Cert-IST annual review for 2015 regarding flaws and attacks

1. Introduction

Each year, the Cert-IST makes a review of the previous year. The goal of this document is to present the trends regarding attacks and threats, and to help readers to better protect their assets.

We present first the most significant events of 2015 (see Chapter 2).

Then, we provide a summary of the Cert-IST productions during this year (see Chapter 3).

The conclusion (see Chapter 4) drawn a global picture for the cyber-threat current situation and the challenges the companies must face with.

Note: The blue insets enclosed all over the document are articles or announcements taken from the Cert-IST monthly bulletins published during 2015.

➢ Regarding the Cert-IST

The Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam **- I**ndustry, **S**ervices and **T**ertiary) is a centre for alert and reaction to computer attacks and cyber threats dedicated to companies. Established in 1999, it analyzes daily the new vulnerabilities discovered, assesses their severity and identifies the possible protective measures. In the event of a security incident impacting one of its members, the Cert-IST can assist in the investigation and the resolution of this incident and allow a fast return to secure operational state.

2. Most significant events of 2015

2.1 Attacks targeting Adobe Flash

Numerous vulnerabilities have been discovered in Adobe Flash, and that component has undergone multiple attacks during 2015. We released this year for that component 18 advisories and 5 DGs (for a total of 12 DGs). The “Recorded Future” Company released a report including the analysis of a hundred kit exploits: it concludes that Flash vulnerabilities are intrusion points in 8 cases out of 10, ahead of Internet Explorer.

This has led many web actors to act for the abandonment of Flash:

- Mozilla has blocked by default Flash content,
- Alex Stamos, the Facebook security chief Officer asked to Adobe, through a tweet, to give a date for the end of life for the plugin,
- YouTube abandoned Flash for HTML5.

We also note that the Java plugin, another component that took the spotlight in terms of attacks in recent years, also appears to be on the hot seat.
While many browsers had blocked this plugin for several months, Oracle has announced its disappearance and called to use Java Web Start in its place.

The browsers evolution towards plugins abandonment is so confirmed.

Extract of the Cert-IST bulletin Headlines - January 2015

Multiple new vulnerabilities affecting the Flash component were discovered late January when they were used in 0-day attacks. We give details on this in our “Attack of the Month” section. This event recalls what was seen in 2010 (with multiple attacks through PDF and Flash), and 2012 (attacks through Java), and shows again that user’s workstation is highly exposed to attacks while browsing the web.

Extract of the Cert-IST bulletin Headlines - June 2015

Once more, attacks against Adobe Flash Player have been seen. This component is now at the top of the most dangerous software for workstation.

Extract of the « Attacks of the month » section – June 2015

Attacks against Flash are not new: during the last years, we have regularly released Potential Danger or Vuln-coord messages about Flash attacks. But Flash attacks are now taking the lead in front of other software such as Java or Adobe (PDF) Reader which are now less frequently targeted by attacks. This trend leads to ask the question: should we keep Flash or should it be better to disable it when browsing the web? The journalist Brian Krebs tried an experiment (see his article "A Month Without Adobe Flash Player") which he concluded that he missed Flash only 2 times: if you cannot prohibit Flash, you should therefore try to disable Flash most of the time and reactivate it only when strictly necessary, for example with a mechanism such as "Click to play".

2.2 The offensive security unveiled: the "Hacking-Team" case

The security offensive sector is growing for several years (see the previous year's annual review). Initially, it was discovered that States were active in this sector and it was feared that private companies invade the market. The 2015 events confirmed this concern.
Following the hacking of the Hacking-team Company, the stolen data have highlighted the development of offensive tools as well as the existence of 0-days markets.
Hacking-team has actually bought 0-days to several suppliers called "0-day brokers".

Beyond the few "0-day brokers" highlighted on this occasion, we have also seen the emergence of new brokers.
The zerodium.com company (founded by the creator of VUPEN) has been created in 2015 and has announced it had bought $ 1 million a 0-day attack against IOS.

At the beginning of 2016, the explosion of brokers continues: the creation of 2 or 3 new companies of this type was announced. It is possible to imagine an "uberisation" of computer security where individuals sell vulnerabilities they have discovered.
The model where companies buy audit service (classic) would be replaced by a model where companies buy flaws discovered by individuals (collaborative model).

