Cert-IST annual review for 2011 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 (2011) 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 that 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.

➢ About Cert-IST

The Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam **- I**ndustrie, **S**ervices et **T**ertiaire) 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) Vulnerabilities, viruses and attacks seen in 2011

2.1 The attack targets has changed

➢ The cyber-threat has changed and is more indirect

In terms of threats, the year 2011 marks a change from previous years. Until 2010, the most common threats were related to the discovery of new vulnerabilities impacting equipment or software (and in particular the discovery of "0-day" vulnerabilities, that is to say, vulnerabilities which were never disclosed until they have been used in actual attacks), or the spread of a massive attack (e.g. large scale compromise of web sites, or massive spread of worms that has been seen about ten years ago). In contrast, the threats seen in 2011 were of a different nature and more indirect. Typical examples of these new threats are: the theft of SecurID data at RSA, or the multiple TLS/SSL incidents (e.g. the "BEAST" attack or the compromises of Comodo and DigiNotar Certification Authorities). In 2011 the security teams of companies had to address questions such as:

- Is my VPN access still secure (after the RSA SecurID incident)?
- Can we still trust HTTPS (following the TLS/SSL incidents)?
- Should we be more proactive to protect us against DOS attacks (after the release of DOS attack tools)?
- Should we take into account the "Anonymous" group threat?
- Etc ...

As we can see on these examples, the 2011 threats were more indirect than those treated in previous years (they were mainly the consequences of attacks targeting a third party) and often complex to evaluate (is my IT system actually impacted by these security events?).

In 2011, despite the facts that the number of vulnerabilities has not increased very significantly, and the number of alerts has been low (see section 2.2 below), the threats were significantly high because of these new type of events. And the number and the severity of the incidents publicly announced this year have greatly increased (probably because of the new lawful obligations in this field).

➢ Attacks that use IT to target the company

The 2011 security events confirm that cyber attackers have changed their objectives (or rather have added a new objective to those already adopted):

- In the 2000s, attacks aimed at saturating networks (with the exponential viral propagation).
- Since 2006 the attacks have turned their interests to the user’s workstation with the objectives to steal him some money (e.g. via fake antivirus scams), or to include the computer in a botnet.
- In 2011 the attacks are aimed at business (industrial espionage or either sabotage) and computer attack is simply a tool to achieve the intended purpose. For the attackers IT is now just a vector to penetrate the company and also a place where enterprise’s vital data are stored.

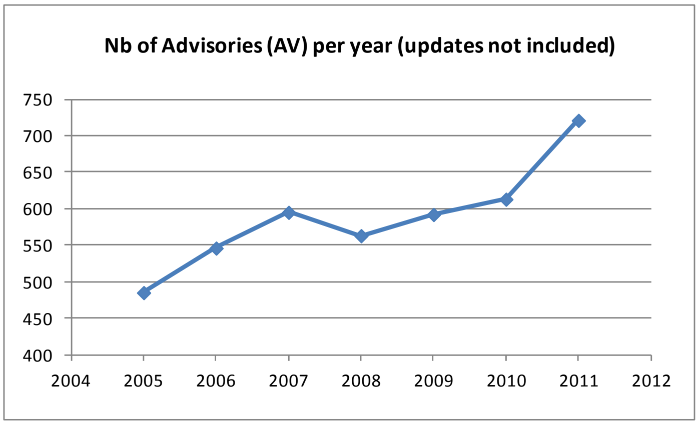
2.2 2011 figures

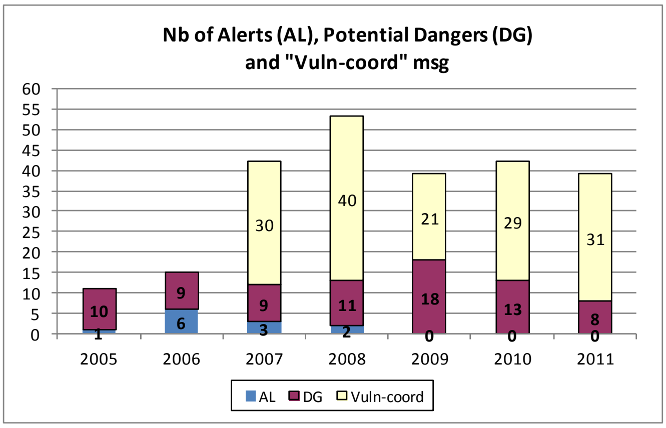
➢ Security Advisories and Alerts

In 2011, the Cert-IST released:

- **721 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 2427 minor updates and 84 major updates (major updates are often released because an "exploit code" - which allows to easily perform an attack - has been made available). Compared to 2010, the number of advisories has increased (see the curve on the next page), but this increase is mainly due to the increase of the number of products monitored by Cert-IST. As of December 31th, 2011, the Cert-IST followed the vulnerabilities for **1150 products** and 9248 versions of products.

