Annual Report on Attacks and Vulnerabilities seen in 2020

Released on February 2021

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 begins with a summary of 2020 major security events (chapter 2). From there we analyze the key trends (chapter 3). We also explore the Cert-IST activity throughout 2020 (chapter 4).

Finally, we conclude (chapter 5) 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 2020?

The following table summarizes the key events of 2020. You will find events which were highly mediatized or the events that are considered as major indicators of the cyber threat evolution.

January 2020	**Travelex**, currency exchange specialist was hit on 31-Dec-2019 by the Sodinokibi **ransomware**. This cyberattack was the trigger for a broader crisis (in a difficult Covid-19 context) which led Travelex to significantly restructure its activity. Numerous ransomware attacks will be announced throughout the year. Among the very numerous victims in France were **Bouygues Construction**, **Carlson Wagonlit Travel**, **SopraSteria** or **Rouen's CHU hospital**, and abroad **Carnival** (cruise), **Brown-Forman** (Jack Daniel's whiskey), **Garmin** (GPS), **Enel** (Electricity), **Software AG** (software), …
January 2020	**Citrix Netscaler and ADC** (CVE-2019-19781): A wave of attacks targeting these Citrix equipment forces the editor to urgently develop patches. This crisis, which lasted throughout the month of January, has been nicknamed **Shitrix** by some people.

January 2020	**CurveBall: the NSA's bug** in elliptic cryptography. Microsoft fixes this CVE-2020-0601 vulnerability in Windows 10 which affects the verification of digital signatures when they use elliptic cryptography. This vulnerability has been in the news because it was discovered by the NSA (hence its name "NSA's bug") and that it breaks electronic signature everywhere (on Windows 10): in emails, websites, executables, etc...
January 2020	Others Microsoft vulnerabilities also had been given a nickname in 2020, without really provoking large-scale attacks: **Bluegate** (RDP Gateway vulnerability in January), **GlueBall** (vulnerability in the cryptographic signature of MSI files, in August) or **Badneighbor** (ICMPv6 vulnerability, in October). We also talk below about the following more severe flaws: **SMBGhost** and **SMBleed** (March), **SIGRed** (July), **ZeroLogon** (September) and **Bronze Bit** (November).
January 2020	**Intel CacheOut**: a new attack against Intel processors is released. Since Spectre and Meltdown in January 2018, discoveries of this type have multiplied. For 2020 there is also the followings: **L1DES**, **VRS**, **LVI** (Load Value Injection on Intel), **Take A Way** (AMD), **CSME IOMMU CVE-2019-0090** (Intel), **StarBleed** (FPGA Xinlinx), **Platypus** (Intel power leakage) and **Crosstalk**.
February 2020	**Ghostcat** (CVE-2020-1938) a critical vulnerability in the AJP connector of **Tomcat** (the Java web server from Apache foundation) allows an attacker to read any file from the web server (and execute arbitrary code if file upload is allowed). This vulnerability was widely used in 2020 in attacks against Tomcat servers.
February 2020	**Kr00k** vulnerability in **WPA2**. This is a variant of the KRACK (Key Reinstallation Attack) attack of 2017 and its name was built by replacing 2 letters of KRACK with zeros (the attack uses the fact that the WPA2 key is overwritten with zeros when de-association occurs).
March 2020	**SweynTooth**: it is the name given to a series of 12 vulnerabilities (of variable severity) in **Bluetooth** chipsets of some manufacturers (including Cypress, NXP and Texas Instrument). Other Bluetooth vulnerabilities will be released during the year: **BLURtooth**, **BLESA** and **BleedingTooth**.
March 2020	**SMBGhost**: Due to a mistake, the CVE-2020-0796 vulnerability in the Windows SMBv3 compression was accidentally revealed 3 days before the release of Microsoft patches that fix it. This wormable vulnerability is critical and there are fears of massive attacks as for EternalBlue (WannaCry) in 2017. Exploit programs are announced (in particular by the ZecOps.com company) and finally delayed. They are finally released in June and the Cert-IST raises its CERT-IST/AL-2020.005 alert to orange level. In June Microsoft fixed additional SMBv3 vulnerabilities, including the **SMBleed** vulnerability (CVE-2020-1206) that ZecOps uses in its exploit program in combination with SMBGhost. So far there have been no massive attacks using these vulnerabilities.
April 2020	**Zoom**: This video conferencing solution is suddenly attracting interest because of the lockdown. Concerns about its security lead some organizations to ban its use. The Zoom company is responding by intensifying its efforts on the product security (which until then did not seem to be a priority).
May 2020	**Strandhogg 2.0**: This **Android** vulnerability takes its name from a similar vulnerability released in December 2019, and allows to spy on applications launched on the smartphone. It had been corrected in April by Google, before being disclosed in May.
May 2020	**SaltStack** (a tool for managing pools of servers in a datacentre, and similar to software such as Puppet, Ansible or Chef) fixes critical vulnerabilities (CVE-2020-11651 and CVE-2020-11652) which are used by a wave of attacks the following weekend. The attack allows to take control of all machines in datacentres managed with SaltStack.

