Cert-IST annual review for 2010 regarding flaws and attacks

1) Introduction

Each year, the Cert-IST makes a review of the passed year. The goal is to sum-up the major events of the last year (2010) in order to highlight the trends regarding attacks and threats, and to help readers to better protect their assets.

At first, we examine in Chapter 2 the major attacks occurred during the year.

Then in Chapter 3, we analyze more broadly the evolution of technology and identify areas where security is a growing concern.

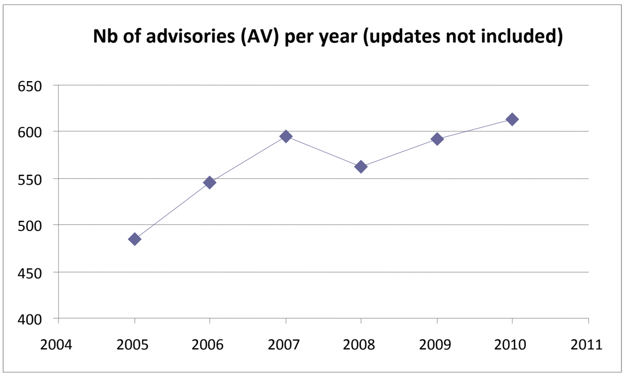
2) The attacks seen in 2010

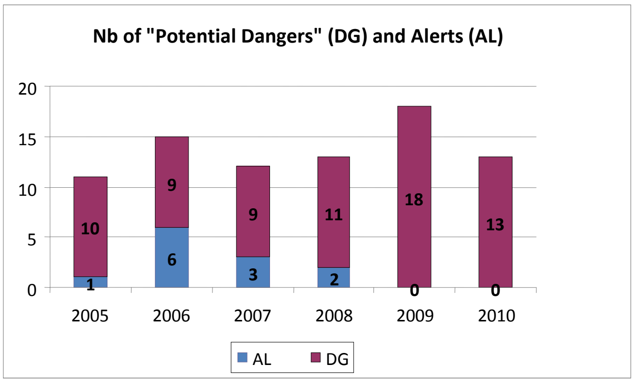
2.1 Some figures

All along the year, the Cert-IST publishes messages to inform the operational teams of its members about potential attacks, and provide protective measures to address them. In 2010, the Cert-IST issued:

- **613 security advisories**. These advisories describe the new vulnerabilities discovered in the products monitored by Cert-IST. These advisories have been continuously updated to reflect the latest information available; this lead to 1798 minor updates and 82 major updates (major updates are often released because an "exploit code" - which allows to easily perform an attack - has been made available). Compared to 2009, the number of advisories has increased (see the curve below). And Microsoft contributes largely to this increase, because 2010 was a record year for Microsoft, with 106 security bulletins issued during the year.

- **13 Potential Danger Notices and 0 Alert**. Potential Danger notices are sent by Cert-IST to inform about a significant threat (which requires special attention) but not yet imminent (or of a moderate severity) and for which the Cert-IST consequently recommends specific protection measures. On the other hand, Alert notices are sent for major threats which require immediate reaction. In 2010, the number of Potential Dangers released is low compared to 2009 (see the histogram below), and returns to a value comparable to previous years. Like in 2009, Cert-IST released no Alert in 2010. The last Alert remains the one issued late 2008 for the Conficker worm. This means that overall, the threat persists (Cert-IST released about the same number of Potential Dangers during the year), but no widespread attack (for which the Cert-IST would have issued an Alert), did occur. Beyond this trend, we analyze in greater details in the next chapter the nature of the threats addressed in 2010.





Note: New products are added to the Cert-IST product catalogue as required by its members. As of December 31th, 2010, the Cert-IST followed the vulnerabilities for **996 products** and 8216 versions of products.

2.2 The nature of the threats addressed in 2010

The 13 Potential Danger notices issued by the Cert-IST in 2010 are all for attacks that target the user's workstation. This confirms and reinforces a trend already highlighted in 2009 (in 2009 we noted that 70% of the attacks targeted the workstations and 30% the infrastructure equipments).

This means that the main threat that organisations have to face today is the attack against users. The typical scenario used by attackers for such an attack is first to convince the user to visit a trapped website and then to infect the user's workstation automatically when he browses the site (such an attack is called a "drive-by download" attack). For this, the attacker can:

- either send to the user an email enticing to visit the trapped website. He may also attract his victim by other ways, such as a Twitter message, or a comment on a blog, etc ... .This first case is a direct attack scenario.
- or infect legitimate (poorly protected) websites and change their content in an invisible way in order to subsequently attack visitors. This second case is an indirect attack scenario.
- or even to insert a booby-trapped advertisement in the middle of the regular advertisements run by a legitimate advertising agency. The booby-trapped advertisement is later (unintentionally) broadcasted on any websites that rent advertising space, and ultimately attacks the people visiting these websites. This third case is a double-indirect attack scenario.