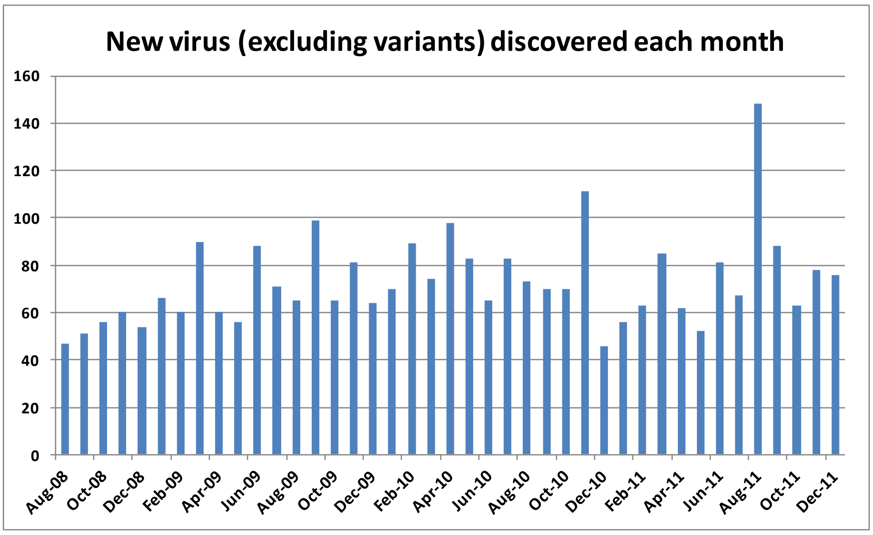
- **0 Alert, 8 Potential Danger notices and 31 "Vuln-coord" messages**. The Cert-IST Alerts are sent for major threats which require immediate reaction. Potential Danger notices are sent by Cert-IST to inform about a significant threat (which requires special attention) but not yet imminent (or of a moderate severity) and for which the Cert-IST consequently recommends specific protection measures. Finally, the "Vuln-coord" messages are coordination messages that draw attention on particular vulnerabilities (often hyped up by the press) but of less importance. These 3 complementary publications are driven by attack probability while security advisories systematically document each vulnerability. In terms of attacks, the 2011 figures are lower than the previews years (see the number of Dangers and Alerts in the histogram at the next page). However, as previously stated the threat nature has changed: there is less attacks but their potential consequences could be very serious.





➢ The virus in 2011

The Cert-IST continuously monitors the threats induced by newly discovered virus, by reviewing the data published by the major antivirus vendors. This analysis is done on new viruses, and does not take into account the variants which later appear for each virus. The histogram below gives a summary of this activity. It shows that, apart from the epiphenomena that should not been taken into account (the peaks that appear on the histogram), the curve as a whole remains relatively stable (around 60 viruses per month) all along the years. At the same time, the number of variants identified by antivirus vendors exploded. To be convinced, just visit the McAfee or Sophos pages that list the latest viral variants: 3 years ago the variant where named as "Virus.B" (which is the variant B of a given virus), and now they have names such as "Generic.dx!12536D125737" (which is the variant "12536D125737" of a generic behavior considered as malicious).



2.3 The 2011 attacks

The table below sums-up of the attacks and vulnerabilities that caught the most of the media attention in 2011.

