Annual Report on Attacks and Vulnerabilities seen in 2019

Released on March 2020

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 2019 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 2019 (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 2019?

The following table summarizes the key events of 2019. You will find events which were highly mediatized or more generally because these events are considered as major indicators of the cyber threat evolution.

January 2019	**Collection #1, Collection #2, …, Collection #5**: The year 2019 begins with the publication (for free) of 5 multi-gigabyte datasets containing lists of accounts and passwords. Then, from February to April, another hacker named **Gnosticplayers** will release on the Blackmarket nearly 1 billion accounts recently stolen by hacking more than 40 companies. We analyze this phenomenon in paragraph 3.6.
January 2019	**Modlishka**: this is the name of a new open-source tool to perform phishing attacks against **2FA** (two-factor authentication) systems.

January 2019	**FaceTime bug**: A bug in Apple's FaceTime application allows you to listen to your correspondent before he picks up the phone. This bug will be in the news and will be fixed by Apple a week later. It was discovered by chance by a 14-year-old teenager while playing Fortnite.
January 2019	**LockerGoga**: The ransomware LockerGoga attacks ALTRAN. It is the first French victim of a long series that will occur throughout the year, known as "**Big-game hunting**". We analyze this phenomenon in paragraph 3.2.
February 2019	**Bug 'PrivExchange' in Microsoft Exchange**: This bug allows to attack the Active Directory by taking advantage of the privileges of Exchange in the AD.
February 2019	**Docker RunC**: A critical vulnerability in the RunC command allows an attacker who would be 'root' in a container to become 'root' on the host platform.
March 2019	The NSA publishes **GHIDRA**, a reverse-engineering tool that the US agency uses internally. This tool is quite popular and is sometimes compared to the (much more advanced) commercial tool IDA pro.
March 2019	**10KBLAZE**: Onapsis publishes 10KBLAZE, an attack tool targeting SAP. These are old attacks exploiting well-known **SAP** configuration or architecture flaws.
March 2019	Microsoft launches **Azure Sentinel**: a SIEM solution running in the Microsoft Cloud (ZDnet article).
March 2019	**Norsk Hydro** is also attacked by LockerGoga ransomware (as well as Altran in January), and is distinguished by its very active communication.
March 2019	**ShadowHammer**: Kaspersky discovered an attack on the "ASUS Live Update" software that is pre-installed on ASUS computers. The attack seems to be much targeted since it is only triggered on very specific workstations (recognized by their MAC address). Subsequently, Kaspersky indicated that this attack seemed to have links with the 2017 (Chinese?) attacks targeting **CCleaner** and **NetSarang**.
March 2019	**WinRAR**: A vulnerability discovered in WinRAR is immediately used, on the event of the Hanoi summit between North Korea and the United States, to carry out cyber-espionage attacks. It will be widely used throughout the year in other attacks.
April 2019	**Dragonblood** is the name given to a series of vulnerabilities in the very recent WIFI **WPA3** protocol. This name refers to the Dragonfly cryptographic protocol. In September, the same researchers will publish 2 additional vulnerabilities.
April 2019	**Julien Assange** is arrested by British police at the door of the Ecuadorian embassy in London where he took refuge in 2012.
April 2019	**WIPRO**: This Indian IT company is hit by a cybercriminal attack that actually targets WIPRO's customers. We analyze this phenomenon of bouncing attacks in paragraph 3.3.
April 2019	**Tchap**: The French government launches "Tchap", an encrypted messaging system for French government agents. A (quickly fixed) vulnerability is found a few hours later, and a bounty bug program is launched afterwards.

April 2019	**Sea Turtle**: Cisco TALOS announces a cyber-espionage attack based on DNS hijacking. It is similar to DNSpionage, but much more sophisticated. We discuss this attack in section 3.4.
May 2019	**Israel bombed a building sheltering Palestinian hackers**. This is the first public case of a physical (violent) counter-attack to a cyberattack.
May 2019	0-day **WhatsApp CVE-2019-3568**: WhatsApp announces that it has fixed a vulnerability that allowed remote execution of code on an Android or iPhone device with a simple WhatsApp call (even if it is not picked up). This vulnerability has been discovered and used by the NSO Group company which sells spyware to government agencies. We discuss these attacks on mobile phones in section 3.4.
May 2019	**ZombieLoad, RIDL and Fallout**: These Intel CPU vulnerabilities are similar to Meltdown and are collectively referred to as "Microarchitectural Data Sampling (MDS) vulnerabilities". In September 2019 other attacks targeting Intel will be released: SWAPGS and NetCAT. Then **ZombieLoad2** (in November) and finally PlunderVolt (in December).
May 2019	**BlueKeep**: Microsoft announces that it has fixed a vulnerability in the Windows RDP service that could lead to attacks as serious as Wannacry (2017). We discuss this vulnerability in detail in section 3.1.
June 2019	**GandCrab shutdown?**: The authors of this ransomware announce that they are ceasing their activities. One month later appears **REvil** (Sodinokibi) which seems to be the successor of GandCrab.
June 2019	**RAMBleed**: This new hardware vulnerability uses the RowHammer (2015) vulnerability to read unusually inaccessible memory spaces. RowHammer was an integrity attack (accidental change of a memory bit) while RAMBleed is a privacy attack (memory leak).
June 2019	**Have I Been Pwned** is for sale. Troy Hunt, the creator of this database which lists accounts appearing in lists of stolen accounts, announces that he wants this project to be taken over by a third party.
June 2019	**SIM swapping**: A series of "SIM swap" based attacks are once again hitting users to steal their wallets of crypto-money. We have already discussed this type of attack in 2018. They also target traditional bank accounts. At the very beginning of 2020, several articles (1, 2, 3) will be published to explain how hackers get into telecom operators to carry out these attacks.
June 2019	China is conducting **DDOS attacks against Telegram** to prevent its use by protesters in Hong Kong.
June 2019	Linux **TCP SACK Panic**: This CVE-2019-11477 vulnerability in the SACK (Selective Acknowledgement) feature allows to remotely cause a vulnerable Linux system to shut down abruptly ("kernel panic" error).
June 2019	The USA launches **cyber-attacks against Iranian missile systems**. These attacks are presented as revenge against attempted Iranian cyber-attacks on US critical infrastructure, and occur one week after the destruction of an American drone by the Iranians.