These scenarios have been known for several years and have already been detailed in our 2009 report. They are the preliminary phase to the attack itself, which consists of sending an attack code that exploits a vulnerability in one of the software installed on the victim's computer.

The table below gives the details of the new vulnerabilities discovered in 2010 for which the Cert-IST issued a "Potential Danger" notice (because the risk of attack using this vulnerability was high).

Number of "Potential Dangers" issued by the Cert-IST in 2010 (ranked by type of vulnerability)	
Attacks targeting users while browsing the web	
- Attacks using PDF (Adobe Reader) or Flash (Adobe Flash Player)	6 (46%)
- Other web based attacks : QuickTime, Windows Help Center, trapped websites	3 (23%)
- Attacks using Internet Explorer	2 (15,5%)
Attacks against Windows (not related to web browsing) : .lnk/stuxnet and dll hijacking	**2** (15,5%)

We note that:

- For the second consecutive year, PDF and Flash vulnerabilities are at the top of this ranking. This category extends its lead and now represents 46% of the Potential Dangers (instead of 31% in 2009),
- Microsoft Office, or ActiveX, no longer appears in this 2010 ranking, but Internet Explorer is still present.

The vulnerabilities described above are new attacks vectors that were discovered in 2010. They actually are added to the toolbox of already known attacks used by hackers, and especially to the "Exploit-kits". "Exploit-kits" are all-in-one hacker tools designed to attack visitors by launching a serie of pre-recorded attacks. The "Exploit-kits" were introduced in late 2006 (“Mpack” is the first known example) and have largely developed since: Eleonore, Fragus, Neosploit are examples of contemporary "Exploit-kits".

3) The major facts for 2010

Beyond the new vulnerabilities identified daily (presented in Chapter 2) Cert-IST also analyzes trends, and the overall evolution in computer security. This chapter presents the most significant phenomena for 2010:

- APT (Advanced Persistent Threat): Infiltrating organisations through IT attacks,
- Stuxnet and SCADA security,
- iPhone, Android or Phone7: a mutation in the mobile phone practices,
- Cloud computing,
- Reinforcement of the legal framework,
- Botnets: Attacks and dismantlings follow each other.

3.1 APT (Advanced Persistent Threat): Infiltrating organisations through IT attacks

The term "APT" exists since at least 2007, but really became popular in 2010. It is used to designate computer attacks that aim at infiltrating the IT system of a targeted organisation. An APT attack typically:

- First infects an internal information system component (e.g. a user's workstation),
- Then, stays hidden and remains undetected as long as possible on the infected system,
- And finally, performs malicious actions, often being remotely piloted by the attacker.

What differentiates an APT from a conventional attack (e.g. the infection of a workstation by a botnet) is that APT attacks often have a "strategic" objective and are built to attack a specific organisation. The compromise of the user's workstation is not the objective of the attack, this is just a way for the attacker to infiltrate the organization and to conduct from there an offensive action with a specific purpose, such as industrial espionage.

Two APT attacks were particularly highlighted during 2010 and were heavily covered by media:

- In January 2010 the "**Aurora**" case. At that time, Google publicly announced that it suffered an attack from China that severely infiltrated its IT systems. More than two dozen other U.S. companies (including Adobe and Juniper Network) subsequently confirmed that they were also targeted by the same kind of attack. Hackers have used booby-trapped PDF files, or vulnerabilities in Internet Explorer 6, to infect the workstation of some employees of the companies mentioned.
- In July 2010 the "**Stuxnet**" worm, which targets industrial systems (SCADA), was discovered. The worm was designed to spread from computer to computer until it reaches computers used to control industrial equipments. It seems (but it is difficult to verify) that Stuxnet was designed by the Israeli government to destroy Iranian nuclear enrichment equipments.

These kinds of targeted attacks that aim at industrial espionage, does not date from 2010. Older examples (with less media attention and perhaps less sophistication) had existed for a very long time (see for example in 2004 the Titan rain case where it was alleged Chinese attacks against U.S. military sites, or the Michaël Haephrati case that highlighted the use of Trojans for industrial espionage). Moreover, in July 2005, we devoted the Editorial to our monthly newsletter on this subject. But these new 2010 cases, and the large public reports about these attacks, show that APT attacks are real and are now part of the standard arsenal available to attack a competitor.