Event	Description
Attack against the French Ministry of Economy and Finance (March 2011)	In early March 2011, the French Ministry of Economy and Finance announced that it had suffered an attack aimed at stealing documents related to the G20. The attack began in December by the silent compromise of several workstations and apparently required later heavy works to totally disinfect and secure the impacted networks.
Attack against **RSA** and threat of SecurID data (March 2011)	In late March 2011, RSA announced that he had been attacked and that data related to the SecurID authentication tokens have been stolen. Some of these data will be used later, in late May 2011, to attack the company Lockheed Martin. It is the most demonstrative example of the many APT attacks announced in 2011 (see the list given in Chapter 3.1.2), including the attack of the Ministry of Economy and Finance (listed above) or of the Areva company (specialized in nuclear energy) in September.
Mac Defender: a fake antivirus for Mac-OS X (May 2011)	In early May 2011, the Intego company has discovered a malware masquerading as an anti-virus for MacOS X. It traps the users that are using search engines by displaying messages telling them that a virus has been detected on their system, and by offering to install anti-virus software named Mac Defender. Once installed, this fake antivirus will collect sensitive data (bank information) on the user's computer. While fake antivirus applications are very common in the Windows world, Mac Defender is the first case of such a malware on Mac OS.
Lulzsec and **Anonymous** attacks	Since the end of 2010, cyber-activism actions, such as the ones performed by the groups named Anonymous and Lulzsec, have multipled; This includes the DOS attacks against Paypal, Visa, MasterCard and Sony by the Anonymous group, and the attacks against the U.S. Senate and the CIA by the Lulzsec group. In June 2011, these two groups have merged and founded the movement called Operation AntiSec which targets the governments curtailing freedom of expression.
Attack against **Sony** (April 2011)	A massive attack that occurred between 17th and 19th April 2011, took off-line the Sony online gaming platform (PlayStation Network). The platform was not able to restart until 15th of May 2011. During this attack, millions of personal data were stolen.
DOS tool against Apache: "**Apache killer**" (August 2011)	In August a program called "Apache killer" was released on the Internet. It uses the HTTP fragmentation feature (HTTP header "Range") to saturate an Apache server.
DOS tool against SSL: **THC-SSL-DOS** (October 2011)	In October, the THC group released a tool that uses the SSL "re-negociation" feature to overwhelm a remote SSL server (typically an HTTPS web server).
Morto worm (August 2011)	Morto is a worm that spreads by searching for Windows computers exposing an RDP access. It tries a sequence of trivial passwords on any RDP access found. It was the first case of an RDP worm and its propagation was not very wide (according to this Microsoft analysis).
SSL Certificat Authorities (CA) compromises **Comodo** (March 2011) and **DigiNotar** (September 2011)	In March 2011, the Certificate Authority company named Comodo announced that it has been hacked and that the hacker was able to generate 9 fake SSL certificates. Such a certificate can allow a malicious person to impersonate geniune web sites and to perform harmful actions on vulnerable systems (authentification credential or sensitive information theft, etc.). On August 30, 2001, Google sent an alert to its customers about a fraudulent digital certificate issued by the Dutch Certificate Authority named DigiNotar and pretending to be "google.com". This was due to a cyber-attack

	that breached DigiNotar IT system. The analysis that was done on that incident revealed (see this report written by FoxIT) that the cyber-attack occurred early in July and that the security of DigiNotar infrastructure was very weak. The latter finding is very disturbing because a Certificate Authority is supposed to be very secure (it is a key component of digital certificate security). The attackers who breached DigiNotar security was able to generate more than 250 fake certificates to impersonate web sites such as google.com, microsoft.com, twitter.com, facebook.com, etc. Following that incident, DigiNotar went bankrupt and was closed.
"**Beast**" vulnerability against SSL (September 2011)	Two security researchers (Juliano Rizzo and Thai Duong) were able to exploit a flaw in the SSL/TLS 1.0 protocol. They presented their work (including a demonstration tool dubbed as BEAST: Browser Exploit Against SSL/TLS) during the Ekoparty conference in Buenos Aires, on September 23rd, 2011.
DuQu malware (October 2011)	The DuQu malware (its name comes from the « ~DQ » files it creates on infected computers) was first announced as being the son of Stuxnet because their codes have high similarities and DuQu impacted some industrial firms. But both assertions were later proved to be wrong. DuQu should have been used selectively (with no automatic spreading) to infect a small number of companies (chosen by the attackers). It should be ranked as an APT attack.
JBOSS worm (October 2011)	JBOSS is a J2EE compliant web server. The JBOSS worm uses a known vulnerability that has been fixed more than a year ago, and spread on vulnerable JBOSS servers. Infection cases have been seen in France as well.

3) The major facts for 2011

3.1 Infiltration attacks (APT): The major threat for 2011

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.

We already talked about these attacks in our annual review for 2010, but year 2011 reinforces our conclusions for 2010: infiltration attacks have become a major threat for businesses.

- Many such attacks were made public in 2011.
- They often target the most strategic elements for the company: data theft (industrial espionage) or cyber-sabotage.

The attack suffered by RSA in March 2011 is a typical example of such an infiltration attack. We detail it below.

3.1.1 A typical APT attack example: the cyber-attacks against RSA and Lockeed Martin

In March 2011, RSA (an IT company best known for its cryptographic products and its "SecurID" authentication calculator) was attacked by hackers. The attack scenario, as described by RSA (in the Annex to the Anatomy of an Attack document) is the following:

- A booby trapped e-mail was sent by hackers to some RSA employees. The e-mail comes with an Excel attached file with an embedded malicious Flash content which uses the 0-day vulnerability CVE-2011-0609 to infect the computer of the e-mail reader (this 0-day vulnerability was later fixed by Adobe and is described in the **CERT-IST/AV-2011.151** advisory).
- A variant of the "Poison Ivy" remote administration tool is then automatically installed on the compromised computer. It is later used by hackers to remotely execute commands on this computer.
- The attackers used that first compromission stage to illegally reach various IT systems from RSA. This resulted in confidential data collected and sent to FTP servers outside RSA.