June 2019	**Cloud Hopper**: this Chinese attack revealed in 2017 by PwC UK and BAE System and then by US-CERT (**TA17-117A**) continues to be discussed in 2019. Reuter announces that in addition to HP and IBM, other outsourcing companies have also been compromised: Fujitsu, Tata Consultancy Services, NTT Data, Dimension Data, Computer Sciences Corporation. In December 2019 The Wall Street Journal also publishes an article (picked up by FoxBusiness) that further extends the list of victims.
July 2019	**Capital One** announces a data leak affecting 100 million U.S. citizens and 6 million in Canada. The investigation will then show that the attack was carried out by a former Amazon employee who also stole data from 30 other companies.
July 2019	**URGENT/11**: Armis announces that it has discovered 11 critical vulnerabilities in WindRiver's **VxWork** real-time operating system (RTOS). In early October, Armis reports that other RTOS are affected (particularly medical equipment) because they share a common software strain with VxWork.
August 2019	**Vulnerabilities of SSL VPNs Fortinet, PulseSecure and Palo Alto Network**: 2 researchers from DevCore present at the BlackHat USA 2019 conference, their study on SSL VPNs. Attacks targeting **PulseSecure** will start a few weeks later and will become one of the most active attacks of 2019. We discuss this event in section 3.1.
August 2019	**Retadup** takedown: The C3N of the French national Gendarmerie announces that it has dismantled the Retadup botnet and disinfected 850,000 computers worldwide. To our knowledge, this is the first time this kind of takedown has been carried out by French policies.
August 2019	**WS-Discovery amplification** (WSD): A new method of DDOS attack by amplification (discovered in May) is seen in real attacks, with traffic peaks of around 35 Gbps.
September 2019	**SimJacker attack**: The company AdaptiveMobile Security explains an attack already known by some experts, which uses specific SMS messages to remotely activate functions on mobile phones SIMs via the S@T-Browser or WIB-Browser services available on these SIM cards.
September 2019	New attack attempted against **CCleaner**: Avast announces that it has stopped an attack aimed at inserting a backdoor into the CCleaner software. This software had already suffered a similar attack (supposedly Chinese) in 2017.
September 2019	**Emotet** is back: After almost 4 months without activity, new malicious Spam campaigns spread the malware Emotet.
October 2019	**Adwind RAT** is used in attacks targeting the oil sector in the US. This RAT (Remote Access Tool), which has been known since 2013, continues to be very frequently identified in attacks targeting individuals or companies.
October 2019	**M6 French TV channel** is impacted by an attack by BitPaymer ransomware. It will be one of the countless victims of these ransomware attacks that will target companies and organizations in 2019 (see our chapter 3.2).

November 2019	**DoH: DNS over HTTPS**: Microsoft announces that it will support DoH in a future version of Windows 10. DoH helps ensure the confidentiality and integrity of DNS queries, but raises concerns for ISPs and security products based on DNS traffic. Mozilla Firefox and Google already support this protocol, which has earned Mozilla the "Villain of the Internet" award.
December 2019	**President Fraud**: A Chinese investment company was defrauded of $1 million by sending its payment to a hacker rather than to an Israeli company it wanted to support. In the area of fraud to the president, we can notice that in October, authors of such attacks were arrested in Spain.
December 2019	**PlunderVolt**: This new CVE-2019-11157 vulnerability impacts Intel processors and allows, by fluctuating the voltage of a CPU, to illegally access SGX enclaves on Intel.

3. Analysis of 2019 key trends

3.1. BlueKeep: The attack that has not occurred (yet)

- **Chronology of the #BlueKeep crisis**

In May 2019, Microsoft announced that it has just fixed a serious flaw (CVE-2019-0708) that affects the Remote Desktop Service (RDP) of Windows. This flaw could lead to massive attacks similar to **Wannacry** (in 2017) and Microsoft recommended to apply the patches as soon as possible. This flaw has been dubbed **#BlueKeep** by the cyber community.

We summarize the detailed chronology of this vulnerability below, and (fortunately) so far the feared mass attacks have not yet occurred. However, it is very likely that the vulnerability has been used on an ad hoc basis to attack vulnerable machines specifically, without being done on a large scale (or by a worm).

Why hasn't there been a massive attack yet? An important parameter for the attacker is to act stealthily if he doesn't want his attack to be detected, which would then expose him to a possible counterattack. In case of high-profile breaches, the counterattack could be severe (e.g. lawsuits and jail time). There is therefore always a risk/benefit tradeoff to be taken into account when an attacker decides to start a campaign.

Comprehensive timeline for the #BlueKeep vulnerability in Microsoft RDP:

