the Monero (whose symbol is XMR) because it is difficult to trace and relatively easy to mine. While Monero crypto jacking existed since its creation (back in 2014), its popularity exploded in mid-2017 when the prices of all cryptocurrencies rose dramatically. A significant drop in the prices occurred at the end of 2017, although the number of crypto-jacking infections remained very high throughout 2018. In number of incidents, in late 2017 and throughout 2018, crypto jacking took the lead behind crypto ransomware incidents (which had been the most common incident in 2015 and particularly in 2016). Nevertheless, it seems that this cryptojacking phenomenon is in decline in the beginning of 2019.

Crypto jacking is an attractive business for cyber crooks (because of the soaring of crypto-currencies prices) but this market seems to be lucrative only for the big players. A recent university study estimates that:

- all crypto jacking campaigns surveyed represent 4.32% of the total amount of Monero on the market,
- this 4.32% has generated a total of $57 million (USD),
- **99% of the campaigns produced less than 100 XMR** (= $4,500) per campaign, while the most successful campaign produced $18 million in 2.5 years on its own (and the top 10 produced a cumulated total of $34 million).

4. Recurring threats not to forget

In this paragraph, we highlight threats that are not particularly new but that remain very active. It is therefore a reminder not to forget these recurrent threats.

4.1. CEO frauds (and GDPR frauds too!)

We have been discussing these attacks since 2014 (see Chapter 2.4 of our 2014 annual report, or 2.8 of the 2016 annual report) but they remain prominent. For example, in March 2018 Pathé movie theaters were defrauded 19 million euros because attackers impersonating the group's management asked the Pathé branch based in the Netherlands to transfer money for a so-called acquisition in Dubai.

Note: these scams are also called Business E-mail Compromise scam (BEC scam) in the United States. From 2013 to 2018, the FBI identified more than 40,000 victims in the US with a total loss amount of more than $3 billion.

On a minor scale of costs, we can notice the emergence of **GDPR scams** this year: companies send to SMBs fake formal notices urging them to use their services in order to be GDPR compliant (the French CNIL agency has issued a disclaimer on this subject).

4.2. Remote access and two-factor authentication (2FA)

Authentication with a simple password is now an obsolete security measure for a service accessible over the Internet. There is tons of incident reports where usernames and passwords where stolen either by phishing attacks or by breaching vulnerable website's account databases.

The use of strong authentications, for example 2FA (2-Factors Authentication), is therefore a **mandatory requirement** when accessing outsourced services in the cloud, such as Office 365 email, or even an extranet service such as a simple webmail.

Note: Not all 2FA mechanisms are equivalent. 2FA SMS (reception of a code by text message) and OTP-based 2FA (such as Google Authenticator, Authy, or Microsoft Authenticator Apps) are no longer considered safe. For public consumers, the only safe 2FA protection available is a 2FA device compliant with FIDO (U2F or FIDO2) standards.

4.3. Cloud Security

Today, there is no doubt that the Cloud is definitively a part of companies' IT infrastructures. However, if theoretically we are convinced, implementation is sometimes much more hazardous and we are observing more and more security incidents impacting cloud environments:

- Data leaks impacting AWS S3,
- Compromise of Office 365 mail infrastructures,
- Attacks via information collected on GitHub,
- Installation of illegal crypto-miners in Docker infrastructures,
- etc.

Cloud solution providers are conscious of this situation, and since at least 2017 have significantly strengthened their solutions to implement and monitor security. But the Cloud Solution Provider is only a piece of the project implemented by an organization. In fact, it is quite likely that the **security incidents observed, are actually due to projects that were deployed too quickly** and did not take the time to analyze the security exposure of the cloud solution they were building. We should not forget that Cloud providers only provide security by default on layers they operate. **For the higher layers, security is still the responsibility of the projects**, and this is probably where the security flaws that made the incidents possible are to be found. Regarding Cloud security topics, the motto should always be “Be careful with solutions deployed too quickly and without thinking at the security!”.

5. Summary of Cert-IST activity in 2018

5.1. Threat & vulnerability advisories

As part of its monitoring activity on vulnerabilities and threats, Cert-IST continuously monitors various sources for information (vendor announcements, security blogs, mailing lists, communications among CERTs, etc.) in order to be informed of new vulnerabilities. Every day, these data are analyzed to provide to our members sorted, qualified and prioritized information.