The data stolen from RSA are related to the RSA "SecurID" authentication tokens. Although RSA never confirmed this information, the data stolen could be the list of "(serial number, secret key)" records for all (or a subset of) the SecurID tokens that RSA sold to its customers. These data are very sensitive because they allow the attacker to produce exact copies of the existing SecurID tokens. The attacker could then use these clones to illegally gain access to the IT infrastructure of RSA clients. However, this requires additional information (such as the login-name of the user on the IT infrastructure and the user's PIN for the SecurID token, etc ...) that makes this attack a non-trivial one.

Two months later (in late May 2011) the Lockeed Martin company (one of the major US Defense contrators) announced that they repelled attack attempts, and that the data stolen from RSA were used in these attack attempts. This information was later confirmed by RSA (see this RSA announcement) and RSA then offered to replace all the SecurID tokens that was tampered during the March attack.

These attacks against RSA and SecurID show that:

- A leading company in the field of security may suffer a severe attack, which penetrates deeply their networks and leads to highly confidential data theft.

- The attackers do not act randomly. They develop detailed plans with long-term goals. The data stolen from RSA have enabled the attacker to set up the attacks that were later attempted against the Lockheed Martin company.

In October 2011, at the RSA annual conference, one of the leaders of this company has indicated during his speech that the attack suffered by his company has certainly been orchestrated by a state (without specifying whether or not that state was China, which is the country most often cited for such attacks).

3.1.2 The other infiltration attacks discovered in 2011

The attack that targeted RSA is not the only occurrence in 2011 of attacks by infiltration. Here is a non-exhaustive list of such attacks publicly announced in 2011.

« Night Dragon » attack (February)	McAfee published a report in February 2011 for attacks by infiltration dating to the end of 2009. These attacks were directed against energy, oil and petrochemical companies.
NASDAQ	In February 2011, the FBI announced that the U.S. exchange NASDAQ was the victim of a computer intrusion. The intrusion targeted a web portal named "Directors Desk". Suspicious files were indeed found on the NASDAQ OMX Group servers that host this portal (see this article about that event).
The French Ministry of Economy and Finance - Bercy (March)	The French Ministry of Economy and Finance announced that it suffered an attack aimed at stealing documents relating to the G20 (see this article in French published by « Le Monde »).
The European Commision	The European Commission announced it suffered a serious attack. The nature of the attack is not detailed (see this article published by ComputerWorld).
The Parliament of Australia (March)	The computers of the Australian Prime Minister and several members of the government have been victims of cyber-attacks. These attacks, which would have started in February 2011, would have impacted 10 Australian ministries and gave the attackers access to thousands of e-mails (see this article).
Areva (September)	The French nuclear group Areva has been the target of cyber-attacks, which led it to take security measures in an emergency. These attacks, according to company officials, would impact non-critical information, but would have lasted for several years.
Mitsubishi Heavy Industries (September)	This Japanese Defense company announced that it had been the subject of cyber-attacks (see this Reuters article). Data about military equipments and nuclear power plants would have been stolen (see this Reuters article).
« Lurid » Attacks (September)	Series of targeted attacks that use a malware named "Lurid". They affected 1465 computers of diplomats, government ministries, research agencies and companies in the block of the former Soviet Union. Discovered by TrendMicro, this attack would be a combination of several attacks that exploit vulnerabilities in popular software (Adobe, Microsoft).
« Nitro » Attacks (October)	Cyber-attack, unveiled by Symantec that affected big names in the chemical industry and defense. It took place from late July to September 2011 and used a simple but effective technique: sending of infected e-mails to install the malicious Trojan horse named "Poison Ivy" on the victims' computers.
Attacks of Norwegian companies in the field energy and defense (November)	The Norwegian government announced in November 2011 that at least a dozen of Norwegian companies have been victims of cyber-espionage during the year (see this WashingthonPost article).

3.2 Networks not secure enough

Some of the attacks seen in 2011, such as those suffered by RSA or DigiNotar, raise serious questions about the effectiveness of security within these organizations:

- For RSA, how the compromise of two workstations may allow an attacker to gain access to critical internal servers and to steal sensitive data on these servers (authentication data of the SecurID tokens sold to RSA customers)?
- In the case of DigiNotar, how an external attacker could have penetrated inside the IT system and generated more than 500 false digital certificates? A certificate authority (such as DigiNotar) is supposed to be an organization with a high level of security. This attack shows that it is far from being the case with DigiNotar.

