Cert-IST annual review for 2012 regarding flaws and attacks

1) Introduction

Each year, the Cert-IST makes a review of the past year. The goal is to sum up the major events of the last year (2012) in order to highlight the trends regarding attacks and threats, and to help readers to better protect their assets.

First, we present a digest of the 2012 events (in chapter 2), reviewing the main threats identified by the Cert-IST, and the major topics discussed in the security community.

Secondly, we identify the major evolutions for businesses, and analyze how to take them into account (see chapter3).

Finally, we draw a quick summary of the Cert-IST production for 2012, where we provide for example, figures of the number of advisories or alerts published during the year (see chapter 4).

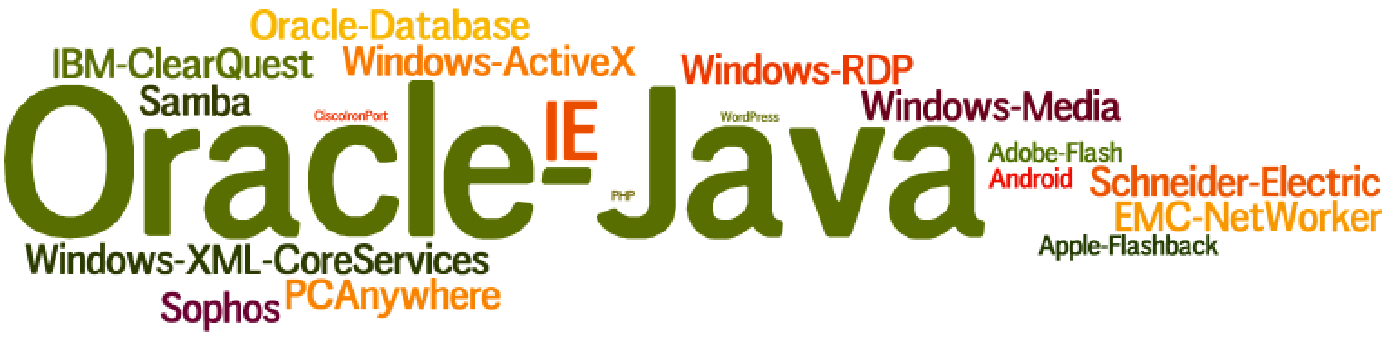
➢ About Cert-IST

The Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam **-** **I**ndustrie, **S**ervices et **T**ertiaire) is a center 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) Digest of the 2012 security events

2.1 Threats identified by Cert-IST

This chapter lists the technologies for which Cert-IST has released, during 2012, warning messages (as standalone publications such as Alert or a Potential Danger notices[1], or as sections in our Monthly Bulletin), because there was a high risk of attack for it. The size of each technology in the graphic below reflects the risk level for each.



[1]: The different types of Cert-IST publications, such as Alert or Potential Danger notice are presented in § 4.1

We comment below the most important risks highlighted by the tag cloud graphic.

- **Oracle-Java**

Attacks targeting the Java client installed on workstations (the JRE component) multiplied during 2012. These attacks happen silently and automatically during web browsing (no antivirus alert, no crash of the victim browser) when the victim visits regular websites which have been infected. This is not a new phenomenon: our first warning sent to our members about this Java risk was in August 2010. But this is gaining in importance and accelerating, and new vulnerabilities which are discovered in Java are now integrated more and more quickly into attack tools. In 2012 we released 1 Alert and 3 Potential Dangers notices about Java/JRE attacks.

- **Internet Explorer**

In 2012, Internet Explorer was targeted by 2 series of attacks:

- **In June,** we released the **CERT-IST/DG-2012.008** Potential Danger notice about the **CVE-2012-1875** vulnerability. Discovered on June 1st by McAfee (but probably used before in a targeted attacks), and kept secret until the issue of a fix by Microsoft (on June 12th, in their MS12-037 security bulletin), this vulnerability allows to infect the user's system during web browsing. Following the issue of fixes by Microsoft, many exploit programs were released on the Internet aiming at this vulnerability (especially in the Metasploit framework). Consequently, we issued on June 15th the **CERT-IST/DG-2012.008** Potential Danger notice to warn our community against the increasing risk of attack, and the emergency to deploy Microsoft patches.

We are often asked which browser is the most secure. No browser is exempt of vulnerabilities, but experience showed that most of the times, Internet Explorer is the targeted browser. This is probably caused by the fact that Internet Explorer is the most used browser, at least in business environments, and therefore attacks focus on this type of web browser. Whether it is 0-days or opportunist attack waves which exploit recently fixed vulnerabilities, Internet Explorer is therefore particularly exposed.

- **In September,** we released the **CERT-IST/DG-2012.014** Potential Danger notice about the **CVE-2012-4969** vulnerability. This time, the vulnerability was revealed (on September 16th) before a Microsoft fix was available (Microsoft produced the MS12-063 bulletin on September 21st). Several exploitation programs were quickly released, which made us issue the **CERT-IST/DG-2012.014** Potential Danger notice on September 18th.