05/15/2019	Microsoft is releasing patches for the CVE-2019-0708 vulnerability as part of the monthly (Microsoft Tuesday) patches for May. Cert-IST publishes the **CERT-IST/AV-2019.0601** security advisory to describe the vulnerability and the available patches, then the next day the **CERT-IST/AL-2019.007** yellow alert, to warn that it is very likely that the vulnerability will be used to perform massive attacks.
06/04/2019	The Cert-IST increases its alert to the Orange level because more and more researchers announce to have created a private exploit program for this vulnerability. It is now likely that a massive attack could occur even if no public exploit has been released yet. Microsoft also published a few days earlier an article on its MSRC (Microsoft Security Response Center) blog reminding that it is urgent to patch vulnerable systems.
08/13/2019	As part of its monthly patches (Microsoft Tuesday), Microsoft is expanding the initial patches as new wormable RDP vulnerabilities have been found by Microsoft (CVE-2019-1181 and CVE-2019-1182, described in **CERT-IST/AV-2019.1031**). These vulnerabilities have been named #DejaBlue by some people.
09/06/2019	A first public exploitation program (on Metasploit) is published on the Internet. Its functionalities are still limited, since the attack only works correctly for some Windows systems.
11/02/2019	Researchers Kevin Beaumont (@GossiTheDog) and Marcus Hutchins (@MalwareTechNews) announce that they have discovered a fairly extensive attack that exploits the BlueKeep vulnerability. The aim of the attacker is to install crypto-mining software on vulnerable systems. Due to the limitations of the exploit program used (based on Metasploit's one), most of the time the attack ends with a reboot of the targeted machine. Microsoft will publish an analysis of this attack a few days later.
	A few days later, the author of the BlueKeep exploit on Metasploit announces that he has improved it to avoid the "crashes" often observed with the previous version.

	To this day, no massive attacks have been observed. However, it is likely that the vulnerability is used on a one-time basis (without automatic "worm" propagation) to attack vulnerable machines.

- **Other attacks that occurred in 2019**

In addition to #BlueKeep, here are the attacks that are for us, the most significant of 2019:

- **Pulse secure SSL VPN (CVE-2019-11510):** These attacks against this SSL VPN system started on 08/22/2019, a few weeks after a presentation at the Black Hat USA 2019 conference that gave technical details about recently fixed vulnerabilities in Pulse secure SSL VPNs (CERT-IST/AV-2019.0520 advisory created on 04/24/2019) but also Palo Alto Networks GlobalProtect (CERT-IST/AV-2019.0903 advisory, 07/17/2019) and Fortinet (CERT-IST/AV-2019.0668 advisory, 05/24/2019). For these attacks, we first issued the yellow alert CERT-IST/AL-2019.010, then raised it to orange on 10/11/2019 when the number of reported attacks increased.
  These attacks were very active throughout the last quarter of 2019. This is probably this Pulse Secure vulnerability that led to the ransomware attack that hit the foreign exchange company Travelex at the end of December 2019.

- **Microsoft SharePoint (CVE-2019-0604):** This vulnerability allows an attacker to remotely execute malicious code on a vulnerable SharePoint server. It has been fixed by Microsoft on 02/12/2019 and the first attacks (Chinese cyber-spying) have been observed in early May in Canada and Saudi Arabia. On that date, we issued the yellow alert CERT-IST/AL-2019.006, which we raised to an orange alert in early June when it was confirmed that this attack could be carried out remotely without a SharePoint account. **Several attacks using this vulnerability (probably cyber-espionage from China) were seen afterwards**, for example those reported by the FBI (see this ZDnet article of January 2020), or the attack on the UN in Geneva and Vienna (see this TheRegister.co.uk article of January 2020).

- **Oracle WebLogic (CVE-2019-2725)**: for the last 2 years, the WebLogic (Java) web server has been victim of attacks on Java de-serialization features, and each time a known deserialization vulnerability is fixed by Oracle, another one is discovered few months later. We already reported this phenomenon in 2018 (we published 2 Oracle WebLogic alerts in 2018). The phenomenon continues in 2019, and we issued the **CERT-IST/AL-2019.005** alert on 04/29/2019. **These vulnerabilities were often used to install crypto-mining software on vulnerable servers.**

- **The evolution of crypto-mining attacks**

We mentioned last year that 2018 was a year of "crypto-miner mania", i.e. attacks using crypto-miner software had grown exponentially. This phenomenon continued in 2019 with some evolutions:

- Most of the attacks are now targeting vulnerable servers, to install crypto-mining software. Currently, as soon as an exploit for a new vulnerability on a server is released, we see waves of attacks that use it to install crypto-miners. This has been the case for example for the **Oracle WebLogic** vulnerabilities (CVE-2019-2725 already mentioned above), or **Atlassian Confluence** (CVE-2019-3396, **CERT-IST/AL-2019.003** alert) or **Jenkins** (CVE-2018-1000861 end of 2018, **CERT-IST/AV-2018.1362** advisory).

- It is also quite common for hackers to install crypto-mining software on infected end-user workstations (and consumer).
- On the other hand, crypto-jacking attacks, which consisted in installing a mining code (Javascript) on websites so that Internet users visiting the site would execute it, is a type of attack that has declined significantly.

3.2. Surge in ransomware attacks specifically targeting companies and organizations

Ransomwares have been around for a long time and were one of the major causes of attacks from 2013 to 2016. At that time, they targeted companies and individuals indiscriminately. But in 2018 a new form of attack emerged, in which this time ransomware specifically targets a company chosen by the attacker. Crowdstrike calls this phenomenon "Big-Game Hunting". **2019 is the year in which big-game hunting has become a major phenomenon in the cyber threat landscape.**

Apart from companies, these attacks target any organizations that cybercriminals consider "profitable", i.e. likely to pay large ransoms. Several attacks have targeted hospitals (e.g. the Rouen hospital in France), and many municipalities in the United States.

List of companies that have been affected by severe ransomware attacks in 2019. Non-exhaustive list as these are only the ones that have been announced in the press.