Similarly, it is disturbing to see the number of "trusted" web sites that have been compromised in 2011:

- SourceForge.net (January 2011)
- Wordpress.com (April 2011)
- Kernel.org (August 2011)
- MySQL.com (September 2011)

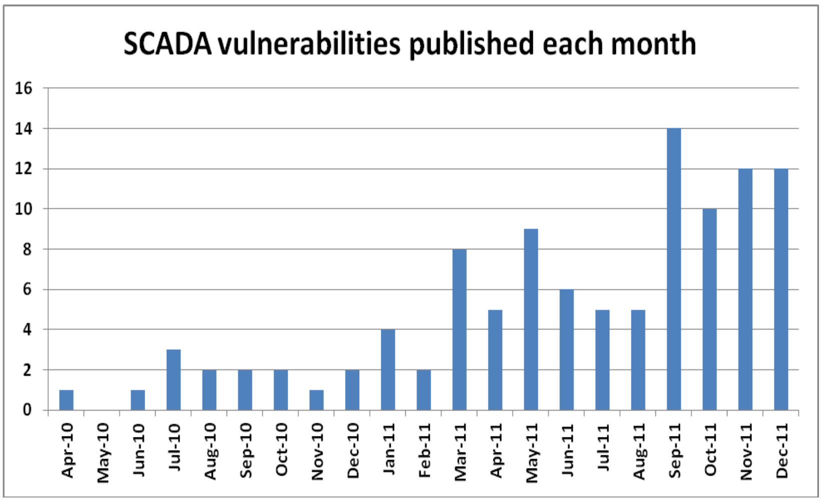
Several factors may explain this observation:

- The human factor. Quite often these compromises are the consequences of human weaknesses. A typical example of such weakness is the case where a user has the same password for multiple different accounts (e.g. FaceBook account vs. server account).
- Weak security architectures in place. In some cases, security architectures within firms appear to be insufficient. Economic constraints and the search for maximum efficiency often lead to "low cost" security which is incompatible with the increasing exposure to the threats of the today IT systems.
- Daring attackers. The recent attacks show that the attackers did not hesitate to attack companies and sometimes to deeply penetrate their IT systems. The cyber-attack is now just another tool, in the toolbox available for activist groups (aspect developed in Chapter 3.4) or espionage groups (by competitors or states) that want to target a particular company.

3.3 SCADA: the coming threat?

In 2010, the Stuxnet worm, which was designed to attack specific SCADA systems, has shown the kind of danger the SCADA systems could have to face with. Stuxnet was a live example of a theoretical threat that companies knew for years, but had never imagine to see right now. It was for no doubt a booster for the work already underway on securing the industrial infrastructure.

The year 2011 shows that vulnerability researchers (who sometime discovered the SCADA systems with Stuxnet) are now very interested by SCADA systems. The graph below shows the evolution of the number of SCADA vulnerabilities published each month (data taken from the Cert-IST monthly "SCADA security" bulletin); in 2011, more than 70 vulnerabilities were announced: this is 5 times more than the previous year.



Most of the vulnerabilities discovered in 2011 were "easy" to discover. This is because a lot of industrial systems today in operation were not designed with computer security in mind (i.e. to resist to deliberate attacks against computer systems) and therefore include many classic security weaknesses (hard-coded passwords, non-defensive programming, memory overflow bugs, etc ...). With the range of vulnerability testing tools available from the IT world, it is quite easy for a researcher to discover these classical flaws in SCADA equipments. It is worth noting however that, fortunately, most of these vulnerabilities can be exploited only by an attacker that is already inside the industrial plant.

In 2011, some researchers published « SCADA vulnerability packs »:

- In March 2011, an Italian researcher named Luigi Auriemma published a pack of 34 vulnerabilities that impact 4 SCADA products (counted as 4 vulnerabilities in the histogram above). He added 15 new vulnerabilities to this pack in September (that impact 10 products), 5 in October, etc... This demonstrates the interest of that researcher for SCADA products (19 SCADA products tested) and the large number of vulnerabilities found (54 vulnerabilities in 2011).
- In May 2011, the Gleg company released a pack (named « Agora SCADA+ exploit pack ») that include 18 SCADA vulnerabilities previously published by various sources and 5 new vulnerabilities (see the details published by ICS-CERT). This pack is updated regularly and claims to include all the vulnerabilities known for SCADA equipments (including the vulnerabilities published by Luigi Auriemma).

As we can see, the SCADA vulnerability researcher community is currently very active. SCADA security experts, however, indicate that the vast majority of the published vulnerabilities currently just search for IT vulnerabilities (and typically Windows vulnerabilities) in SCADA systems. And the vulnerabilities specific to SCADA technologies (e.g. related to PLC) are still largely unexplored yet.