This is here 2 examples of 0-day vulnerabilities: these vulnerabilities were kept secret until they were used in attacks.

- **Windows**

Windows remains a prime target for attackers and we produced this year 4 Potential Danger notices concerning the following Windows components:

- **Windows Media** (January 2012). This was a vulnerability in MIDI music files (CVE-2012-0003) which allowed executing code on the workstation of user visiting a website hosting a malicious MIDI file. This vulnerability was fixed on January 10th by Microsoft in the MS12-004 bulletin. It caused several waves of attacks which made us issue the **CERT-IST/DG-2012.001** Potential Danger notice on January 30th.
- **Windows RDP** (March 2012). This vulnerability (CVE-2012-002) allows taking control of a computer where the RDP service (Remote Desktop Protocol) is activated. Given the severity of this vulnerability, we issued the **CERT-IST/DG-2012.003** Potential Danger notice right after the apparition of the first exploit programs, 3 days after Microsoft released fixes for this vulnerability (MS12-020 bulletin dated of March 13th 2012).
- **Windows ActiveX** (April 2012). This is a vulnerability (CVE-2012-0158) that affects 4 ActiveX controls included in the « Common Control » component (MSCOMCTL.OCX) of Windows. It

allows executing code on a computer visiting a website or opening a crafted malicious Office file. Fixed on April 10th by Microsoft (MS12-027), this vulnerability caused several infection campaigns and made us release the **CERT-IST/DG-2012.005** Potential Danger on April 27th.

- **Windows XML CoreServices** (June 2012). This vulnerability (CVE-2012-1889) in the MSXML services allows a malicious website to execute code on the victim's workstation visiting the website. It gave rise to 0-days attacks reported on June 12th by Microsoft quickly followed by the release of exploit programs. This led us to issue the **CERT-IST/DG-2012.008** Potential Danger on June 18th. Microsoft finally released fixes addressing this vulnerability on July 10th in their MS12-043 bulletin.

Even though during these last years, attacks turned from Windows to focus on less protected pieces of software such as Adobe Reader, Flash or Java (see our 2010 and 2011 annual reports for more details about this trend), **Windows remains a very popular target for attackers,** who are perfectly experienced in the use of attack techniques for this environment. Today, vulnerabilities discovered in Windows are very quickly integrated into attack frameworks.

Other OS are of course also at risk. Apple sadly experienced this in April 2012 with the **Flashback** virus which infected more than 600 000 Mac OS-X computers, thanks to a vulnerability in Java-JRE. In June 2012, Apple also changed its marketing slogan replacing "*It doesn't get* PC viruses" by "*It's built to be safe*" (see for instance this article from PCWorld.com, June 2012). In terms of vulnerabilities management, Apple tries to enhance its processes in order to be more reactive: Kaspersky provocatively claimed that Apple is 10 years behind Microsoft and it is clear that Apple should effectively be inspired from the efforts Microsoft made in this field.

- **Oracle-Database**

We produced in April the **CERT-IST/DG-2012.006** Potential Danger concerning a 0-day vulnerability in the **TNS-Listener component of Oracle** (in the 8i to 11g versions of Oracle Database), which allows a remote attacker to eavesdrop communications (communication sniffing) or to inject arbitrary commands in these communications (session hijack). The release of an attack tool, on April 18th, results from a misunderstanding between the discoverer (who thought the vulnerability he discovered in 2008 was corrected by Oracle at the beginning of April) and Oracle (who wished to correct the vulnerability in the future versions of the product only). This accidental release made this flaw public, and given the risk implied, we issued our Potential Danger on April 27th. Fixes from Oracle were finally available a few days later (on April 30th).

- **PCAnywhere**

We released on June 28th our CERT-IST/DG-2012.009 Potential Danger, following the publication of an exploit program targeting a vulnerability (CVE-2011-3478) in PCAnywhere 12 from Symantec. This vulnerability was known since January 2012 and seems to be linked to the theft of the source code of several Symantec products (see our insert). Indeed, Symantec announced this vulnerability (and issued remediation for the most recent versions of PCAnywhere) immediately after confirming the theft.

- **Schneider-Electric**

For the first time since the Cert-IST launched its SCADA service, we issued in 2012 a Potential Danger (CERT-IST/DG-2012.004) concerning a SCADA device. This is about the **Modicon Quantum** PLC from Schneider Electric, for which exploit programs allowing an attacker to take control of a vulnerable PLC were published.