June 2020	**Australia** announces that it is victim of a large scale attack targeting all sectors of activity and coming from a state attacker (may be China). It describes in detail the operating procedures in a report entitled « **Copy-paste compromises** – TTP used to target multiple Australian networks » (see § 3.6).
June 2020	The JSof-Tech.com society publishes **Ripple20**: a set of vulnerabilities that affect the TCP/IP stack developed by Treck, which is used in a large number of products (connected devices, industrial or medical equipment, etc.). This event reminds similar publications: Urgent/11 (Summer 2019) and Amnesia:33 (see in December below).
June 2020	**An UPnP vulnerability "CallStranger"** is published. It is of moderate severity except when the vulnerable UPnP equipment is attached to 2 distinct networks: with this vulnerability such equipment could be used as a relay to reach protected network from a general purpose network. We have issued **INFO-2020.018** to draw attention to this vulnerability.
July 2020	**22 900 MongoDB databases** that were unprotected and reachable from Internet have been erased by a hacker (see this article from ZDNet).
July 2020	Spectacular police operation in France (C3N) and Netherlands against **EncroChat phone users**. These secure phones sold to criminals used a server located in France, which allowed infiltration by C3N.
July 2020	Microsoft fixes the **SIGRed** vulnerability (CVE-2020-1350) that affects its DNS server and allows a remote attacker to execute arbitrary code with SYSTEM privileges. There was no massive wave of attacks, but this vulnerability is in the Top 25 vulnerabilities used by Chinese attacks (see § 3.6). We have issued the **CERT-IST/AL-2020.009** alert for this vulnerability.
July 2020	**SAP RECON** (Remotely Exploitable Code On NetWeaver) vulnerability: Onapsis recommends applying SAP patches for this vulnerability in the NetWeaver component as soon as possible.
July 2020	The **BootHole** (CVE-2020-10713) vulnerability was widely publicized in the media but its impact remains moderate since it mainly affects Linux. It affects the GRUB2 boot-loader and allows to execute malicious code at boot time (bootkit attack).
September 2020	**ZeroLogon**: This attack exploits the CVE-2020-1472 vulnerability in the Windows NetLogin service. It allows an attacker who has already penetrate the company to instantly obtain administrator privilege on any Windows Domain Controllers (DC) that are not patched. This vulnerability is often the first one used by an attacker once he has penetrated a company (because it is easy to perform).
September 2020	**DDOS attacks and blackmail** are observed in late August and early September (see § 3.5). These attacks started again at the end of the year. They did not have strong consequences but show that DDOS attacks are a nuisance that cannot be ignored.
October 2020	A joint action of several vendors (Microsoft, ESET, etc.) tries to **neutralize the Trickbot Botnet**. The operation is partially successful (120 of 128 Trickbot's C&C servers have been neutralized) but the malware reorganized itself afterwards and strengthened its architecture by using EmerDNS (a resilient DNS system of the Emercoin project) and C&C with the **.bazar** extension. One of the goals of the Microsoft operation would have been to disrupt Trickbot during the U.S. elections in order to avoid attempts to influence the vote.
November 2020	**SAD DNS** (CVE-2020-25705) is a new method to carry out the "DNS cache poisoning" attack discovered in 2008 by Dan Kaminsky and corrected the same year. SAD DNS bypasses this correction by using a new method (a "side-channel") based on "ICMP rate limit" messages to guess the UDP port used by the DNS server.

November 2020	**Cobalt Strike**: Some of the sources of this offensive tool have been published on Internet. Cobalt Strike is a commercial tool for pentesting, but it is more and more often seen in real attacks (see § 3.7.3). It was, for example, heavily used during ransomware attacks in 2020.
November 2020	A list of **50,000 Fortinet devices** affected by CVE-2018-13379 flaw is circulating on Internet. This vulnerability was fixed by Fortinet in May 2019 but the vulnerable devices have probably not been updated for one and a half years.
November 2020	**Kerberos Bronze Bit** is a new Kerberos attack, similar to the "Golden Ticket" and "Silver Ticket" attacks. It allows, by changing a few bits in a genuine Kerberos ticket, to illegally increase the privileges of a logged-in user.
December 2020	**Amnesia:33** is the name given by the Forescout company to set of 33 vulnerabilities discovered in 4 open-source TCP/IP stacks (uIP, FNET, picoTCP and Nut/Net) used in many products (smartphones, games consoles, captors, etc.). These discoveries come from a project inspired by Ripple20 (see above in June) by looking for flaws in other TCP/IP stacks.
December 2020	**Orion SolarWinds attacks**: This attack (supposedly Russian) is a major event of 2020 (see § 3.4) by its nature (supply-chain attack by trapping the Orion software of the SolarWinds company), its scale (compromising several U.S. agencies and leading companies such as FireEye and Microsoft) and its sophistication.
December 2020	**Flash Player** is over! Late 2020 Adobe discontinues this flagship product of the 2000s. Initially developed by Macromedia (a company acquired by Adobe in 2005), the product experienced many security issues from 2008 to 2012. Since 2010 Apple refused to allow it on its tablets and phones. Flash was then gradually overtaken by the native features of HTML5.

3 Analysis of the most striking phenomena of 2020

In this chapter we analyze the most significant events of the year:

- The cyber threat induced by the Covid-19 crisis
- Ransomware's attacks against companies
- Attacks against VPN access and exposed Appliances
- Orion SolarWinds and Supply-chain attacks
- DDOS attacks
- Increasingly sophisticated state-sponsored attacks
- Technical developments observed in 2020

In brief, …

There are no real surprises in our list of the most striking phenomena of 2020: Covid-19, Ransomware, and SolarWinds attacks are of course in the list. The rest of this chapter analyzes each point in more detail, but if you only have a few minutes to read this report, here's the gist of it.

- Covid-19: To date, there are no known cases where an intrusion has been formally attributed to the technical measures taken to enable teleworking. However, it is sure that to face with the emergency and quickly implement telework, some companies **have exposed themselves to an increased risk of intrusion.**

- Ransomware: Already a major phenomenon in 2019, ransomware attacks exploded in 2020 and there is still no sign of a decline. Cybercriminals are multiplying their means to put pressure on companies and collaborating with other miscreants in an increasingly organized ecosystem.

- VPN attacks: These attacks often target equipment that seems to us too vulnerable (hard on the outside but weak inside). More and more often, these attacks are used as a starting point to penetrate deeper Company's internal network.

- SolarWinds attacks: Beyond highlighting supply chain attacks, the SolarWinds attack shows that the Cloud Office 365 environment is a coveted target.

- DDOS attacks: They are always there and constitute a threat for which the company must have a response in place.

- State-sponsored attacks: Some states have demonstrated in 2020 advanced capabilities in cyber-attacks. For example, China has demonstrated its know-how in industrializing vulnerabilities that have been made public, and Russia has demonstrated its expertise in designing complex attacks.

- Technical developments: Microsoft Exchange, SAML and OAUTH attacks, and Cobalt Strike are 3 of the technical areas that we have identified as milestones for the year 2020.

3.1 The cyber threat induced by the Covid-19 crisis

The COVID-19 crisis is first and foremost a health and economic crisis. But it has also generated sustained concerns from an IT point of view, and these concerns can be divided in 3 areas that have occurred (almost) one after the other all along 2020:

- Mail and web attacks that use Covid-19 topics to attract victims,
- Attacks that target teleworkers and related IT infrastructures,
- Attacks against hospitals, research and vaccines.