3.4 Cyber-activists: should we care about?

2011 is the year when hacktivists (word constructed by contraction of "hacker" and "activist", designating the people who use hacker tools to support protestation movements) have gained in importance and caught media attention.

The « **Anonymous** » is one of the most known examples of hacktivist groups. It started to be known by the general audience in 2010, when it took the defense of Wikileaks and invited all the sympathizers to participate in a denial of service attack to block Paypal, Visa and MasterCard web sites. Its success in blocking MasterCard and Visa demonstrated the power that could have such a collaborative movement.

Today, protest actions similar to those launched by the Anonymous group, represent a new threat for companies: a few thousand sympathizers, who are willing to install on their PC an attack tool distributed by the hacktivist group, are indeed able to block the website of most companies. In 2011, the cyber-attack has become another tool for protesters, to be added to the conventional actions such as petitions or seatings.

To adapt to this situation, companies must prepare and take these hacktivist attacks as a new risk to consider. In particular, they must define technical measures to deploy, prepare crisis committees and identify the type of communication they would adopt in case of attack. Up to now hackitivist attacks were not highly technical attacks in comparison with the targeted attacks companies must face with when dealing with professional attackers.

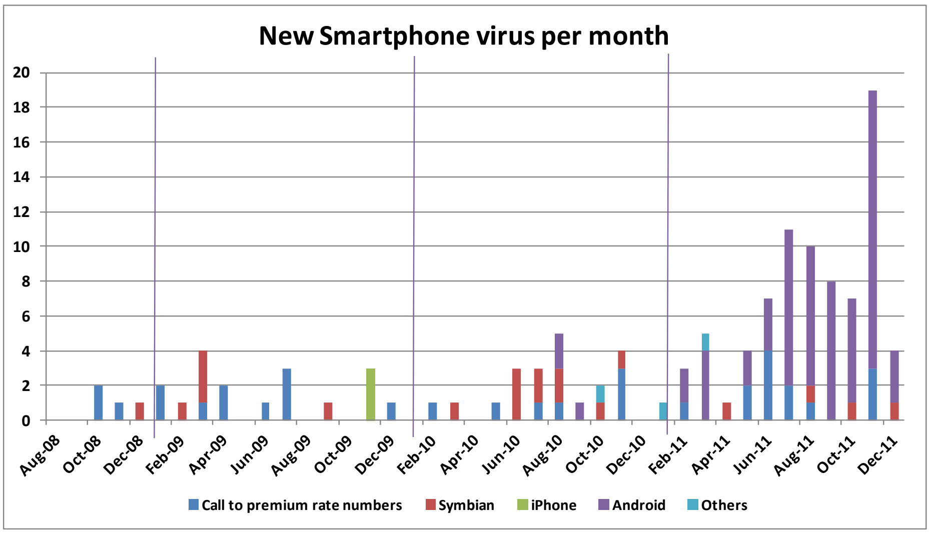
It is difficult to evaluate how much attention should be given to these movements. With motives ranging from fun, fame seeking, destabilization or modern form of protest, it is difficult to separate things. Hacktivist groups that took the most of the media attention during 2011 were Lulzsec and Anonymous:

- The "Lulzsec" group ("Lulzsec" comes from "Lol Sec" which can be translated as "security laughs") seems to be seeking for fame and its attacks were directed first to high profile web sites which were poorly protected.
- The "Anonymous" group is more difficult to understand because it is a multi-folded movement (a lot of distinct groups identified themselves as being part of Anonymous). There is no real cohesion of the group around a common claim and the group seems sometime rather looking for the causes it could defend.

These groups (we consider here only the groups that claim to have skills for computer attacks) are part of a wider social protest movement: « Los Indignados » movement in Spain, Occupy Wall Street in USA, etc...

3.5 Smartphone

During 2011, we observed a significant increase in the number of malicious applications designed for smartphones, especially for Android (see the histogram below). The main reason for this increase is the fact that Android is an easy target for malware designers. For example, it is apparently quite easy to construct a malicious Android application by cloning a legitimate application and to add it a malicious hidden function.



The soaring number of smartphone malware raises the question of the need to install protective software such as antivirus on these devices. But the experts seem rather sceptical about the quality of antivirus currently available for these platforms. A recent test on that topic concludes that existing free antivirus software for Android fail to detect most of the current malware (see this article).