In 2012, **several source code thefts** were revealed:

- **Symantec** in January 2012 confirmed a theft of the source code of some of their products (Norton Antivirus Corporate Edition, Norton Internet Security, Norton Utilities, Norton GoBack and PCAnywhere). This theft was claimed by a hacker group declared as members of the Anonymous. A ransom demand was made by the thief who finally published extracts of the source code of Norton Utilities, PCAnywhere, and Norton Antivirus (see this article which sums up these events).
- **VMware** in April 2012 confirmed that part of the source code of VMWare ESX was stolen (probably at a partner which VMWare shares code with) and published on the Internet. The thief has indicated he stole the code from a Chinese industrial (see this article). Two weeks later, VMware released, as a precaution measure, security fixes (see this announce). In November, they reiterated their recommendations and encouraged its clients to scrupulously apply all the security updates.

- **Other vulnerabilities**

We summarize below the other threats mentioned in our tag cloud graphic. In most cases it was warnings about attacks targeting critical vulnerabilities recently corrected in a widespread product. These 2012 events were not widely discussed by other media (especially when they did not target popular technologies), but the threat was real for the concerned installations. The dozen of such warning messages sent by the Cert-IST all along the year, allow our members to stay informed about these threats.

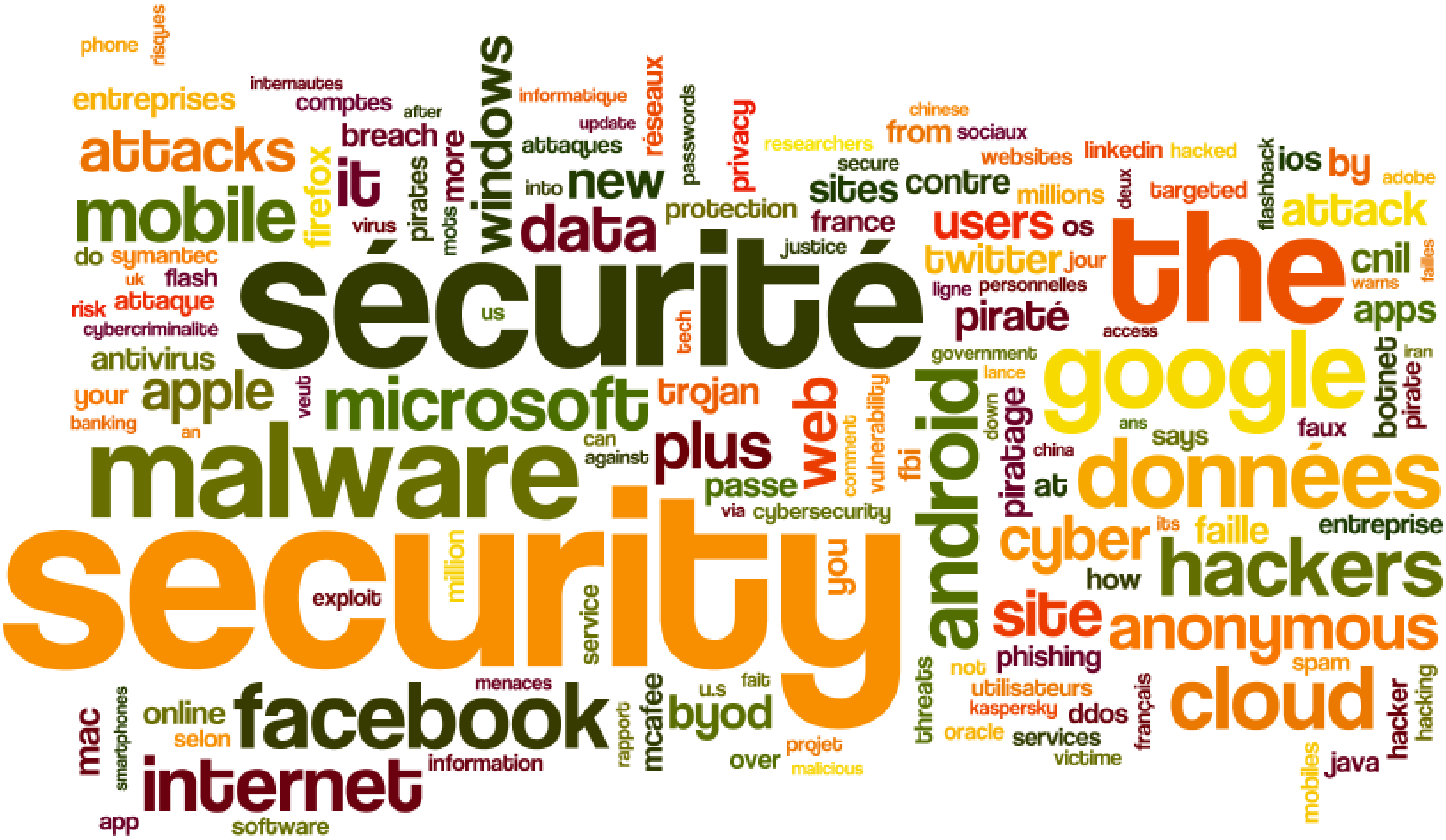
- **Cisco Iron Port**: In January we have drawn your attention on a very critical vulnerability affecting the Linux « telnetd » daemons, because this vulnerability was also affecting the Cisco IronPort appliances.
- **WordPress:** In March, and then in October, two waves of infection for WordPress sites were observed.
- **Adobe Flash:** In May, and then in August, exploitation codes were published for Flash vulnerabilities (CVE-2012-0779 and CVE-2012-1535) recently corrected by Adobe.
- **PHP**: In May, a vulnerability (CVE-2012-1823) affecting web servers using CGI scripts in PHP could allow to take remotely control of vulnerable web servers.
- **IBM-ClearQuest:** In July, an exploitation code was published for a vulnerability (CVE-2012-0708) fixed earlier in April in the CQOle ActiveX control from IBM Rational ClearQuest. There was a high risk of attack for non-updated computers.
- **Samba**: In September, an exploitation code was published for a vulnerability (CVE-2012-1182) fixed earlier in April in Samba. Attackers could use that code to take control of remote Samba servers that have not been kept up to date.
- **Sophos**: In October, a security researcher named Tavis Ormandy published a study that described a set of vulnerabilities affecting Sophos antivirus. Some of them could allow an attacker