3.2 Stuxnet and SCADA security

Stuxnet, which has been introduced above about APT, is also a major fact of 2010 because it demonstrates a risk that was seen previously only as a theoretical risk: a computer virus designed to attack an industrial system.

Beyond speculations about the authors and their objectives (is it a cyber-weapon built to destroy Iran's nuclear centrifuges?), the Stuxnet phenomenon is primarily worrisome for two reasons:

- First, it shows that industrial systems should be prepared to deal with cyber attacks, and that these attacks can be very sophisticated and specifically designed to reach these industrial systems.
- Then, it shows that even industrial sites that feel they are not potential targets, are also concerned. Stuxnet probably aimed at a single target, but it has also infected by a "collateral effect" almost 100,000 other systems worldwide. It is designed to recognize its target and trigger its payload only on this target. But can we be sure of the reliability of this recognition mechanism?

Stuxnet is undoubtedly a major event for the world of industrial control systems (a world often called "SCADA" for convenience). It demonstrates that a latent threat that companies were already aware of for years (a cyber attack against an industrial system) is now urgent to address. It will undoubtedly be a boost to the work already underway to secure these industrial systems.

Note: Since early 2010, the Cert-IST has integrated to the field of its activities the monitoring of the threats that could impact SCADA equipments.

3.3 iPhone, Android or Phone7: a mutation in the mobile phone practices

- **The current attacks are mostly scams**

In the recent years, with the widespread use of mobile phones, there were fears that the attacks already affecting standard information systems (viruses, botnets, spam, etc...) do also affect mobile phones. So far this threat did not occur, or at least not at a scale large enough to constitute a major issue. Several reasons are often put forward to explain this observation:

- Mobile phones operating systems are heterogeneous: at least 5 different operating systems exist, and for the same OS, the code developed for a given phone model is not always compatible with other models of the same brand. This segmentation of the market makes it difficult to design an attack code that could create a large-scale attack.
- Hackers are not necessarily interested in creating large-scale attacks since their motivations have changed. It is now better to carry out small attacks that will make profit (e.g. SMS sent to premium taxed numbers), rather than launching major attacks which just result in disturbing the infrastructure.

In 2010, we continued to see malicious activity showing that the risk of attack against mobile phones is still present. For example, the first case of a "botnet" targeting Android phones was discovered in December 2010 (the "Geinimi" Trojan). Examples of scams designed to generate calls to premium rate numbers, were also very common (e.g. this example for Windows Mobile in April 2010).

- **New practices induce new risks**

More than those conventional attacks, we believe 2010 marks a significant change in practices. This change is due to a broader usage (democratization) of smartphones (typically iPhone, Blackberry, Android):

- They are multi-purpose devices (phone, PDA and Internet terminal) on which the user can install third party applications (downloaded from portals such as "Apple Store" or "Android Market").
- They are often used by users almost always connected to the Internet, e.g. through applications such as Twitter and Facebook.

In fact the boundary between business world and private life is increasingly difficult to identify for these users:

- The same phone is used for business and private activities. And it is not unusual that an employee chooses to purchase his own device and to use it also for business (rather than using the device provided by his company).
- He has direct access to Internet (via a subscription to a "data service"), which does not necessarily transit via the company's infrastructure. And, in order to have a universal access to his data (both personal and professional) from anywhere (inside or outside the company), some users will even be tempted to put on the Internet business data (such as his address book or calendar via Google services).
- The user installs third-party applications without caution: The offer of free applications is huge and the user is unaware that some of these applications may be malicious.

This leads to the significant risk that the smartphone may become:

- A source of data leak for the company,
- And a prime attack vector for targeted attacks.

This finding is reinforced by the fact that when a security flaw is discovered and fixed, the update of the affected smartphones is a tricky operation (it is not a routine operation), especially if the company smartphone fleet is heterogeneous.

2010 is a boundary year where all these issues become critical. It appears now essential that companies review these new risks and explore solutions for the creation of a security policy covering smartphone devices and mobile device management. Recognizing this trend, the ENISA (European Network and Information Security Agency) published late 2010 a guide about the security risks posed by smartphones. It draws the attention of organisations on the need to manage the smartphones devices (and for example to provide data erasure procedures) and to protect the company against possible data leakages.

3.4 Cloud computing

"Cloud computing" did stay at the top of the marketing news all along 2010. Gartner indicated in its annual report on emerging technologies (published in September 2010) that "Cloud" is at the top of the user expectations curve, and that it will take several years before it will be truly adopted. If the "Cloud" generated so much interest, it is because it is seen by IT departments and Managing Directors as an opportunity to reduce costs.