Most of the time, malicious applications are available only on alternate places (not on the official Android Market place) and there is a low risk that a regular user would download them (because only skilled users use alternate market places). But malicious applications could also be published on the official Market Place (see this example about the DroidDream malware). Such malware will be erased as soon as discovered (typically following users' complaints) and automatically removed from all the devices that installed it. Of course it is a reactive approach with severe limitation (see for example this article that shows how a malicious application can reappear quickly after being deleted by Google).
Note: This principle of a controlled repository (the "Market") where approved applications are made available is called a « walled garden » approach. It introduces a new security model where the official applications are available in a place controlled by the phone designer: Android Market, iPhone Apps Store, Blackberry App World, Phone7 MarketPlace.

Beyond the multiplication of these malicious applications, the most usual effect of a malicious smartphone application is still to generate calls to premium rate numbers. The same result could of course also be obtained by sending to the victim a simple SMS enticing the recipient to call the premium rate number (without any malicious application) …

The most sophisticated malware seen in the smartphone world in 2011 are probably the ZitMO (Zeus in the MObile) and SpitMO (Spyeye in the MObile) series. First discovered in September 2010, these malware can be installed on any type of smartphones (versions exist for Windows Mobile, Symbian, Blackberry and Android) and have the main purpose of intercepting SMS messages sent by banks to customers who request funds transfer (see for example this Kaspersky article and that one from McAfee). This feature allows the malware to defeat the 2-factor authentication SMS scheme that some bank implement to protect customer against fraudulent funds transfer request (when funds transfer is initiated by a customer, the bank sends a secret code on the mobile phone of the account owner and this secret code is required to complete the transfer request).

4) Conclusions

➢ Infiltration attack is now a major threat

The year 2011 marks a significant milestone in the evolution of the threats that enterprises must take into account.

If we look retrospectively at the categories of attacks that we have seen since the 2000s, we could identify three successive steps:

- The massive virus attacks that saturate the infrastructure (such as the worms seen in the early 2000).
- The attacks against infrastructure equipments (e.g. DOS attack) or institutional web sites (defacement of web servers).
- The attacks against user workstations, with the primary goal of creating large botnets.

These three threats were aimed first at attacking computer equipments (to disable, to take control, or to steal the contents). In contrast, in 2011 a large number of attacks by infiltration were found. For these attacks, which are often called "APT" (Advanced Persistent Threat), taking control of a computer equipment is no longer a goal; it is just a step to further penetrate the enterprise up to the point the attacker reaches his goal (e.g. disclose confidential documents, perform cyber-espionage activities or perform sabotage).

Unlike previously known threats, attacks by infiltration are not aimed at attacking the IT system of the enterprise (this is not the goal of the attack), they are aimed at attacking the enterprise assets (to steal its secrets or to alter its most vital components).

The attacks seen in 2011 against the French Ministry of Economy and Finance (Bercy), RSA or Areva are examples of such targeted infiltration attacks.

Of course, the risk of an intrusion in the IT system is known forever, and targeted attacks related to industrial espionage have been seen before 2011. For example, in 2004, they were the « Titan Rain » attack (supposed Chinese) against U.S. military sites, or the Michael Haephrati case which highlighted the use of Trojans for industrial espionage. **But the number of targeted attacks that occurred in 2011 shows that this threat has changed in scale: it has grown from a marginal phenomenon (a theoretical risk) to a major phenomenon that must necessarily be taken into account.**

As stated by M. Pailloux (Director of ANSSI, the French National Agency for IT Security) during his speech at our Forum 2011 conference day, the question is no longer whether or not an organisation will be affected by a cyber-espionage attack (like those that occurred at Bercy in early 2011); it is to know when the attack will happen (because it will happen) and how long the organisation will take to detect and counter it.

China and Russia are often pointed as the originators for this type of attack (see this report published by the U.S. government), but it would be unrealistic to think that they are the only countries acting in this field. Cyber-attacks are now an integral part of the espionage arsenal, targeting governments as well as private enterprises.

➢ It is the beginning of a new security hardening cycle

Since the disappearance of massive virus attacks (such as CodeRed and Nimda in 2001, Slammer in 2003 or Sasser in 2004), enterprises have not suffered large attacks that significantly disrupted their IT systems. As we said in our 2006 annual review, the CSO life should then seemed quieter. But we showed also in 2006 that it was not true and that in fact the threat became less visible, but more pernicious. Conficker (late 2008) also showed that the risk of a massive attack could never be definitely ruled out.

In fact, after 2004, people who were not directly involved in IT security could have thought that the cyber threat was decreasing and that it was time to gradually relax the security constraints.

But in the same time the real cyber threat has continued to evolve:

- Emergence of the "fuzzer" technology to automate vulnerability search,
- Leading to the 0-days attacks phenomena, and to an underground vulnerability market place,
- Resulting in the apparition of cyber-criminals (driven by money expectations) attacking mainly unprotected home users (via phishing, bank account data theft and bank fraud).