01/24/2019: Altran (IT consulting and services) in France.
03/12/2019: Hexion and Momentive, 2 American industrial companies belonging to the same group.
03/15/2019: Mitsubishi Aerospace in Canada.
03/19/2019: Norsk Hydro, a Norwegian industrial company producing aluminium.
03/21/2019: Arizona Beverages in the United States.
04/11/2019: Fleury-Michon (food industry) in France (it is not formally established that it was a ransomware).
04/16/2019: Aebi Schmidt in Switzerland (specialist in snow removal and road cleaning equipment).
04/17/2019: Verint (Cyber Security Company) in Israel. The attack seems to have failed (it was contained in a DMZ).
06/02/2019: Eurofin Scientific (bio-analysis laboratory) in Luxembourg.
06/07/2019: ASCO (avionics manufacturer) in Belgium.
08/10/2019: Ramsay General (hospital group) 120 French health centers affected.
09/03/2019: Demant, a Danish hearing aid company.
09/11/2019: Defence Construction Canada (DCC).
09/24/2019: Rheinmetall Automotive in Germany.
10/12/2019: M6 TV Channel in France.
10/23/2019: Go Sport (sports stores) in France.
11/04/2019: Everis (IT) and Cadena SER (Radio) in Spain.
11/10/2019: Pemex (oil company) in Mexico.
11/12/2019: Edenred (known for its "Ticket Restaurant" brand) in France.
11/27/2019: Prosegur (security and cash transportation) in Spain.

12/31/2019: Travelex (foreign exchange company) in the United Kingdom

The large-scale incidents caused by big-game hunting attacks in 2019 have significantly changed several aspects of incident response:

- **The need to know how to rebuild the IS.** These attacks affect a large number of workstations, which often become unavailable for several weeks. In addition to the degraded (or totally stopped) operation, these attacks require the reconstruction of the IS to return to a normal operation. This is a case of disaster that most of the time was not foreseen in the BRP (Business Recovery Plan) of the affected companies.
- **Communication in the event of a crisis.** The habit is often to minimize public communication in case of incidents. However, in March 2019 Norsk Hydro chose the opposite approach, which is now considered a model (see, for example, this ZDNet article): it communicated continuously, from the very beginning of the incident and in a very transparent way.
- **Whether or not a ransom should be paid.** While the general statement is always that paying a ransom to the attacker is dangerous (unethical and with no guarantee on the technical result), paying anyway (at the last end when no other solution is possible) is more and more an option or at least less taboo choice. But everyone agrees that it is the worst solution and that its result is highly dubious.
- **Cyber insurance is increasingly considered as an essential measure** to cover part of the costs involved in an incident. In some cases, it even seems that insurance companies are involved in negotiating with the attackers to minimize the amount of the ransom.

3.3. Cybercriminal attacks are back in the headlines

On the attack side, the two most common actors are cybercriminals (motivated by money-making) and states (the cyber being one of the tools for States to establish its power on the world stage). Cybercriminals seek discretion, so as not to draw attention to their activities, while states may have an interest in showing their strength. If we look back in 2018, the news had been then dominated by attacks by states, and cybercriminal attacks had remained rather quiet.

This changed in 2019: cybercriminals were very present in the news, in particular through 3 events:

- The **ransomware attacks** that we mentioned in the previous paragraph (§ 3.2),
- **Magecart attacks** targeting online purchases by Internet users,
- **Attacks on IT service providers** and their customers.

We analyze these last 2 phenomena below.

- **Magecart attacks targeting online purchases by Internet users**

Magecart-type attacks made a spectacular comeback in 2019. These attacks consist of installing a "web skimmer" on poorly protected websites in order to steal the data input by Internet users (credit card data) when paying for their purchases. We have already talked about Magecart in 2018 in an article of

our Monthly Bulletin about the Ticketmaster and British Airways attacks, in our CERT-IST/ATK-2018.084 attack sheet, and in our annual review of the attacks in 2018. In 2019, the phenomenon was further enhanced with more and more incidents of this kind. As an example, in 2019 Magecart was mentioned in 32 Cert-IST media watch bulletins (in 2018 it was mentioned 13 times). It is clear that more and more cybercriminal groups are using this technique.

Note: Magecart refers to an attack technique that is used by several cybercriminal groups. RiskIQ identifies at least 8 distinct groups.

- **Attacks on IT service providers and their customers**

Several attacks revealed in 2019 show that cybercriminals are increasingly seeking to infiltrate IT companies and then infect the clients of these IT companies through the privilege accesses they have been granted.

These IT companies can be:

- Small structures providing IT maintenance for various companies,
- Specialized service providers, e.g. solution providers for doctors, dentists, etc., are also involved.
- Large IT outsourcing companies.

These are generally referred to as MSPs (Managed Services Providers).

For example, this type of incident occurred in April 2019 (see this article by Brian Krebs) at **WIPRO** (an international IT consulting and outsourcing company headquartered in India). Subsequently, RiskIQ published a study (entitled Gift-Card Sharks) showing that WIPRO was only one victim of a larger operation targeting other companies in several industries, and in particular the **Infosys** and **PCM** IT companies. The purpose of the operation was to gain access to third-party companies to steal gift cards (hence the name of the study) and other coupons that could then be exchanged for cash.

Many other cases of infections via IT service providers were intended to install ransomware on their customers' machines. See for example this case in January 2019 (ransomware GandCrab) and this one in June 2019 (ransomware REvil/Sodinokibi).

These attacks through service providers are a reminder of the **Chinese Cloud Hopper attacks**, **revealed in the spring of 2017**, which targeted major players in the field such as **HP** and **IBM** (in the United States) and **NTT Data** and **Fujitsu** (in Japan). In the case of Cloud Hopper, on the other hand, the attacks were state-sponsored and were intended for cyber-espionage.

The news of 2019 thus shows that this attack strategy is spreading in two directions:

- More and more cybercriminals are using this tactic.
- It was first seen a few years ago in the field of cyber-espionage attacks and is now also used by cyber-criminal groups for financial purposes.

3.4. State-sponsored attacks are still prominent

- **Attacks against Uighur community**

For several years (2009 at least), published reports have shown cases of attacks against ethnic minorities under surveillance in China, mainly Uighurs and Tibetans. These attacks have so far been rather unsophisticated, often using known malware and targeting Windows systems. Since 2018, attack techniques have become more and more professional, with more and more social engineering; attacks are now more oriented towards Apple IOS or Google Android mobile phones. For example, in September 2019 Citizen Lab, Google Project Zero, and Volexity published articles about one such attack named "Poison Carp" (or "Evil Eye").