to take control of computers running Sophos antivirus. Sophos released a patch fixing the most serious vulnerabilities shortly after that event.

- **EMC NetWorker**: In November, an exploitation code was published for a vulnerability (CVE-2012-2288) fixed earlier in August in EMC Networker. Attackers could use that code to take control of remote computer running non-updated EMC Networker backup software.

2.2 Top 2012 security matters, as seen by Online Press

In addition to its technical watch on vulnerabilities, the Cert-IST also follows more widely the technology evolution and news in computer security. We thus release each day in our daily Media Watch Bulletin a list of the most interesting articles we saw in the French and English press. The figure below presents the most cited words in the 2012 Cert-IST Media Watch.



In the rest of this chapter, we comment the main topics highlighted by this tag cloud: these are the top security matters for 2012.

- **Cloud and BIG-Data**

This year again, there were many discussions about « Cloud Computing ». Security aspects to be taken in account were already widely discussed in 2010 and 2011. Discussions in 2012 were mainly focused on CISO’s reluctance to adopt cloud solutions because of the induced security risks. Discussions on Cloud topic these latest years could be sum-up as following:

  - **2010: Cloud = Danger!:** Experts warn that the enthusiasm, which grows about Cloud technology will face important security issues.

- **2011: Here are the difficulties**. Experts give the details of the difficulties to be faced with Cloud Computing, either on the contractual, juridical or technical aspects.
- **2012: Ready for implementation?** CISOs now know the difficulties to cope with, and the various aspects to cover. The effort to deploy is of course proportional to the security requirements for the project.

In parallel, the press started talking in 2012 about « **Big data** » and security. « Big data » first refer to the explosion of the amount of data handled at some places, and the fact that these data come from many different sources. This implies new technologies such as Hadoop or NoSQL. On the topic of security, discussions about Big Data focus around 2 questions:

- « **Big data = small security?** ». Because of high constraints on data volume and data sources diversity, the architecture designed for « Big Data » infrastructures could be tempted to neglect security.
- « **Big data = Big Brother?** ». The ability to collect and handle high volumes of data makes attractive the idea to collect as much as possible data about people and their habits. This clearly implies privacy issues. And one could be worried about all the data collected by companies such as Google or Amazon about customers' life habits and daily activities.

> Even if the volume of data handled by many systems is indeed soaring, **« Big Data » remains a niche market** (few companies really need to set up a "big data" infrastructure), as computing grids are for many years. On the other hand, **the explosion of the amount of data collected about people and their habits also leads to societal problems** (with phenomenon such as "The Internet of Things" or consumer profiling) with possible attempts to privacy.

- **Smartphones**

In 2012, there was no significant evolution of the threat regarding smartphones. If we exclude the "BYOD" aspect (that we cover below in another paragraph), what we said in our 2011 report remains true:

- Android is the favorite platform for mobile malwares.
- The number of malwares identified by antivirus solution providers is skyrocketing (but as this article mentions it, this could be caused by the number of variants rather than the number of viral samples).
- Most of attacks consist in cloning popular applications and adding hidden functions to them to make generate automatic calls to expensive premium phone numbers.
- Those malicious applications are most of the time distributed via unofficial alternate markets, and targets "rooted" devices.

One can notice that:

- The new techniques integrated in 2012 in Android malwares reproduce those we already know in traditional computing (e.g. drive-by download, botnet, Ransomware).
- Data theft on smartphone (via malicious - or simply unscrupulous applications) is a real risk that is not well controlled yet. In the case of attacks targeted people, mobile phone trapping is without any doubt a technique already used in some underground circles (espionage technique). However, these techniques are going to generalize with the development of platforms such as Android. The unfair collect of personal data is another illustration of the same category of risk.
- As a counterpoint, and even is this could seem paradoxical, several organizations announced in 2012, that they chose Android as a base to build secure mobile communication solutions (for instance the NSA, Boeing, the German government). Android is not chosen here because of its inherent security, but because it is an open platform.