We examine each area below, but two preliminary questions help to better understand the cyber threat induced by the Covid-19:

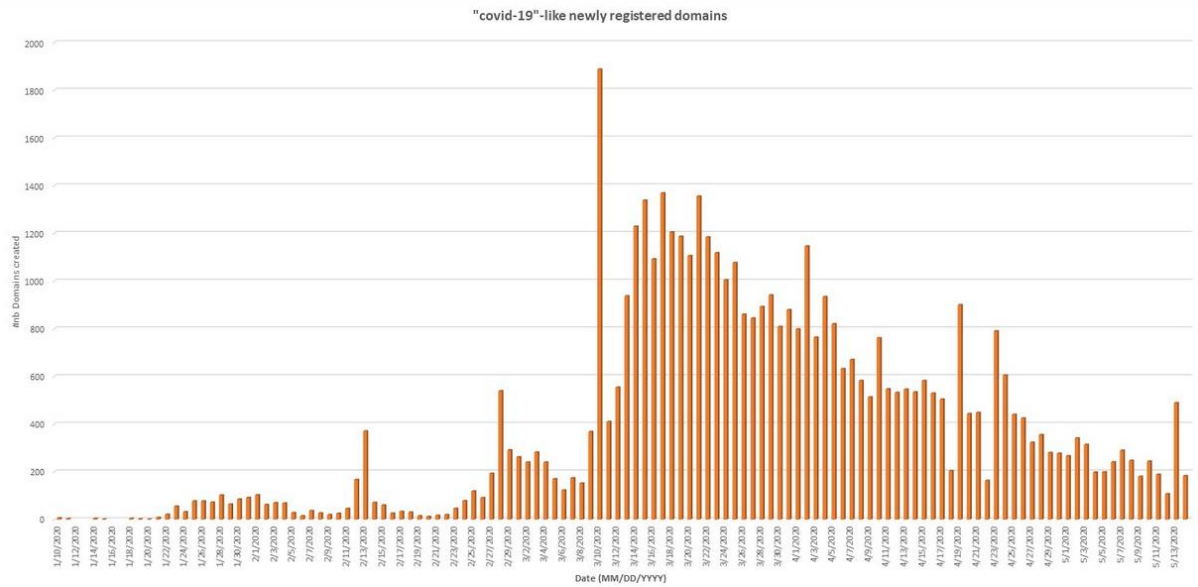
- Who are the attackers? We find for these attacks, 2 well known groups in the cyber threat landscape: cyber criminals seeking to make money through the Covid crisis, and cyber-spies (state sponsored attacks) that have strategic interests related to the Covid.
- Who are the targets? For the most part, cyber-espionage targets businesses, while cyber-criminals target anyone who is likely to pay (the general public, businesses, hospitals and states). However, cyber-espionage also uses sometimes bounce attacks, targeting employees at their homes in order to reach their companies. And this last aspect is very important in the case of the Covid-19 crisis.

We can see through these 2 questions that the Covid-19 does not fundamentally change the threat landscape (same attackers and same targets). On the other hand, two aspects are very specific the Covid-19 crisis:

- **The number of attacks**: There has been huge increase in the number of attempted attacks, due to a windfall effect (Covid theme interests everyone) and also an emergency effect (hackers must react quickly, to take advantage of the windfall, but also to take advantage of people anxiety-with this pandemic).
- **Bounce attacks** targeting teleworkers are eased by the implementation of lockdown and the rapid deployment of technical solutions for teleworking.

• Mail and web attacks

The first effect of the Covid crisis was an outbreak of e-mail attacks that used the Covid-19 topic to infect the victims' computers with infected attachments, or lure them to malicious websites. These attacks have been used by all types of actors: crooks (selling products, fake SMS, etc.), usual Botnets (Emotet, Trickbot, etc.) and cyber-spying attacks (Spear-phishing).



The figure above shows the evolution of the number of domains created with names related to Covid-19 from January to mid-May 2020. A large part of these domains was malicious and this curve is an indicator of the number of email and web attacks observed. The first attacks were MalSpam Emotet at the end of January 2020. The attacks multiplied from the 25-Feb-2020 then blew up in mid-March. They then gradually decreased. At the end of 2020, a slight increase was observed, probably related to the availability of vaccines.

• Attacks related to teleworkers

Secondly, lockdown measures have forced companies to set up (or expand) teleworking. This has led to problems of several kinds:

- The implementation by organizations of poorly secured access solutions (the only ones available immediately): opening unprotected RDP accesses, re-commissioning outdated (not updated) access equipment, etc.
- The implementation by users of their own solutions: use of personal computers and messaging, use of multiple video conferencing tools installed from insecure sources (see for example this fake Zoom application),
- Difficulty for companies to maintain nominal security rules: postponing updates for nomadic workstations (due to the fear of malfunctioning or lacking network bandwidth), relaxing password expiration rules, accepting multiple exceptions, etc.

There is still a lack of data to quantify the real impact induced by these weaknesses, and to our knowledge there are no known cases of severe incidents formally attributed to the technical measures put in place during Covid-19. It is certain, however, that many organisations did the best they could, and exposed themselves to an increased risk of intrusion. It is important to limit the duration of this period of vulnerability and to consider measures for:

- Improve (if necessary) the security of the teleworking solutions put in place,
- Detect as early as possible any data leaks or successful intrusions that may have occurred.

This last point (detection) has been a growing concern for several years now: if we cannot prevent 100% of the attacks, we must detect them as quickly as possible (reduce the "Time to Detect") and limit their impacts.

• Attacks against hospitals, research and vaccines

This latter aspect occurred at several moments of the crisis:

- The attacks against hospitals came at the beginning of the crisis and then faded afterwards. There have been multiple attacks. On one hand, some attackers probably hoped that hospitals would pay quickly to get rid of computer problems (this has not been the case to our knowledge) and focus on caring for the sick. On the other hand, some of the first attacks probably hit health care structures by mistake (randomly), without the aim to take advantage of the Covid-19 crisis. Subsequently, some attackers decided to stop this kind of victim, but this instruction was not followed by all.
- Attacks on research and vaccines. These attacks were revealed later (by end of April 2020, during the summer, and in December 2020) and this time they were cyber-espionage or disinformation attacks. Vietnam, China, Russia and North Korea have been credited for these attacks. In December 2020 the European Medical Agency announced that it had been the victim of a cyber-attack (probably Russian) targeting vaccine qualification data (see the official announcement and this article by Kaspersky).

3.2 Ransomware's Attacks against companies

Ransomware attacks targeting companies (often referred to as Big-Game Hunting) were already one of the major phenomena for year 2019 (see our 2019 annual report). And clearly the phenomenon got even worse in 2020 with:

- An increase in the number of cyber-criminal groups that have adopted this extortion technique (because it is profitable),
- Increasingly pressure techniques to convince the victim to pay (see below).

French ANSSI (National Agency for Cyber Security) announced a fourfold increase in the number of attacks handled in France in 2020 compared to 2019 (192 attacks compared to 54 in 2019).

Attackers' pressure techniques:

In addition to encrypting data from as many of the victim's computers as possible, all along the year the attackers gradually added other techniques to force the victim to pay the ransom:

- Stealing company data and threatening to publish or auction it off. This technique was first seen in November 2019 (Maze ransomware versus Allied Universal), but became almost systematic from 2020. Several victimized companies reported in 2020 paying ransoms to keep stolen data from being published, rather than to get computers unlocked.
- Publish the names of the victims on a website and post a countdown to the release of the stolen data. This advertising about the attacks even seems to turn into real press campaigns since very recently (in January 2021) the attacking group DarkSide invited the press to contact them to be kept informed of the ongoing negotiations with the victims.