- **Mobile phones used to spy on opponents**

Attacks on phones are not limited to Chinese opponents. Of course, all intelligence services are probably interested in having 0-day attacks against IPhone or Android, so that they can spy on the phones of individuals considered as dangerous. While this may be understandable to fight against terrorism, for example, this can also lead to human right abuses, particularly in totalitarian countries.

In 2019, abuses have been reported with the Exodus software developed by the Italian company **eSurv**, and of Pegasus developed by the Israeli company **NSO Group**.

Another notable phenomenon of 2019 is that attacks on smartphones, rather than targeting the operating system itself (Android or iOS), are now also targeting the applications installed on those phones, such as **WhatsApp** (0-day CVE-2019-3568 attack) or **iMessage** (Karma attack used by the United Arab Emirates).

- **Sea Turtle and DNS hijacking attacks**

In January 2019, the American CISA (an organization above the US-CERT), then ICANN, published alerts following the **DNSpionage** attacks revealed by Cisco TALOS in November 2018. In April, Cisco TALOS announced a second attack of the same type, but more sophisticated, named **Sea Turtle**.

In both cases, these were large-scale attacks, probably carried out by states, which made it possible to steal the victims' access credentials (email or VPN) by redirecting them to fake sites at the time of their connection. This hijacking of connections was carried out by altering DNS data.

The DNSpionage attacks seemed to come from Iran. Sea Turtle is considered a much more sophisticated attack, and a very recent article indicates that the attack is linked to Turkey.

- **United States, Russia, Iran: the visible part of the iceberg**

In last year's report, we explained that a few years ago the United States adopted the "Name to Shame" policy for the cyber sector and named three countries in particular: Russia, North Korea and China. This year we can add Iran (see this AA20-006A alert published in early 2020), and this is of course also the result of the current high tensions between these two countries.

Iran has been known for many years to have offensive cybersecurity capabilities (capabilities developed in response to the Stuxnet attack of 2010 which targeted Iran); it has indeed been cited many times in the 2019 news for cyberattacks, for example:

- Attacks targeting research institutes using **dnaLIMS** DNA sequencing software
- Outlook attacks by the Iranian group APT33 (Elfin)
- LinkedIn user attacks by the Iranian APT34 group (OilRig)

It can also be noted that in 2019 hackers (using the pseudonym "Dookhtegan") published on the Internet attack tools belonging to Iranian groups. It is difficult to say whether this is a destabilization attempt, or simply an isolated act by a hacker. Kaspersky indicates that it could be a disinformation attack by the Russian group Sofacy (APT28). This Russian group has already been cited many times for many attacks, including disinformation attacks (e.g. attacks against the US Democratic Party during the 2016 US elections, or Macron-leak attack in 2017).

Russia has also been cited many times this year, as a victim of attacks (this is quite unusual):

- Reuter announced in June 2019 that the United States (and its allies) had compromised the Russian company Yandex (the Russian equivalent of Google).
- The New York Times announced in June 2019 that the United States had carried out attacks against electricity networks in Russia.
- A previously unknown hacker group announced that it had hacked into an FSB subcontractor and stolen several terabytes of data describing projects carried out for the FSB.

3.5. With ATT&CK and Open-CTI the analysis and response to incidents is growing in maturity

ATT&CK is a project of the American organization **MITRE** which has become the reference for modeling the behavior of attackers. It enables the development of a defense system focused on already known attack behavior, for example by identifying missing defense mechanisms or by measuring the detection capabilities of a SOC. Started in 2013, and made public in 2015, ATT&CK became highly prominent in 2018 (the first conference dedicated to this subject took place in October 2018: ATT&CKcon). **2019 confirms the community's interest in ATT&CK.** This model federates around it many initiatives, such as Atomic Red Team (test dataset simulating attacks) or Atomic Blue Detection (EQL Analytics library to detect an attack).

Also in the field of CTI (Cyber Threat Intelligence), in 2019 French ANSSI and CERT-EU published the **OpenCTI** project in open-source. This tool makes it possible to classify and structure the data available about attacks, attackers, and their tools. **OpenCTI** thus completes the existing offer in the CTI domain which includes both open source tools such as **MISP** and commercial tools such as: ThreatQuotient, Anomali, ThreatConnect, ...

Finally, the **SIGMA** format (which appeared in 2017) is gradually establishing itself as a de-facto standard. SIGMA is a language for describing a SIEM alert in a neutral format independent of the tool used.

Brief published in the Cert-IST newsletter of June 2019

Sysmon and Sigma

Sysmon and Sigma are two "tools" that are becoming increasingly popular in the field of log monitoring and attack detection. We present them in this short article.

Sysmon is a Microsoft tool that generates additional logs on a Windows computer. The main advantage of these new logs is that they allow to precisely track the processes launched, and thus to detect dangerous ones. Sysmon also logs other events such as file creation, network connections, and most

recently DNS resolutions. The logs generated by Sysmon are sent to the standard Windows event log. There are many examples of abnormal behavior that can be detected with Sysmon (see for example the Sysmon-DFIR page). For example, it can detect:

- Mimikatz tool,
- Malicious Powershell scripts,
- Suspicious WMI subscriptions (which is a means of persistence).

Sysmon has existed since at least 2014 (oldest article found on this subject), but became very popular in 2017. It is part of the SysInternals tool suite developed by Mark Russinovich.

Sigma is a language developed by Florian Roth (@Cyb3rops on Twitter) that is used to describe a SIEM detection rule. Sigma is therefore the equivalent in the field of logs of what YARA is for file search. Sigma project also provides a converter (called "sigmac") that transforms a Sigma rule into a format suitable for various detection systems, among for example: ArcSight, ElasticSearch/Kibana, Graylog, Grep/PowerShell, LogPoint, Qradar, Qualys, Splunk, SumoLogic.

More than 200 open-source detection rules are available on the Sigma website.