The smartphone is a technological platform that opens powerful perspectives for cyber-espionage. This was demonstrated for example, in 2012, by the release of the « PlaceRaider » demonstrator. This software rebuilds a scene from photos randomly taken by an infected smartphone. However, incident cases where smartphone technologies were used are publicly not known yet.

- **Social Networks**

We did not notice any real innovation in 2012 on the social networks topic, but these tools definitely remain very present in the news.

- **Hacktivism**

In 2012, hacktivist movements continued to lead a series of actions against companies or states. Several Anonymous episodes also showed some of the limits of such a group, particularly because of fanciful claims such as:

  - Sensationalist announces for unrealistic future attacks (such as the announcement on March 31th of an attack on DNS root servers – Operation « Blackout »),
  - Claiming to be the origin of incidents unrelated to them (for instance the GoDaddy Denial of Service attack, or the announcement of the theft of 1 million Apple credentials on a FBI workstation).

In the case of a movement such as the Anonymous (where everyone can claim to be a member of Anonymous), this type of events is of course not controllable by the group. This does not change the fact that hacktivism is a threat, which must be taken in account by companies.

- **BYOD (Bring Your Own Device)**

In our tag cloud graphic, the BYOD tag has a modest size in comparison to the impression we had from our daily watch: **BYOD is for us the topic that was the most discussed by the press in 2012**.

Today the BYOD phenomenon is mainly constituted with personal smartphones and tablets that some employees also use for their professional activities. This is an emerging phenomenon, but which has high chances of amplification. On the long view, we can consider BYOD as an externalization phenomenon complementary to the Cloud: with the Cloud, servers leave the company, and with BYOD, the user terminal disappears from the enterprise IT systems. There are multiple induced risks (data leakage on the Internet, intrusion in the company via the BYOD terminal, etc.) and solutions are yet to be discovered (securing the terminal versus not storing any data on it and consider the terminal as a simple screen?). Moreover, the issue is not only technical: impact on the business organization and juridical responsibility of the company are aspects at least equally difficult to solve.

> **BYOD is an underlying threat,** but there is no known incident yet, where BYOD terminal were used as an attack vector. Compromising the BYOD terminal of a private individual and using it as a way to penetrate the company is without any doubt a realistic attack scenario nowadays, but we will probably see it only if it aims at high value targets, for which other attack scenarios were not possible or too complex.

- **Cyber-espionage and APT**

Infiltration attacks (commonly known as APT – Advanced Persistent Threats) were the major event of our 2011 report. Of course this phenomenon still carries on in 2012 and **constitutes, from our point of view, the most worrying threat for companies**. We analyze more deeply this major phenomenon in chapter 4.2.

- **The rise of the states**

For several years, states have taken a growing importance in the cyber landscape:

  - On one hand, because they **setup or reinforced specific structures dedicated to cyber security**. This could be the creation of national agencies dedicated to computer security (such as the creation of the "National Information System Security Agency" ANSSI in France, in 2009), but also more recently the formalization of the possibility of cyber-wars. On this second topic, it is worth mentioning, in spring 2011, the publication by USA of the "Cyber 3.0" plan in which the DoD (Departement of Defense) announced that digital space becomes a war domain in itself as earth, sea, air and space are. In 2012, NATO also released the "Tallinn manual", which studies cyber warfare law.

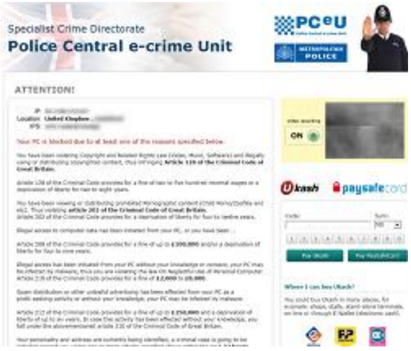
- On the other hand, because of **the disclosure of incidents, where attacks might have been sponsored by states**. China is regularly cited as probably involved in cyber-espionage attacks, as well as the USA or Israel (suspected of the Stuxnet attack against the Iranian nuclear plant). In 2012, Iran was also suspected of the Shamoon attack against Aramco (the national oil company from Saudi Arabia).

- **Cybercrime**

The « cybercrime » term is used to designate frauds that aim at stealing money from individuals by computer means. This is a phenomenon which became a major threat in 2005, and includes elements such as:

- Botnets (massive infection of machines used afterwards in malicious activities such as DDoS, Spam, etc…),
- Banking data thefts (phishing),
- Fake antivirus software,
- Etc…

In 2012, we observed a rise in the « **ransomware** » phenomenon, particularly with the "Reveton" malware (also known as the "Police malware"): this malware displays a message pretending to be coming from the Police, that indicates that the victim's computer was implied in illegal activities (for instance illegal downloads), and asks for the payment of a fine. This is a large operation that was particularly well built (the same message was translated – including references to the appropriate law articles - for at least 25 countries).