- Carry out DDOS attacks to overwhelm the company's Internet access. This technique was used for example in September 2020 with the SunCrypt ransomware, but has not become widespread since then. It is possible that this technique was inspired by the series of DDOS attacks seen in September 2020 (see § 3.5).
- Physically intimidate (through threatening phone call) to make victim companies pay. In December 2020, the FBI reported that this practice had been observed since February 2020.

For the victims we have also seen several changes:

- In 2019, paying the ransom (and talking about it) had become an accepted practice (as a last resort). In 2020, paying a ransom seems less and less of a solution if we cannot guarantee that the attacker (or another attacker) will not come back with a new ransom demand, because he has kept an access (backdoor) within the company or has kept stolen data that he now wants to negotiate.
- The use of insurance (to cover part of the costs of reactivation) and the intervention of companies specialized in negotiation (to dialogue with the attackers and lower the ransom) are becoming common and recommended practices.

• The cybercriminal ecosystem:

Ransomware attacks involve a whole set of actors who collaborate and constitute an ecosystem where each one is paid according to the services he provides.

At the top of this pyramid is the group that directs the infections. It is often referred to as the RaaS Group (Ransomware as a Service). It provides the ransomware and an initial access to a victim's network to an affiliate who is responsible for exploring the victim's network and installing the ransomware. Initial access to the victims' network were previously obtained on underground forums from a broker, who purchases these accesses (email address or login, and associated password) from ATO specialists (Account Take Over). They steal these accounts by organizing phishing campaigns or by mass testing login and password pairs (a so-called "password stuffing" attack) obtained during data leaks. A last category of actors is specialized in data leaks attacks (theft of account databases) or direct attack of servers (they then sell access to the backdoor they have installed on the attacked machines).

Note: We have known for decades about brute force attacks against SSH accesses, but this phenomenon has greatly increased in recent years with data leaks and password stuffing. Overall, according to Akamai, ATO attacks account for 98% of the attacks seen on Akamai's infrastructure (figures given during a presentation at the BotConf 2020 conference).

The following is excerpted from the headline of our October 2020 monthly Bulletin.

According to a report published in November 2020 by Coveware.com (and which is consistent with what has been published by other sources)

- Median ransom amount is **about $100,000** (for Q3-2020), but the amounts rise rapidly for attack targeting large companies (see note below). Attacking these large companies is therefore the most lucrative business for the attackers.
- Paying a ransom to avoid publication of the stolen data is probably a bad choice because in several cases the data was finally published.
- **Poorly secured RDP access** remains the number one vector of attack (ahead of phishing and software flaws).
- The average downtime caused by a ransomware attack is **19 days**.

Note: According to published reports, ransoms in the range of $5 million are not uncommon.

3.3 Attacks against VPN Access and Exposed Appliances

During 2020, attacks targeting corporate VPN accesses (and more generally the Appliances connected to Internet) have multiplied. This phenomenon began in September 2019 with the attack against PulseSecure and Fortinet equipment and amplified in 2020 with more equipment affected.

Here are the devices targeted by these attacks and the references of the advisories or alerts issued by the Cert-IST on these subjects (see chapter 4 for the distinction between these 2 types of Cert-IST publications). **Companies that use these equipment must ensure they have patched these vulnerabilities.**

- **F5 BIG-IP (CVE-2020-5902):** **CERT-IST/AV-2020.0878** advisory dated 01-Jul-2020 and **CERT-IST/AL-2020.008** alert**.**
- **Palo Alto Networks (CVE-2020-2021):** **CERT-IST/AV-2020.0868** advisory dated 30-Jun-2020 and **CERT-IST/AL-2020.007** alert**,** and **Global Protect VPN (CVE-2019-1579)** : **CERT-IST/AV-2019.0903** advisory dated 19-Jul-2019, and **CERT-IST/AL-2019.010** alert.
- **Citrix ADC and Citrix Gateway (CVE-2019-19781)**: **CERT-IST/AV-2019.1624** advisory dated 18-Dec-2019 and **CERT-IST/AL-2020.001** alert**.**
- **Pulse Secure VPN (CVE-2019-11510):** **CERT-IST/AV-2019.0520** advisory dated 25-Apr-2019 and **CERT-IST/AL-2019.010** alert.
- **Fortinet VPN SSL (CVE-2018-13379:** **CERT-IST/AV-2019.0668** advisory and **CERT-IST/AL-2019.010** alert.

• Are appliances hard on the outside and weak inside?

Most of these vulnerable equipment are Appliances, i.e. machines built to provide a specific service (firewall, antispam, WAF, etc…). An Appliance is often built using a custom-configured standard OS (e.g.

Linux, FreeBSD, etc.) and proprietary application software. The attacks seen in 2020 highlight that some of these Appliances are "hard on the outside, but weak inside":

- The external layer is hard: there are few exposed network services and they are hosted by a robust OS.
- But the internal components are rather weak: if a first minor vulnerability is found (e.g. a "directory traversal"), the attacker can then reach internal components that are not strong enough to resist deeper attacks.

Due to a lack of compartmentalization and defense in depth (which is a concern for equipment designed to be connected directly to Internet), a small vulnerability allows in the end (by chaining other vulnerabilities) a complete takeover of the equipment.

• An attractive target for attackers

These devices have often a front-end on the Internet and as soon as a vulnerability is found, attacks occur. Some attackers simply install a crypto-miner (software that hijack the CPU to generate crypto-currencies) on the vulnerable computer, but more and more often (and this is a 2020 trend) **such attacks are used as a starting point to go deeper inside the company**. For example, the attacker can then install a ransomware within the company (cybercriminal attack) or carry out cyber-espionage (state attack).

We also note that **vulnerable devices remain vulnerable for a long time, even for highly mediatized vulnerabilities**, because these devices have in fact been forgotten and left running unmonitored. For example (as we stated in our **INFO-2020.035** message), in November 2020, a list of nearly 50,000 Fortinet machines was circulating on the Internet, probably vulnerable to the CVE-2018-13379 which is a flaw fixed by Fortinet since May 2019 (these equipment have not been updated for a year and a half while the flaw has been highly covered in the media).

3.4 Orion SolarWinds and Supply-chain attacks

Announced on 13-Dec-2020, the attack through SolarWinds' Orion software will undoubtedly be better understood in 2021 when more elements will be available. But it is already obvious that this attack brings to the forefront a risk that we have already mentioned in our annual reports (see our 2018 and 2019 reports): the attacks via the supply chain (without the supplier's knowledge).