Extract of the Cert-IST bulletin Headlines - July 2015

The highly controversial Italian offensive security firm named "Hacking Team" has been hacked in early July, and 400 Gb of data stolen there have been made available on Internet. The examination of this huge among of data (which includes emails, source code for their attack tools, etc.) led to a lot of press articles that put the light on facts we already know.
This includes the followings:

- Any company can be hacked!
- The 0-day market is prospering (see this article, as well as this mail from Hacking Team) and a lot of vulnerabilities are sold on this market (with prices such as 45 000 dollars for a Flash flaw),
- States seem very interested in offensive security topics. This includes democratic States (e.g. these exchanges supposedly with the FBI - with possibly legitimate usages in mind) as well as totalitarian States (in order to track down opponents).

2.3 Dridex and Crypto-Locker: very well orchestrated nuisances

Companies were attacked this year by the Crypto Locker infection waves (early this year) then Dridex (from June).

These malware use the basic attack technique, widely used in the 1990s, based on email trapped in such a way to infect the systems of users who open the attachment or who go to the website pointed by the e-mail.

Observers have noted the return of macro viruses which had almost disappeared (see a short news in our June bulletin).

But, although less technically sophisticated than the attacks of cyber-spying as those of APT type, these attacks were very effective and they apparently caused damage as they are very well orchestrated and antivirus do not always immediately detect them.

As Dridex messages were often bills related to orders, it is likely that these attacks targeted the companies. These latter are probably more likely to pay ransoms requested to retrieve valuable documents.

It may be noted the difficulty to dismantle these gangs: a large "take-down" campaign was launched in September against Dridex with mixed results since the waves of infection have continued.

Companies have seemed rather helpless to address these attacks, and it is interesting to note that some of them have used IOC to implement blocking rules related to network flow.
That questions us about the effectiveness of existing protection measures and their development.

VulnCoord-2015.020: Large DRIDEX/DYREZA spam and malicious Office Macros
Extract of the « Attacks of the month » section – June 2015

This is another important event that occurred in June 2015: on Monday 8th of June 2015, a wave of malicious mails targeting French users appeared. The mail is written in French, is about a pending invoice, and comes with a ".doc" (or ".zip") file attached. When this file is opened, it displays a message like "You must allow macros to correctly display this file". If the user does so, a malicious macro is launched: it downloads and installs on the user's computer a banker malware belonging to the "Dridex" family.

Although this is a very classical attack scheme, it highlights persistent issues:
- Antivirus software did not detect the attack, and the disinfection procedures were hard to develop. A full re-install of the affected computers was most of the time the safest sanitization procedure available.
- Although they almost disappeared, macro virus (malicious Office macros) make a successful come back. We further examine this topic in the article section of this bulletin.

Finally, it worth noting that cyber criminals who set-up such attacks are well organized. For example, the Dridex malware used in these attacks communicates with its C&C server via a set of bounce servers (proxies) which were installed by the attacker on compromised SOHO network devices (see this article for more details). This makes more difficult to neutralize this network infrastructure.

2.4 TV5-Monde: The rise of sabotage attacks

This attack suffered at the beginning of April by TV5-Monde was widely publicized. However, very few technical elements were published on the attack. This allowed lot of speculations, especially on the authors. The first suspicions focused on Islamists have then moved toward Russian attackers.

This event is a "French" illustration of the attacks suffered by Sony at the end of 2014, and it showed:

- the extent of damage that can make a cyber-attack,
- that all companies are potentially exposed to such attacks,
- that companies must consider to be the target of attacks causing the complete destruction of their information system (overwriting of the MBR of all infected machines).