On the topic of Sigma, it is worth to mention the uncoder.io website which also provides a tool to convert detection rules from one format to another. Sigma is used by this site as a pivot language to switch from one format to another. This site can be used to quickly browse various examples of Sigma rules (using the "Select document" drop-down menu).

For more information:

- Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- Sysmon – DFIR: https://github.com/MHaggis/sysmon-dfir
- Technet: https://blogs.technet.microsoft.com/motiba/2017/12/07/sysinternals-sysmon-suspicious-activity-guide/
- Sigma: https://github.com/Neo23x0/sigma

3.6. Data leaks: 9 billion passwords; what's next?

For several years now, the number of attacks and the volume of stolen data has been steadily increasing. The year 2019 did not disprove this trend, with even a paroxysm in terms of password leaks:

- In January 2019, lists containing millions of account names and passwords were published on the Internet. They were gathered in packages called **"Collection #1", "Collection #2", ... , "Collection #5"**. These are mostly old lists of names and passwords that have been circulating in the underground for a long time.
- From February to April 2019, a hacker named **Gnosticplayers** then put on sale on the DarkMarket 5 series of new lists containing a total of **932 million new accounts** (see this ZDnet article).

The Have I Been Pwned website, which lists all the accounts stolen in recent years, indicates that it currently has a base of more than **9 billion accounts**, which shows the extreme scale of this phenomenon.

Note: Have I Been Pwned is not a malicious site, anyone can consult this site to find out if one of their personal accounts is in the lists of stolen accounts circulating on the Internet. Inspired by this site, others offer the same service, for example Firefox and Chrome.

- **What happens to the stolen data?**

Relatively little reliable information is available on the exact nature of stolen data and its ultimate use.

The most publicized cases concern:

- Personal data such as name, address, date of birth, etc. Most often, these are extracts from the customer databases of the companies that have been breached, and we now about these leaks through the official declarations of the affected companies (due to the legal reporting obligations).
- E-mail addresses, passwords or even credit card data. These data are clearly of value for cybercriminals. They are therefore re-sold on the Black Markets

The rest is much more obscure. It is easy to imagine that a hacker who finds data during an intrusion will copy it if he thinks it has value and knows how to resell it, and ignore it when the data has no meaning for him. In this area, state attacks are more dangerous (many things are of interest to states) and attacks from competitors (which target industrial property) are critical.

Cybercriminals may have realized that stealing industrial property information (without acting on command) is a new and profitable field and this is a concern for the future. Indeed, we saw in late 2019 a first case (see this testimony of BleepingComputer.com about the company **Allied Universal**) where during ransomware attacks targeting a company, the attacker stole data and then threatened to publish it if the ransom was not paid. In another troubling case, in April 2019, hackers announced that they had hacked the German company **CITYCOMP** and threatened to publish data from their customers, which included Oracle, Airbus, Toshiba and Volkswagen (see this article published by Vice.com). The affair did not have a public follow-up and remains quite mysterious.

4. Recurring threats not to forget

In this chapter, we highlight threats that are not new but are still very prevalent problems. It is therefore a call for vigilance in some areas that we believe require special attention.

- **Remote access protection and 2-factor authentication (2FA)**

Authentication by the use of a simple password is today an obsolete security measure for a service accessible from the Internet. Indeed, there are countless cases of data leakage (theft of a website's account list) or password theft by phishing.

The use of strong authentication, for example 2FA (2-Factors Authentication), is therefore essential when accessing external services in the Cloud, such as an Office 365 email service or even an extranet service such as a simple webmail.

Note: Some 2FA solutions are no longer considered secure (in particular 2FA by SMS) and we devoted an article in our February 2019 monthly newsletter to this subject. However, it is also obvious that against an ordinary attacker, it is better to have a weak 2FA solution than no 2FA at all!

- **Cloud security**

This is also a well-known fact, but it's important to remember that deploying a solution in a secure Cloud does not guarantee its security. There have been many incidents where cloud spaces have been hacked (typically Amazon S3 storage spaces) because they had been poorly secured by the Cloud customer. The Cloud service provider only provides security on the layers they operate. For the higher layers, security is still the responsibility of the project who designs the global architecture and who must analyze the security of its architecture. So beware of cloud solutions deployed too quickly, without a technical analysis of the security of the architecture!

- **Attacks by suppliers and partners**

More and more frequently, attacks are no longer direct, but rather pass through suppliers or partners. For example:

- An email spear-phishing attack is attempted by sending an email from a provider that the victim knows and trusts,
- A network intrusion is launched from a partner's network that has been attacked to serve as a bounce point.

We discussed these aspects in last year's annual review and the subject is still very prominent in the 2019 news, as we saw for example in the case of attacks passing through the structures of IT service providers (see §3.3), or the attack against **Airbus** in 2018 and 2019.
To mitigate this threat, we think that several points are important:

- Network interconnections with partners and suppliers must be filtered and monitored,
- It must be considered that a user workstation will probably be compromised one day or another, for example by a successful email attack. When this will occur, the company must detects this attack and stop its spread before the attacker is able to gain access to more sensitive parts of the information system.

- **Software (or even hardware) trapping**

There are a growing number of examples of attacks where software has been modified without the owner's knowledge in order to act as a backdoor once this software is installed and used by the targeted victim. Until now, these attacks have mainly been sophisticated intrusion cases by state-sponsored attackers (CCleaner and NetSarang attacks in 2017 or ShadowHammer in 2019).

Most companies probably do not have the capacity to implement effective protective measures against these types of attacks. As for the case of the workstation attack mentioned above, we think that the effort should then be focused on the ability to detect an attack afterwards and to limit its progression within the company.

5. Summary of Cert-IST activity in 2019

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.