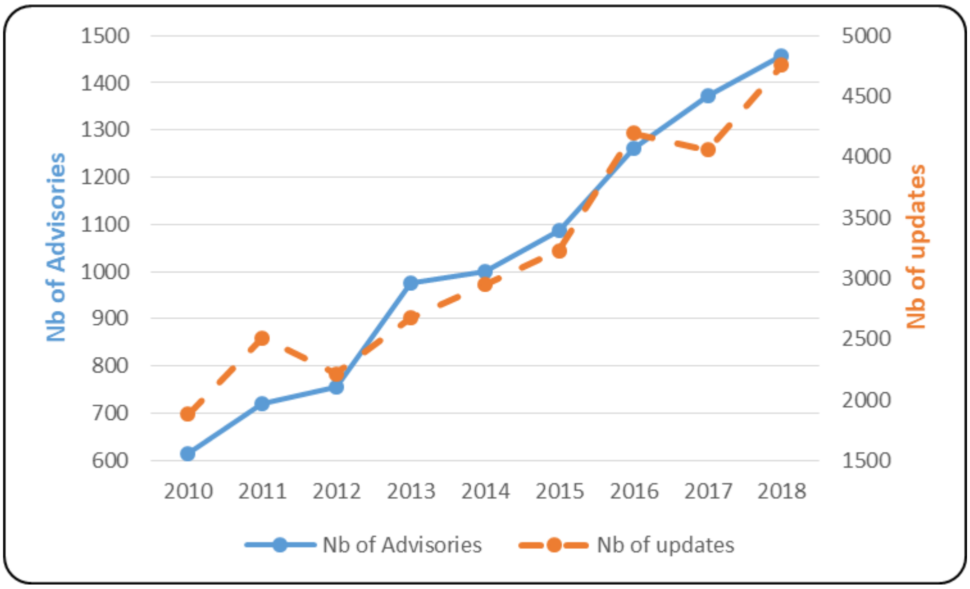
Cert-IST thus produces various types of publications:

- **Security Advisories (AV)**: they describe the new discovered vulnerabilities in products monitored by Cert-IST. These advisories are continuously enriched with minor or major updates. The latter typically correspond to the situation where exploits are publicly disclosed.

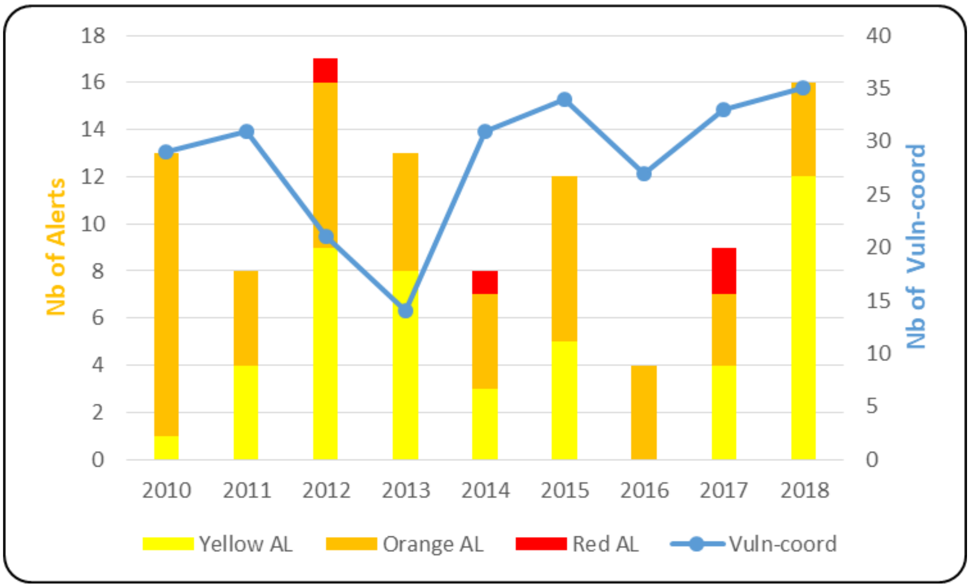
- **Alerts (AL)** which are issued when there is a particular risk of attack, and **"Vuln-coord" messages**, which provide an analysis for particular vulnerabilities (e. g. mediatized) but of lower immediate danger level. These 2 categories focus on the attack risks, while security advisories systematically identify all vulnerabilities (regardless of their probability of being used in attacks and their dangerousness).

- **Attack reports (ATK)** and **indicators of compromise (IOC)** via a shared MISP database. These productions list major attacks, whether they are recurrent threats (MalSpam, Exploit-Kit, Ransomware), or cyber-espionage incidents (APT attacks).