During 2010, the "cloud" landscape has been somewhat clarified, and the most significant areas that should most likely survive to the marketing hype are:

- Private cloud: This is an in-house technical infrastructure that is used by the company to host its business applications on distributed virtual platforms. This kind of solution is still emerging (the offers are recent). It can be seen as an extension of the work already done during the recent years in the field of virtualization. Security issues in this case are limited within the company, which greatly reduces the risks.

- SaaS (Software as a Service): This is the case where a supplier provides business applications hosted in its premises accessible to users over the Internet. This area is booming and suppliers offering SaaS solutions are soaring. There are applications for the enterprise (e.g. Customer Relationship Management solutions - CRM - such as SalesForce.com, or collaborative work solutions based on internet based web-conferencing or shared storage services) or even for the general public (with free offerings like Google Docs or Microsoft Skydrive). The offer is large and very attractive. It also presents real security risks to the business if the practices are not regulated and guided.

The uncontrolled deployment of SaaS solutions is a real risk for companies because, like for smartphones or social networking, these offers are highly attractive to the users. For example, a user may be tempted to use the free desktop environment offered by Google Docs to work on documents with partners, or free online storage solutions (such as Dropbox) to access its business data from anywhere (from his mobile phone, from home or from enterprise offices). Security risks are then multiple: data leaks, of course, but also the loss of control for the enterprise of the data stored "in the cloud". For example:

- Who is the owner of a document created by an employee on a free "cloud" service? : the service provider, the user or the company?
- How can companies recover these documents if the user leaves the company or is unavailable?
- How to proceed to perform a post incident investigation on a "cloud" based system?

These examples shown that the security policy of a company could be undermined by an improper use of this type of "cloud" solutions and that legal remedies are still lacking in this field (who is responsible in case of problem?).

During 2010, we noted several security incidents affecting "cloud" solutions (see below). None of these incidents is really worrying at the moment. They show mainly that hackers are also interested in the "cloud" technologies and are currently exploring their possibilities:

- The authors of malicious code designed methods enabling them to bypass cloud based antivirus protection (see for example this article: Trojan Bohu, the first attack against the cloud antivirus system),

- The computational power of "cloud" solutions can also be exploited for malicious purposes, e.g. for breaking passwords (see for example this article: GPUs crack passwords in the cloud), or to perform DOS attacks (Amazon Cloud DoS attacking ITSPs)

- A cloud-based service is not immune to failure (see for example this article about the unavailability of the Micorosft Hotmail service: Hotmail Data Loss Reveals Cloud Trust Issues).

3.5 The legal framework is strengthening

Note: The facts depicted below are mostly French-centric, but the findings apply worldwide.

The year 2010 marks a strengthening of the French legal aspects in the field of IT security, especially in the field of protection of personal data. The Détraigne & Escoffier Bill (filed late 2009) which proposes to make mandatory the nomination of a CIL (“Correspondant Informatique et Liberté” equivalent to the US Chief Privacy Officer) in every company, and the notification of security incidents (if they are related to personal data) led many questions. It is not clear yet if this proposal will be adopted soon by the French National Assembly, but it is more than likely that this kind of data breach notification requirement will be added in a near future in the French law. This requirement already exists at European level for the Telecom operators (see the "Telecom Package" which was adopted by the EC in November 2009) and the European Community already announced that it plans to extend this requirement to other market sectors.

This requirement has significant implications for all the companies (since all of them operate or host customer records and other nominative data) and must therefore be prepared.

This legislative strengthening seems in fact a natural extension of the efforts made over the last decade in the regulatory field (the Sarbanes-Oxley Act dates back to 2002) and more recently in the field of security standards (ISO-27001 for example).

3.6 Botnets: Attacks and dismantlings follow each other

For several years now, the fight against cyber-criminals is on-going. In our 2008 annual review, we already mentioned that fact and took as example the take-down of unscrupulous hosting services (McColo and Atrivo) that were used to host botnet command & control servers. These types of actions are continuing and are intensifying. For example, early 2010 we have seen a series of announcements about the dismantling of several botnet networks: Kneber, Waledac, Mariposa. A general audience could have discovered on this occasion that organized large-scale hacking exists and that a group of hackers could be able to gain control over tens of thousands of computers.
But such dismantlement also demonstrates that the ability to respond to these illegal actions has greatly increased in efficiency in the recent years. Multinational groups of computer experts and law enforcement teams are now able to cooperate to carry out such large-scale actions. This demonstrates once again, as we said in the conclusion of our 2008 yearly report, that on the attack realm, positions have hardened and professionalized: attackers and defenders are becoming more experienced and determined than ever.