The attacker (supposedly Russian) first broke into the SolarWinds company and modified the Orion software production line to add a backdoor (named Sunburst) in Orion. The trapped versions of Orion were distributed by SolarWinds to all customers who applied the official product updates. The attacker then used Sunburst backdoor to penetrate some of the affected customers (the most interesting for him), in particular U.S. government agencies and U.S. companies at the cutting edge of the cyber field (for example FireEye and Microsoft).

It is not the first time that we see an attack where a legitimate software is trapped on the official website of its publisher. Examples include NotPetya in 2017 (MeDoc software trapped, supposedly Russian attack), or CCleaner in 2017 (CCleaner software trapped, supposedly Chinese attack). **However,**

the SolarWinds attack will undoubtedly serve as an example, and this form of attack will develop and interest more and more groups of attackers.

The different types of attacks via suppliers:

It should be noted that there are several forms of supply chain attack and that they have different levels of maturity and risk:

- equipment trapping (which had been evoked for example in 2018 for SuperMicro motherboards). This kind of attack has never been demonstrated for a large-scale attack. It raises a lot of concerns in strategic committees (see for instance the concerns about 5G technology deployment), but rather represents a theoretical risk for companies. Note: equipment trapping, on the other hand, is already used, and has been for a long time, for highly targeted attacks on a few individuals (by secret services or serious crime). But in this case, it is no longer really a supply chain attack.
- software trapping (as for the SolarWinds attack). These attacks have already been seen and the example given by SolarWinds will undoubtedly be taken up by others, first for state sponsored attacks, but also later for cybercriminal driven attacks. **The SolarWinds case is a signal of a risk that is increasing and that will have to be addressed.**
- bounce attack via a supplier or partner. These attacks are already common, both in state sponsored attacks (e.g. the Chinese **Cloud Hopper** attack in 2017) and cybercriminal attacks (e.g. the attack on **Target** stores in 2013).

• The targets of these attacks are often the most protected companies

Attack by trapping a supplier's software is very powerful because the victim cannot detect it until the software is installed. It bypasses all protection mechanisms (it can however be detected if it triggers alarms while wandering inside the victim's internal network). On the other hand, it is complex to implement for the attacker. It will probably only be used if there is no simpler method for the attacker to compromise the victim's network.

If the risk of attack is real (and proven), it is therefore probably not yet a priority for most companies. To date, there are few studies on methods to reduce this risk, but it is clear that this topic will now be actively explored. Monitoring the internal network, in order to identify suspicious behaviour, is undoubtedly one of the elements of the technical response.

• Sophisticated attack against Cloud Office 365

Another element highlighted by the SolarWinds attack is the attack against the Office 365 environment (offer renamed as Microsoft 365 in 2020). Investigations published so far show that once the attackers breached the companies, they sought to access the information stored in Office 365 and especially emails. To do so, they stole the SAML signing key (or in some cases added a new signing key) in order to generate valid SAML authentication tokens. Once this goal is achieved, the attacker can access the company's Office 365 environment from anywhere on the internal network, but also from outside the company. These SAML attacks (as well as the OAUTH attacks we will talk about later) are rather new and are part of the technical evolutions noted for 2020 (see § 3.7.2).

3.5 DDOS attacks

At the end of August and beginning of September 2020, a wave of DDOS attacks targeting companies was observed around the world. The press reported, for example, the attack against the Stock Exchange in New Zealand, or on telecom operators in France, Belgium and the Netherlands. But many other cases, with the same modus operandi, have not been made public. These attacks were accompanied by blackmails that requested the payment of a ransom in Bitcoins to prevent further attacks. The attackers pretended being infamous groups such as FancyBear (Russian cyber-espionage group also known as APT28), Lazarus (North Korean group) or Armada Collective (group known in the 2016's for its DDOS attacks), but this is probably not true. The attacks re-occurred at the end of the year (and beginning of 2021) and the attackers once again blackmailed targets who had not paid in September. Overall, the attacker was very opportunistic (he changed targets quickly if his interlocutor did not react) and rather clumsy in his communication.

Note: The Cert-IST issued **INFO-2020.027** in September 2020 about these attacks.

DDOS attacks are not new and occur on a regular basis on the Internet. But this DDOS campaign aimed at companies is nonetheless noteworthy. It shows that:

- Attackers are looking for every means to put pressure on companies. One can wonder if these DDOS attacks were not inspired by the success of ransomware attacks.
- Seemingly relatively inexperienced groups can easily carry out 150 Gbps attacks.
- DDOS protections (most often relying on an anti-DDOS service provider) seem more and more necessary to face this threat.

3.6 Increasingly Sophisticated State Attacks

If 2020 was the year of cybercriminal attacks using ransomware (see § 3.2), we should not neglect state sponsored attacks. Two such attacks seen in 2020 are particularly interesting.

• The supposedly Chinese "Copy/Paste" attacks against Australia

The Australian government announced in mid-June 2020 that Australia had recently been the target of large-scale attacks on all sectors of activity by a State attacker. This attacker has not been named but many think it is China. For these attacks, the Australian Cyber Security Center (ACSC) has published a technical report entitled: Copy-paste compromises – TTP used to target multiple Australian networks.

Australia does not consider these attacks to be sophisticated because the attack tools used are directly derived from exploits that had been published on Internet. That's why he calls these attacks "copy-paste".

However, these attacks are interesting because they show the professionalism of the attacker while executing the attack: the attack is methodical, progressive and it exploits all known techniques.

For example, for the Spear-phishing phase (which is used by the attacker only when direct intrusion via a vulnerable server has not been possible), the attacker tries successively more and more advanced techniques:

- Classical phishing with an e-mail inviting the victim to visit a page where he has to enter his account and password,
- Then sending an email with a malicious attachment,
- Then sending a phishing email that uses the OAUTH technique (see § 3.7.2),
- And if everything has failed, sending emails via an email-tracking services to see what kind of content the victim is likely to click on. This technique is probably used to identify the victim's interest and to prepare new attempts at Spear-phishing.

Top 25 Chinese attacks:

Another interesting document about the Chinese state sponsored attacks was published in October 2020 by the NSA. This is the list of the 25 vulnerabilities used by the Chinese during cyber-attacks.

This list is interesting because although it does not contain any 0days vulnerabilities, it contains only recent vulnerabilities (the majority are of 2020). This shows that the attacker keeps a close watch on new attack tools published on Internet and that he knows how to industrialize them quickly.