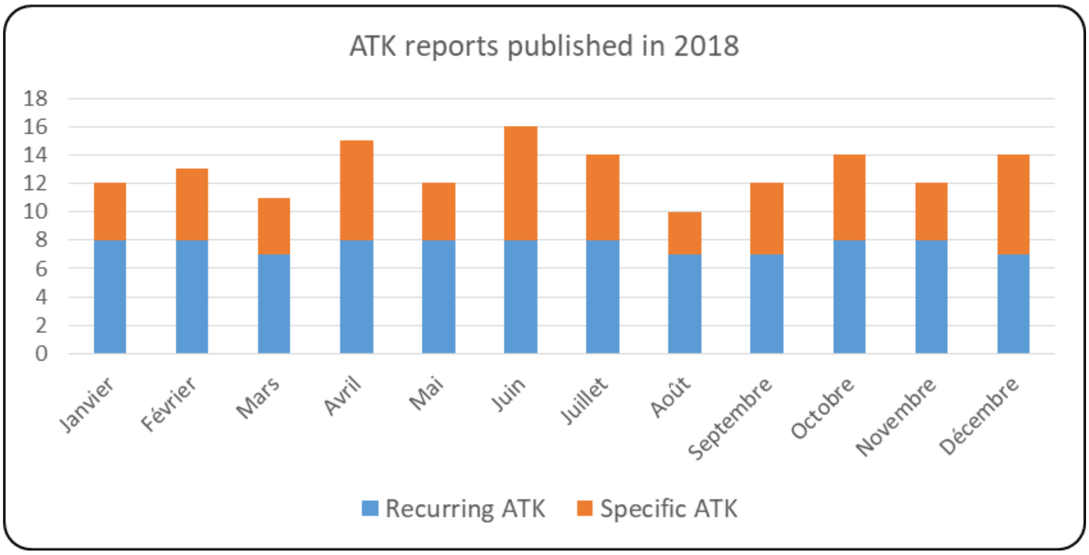
The graphs below show the Cert-IST different productions over the past few years.



Number of security advisories published per year



Number of security alerts published per year
Note: Yellow Alerts and Orange Alerts correspond to what was formerly known as Potential DanGers (DG)



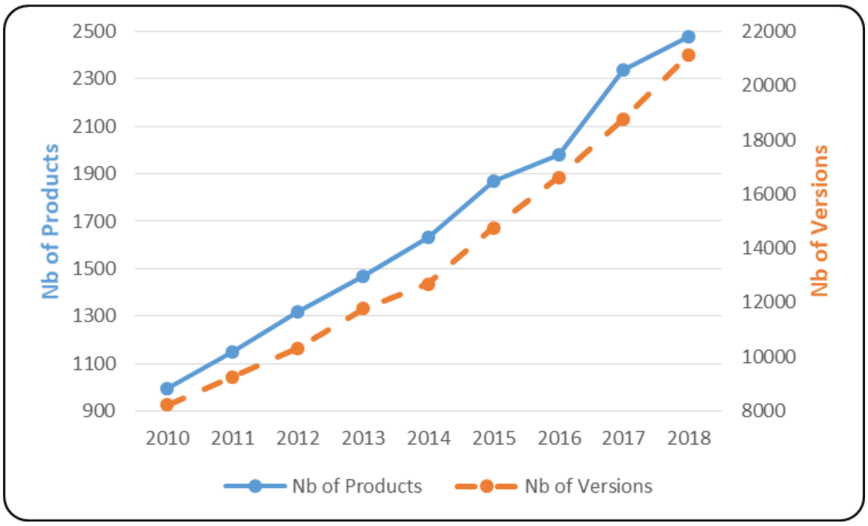
Number of ATK reports published per year
Note: ATK (and IOC) service is available since July 2016

In 2018, Cert-IST published:

- **1,456** security advisories (including 73 SCADA advisories), **4,613** minor updates and **141** major updates.
  The number of advisories has been constantly increasing over the past few years (see the graph above), with an increase of **6%** compared to 2017. This continuous increase shows that the finding of vulnerabilities is a constantly growing phenomenon. The maintenance of an adequate level of security is linked to the constant application of security patches on the environment products.
- **16** alerts and **35** "Vuln-coord" messages. The last red-risk alerts were issued in 2017 (Wannacry and NotPetya). Globally, activity in this category increased significantly, returning to similar levels observed in 2012 (the year of the Java attacks).

- **155** attack reports were published in 2018, containing **1,929** enriched events in the MISP database and **173,720** indicators (IOCs).