Of course the botnet phenomenon has not been stopped by these dismantlements. And today, the main objective of the attacks against the user's workstations (as already discussed in Chapter 2) is precisely the creation of new botnets made up of compromised computers. These botnets are then used to perform malicious actions such as sending spam or performing DDOS attacks. The management of these botnets is highly organized: some hacker groups have specialized in the creation of botnets, others are dedicated in keeping them operational and in renting them to final attackers who buy them just for the time of a malicious activity (such as a SPAM campaign or a DDOS attack). Even worse, now « Do It Yourself » kits are available that enable cyber-criminals to easily build their own botnets. Cyber criminals also deploy various techniques to avoid being the target of the dismantling operations. For example, they divide their botnets (to avoid losing all the infected machines at once) or infect the same computer with several malware with different characteristics. We presented an example of this latter technique in an article entitled Kneber, a botnet’s story that we made public in February 2010.

In the field of botnets, we can finally note for 2010, the arrival of the **SpyEye** banking malware. First found in December 2009, this malware specialized in stealing bank details was quickly presented as the rival of the infamous Zeus malware, in particular because SpyEye has features to fight Zeus and to take the control of any computer already infected by Zeus. Finally, late 2010, the battle between these two malware ended with a private agreement and the merge of the two malware. This results in a new version of SpyEye, even more sophisticated and malicious, and is so far the most sophisticated malware in the field of banking malware.

4) Conclusions

In terms of attacks, the year 2010 is in line with previous years. The number of vulnerabilities discovered each year remains high (over 600 new Cert-IST security advisories released, and nearly 2000 updates made on the advisories during the year).

These vulnerabilities are most often used by hackers to try to compromise user's workstations, with the objective:

- either to include this workstation in a network of compromised machines (a botnet), which is then used for large-scale malicious activities (spam, DDOS attacks, etc ...)
- or to infiltrate deeply into a company and then perform specific malicious actions (industrial espionage, sabotage, etc.) while remaining undetected as long as possible.

The year 2010 even marks an accentuation of the attacks targeting end-users:

- There is a growing number of botnets discovered. The dismantling of some of them during 2010 (e.g. Mariposa or Waledac) was intensively covered by media and demonstrates that an active struggle is on-going between attackers and defenders.
- Cases of targeted attacks have also caught high media coverage during 2010 (e.g the Aurora attack against Google or the Stuxnet worm against SCADA systems). The fact that such “strategic” attacks are now made public shows that this phenomenon is a growing concern.

Whether it was for built botnets, or to perfom targeted attacks, the malicious code seen in 2010 were, as for previous years, at a high level of sophistication and ingenuity.

Organizations have three complementary axes to protect against this threat:

- The first one is to maintain user’s workstations up to date (in terms of security patches) for both the operating system and the third party software (PDF reader, Java runtime, etc ...). This topic is vital because up to now, most of the attacks against workstations use old vulnerabilities for which patches have already been released by vendors. The ability to continuously watch at new vulnerabilities, and to deploy security patches within the organization, is the first line of defence against attacks.
- The second one is the ability to detect, as soon as possible, the compromised workstations. The user is often the first to detect an abnormal behaviour of his workstation. If he is aware of the risks of attacks and has a channel to report its finds, it can be a key factor in the detection of targeted attacks.
- The last one is to enhance the security of the workstation. Beyond the conventional protections (such as antivirus) that have shown their limits in recent years, new tools to protect workstation still have to be found. For example, web browser virtualization could be one approach here. This solution is often proposed to counter web-based attacks, but has not yet fully demonstrated its usability for large deployments.

On the topic of technological evolutions and users expectations, the trend continues to be in offering/demanding more flexibility. User expectations are to have:

- a permanent connection to the Internet, for example through smartphones. As a consequence, it is now often difficult to mark the limit between (and to separate) business and personal activities,

- an information always available, with the temptation to move the business data to the Internet (e.g. via cloud-based solutions).

Without rejecting these expectations, Security Managers must remain vigilant because the security risks induced here are multiples. Possible data leakage (e.g. in case of loss of a smartphone) or even loss of control over outsourced data (e.g. in case of cloud-based services) are examples of such risks. The analysis and the mitigation of these risks must be performed. This should result in the definition of a policy which defines the acceptable practices and in guidelines and monitoring tools to enforce them.

Finally, and quite logically, after the efforts made in the recent years in the regulatory and normative fields (e.g. Sarbanes-Oxley and ISO-27001), the legal aspects are now gaining more importance, especially to face the challenge of protecting personal data. The growing importance of the CPO (Chief Privaty Officer) function, or the ongoing discussions in Europe on possible new obligations to report data breaches are examples of this trend.

End of the document