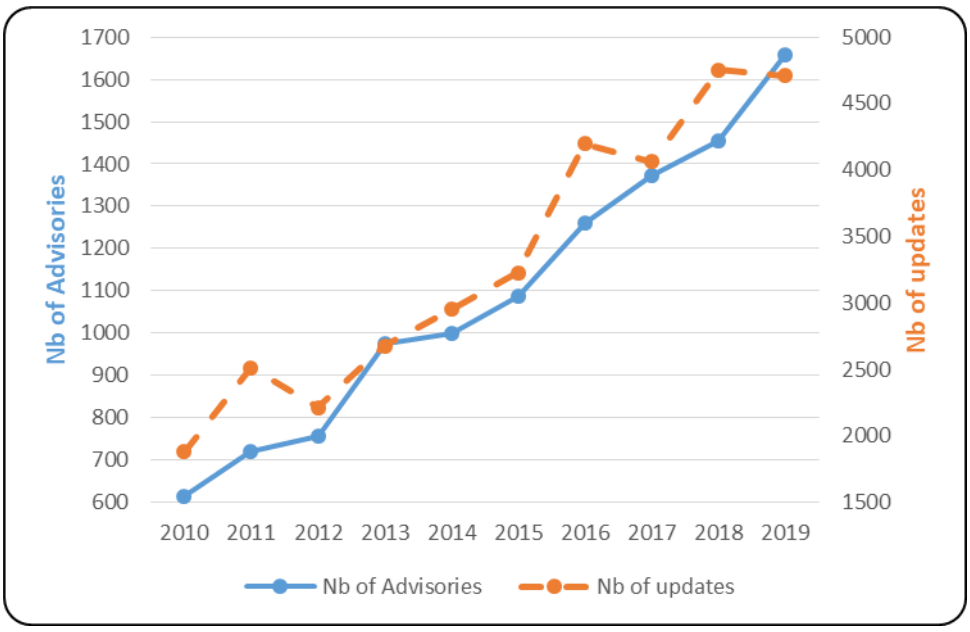
Cert-IST thus produces various types of publications:

- **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.

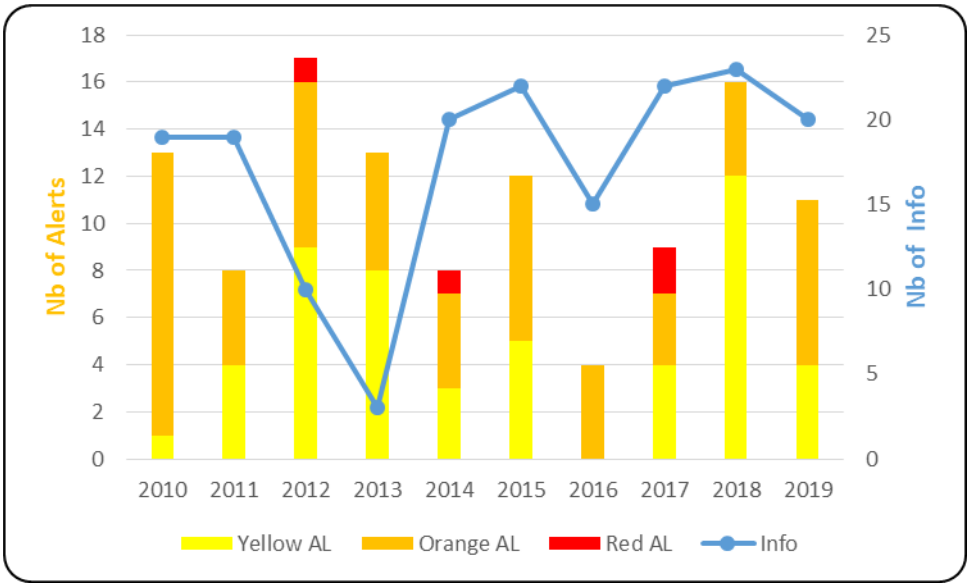
- **Alerts (AL)** which are issued when there is a particular risk of attack, and **INFO messages**, which provide an analysis for particular vulnerabilities (e. g. mediatized) but of lower immediate danger level. These 2 categories focus on the attack risks, while security advisories systematically 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).

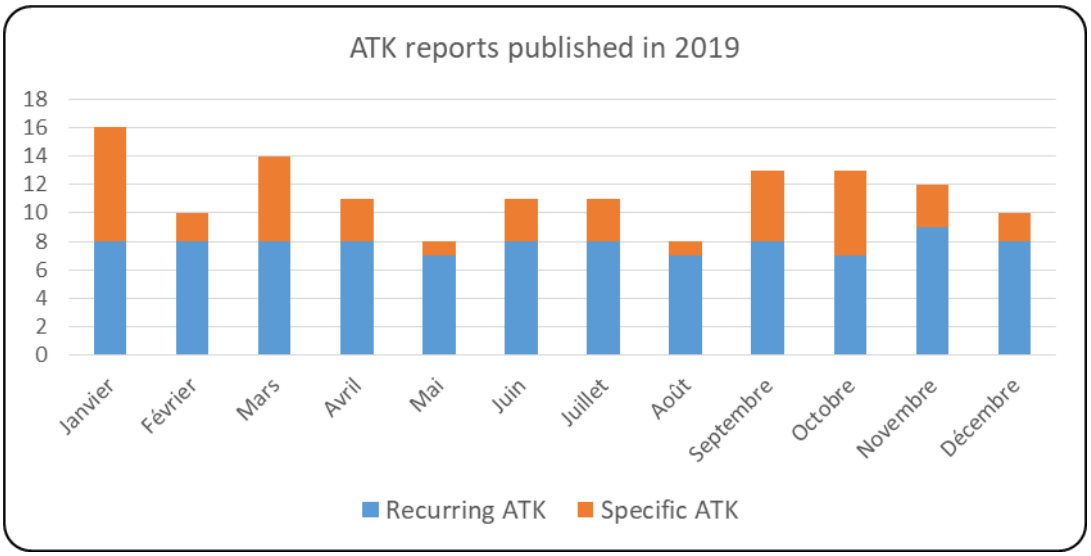
The graphs below show the Cert-IST different productions over the past few years.