• The SolarWinds attack, supposedly Russian, against the United States

This attack (already mentioned in § 3.4) is remarkable for its technical sophistication. According to several sources it is currently the most sophisticated attack seen regarding OPSEC (operational security) aspect, i.e. a lot of effort has been put into preventing the attack from being detected, or cross-checking IOCs with other attacks, or tracing back to the attacker. For example, the same IOC (e.g. an IP address, an executable, etc.) has never been used twice in the operation as far as possible.

It was already known that the most advanced attacks today are those carried out by a few States. They are pioneers in new attack techniques and are often subsequently imitated by other States or by cybercriminals. These 2 attacks (Chinese and Russian) show once again that the capabilities of States in the field of cyber-attack operations have reached a level unequalled so far by other attackers.

3.7 Technical developments observed in 2020

In this chapter, we group together some technical facts that have emerged or have become stronger during 2020. They show the technical evolution of the attacks and the points to be monitored. Generally speaking, for 2020 these elements concern infrastructure servers rather than workstations. The workstation (and phishing aimed at users) has long been the preferred target of attackers. It seems that attacks on servers are now back in the front.

3.7.1 Attacks against Exchange, SharePoint and IIS

We have observed an increase in attacks on Microsoft Exchange, SharePoint and IIS (Microsoft's web server) solutions in 2020.

• Exchange: a hot target for attackers

The Exchange server has long been a coveted target for attackers. It allows access to users' emails (see for example the MailSniper tool published in 2016 to explore the emails of an Exchange server), but also to install a stealthy backdoor (see for example the LightNeuron backdoor used by the Russian group Turla since 2014) allowing the attacker to come back if his main access has been discovered.

In 2020, Exchange was also targeted by direct attacks that aimed to gain an access into the targeted companies through Exchange server vulnerabilities. Two Exchange components are commonly used in such attacks:

- **Exchanges cmdlet**: cmdlets are Exchange functions that can be called remotely using PowerShell scripts. They are designed to perform remote maintenance operations on mailboxes. Several vulnerabilities were discovered in 2020 on some cmdlets. These vulnerabilities allow a user with an Exchange account to perform actions with high privileges (usually SYSTEM privileges) on the Exchange server.
- **Web API**: There are several web services that provide access to Exchange functions through a web interface, such as ECP (Exchange Control Panel), EWS (Exchange Web Service) or OWA (Outlook Web Access). These APIs can be used to carry out attacks targeting cmdlets (vulnerabilities seen above) or attacks targeting the IIS web server hosting these APIs (in particular VIEWSTATE attacks, mentioned below).

Here are the most significant Exchanges vulnerabilities for 2020:

- **CVE-2020-0688** (**CERT-IST/AV-2020.0173** advisory and **CERT-IST/AL-2020.004** alert): Exchange uses a known MachineKey by default, which makes VIEWSTATE attacks possible on the IIS server used by Exchange. This vulnerability allows an Exchange user to take control of the IIS server via the ECP service.
- **CVE-2020-16875** (**CERT-IST/AV-2020.1236** advisory): A vulnerability in the New-DlpPolicy cmdlet allows a user with an Exchange account, via the ECP web interface or a PowerShell script, to execute arbitrary code on the Exchange server with SYSTEM privileges.

- **CVE-2020-17083** (CERT-IST/AV-2020.1583 advisory): a vulnerability in the Export-ExchangeCertificate cmdlet allows a user with an Exchange account, via a PowerShell script, to execute arbitrary code on the Exchange server with SYSTEM privileges.

Microsoft is well aware of this trend and published a blog post about attacks on Exchange in June 2020: Defending Exchange servers under attack.

• SharePoint: fewer attacks than Exchange but highly coveted

The CVE-2019-0604 vulnerability in SharePoint was a "golden" vulnerability for attacker in 2019 (see our **CERT-IST/AL-2019.006** alert of May 2019). It had been used in particular in ChinaChopper attacks (supposedly Chinese).

In 2020 the new SharePoint vulnerabilities were therefore carefully reviewed by attackers to see if they could also be used. Unlike CVE-2019-0604, all vulnerabilities published in 2020 required a SharePoint account in order to be used. However, these vulnerabilities remain serious since they allow to take control of the SharePoint server. It is worth noting in particular: CVE-2020-17017 (**CERT-IST/AV-2020.1572**), CVE-2020-16951 and CVE-2020-16952 (**CERT-IST/AV-2020.1423**), CVE-2020-1147 (**CERT-IST/AV-2020.0938**) and CVE-2020-1181 (**CERT-IST/AV-2020.0764**). Most of these vulnerabilities allow to read arbitrary files, which then enables VIEWSTATE attacks against SharePoint's IIS server.

• IIS: the heart of Microsoft solutions

The IIS web server is a corner stone used in many Microsoft products such as SharePoint or Exchange. And many of the SharePoint or Exchange attacks actually seek to reach the IIS server, especially to perform VIEWSTATE attacks against IIS.

The increase in these attacks has led us to publish an article in our July 2020 monthly bulletin about the VIEWSTATE and how to secure it. In short, the VIEWSTATE is a hidden field included in the IIS web pages. This mechanism (from ASP.NET technology) is vulnerable to de-serialization attacks if the attacker was able to steal the MachineKey stored in the IIS web.config file. The theft of this file then allows the attacker to execute arbitrary code on the IIS web server.

Note: IIS has also been attacked a lot through vulnerabilities in the third-party library TelerikUI from the company Telerik.com.

3.7.2 SAML and OAUTH authentication attacks

This is another trend for 2020. Here are some events that highlight it:

- OAUTH Phishing attacks (see box below) are becoming common. They have been seen in state-sponsored attacks (the alleged Chinese attacks that targeted Australia in Q2 2020) and used by TA2552 group that specializes in phishing.

- In July, we issued an alert (**CERT-IST/AL-2020.007**) for a SAML vulnerability (see CVE-2020-2021 and our **CERT-IST/AV-2020.0868** advisory) in Palo Alto Networks equipment. It allows to connect illegally thanks to falsified SAML authentications.
- US-CERT and NSA warn in December of Russian attacks using **Golden SAML** technique. These are the SolarWinds attacks, but also previous attacks on VMWare Workspace One Access.

Excerpt from the article published in the September 2020 bulletin

OAUTH phishing:

This technique is gaining in popularity. Instead of asking the victim for his login and password, the phishing is an OAUTH windows which asks the victim to allow an App to access his Office 365 account. This technique was first seen in 2015 (see this Trend Micro article about Pawn Storm). There are now open-source toolkits implementing these attacks (PwnAuth from FireEye since June 2019, and O365-attack from MDsec.co.uk since June 2020). It was used in June 2020 in the APT attacks targeting Australia. And Proofpoint reported in late September 2020 that the TA2552 attacker group was using it for phishing attacks.