Specialist Crime Directorate

Police Central e-crime Unit

ATTENTION!

- **Personal data theft**

There were in 2012 a large number of announcements concerning personal data thefts (typically theft of account databases containing logins, passwords, card numbers, etc.). This is not a new phenomenon, but it continues to become more and more important from years to years. Dashlane.com issued in September 2012 a poster that lists the major data thefts for 2012, including:

- Zappos: 24 millions client contact details stolen in January 2012
- LinkedIn: 6,5 millions accounts stolen.
- Apple: 12 millions data relative to iPad, iPhone and iPod terminals stolen in September 2012
- Etc…

3) Major facts for businesses

We describe in this chapter the elements that seems to us to be the most important from enterprises:

- SCADA: the threat increases,
- APT and cyber-espionage: a risk that must be taken into account,
- 0-day attacks: a risk bigger than expected.

3.1 SCADA : the threat increases

In the industrial systems security field, several attacks got a significant media coverage in 2012:

- In April, the ICS-CERT alerts about attack attempts targeting gas pipeline operators (the attack consisted in sending trapped mails to these companies personal).
- During the summer of 2012, the Shamoon malware infected the information system of the Aramco oil operator (in Saudi Arabia). The same malware could also infect at the same time the RasGas gas producer (in Qatar). Some sources think this malware could have been created in Iran.
- In September the Telvent company (Schneider group) announced they suffered from an intrusion. The attack target would be the OASyS product commercialized by Telvent, and the clients using this product. Some sources think this attack comes from China.

The two first cases do not really target industrial systems (as Stuxnet did in 2010). **This is more attacks targeting companies in the energy field rather than attacks targeting SCADA systems**. However the last case is more worrying because it targets a specific SCADA product (OASyS).

Beyond these incidents, the major concerns for SCADA remain:

- **The low level of protection of some industrial installations**. In a note issued in October 2012, the ICS-CERT indicates for example they have the knowledge of a list of 500 000 industrial equipments apparently accessible from the Internet. Also, some manufacturers informed that they are not able to correct some of the vulnerabilities discovered by third parties in their products. Such vulnerabilities first got dubbed as « Forever-day » vulnerabilities (as a reference to « 0-day » vulnerabilities), but are now more commonly named as « Insecure by design » vulnerabilities (which cannot be corrected, because inherent to the design of the product).
- **The boosted activity in the flaw research field**. While in 2011, SCADA vulnerabilities were mostly discovered by SCADA "newbies" (but specialists of classic IT flaw research), in 2012 SCADA specialists also started SCADA vulnerabilities research (such as a project named « BaseCamp » organized by DigitalBond). The last discovery of this group is vulnerability in the CoDeSys product runtime. This runtime is integrated into hundreds of SCADA products which are therefore also affected by the vulnerability.

Industrial security is a field where the cyber attack threat is increasing and the security level of some installations is not satisfactory yet. This situation is worrying.

3.2 APT and Cyber-espionage: a risk that must be taken into account

For several years, more and more companies have been victims of intrusions in their information systems (attacks often designated as APT: Advance Persistent Threats), which are lead against them to perform industrial espionage or even sabotage. The APT phenomenon was ranked as top threat in our 2011 report. In 2012, this threat remains very present. The following table lists the most significant announces made in 2012 for this type of attacks.

February 2012	Verisign announces they suffered APT attacks in 2010.
February	The Wall Street Journal announces that Nortel has been suffering from an APT for almost 10 years.
March	The NASA announces they endured 13 major intrusions in their networks in 2011.
April	Nissan announces they discovered an APT threat in their networks.
July	AlienVault announces that the Sykipot malware would have been used in attacks targeting the aerospace industry.
July then October	Le Télégramme, then L'Express announced that the French government (Elysée) endured infiltration attacks in March 2012.
September	SecureWorks announces that the Mirage malware would have been used in cyber-espionage attacks targeting companies from the energy field.
September	The Telvent company announces they suffered from an intrusion aiming at their OASyS SCADA product.
November	Coca-Cola announces they endured in 2009 an attack which could have caused the failure of an acquisition in China.
December	Japan's Space Agency says rocket information was stolen by computer virus.

The APT risk first concerns companies or organizations which are exposed to international competition. Indeed, the risk of a foreign attacker being sued is low because of the difficulty to perform cross-country judicial actions. In this context, the "gain/risk" ratio is at its highest level and the computer attack is probably the "best weapon" for attackers.

There is no easy solution to counter the APT threat, in particular because these attacks are built specifically to exploit the company weaknesses. The Cert-IST issued several messages about this topic in 2012, first internally to its members, but also more broadly during its annual "Forum" conference day. We recommend the following actions:

- Reinforce the fundamentals: make the users aware to security considerations, harden the passwords, limit the administrator accesses and accounts, protect sensible data on secured servers, apply security patches and setup a security logs collect and management.
- Setup an active monitoring within the company, via a structure accountable for security monitoring.
- Define a reaction procedure in case of incident, which defines the behavior to be adopted and people to imply.