Number of security advisories published per year



Number of security alerts published per year



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

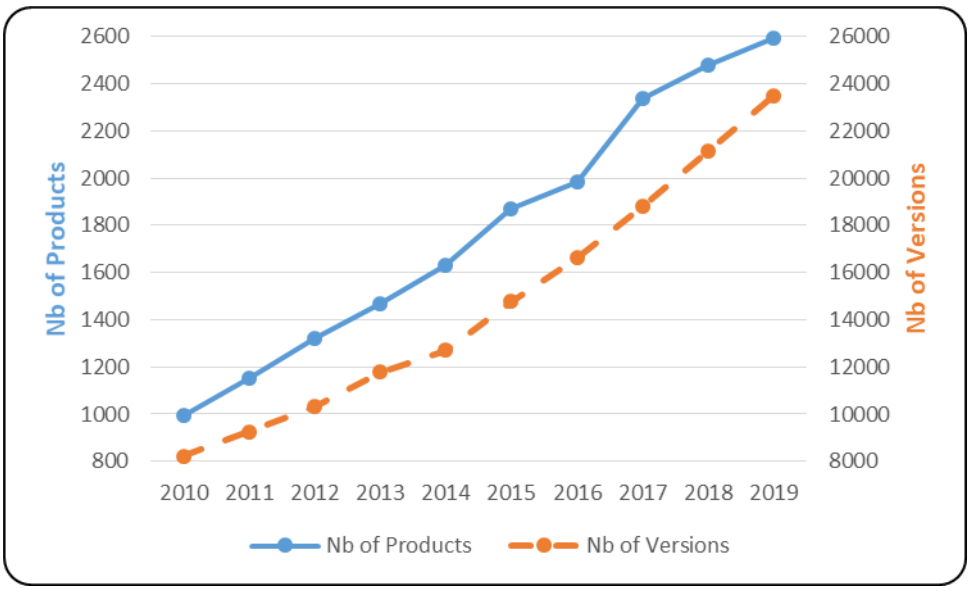
In 2019, Cert-IST published:

- **1 659** security advisories (including **80** SCADA advisories), **4 597** minor updates and **112** major updates.
  The number of advisories has been constantly increasing over the past few years (see the graph above), with an increase of **14%** compared to 2018. 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.

- **11** alerts and **20** Info messages. The last red-risk alerts were issued in 2017 (Wannacry and NotPetya). Year after year, activity in this category is highly fluctuating and there is no trend in the overall evolution.

- **136** attack reports were published in 2019, containing **2 854** enriched events in the MISP database and **498 577** indicators (IOCs).

Regarding the products and versions monitored by Cert-IST, at the end of 2019 Cert-IST followed **2 594** products and **23 504** versions. The following graph shows the evolution of the number of products and versions monitored by Cert-IST over the 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

- **2019: a disturbing rise in ransomware attacks**

2019 shows that unfortunately the cyber-threat is more and more serious for companies and even takes a critical turn if we consider the evolution of ransomware attacks (cf. § 3.2).

Some of the ransomware attacks of 2019 have made press headlines, in France (M6, Fleury Michon, CHU de Rouen, etc...) or in the world (Norsk Hydro, Mitsubishi Aerospace, City of Baltimore, etc.). They all have in common to be attacks specifically targeting large companies (likely to be able to pay substantial ransoms), and to have caused major shutdowns (several weeks) in these companies.

Besides ransomware, anything that makes money is of interest to cybercriminals, and in 2019 the most prominent attacks were (cf. § 3.3):

- Cryptominers: a very large number of the attacks seen in 2019 were aimed at installing crypto-mining software on the servers of vulnerable companies.
- Web skimmers: many e-commerce websites have been infected by **Magecart** attacks (the name given to this attack technique) where a JavaScript code is installed by the hacker to steal the (credit card) data entered in the site's payment form.

- **Companies in the sights of cybercriminals and cyber spies**

Over the past several years, the threat has been growing with attacks affecting an increasingly wide range of companies:

- Cyber-criminal attacks have started (in 2005) against banks and their customers, or against online betting sites. Today cybercriminals are attacking with ransomware any company likely to pay a large ransom.
- State and cyber-espionage attacks became a major phenomenon in 2013 but mainly concerned international companies. Today these attacks often also target sub-contractors of these international companies and then carry out bounce attacks.

While companies have clearly become targets of great interest to cybercriminals, it is also becoming clear that attack techniques are spreading faster and faster, from the most sophisticated attackers to others:

- Cybercriminals are inspired by what they have seen elsewhere: infiltration attacks (discreetly infecting a first company's computer system and then progressing inside the company several weeks to reach high-value targets) were first seen in state and cyber-espionage attacks, but are now also commonly practiced by cybercriminals.
- Cybercriminals know very quickly how to turn an "exploit" (a program allowing to exploit a vulnerability, developed by experts and later made public via open tools such as Metasploit) into a successful attack campaign.

- **Security in depth: an essential defense baseline**

Today, companies that are not paying close attention to IT security are highly exposed to cyberattacks.

This first implies to set up defenses and segregate the different networks. As no system is flawless, one must ask questions (during the design phase of a system) such as:

- What will happen when an intrusion will succeed?

- How can the propagation of this incident be limited?
- What will be the consequences of a data leak?

Another important element is to keep the systems up to date by applying the security patches issued by constructors. After human error (including phishing), un-applied patches are the most important cause of intrusion. It has often been observed that old vulnerabilities still allow intrusions several years after patches are made available. Of course, there is often a portion of "unpatchable" systems within organizations (obsolete, unregistered, etc.), however the deployment of security patches remains a fundamental security practice. For the most serious vulnerabilities, Cert-IST issues alerts (about ten per year) in addition to security advisories (cf. § 5.1). These alerts are indicators for companies that the deployment of patches must be especially fast.

- **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.