The Cert-IST bulletin Headlines - April 2015

The cyber attack suffered early April by TV5-Monde (a French TV network) looks like computer sabotage. No technical details have been officially disclosed and one can only speculate about the true nature of the incident. But apparently, several internal servers were brutally put off (video encoding servers, mail servers were both mentioned in the press). We can then think that the hackers have installed a destructive malware (a "Wiper") on the affected Windows computers. This type of destructive malware was already seen in several attacks: Sony Pictures Entertainment (November 2014 in USA, see our article on this subject) or DarkSeoul (March 2013 en South Korea) or Aramco (August 2012 in Saudi Arabia). It seems more and more common and should be considered as a quite likely risk in case of cyber-intrusion. In 2013, the US-CERT published the ST13-003 tip notice about this risk (and the TA14-353A alert by end of 2014 about the wiper used in the Sony). The recommendations given in it are numerous. But we think that the following actions are the most important ones to address this risk:

- Limit the spread of the intrusion by segregating networks and limiting the accounts with administrator privileges
- Prepare recovery procedures for infrastructure servers and ensure that the case of a voluntary computer attack has been taken into account (e.g. a RAID does not protect against deliberate delete on disks).

Note: For further information on "Wiper" malware, you can for example read this analysis *(of the Sony wiper) from CERT-FR (in French) or* this IBM study *(which reviews the known wiper malware).*

2.5 Data theft: more and more publicized cases

There have been many cases of personal data theft in the 2015 events:

- At the beginning 2015, several cases of health data theft through attacks against some mutual insurances (cf. attack that targeted the Anthem society and which could have resulted in the theft of personal data of 80 million customers) or against some health establishments (laboratories, hospitals...)
- In June, a US agency, the Office of Personnel Management (OPM), was the subject of a cyber-attack that resulted in the theft of confidential data on over 20 million US employees.
- In August, the extramarital dating site "Ashley Madison" was the subject of an attack also remarkable for its scale (10 GB of compressed data, relating to 33 million accounts), and the intimate character of disclosed data.
- In addition to these major attacks many personal data thefts have been disclosed throughout the year: Morgan Stanley, 000Webhost , VTech, etc…

Although these attacks are very different and some are more worrisome than others, they highlight weaknesses in systems containing many confidential data.

It seems that the attacks are moving toward less protected targets but no less lucrative, and that they now rather target personal data and digital identities as bank information.

2.6 Vulnerabilities in anti-virus: all vulnerable?

In 2014, Google security engineers have launched the "Project Zero" program to detect zero-day vulnerabilities and reduce the number of critical vulnerabilities on the Internet. Then, in 2015, several researchers of this project have focused their efforts on security products (antivirus and more generally point to point protection tools).

And up to this day, vulnerabilities have been discovered in several antivirus (from Kaspersky, ESET, Avast, and Sophos) and in FireEye devices.

Perfection being not of this world, it is not amazing that when someone seeks vulnerabilities in these products, some are discovered. And the number of discovered vulnerabilities being fairly limited, this does not undermine their reliability.

Through their work the "Project Zero" teams, participated in improving the safety of these products.

2.7 SCADA, connected cars and Internet Of Things: targets for future attacks

News of 2015 showed that:

- It might be possible to **hack an aircraft**.

  At the beginning of the year announcements said it was possible to hack a plane over the passenger Wi-Fi network. Then the experts said that the separation of networks "theft" and "entertainment" was making these kinds of attacks impossible. And, late in the year the director of the European Aviation Safety Agency (EASA) reported that aviation was vulnerable to cybercrime.

- One could **take control of some cars**.

  In July, two security experts have actually been able to remotely take control of a car via the Internet, by exploiting the vulnerability of an embedded multimedia module in the Fiat Chrysler Jeep Cherokee.

- The security of computer systems of **airports** was too weak to such critical facilities.

  In June, the Polish airline company LOT, had to cancel several flights due to a cyber-attack targeting his system managing ground operations.

  At the end of October, during the Hackito Ergo Sum 2015 conference, a researcher has presented the results of an audit he had done on the security of one of the largest international airports in the European Union. His team found nearly 60 vulnerabilities, some very critical!

  Note: At the beginning of 2016 an attack on the main airport of Ukraine confirmed this threat.

- **Medical devices** were also threatened by cyber-attacks.

  At the Hack.lu 2015 conference Marie Moe (a former head of the Norwegian Cert) made a presentation on the safety of pacemakers to alert not only the population but also devices manufacturers in the medical field on the security issues which began to appear increasingly.