Evolution of the number of Cert-IST advisories mentioning OAUTH and SAML

	OAUTH	SAML
2020	8	7
2019	0	12
2018	4	8
2017	1	4
2016	2	1
2015	3	1

SAML and OAUTH attacks seen in 2020 target Office 365 cloud environments. This trend is expected to continue in the coming years as circumventing authentication mechanisms is a good way to gain access to resources hosted in the Cloud.

3.7.3 The Cobalt-Strike tool

Cobalt Strike is a commercial tool sold to perform penetration tests. It is an offensive tool, like Metasploit, Immunity Canvas or Core Impact.

There are pirated versions of Cobalt Strike on the Internet and **in 2020, Cobalt Strike became the most used tool in real attacks**. It has been seen many times in ransomware attacks, but also sometimes in state-sponsored attacks (e.g. the SolarWinds).

According to a study published in early 2021 by Recorded Future, is the most used offensive tool to remotely manipulate infected machines (ahead of Metasploit and PupyRAT).

3.7.4 ZeroLogon attack

Released in September 2020, the ZeroLogon attack exploits a vulnerability in the Windows Netlogon service and allows an attacker who has already gained access within an organization to gain complete control of a Microsoft domain.

ZeroLogon is now the easiest way for an attacker to elevate their privileges and take control of an organization's Active Directory, if the organization has not applied the patches released by Microsoft in August 2020 (the flaw was patched before being disclosed publicly). It has already been used very often in attacks and is therefore a key event of the year 2020. However, it is not a major technical breakthrough of the year and should not have any further consequences in the long term.

Note: About ZeroLogon, the Cert-IST issued the **CERT-IST/AV-2020.1101** advisory in August 2020 (to describe the Microsoft patches), the **CERT-IST/AL-2020.010** alert in September (to warn of the first attacks). We then kept up to date on the evolution of this threat through the [Microsoft Zerologon] blog in the Cert-IST Crisis Hub (HdC).

4 Summary of Cert-IST activity in 2020

4.1 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.

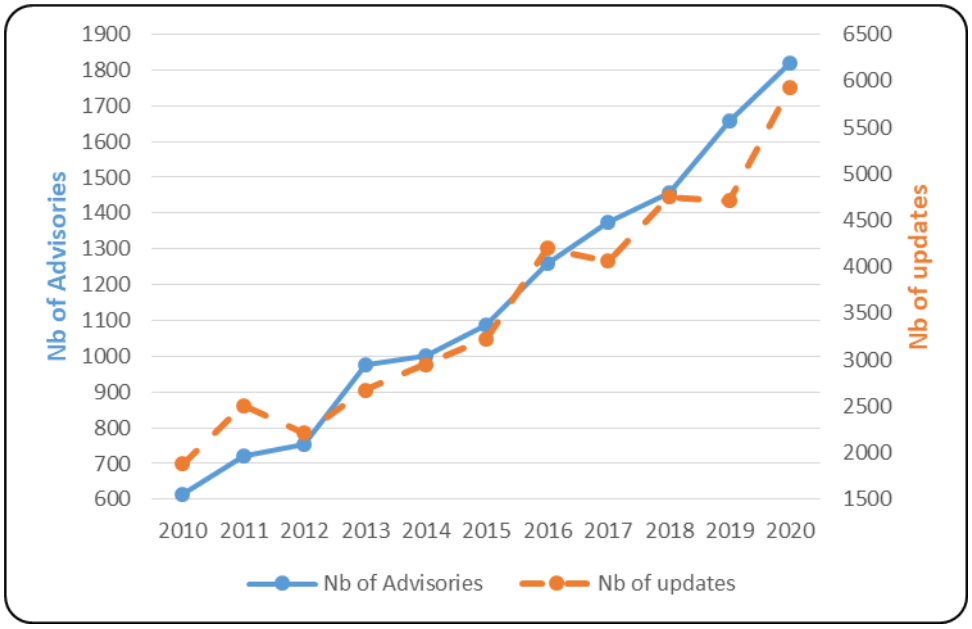
Cert-IST thus produces various types of publications:

- **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.

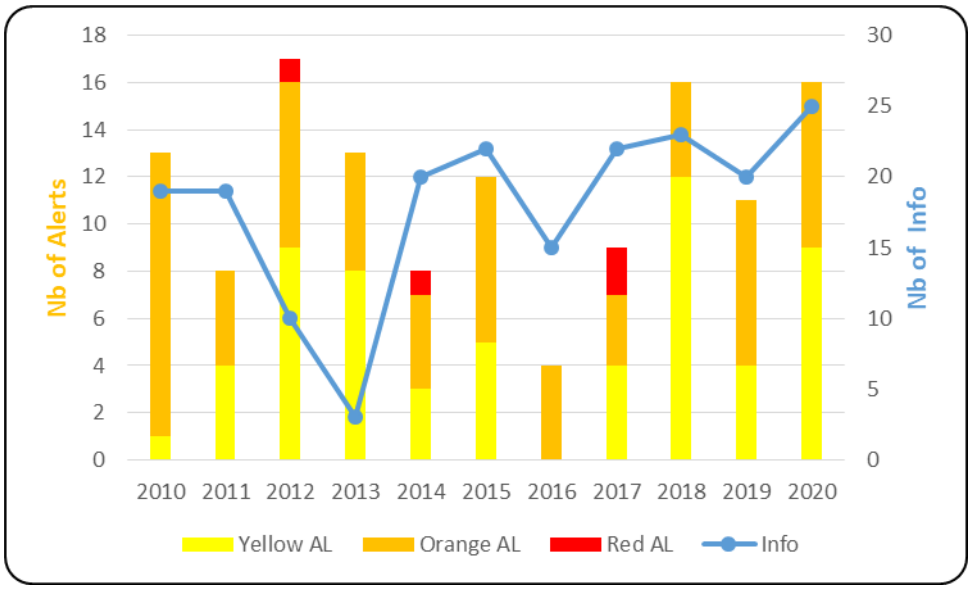
- **Alerts (AL)** which are issued when there is a particular risk of attack, and **INFO messages**, which provide an analysis for particular vulnerabilities (e. g. mediatized) but of lower immediate danger level. These 2 categories focus on the attack risks, while security advisories systematically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