Overall, from 2004 to 2010 attack techniques have improved considerably, and these techniques are now turning to the company by taking many forms in particular:

- Attacks by infiltration,
- SCADA attacks.

Along with this evolving threat, economic constraints, or the search for maximum efficiency often lead to "low cost" security which is incompatible with this new threat.

Enterprises are facing a new risk (or a risk that should be increased) and must adapt their defenses to this new context. It is very likely that this marks the beginning of a new cycle of security hardening.

➢ Enterprises must respond to this threat by strengthening defenses

To address this growing threat the company must act on three axes:

- **Strengthening defenses**. Keeping IT equipments up to date (and especially the user workstations which are often the first attacker targets in case of an infiltration attack) is a key component of the defense, because the new vulnerabilities discovered every day create new weaknesses that, when accumulated, decrease significantly the level of resistance in case of attack. Today, most attacks exploit old vulnerabilities, for which patches are already available from vendors. The objective here is not to apply 100% of the security patches across the whole infrastructure in a fixed delay. It is rather to establish a process to reach the appropriate "patch level" assigned to each IT component (front-end servers in DMZ, internal servers, workstations, etc ...) according to its security requirements. Vulnerability watch and assessment, as well as the ability to deploy security patches appropriately, are key components for keeping security under control.

- **Develop intrusion detection and analysis capabilities**. This is not limited to the deployment of IDS and IPS. Of course these tools are useful (they are the stand guards that give a good indication of the threat level and stop direct attack attempts), but they are not able to stop elaborated attacks. A complementary approach is to seek for successful attacks, with the objective to identify them as soon as possible and prevent them to stay hidden and undetected within the company for a long time. This requires first to be able to detect security abnormalities (by performing log analysis and teaching users to detect and report security incident) and then to establish a security incident analysis team who investigates the suspicious events.

- **Re-evaluate the defenses in place to limit insider threats**. In addition to the paragraph above, it is recommended to improve the defense in place (which are often designed to counter external attacks) against internal attacks. A good scenario to look at here is to evaluate how these defenses will stop an external attacker who successfully obtained an access on the internal network. This analysis should help to identify internal weaknesses and adopt security measures to reduce them.

➢ The year 2011 also shows that cyber-activism must be taken into account

Hacktivism (a portmanteau of hack and activism) is a threat that has grown in importance during 2011. The successful attacks performed by groups such as "Anonymous" (against PayPal, Sony or Monsanto) or "Lulzsec" (against the CIA or American television PBS) showed that companies could indeed be affected by these protesters. So far, these attacks took two different forms: the disclosure of information stolen on servers (internal documents, lists of employees, etc ...) and denial of service affecting websites.

These cyber-protests are a modernized form of the classical protest actions like call to boycott, seating, media attention catching, etc ... From a technical point of view, such attacks are generally not very sophisticated: they take advantage of standard security flaws (for example "SQL injection" vulnerabilities) that could easily be detected by a penetration test, or use DOS techniques at a scale much smaller than the one a professional attacker could deploy. And **the first reason why these attacks were successful is because the attacked sites were not adequately prepared.**

Companies must consider hacktivism as a new risk to cope with, and prepare adequate answers to counter it. They must in particular define the technical measures to deploy, prepare the set up of a crisis structure and define the communication they would make in case of attacks.

➢ SCADA security and Smartphone security

These two topics are threats that occupied a significant part of the 2011 news, but have still a large potential of growth in the future.

For enterprises, the smartphone threat is still limited. For sure, the number of smartphone malware increased significantly in 2011 (especially on Android phones), and the possibility of sophisticated attacks using this new vector has been confirmed (see for example the ZitMO and SpitMO banking malware). But the vast majority of attacks seen today are classic scams that involve convincing users to install a malicious application on their devices and generating calls to premium rate numbers. And the efficiency of protection tools (such as antivirus) for smartphones is currently a subject of debate among experts.

On the other hand, as we explained in our 2010 annual review, **the increasing usage of smartphones clearly induces new risks for enterprises. It appears now essential that companies review these new risks and add security rules** (for example, remote data erasure procedures) **to their mobile device management procedures,** to protect the company against possible data leakages.

On the topic of Industrial Control Systems (aka SCADA), 2011 has seen an explosion in the number of vulnerabilities discovered by security researchers. This illustrates the fact that most of these systems have not be designed to defend against cyber attacks. Fortunately, these systems are often protected in dedicated networks. But the raising of infiltration attacks demonstrated that a motivated attacker may be able to penetrate deep into the enterprise networks to reach their targets. **Cyber attack against SCADA systems is a major threat and the work already underway to secure these industrial systems must be pursued relentlessly**.

End of the document