  At the Derbycon 2015 conference two security researchers (Scott Erven and Mark Collao) presented numerous vulnerabilities they found in different medical equipment (anesthesia devices, cardiovascular equipment, injection systems, pacemakers, ...) .

Extract of the « Attacks of the month » section – August 2015

As already mentioned in our Headlines, in August it was reported several cases of vulnerabilities allowing to attack connected cars (vulnerability in Tesla cars, remote take control of a Jeep, vulnerability in the Megamos Crypto electronic lock system). The most worrying case is the attack against Jeep Cherokee car presented at the Blackhat USA conference. The speakers showed that they took control of the car from Internet, and forced it to leave the road. Fiat Chrysler launched a recall of 1.4 million cars after that. On the topic of connected objects, it should be noted also that in the United States an infusion pump was banned because of critical vulnerabilities.

IT is everywhere and attacks are impacting our real lives: IT is increasingly becoming a central component of daily life. Beyond the visible intrusion in our lives (BYOD, tracing) it is also omnipresent, more discreetly, in automation systems (tolls, embedded computing ...) and in critical systems (airports, factories, electricity grid, etc. ...). Computer attacks on these systems impact us in our daily lives. It is not an intrusion or a computer failure, but an entire region which can be without electricity for example.

Up to this day these attacks are still at a prototype stage and there is an awareness of the crucial need to secure all these critical equipments.

In 2015, in France a decree has defined obligations for essential operators (OIV- Opérateurs d'Importance Vitale), and there will probably soon be binding legislative measures to force connected objects manufacturers to consider security. There could be in the future some "cyber" security standards, as now there are physical security standards for many objects (such as toys, for example).

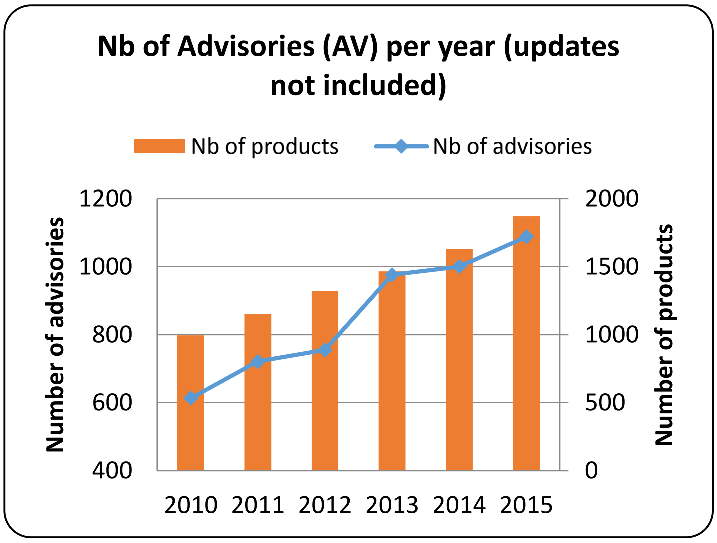
3. Vulnerabilities and attacks seen in 2015

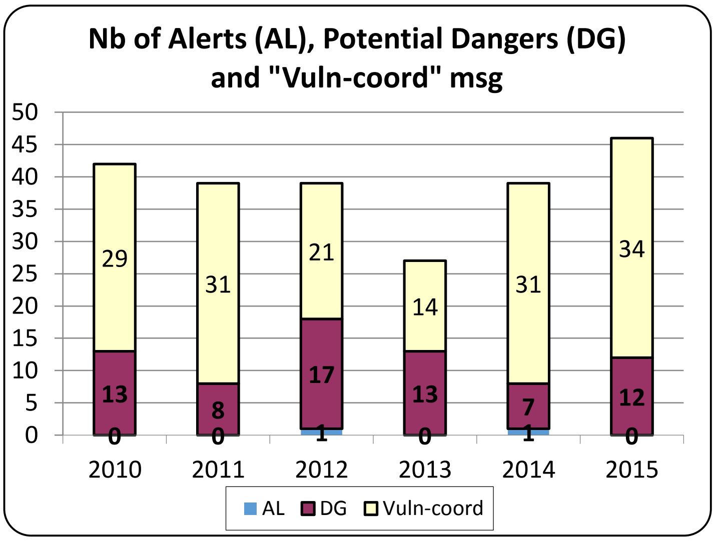
3.1 Daily monitoring on vulnerabilities and threats