Companies exposed to international competition should not wonder if they will be affected one day by an APT, but should rather wonder when this will happen. They should especially prepare to this event by limiting its potential impact and developing their detection and reaction capability to this type of incident.

3.3 0-day attack: a risk bigger than expected

« 0-day » attacks are attacks that use vulnerabilities which were kept secret by its discoverer until the day they were used in an attack: the vulnerability has been known for 0 days before it was used in an attack. Because the used vulnerability is unknown, it is difficult to protect oneself against a 0-day attack and one can only try to limit the impact when such an attack is triggered.

0-day attacks exist for a long time. Around 2005, the development of fuzzers and the intensified research on security vulnerabilities transformed this threat, which was until then quite theoretical, into a real phenomenon. We know since this time that a 0-day attack is a possible risk. However, we now realize that the number of 0-day vulnerabilities the attackers have in stock is greater than we thought until then. In 2010, when it was found that Stuxnet used four 0-day flaws in a single attack, it was considered as an exceptional fact. In 2012, the “Elderwood” study, issued by Symantec, shows that some hacker groups (supposed supported by a state) seem to have access to a large number of 0-day vulnerabilities. Likewise, another study (called « Before we knew it », also from Symantec) shows that a 0-day vulnerability could be used for more than 300 days before finally being discovered.

Taking this risk into account requires the development of capacities similar to those already identified for APTs:

- Be able to detect as soon as possible that a 0-day attack succeed,
- Limit the consequences for the information system of a workstation or server compromising.
- Define procedures for isolation, impact analysis and return to operation, of the compromised elements.

All these elements show that the possibility of a 0-day attack must be considered as a probable event, and must be integrated in the threat management processes. This particularly implies to consider as a certain fact, that one day, an enterprise workstation or server will be the victim of a successful attack.

Note: There exist products that claim to be built to stop 0-day attacks. This is for instance tools able to detect abnormal behaviors (like stack overflows) and to stop them. However these tools are not 100% efficient and do not allow to completely eliminate the 0-day attack risk.

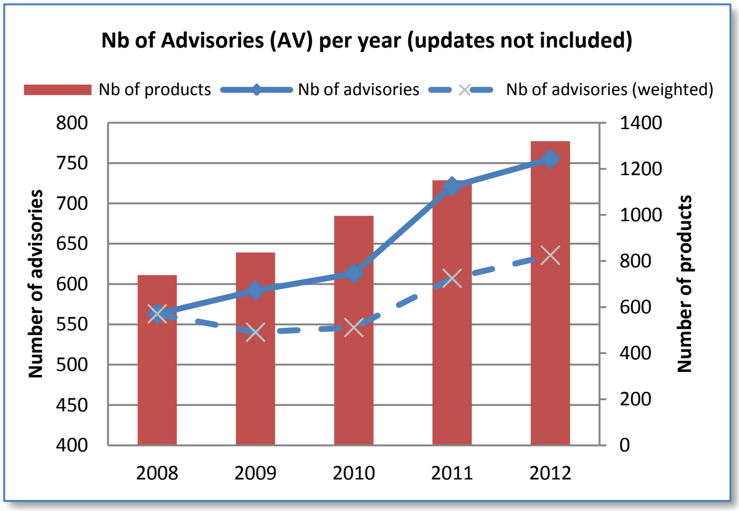
4) Figures about Cert-IST 2012 production

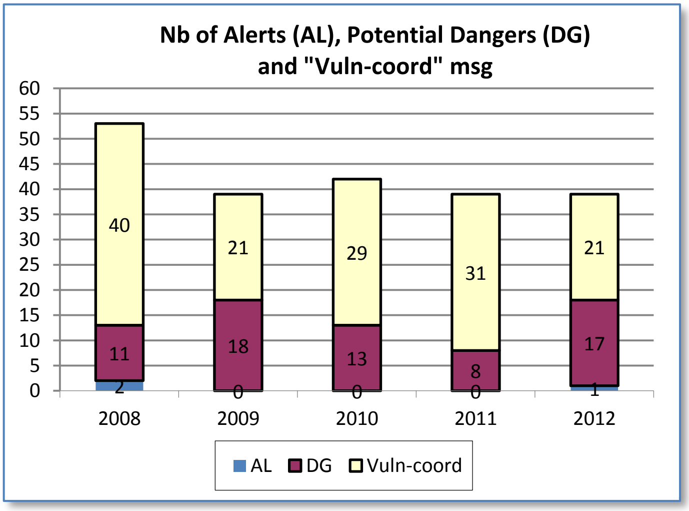
4.1 Daily monitoring on vulnerabilities and threats