Regarding the products and versions monitored by Cert-IST, at the end of 2018 Cert-IST followed **2,476** products and **21,138** versions. The following graph shows the evolution of the number of products and versions monitored by Cert-IST over the year.



Evolution of the number of products/versions monitored per year

5.2. Technology monitoring

In addition to vulnerability monitoring, Cert-IST also produces technology monitoring reports:

- A **daily media monitoring newsletter (press review)** listing the most interesting articles published on French and English websites regarding security topics,
- A **monthly SCADA monitoring bulletin** providing a summary of current events related to the security of industrial systems,
- A **monthly general bulletin** summarizing the month's actuality (in terms of advisories and attacks) and addressing current events through articles written by the Cert-IST team,
- A **monthly bulletin on attacks and IOC** which synthesizes the most significant events in the attack landscape.

6. Conclusions

- **Cyber threat is still a growing trend:**

Again this year, there has been an increase in cyber-attacks:

- **In number**. Every month new examples of stolen data, which are becoming more and more voluminous, are reported. Every week, new reports describing targeted attacks (state cyber-espionage, industrial data leaks or malicious actions by cyber groups) are published.
- **In sophistication**, with for example attacks targeting the banking sector (see § 3.4), State attacks against poorly protected network equipment (see VPNFilter in § 3.5), or attacks via suppliers and partners (see § 3.6).

- **States are more and more playing an important role in the threat landscape**

State-sponsored attacks began to receive media coverage in 2013. Since that time, this phenomenon grown and Russian, Chinese or North Korean attacks are now common headlines. 2018 continues this upward trend. United States has decided for some time to speak up and publicly name it cyber-enemies. After North Korea in 2017, the United States put the focus this year on Russia and designated it several times this year as responsible for attacks against US industries.

While governments are at the center of the news, cyber gangs continue to be there as well. But it is vital for them to remain quiet so as not to draw attention to their activities. Here, large, highly structured actors work alongside a forest of low skill crooks. For example, in the areas of crypto-jacking and crypto-miners (one of the 2018 key topics), a small set of major players have accumulated huge amounts of cryptocurrencies, whereas hundreds of minor actors seem to have made very limited profits (see § 3.8).

- **Improving defenses remains a priority**

In this cyber-threat landscape, it is important for companies to maintain robust defenses. Beyond the traditional technical approach (hardening, in-depth defense), it is also important to better integrate security aspects at the early stage of the system design by considering questions such as:

- What will happen when an intrusion will succeed (because it will)?
- How can the propagation of this incident be limited?
- What will be the consequences of a data leak?

This “secure by design” mindset meets the GDPR “privacy by design” concern. It is clear that the entry into force of GDPR is a major event of 2018. And it shows that the Cybersecurity field is getting more and more mature. After technical concerns (the key driver for security in the early 2000), and the arrival of conformity approaches (ISO 27000), GDPR enforcement highlights the fact that security now needs a stronger legislative framework. While it is too early to measure its impact, it is clear that the European GDPR initiative is of interest to other countries and will undoubtedly lead to similar initiatives around the world.

- **Besides defenses, it is necessary to develop the company's ability to respond to intrusions**

No defense is perfect, so it is in the company's best interest to optimize its actions by searching for the best trade-off between defense and reaction. Once the defense foundation is in place, it is often more productive to monitor your environment and react to threats as they appear, rather than to continue to strengthen the foundation.

This monitoring implies:

- The **implementation of a security supervision**, with the objective of reducing the "Mean Time To Detect" security incidents,
- The **ability to handle incidents** to quickly stop the intrusion and, above all, to prevent its spreading.

It is often said that in cyber security, the attacker has the advantage over the defender because he only needs one vulnerability to succeed in his attack whereas the defender must take care of all the components of the IT system (the whole attack surface). During the Botconf-2018 conference, one of the speakers proposed an interesting point of view that reverses this asymmetry: according to him for an infiltration attack (an APT) **the defender has the advantage over the attacker** because he only needs to find a single trace left by the attacker (and it is difficult not to leave one) to detect his presence and begin a hunt.

To do this effectively, it is also important to be informed about the threats:

- By using a security monitoring service,
- But also by sharing with other companies of the same sector, the TTP (Tactics, Techniques and Procedures) of attacks handled.

Cert-IST is a key partner for companies in these domains.

Cert-IST Organization

3 quai du point du jour
92100 Boulogne-Billancourt
France

info@cert-ist.com

https://www.cert-ist.com

+33 5.34.39.44.88