As part of its watch activity on vulnerabilities and threats, the Cert-IST continuously monitors the different information sources about vulnerabilities (including official announces from constructors/providers, security blogs, mailing-lists, private exchanges between CERT, etc.) in order to be aware of new vulnerabilities. These data are analysed daily to provide our members with a sorted, qualified and prioritized set of information. The Cert-IST therefore releases different types of productions:

- **Security Advisories:** they describe newly discovered vulnerabilities in the products followed by the Cert-IST. These advisories are continuously enriched with minor or major updates. The latter typically occurs when attack programs (aka “exploits”) are released.
- **Alerts**, **Potential Dangers**, and **“Vuln-coord” messages**: Alerts from the Cert-IST are used for major threats which require an urgent treatment. Sending an alert is a rare event: for instance, the Cert-IST released in 2014 one alert for the Shellshock vulnerability. Potential Dangers describe significant threats, which are not imminent yet (or having a limited impact) but for which the Cert-IST recommends specific protection measures. Finally, “Vuln-coord” messages are coordination information which draws attention on particular threats which have a lower severity. These three complementary categories are focused on attack risks, whereas Security Advisories systematically identify all known vulnerability (whatever is the probability that the vulnerability is used in a real attack).

The graphs below show the production of Cert-IST over past years.





Therefore, during 2015, the Cert-IST published:

- **1 088 security advisories**, continuously followed during the year with 3 069 minor updates and 159 major updates. The number of advisories has been in constant increase for several years (see the curve above), with an increase of 12% compared to 2014. This continuous raise shows that the discovery of vulnerabilities is a trend constantly increasing. Maintaining the level of security necessarily needs regular installation of products security patches. On the 31st of December 2015, Cert-IST followed vulnerabilities concerning 1 871 products and 14 762 versions of products.

- **12 <u>Potential Dangers and</u> 34 <u>"Vuln-coord" messages</u>.** In 2015 no alert was issued. The number of potential dangers increased from 7 to 12 (which 5 on Adobe Flash Player product), and the number of "Vuln-coord" messages increased from 31 to 34.

3.2 Monitoring watch

Besides its vulnerability watch, the Cert-IST also releases technology watch reports:

- A daily Media Watch bulletin identifies the most interesting articles released on Internet on a sampling of French and English-speaking websites about security,
- A monthly SCADA Media Watch presents a synthesis of news about industrial control systems security,
- A monthly general bulletin gives a synthesis of the month news (in terms of advisories and attacks) and deals with current subjects in articles written by the Cert-IST.

4. Conclusions

Companies must still and always deal with a situation more and more complex.

The findings contained in our annual review 2014 still current:

- Computer sciences took a central place in our day to day life, both on professional and personal aspects; for the record, the theme of the Cert-IST FORUM 2015 has been «The digital transformation and security»
- The evolution of technologies leads to disseminate information in multiple places around the web (with for instance technologies like Cloud and BYOD) and seeks for making always easier the access to this information.

On the other hand, the risk of intrusion has increased significantly in recent years.

New attackers, targeted specifically companies (with cyber-spying, cyber-vandalism attacks, against businesses) have been identified.

2015 confirms this increase of cyber risks:

- Attacks are more frequent in particular large-scale data theft and the ramsonwares,
- The "cyber" has become a strategic issue for States; in France, the decree regarding the obligations of essential operators (OIV) was released in 2015,
- Industrial systems, connected cars and the Internet of Thinks have become popular targets for attackers and multiple vulnerabilities in these areas have been discovered.

To adapt itself to this situation, the company must first needs be kept informed of threats and their evolutions. The Cert-IST, through its continuous vulnerability watch and its technical reviews, gives a well-argued vision of the threat.

To face with increase of cyber risks, companies must also:

- Assess theirs exposure to this kind of attacks,
- Reinforce their defences,
- Develop their capacity to detect and react to intrusions: collection of logs, security oversight and active search of attacks with the help of IOC (Indicators Of Compromise).

The Cert-IST is currently working on the implementation of a new service around the IOCs.

End of document