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. This information is daily analyzed to provide our members with a sorted, qualified and prioritized set of information. The Cert-IST therefore produces different types of productions:

- **Security Advisories**: they describe newly discovered vulnerabilities in the products followed by the Cert-IST. These advisories are continuously enhanced with minor or major updates. These latter typically occurs when an attack programs (aka “exploits”) is 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 2008 one alert for the Conficker worm and another for the DNS vulnerability (discovered by Kaminsky). 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 2012, the Cert-IST published:

- **755 security advisories** continuously followed during the year with 2128 minor updates and 85 major updates. The number of advisories is constantly increasing since several years (see the curve above), and this phenomenon is not caused by the rise of the number of products followed by the Cert-IST (see the weighted curve, which takes into account the number of products which generated advisories during the year). This continuous increase shows that vulnerability discovery is a phenomenon which does not dry up: from year to year, vulnerabilities are found in products which constitute the company’s I.T. Holding the security level then requires a regular application of the security patches on these products. On the 31st of December 2012, Cert-IST follows vulnerabilities concerning 1320 products and 10 312 product versions.

- **1 Alert, 17 Potential Dangers and 21 « Vuln-Coord » messages.** The alert published by the Cert-IST this year concerned the **Java** client installed on workstations (the JRE component) and result as a consequence of a series of Java attacks seen during the year. Chapter 2.1 furthermore analyzes the alerts and potential dangers released by the Cert-IST in 2012. We can however notice that 2012 figures about alerts and potential dangers are increasing from 2011 and come back to values similar to 2009.

4.1.1 Technological watch

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

- A daily media watch report which lists the most interesting articles found on the Internet over a sample of French and English-speaking websites about security.
- A monthly SCADA watch report presents a synthesis of the news about industrial control systems security.
- A monthly general report 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.

5) Conclusions

- **2012 shows again the importance of vulnerabilities management for companies**

Each year, more than 4000 vulnerabilities are discussed on the Internet. Collecting, analyzing and sorting this information is a significant part of the daily work of the Cert-IST. This implies the production of about 750 security advisories that feed the patch management processes of our members. This background work allows them to maintain their installations at their best security level.

- **Vulnerability management does not limit to patch deployment**

When a specific threat appears, the Cert-IST sends to its community specific messages informing of the imminence of the event (Alert of Potential Danger) and the available means to protect against it. This allows the companies to evaluate their exposure and to decide of the most adapted measures to take and the timing of their deployment.

Additionally, companies must consider that workstation or server compromising is a possible event (because of a 0-day attack or an internal malicious activity) and the information system architecture must be built to resist to this possibility. The quick detection and treatment of infections should enable a fast return to a normal situation.

- **The company must face a higher attack risk**

For many years the company knows how to face with minor infections such as the ones caused by viruses. But the threat had changed, and one must now face intelligent attacks directly controlled by humans. Cyber-espionage attacks (APT) or the increasing threat against SCADA systems clearly show this change.

- **Attacks can be very sophisticated**

0-day attacks or techniques to bypass classic protection systems (antivirus, anti-memory overflows, sandboxes, etc.) show the technical expertise level reached by attackers. Likewise, attack schemes are nowadays much more sophisticated than ever. For instance, an attacker could first compromise a website that he knows to be visited by their victim, to infect them when they browse this website, and then finally propagate from the victim workstation to critical servers inside the company.

Today, attackers are professionals with a large panel of skills: buying 0-days, developing exploits, managing attack infrastructures are many skills they now easily master. Likewise, for the most elaborated attacks, specific developments are possible: trapping a smartphone or a tablet, infiltrating in a cloud infrastructure are for instance perfectly realistic events.

- **In parallel, the technology evolution leads to a large demand to relax security constraints**

Social networks, cloud technologies or BYOD are examples of the quick evolution of technologies. They become more and more present in our daily life, until changing deeply our way to communicate (e.g. Twitter, Facebook) and our use of technologies (many users now require a universal access to their data: anywhere, anytime, anyway). This evolution greatly increases the attack surface of the company.

- **One must find a trade-off with a complex situation**

The CISO is facing a complex situation, between on one hand, more and more sophisticated attacks and on the other hand user demands for a bigger opening to new technologies. The Cert-IST, via its technological watch activity and reports, gives them an enhanced vision of the threat. And from our point of view, this threat is increasing. Moreover attackers know where the company’s weak points are (like sometimes the lack of internal networks isolation, or a weak security monitoring level) and exploit these weaknesses. Many national organizations call for a reinforcement of the security level within organizations. For instance the « 20 Critical Security Controls For Effective Cyber-Defense » guide published in the US, and the French « Guide to Computer hygiene » published by the French ANSSI in October 2012, both recommend a strict application of traditional principles of security in depth (platform hardening, application of security patches, network segmentation, privilege limitation, etc.) They highlight strict measures that sometime may be considered as constraining or inadequate for modern information system. Yet they actually present the reference principles of a secured and controlled architecture.

End of document