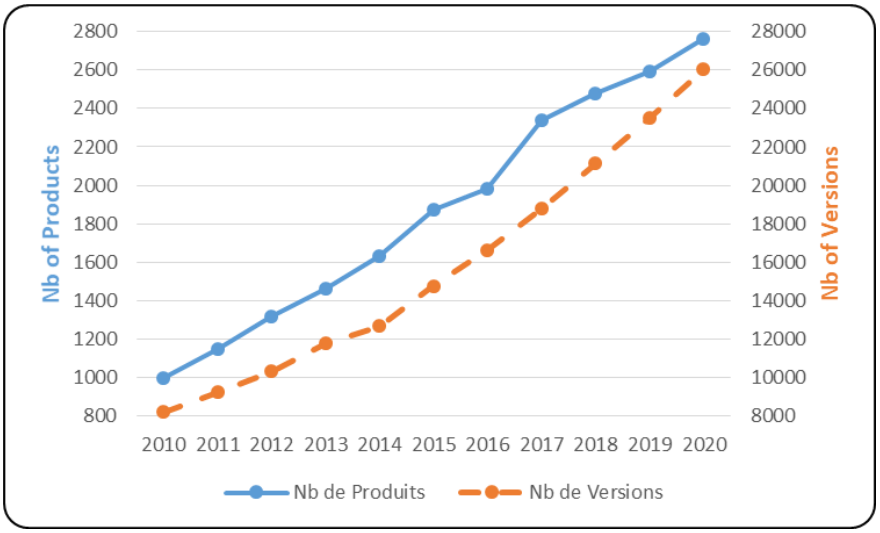
Number of ATK reports published per months

In 2020, Cert-IST published:

- **1 818** security advisories (including **79** SCADA advisories), **5 827** minor updates and **103** major updates.
  The number of advisories has been constantly increasing over the past few years (see the graph above), with an increase of **9%** compared to 2019. 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 **25** 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.
- **135** attack reports were published in 2020, containing **2 884** enriched events in the MISP database and **1 209 983** indicators (IOC) added (There are a total of **4.5 million** indicators in the database).

Regarding the products and versions monitored by Cert-IST, at the end of 2020 Cert-IST followed **2 764** products and **26 021** versions. The following graph shows the evolution of the number of products and versions monitored by Cert-IST over the year.



4.2 Technology Watch

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

- A **daily media watch newsletter (press review)** listing the most interesting articles published on French and English websites regarding security topics,
- A **monthly SCADA watch 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.

5 Conclusions

• The Covid-19 crisis has exposed companies to an increased risk of attack

2020 is first of all the year of the Covid-19 crisis. In companies, the lockdown measures required a rapid and radical adaptation of the work environment. Many had to implement or generalize teleworking, sometimes at the cost of an increased exposure to the risks of computer security incidents (intrusion or data leakage). As detailed in paragraph 3.1, there has been an increase in the number of classic attacks (email bombing campaigns, web scams) because all attackers have sought to take advantage of the crisis. It is also possible (but we still lack hindsight on this aspect) that the tools set up for teleworking have allowed an increase of bounce attacks (attacks targeting the teleworkers to in fact penetrate his company).

To our knowledge, there is no known case of a severe incident formally attributed to the technical measures put in place during the Covid-19. It is sure, however, that many did the best they could, but exposed companies to an increased risk of intrusion. It is therefore important to limit the duration of this period of vulnerability.

• 2020: record year for ransomware attacks

We concluded last year's report on the disturbing spike in ransomware attacks targeting businesses, and 2020 confirmed that fear: attacks have continued to grow and are the most prominent phenomenon of 2020. The attackers have multiplied the means of pressure (see § 3.2) and have shown once again that they form a structured underground economy where everyone is paid according to the services they provide.

Ransomware attacks and data theft within companies is a lucrative market. This attracts more and more cybercriminals. To stem this wave of ransomware, a more effective judicial response is probably needed, with international dismantling operations comparable to what has already been seen for certain Botnets (Trickbot in November 2020, Emotet in January 2021, etc.). It also seems that once inside the company, it is sometimes easy for the hacker to move around, take control of the Active Directory and then stay several weeks or months without being detected. This disturbing finding highlights the need to strengthen the ability to detect unusual behavior within the network (see below).

• SolarWinds attack demonstrates advanced offensive capability of some States

The attack through SolarWinds' Orion software announced in December 2020 by the United States (known victims so far are government agencies and U.S. companies) is exceptional in its scale and sophistication.

The attack technique (software infection at the supplier's site), puts the subject of supply-chain attacks at the center of concerns. However, this is a complex attack that is especially interesting when the attacker is aiming at a target that is difficult to reach with a direct attack, or if he wants to reach a large number of targets (case where the trapped product is widely used). Although it is a real threat, protection against these attacks will probably be a priority only for the organizations with the most advanced security.

Note: We are talking here about software entrapment, which is one of the 3 forms of supply chain attack (see paragraph 3.4 ; the others are hardware entrapment and intrusion via the provider's networks).

Finally, what the SolarWinds attack shows is the complexity of analyzing this kind of incident: it is a stealth attack (the attacker seeks to limit the traces left) discovered more than 10 months after the initial intrusion and targeting in particular the company's Cloud resources (Microsoft Office 365, a very dynamic and rapidly changing environment, and therefore complex). The analysis of such an incident also requires supervision data (logs) from the different components of the impacted Information System (access gateways, workstations, Office 365 environment, etc.).

• Attacks turn to edge devices (VPNs) and the Office 365 cloud

In 2020, in addition to the traditional attacks targeting the workstation (attacks by e-mail or during Internet browsing) two trends have emerged:

- Attacking equipment exposed on the Internet and especially VPN access points (see § 3.3),
- Office 365 cloud attack.

• Improved intrusion detection capabilities are needed

The events of 2020 have shown once again (with Ransomware attacks or advanced State attacks such as SolarWinds) that no defense is invincible and that the company must assume that attackers will one day or another manage to penetrate the internal network.

But between the initial intrusion and the achievement of his objectives, the attacker also needs time. This time depends on the defenses he will encounter (the level of defense in depth) and the level of stealth he wants to achieve. And the whole time he is in the company, the attacker should be careful not to trigger any alarms, which could attract the attention of the defenders and start a hunt for him.

This observation encourages the development of alarm systems on the one hand and alarm reaction procedures on the other. This relies on specific detection devices (e.g. by placing dedicated detectors inside the company: sentinel servers, honeypots, etc.) or by combining already logged events (definition of abnormal behavior) and on qualification and reaction mechanisms driven by security operations centers (SOC).

Reminder of the security principles (extract from the Cert-IST 2019 report):

- Set up defenses and compartmentalize architectures, taking into account the fact that one day an attacker will manage to get through the defenses,
- Keep systems up to date by applying security patches,
- Develop intrusion detection and response capabilities.

Cert-IST Organization
290 Allée du lac
31 670 Labège
France
info@cert-ist.com
https://www.cert-ist.com
+33 5.34.39.44.