Cert-IST annual review for 2014 regarding flaws and attacks

1) Introduction

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

We present first the most significant events of 2014 (see Chapter 2) and highlight phenomena such as the necessity to re-assess the security risks posed by more frequent and more sophisticated cyber attacks, or the increase of cryptographic attacks.

We then cover the vulnerabilities and attacks seen in 2014 (see Chapter 3) based on the daily threat and vulnerability analysis performed by Cert-IST. This includes a summary of the Cert-IST production for 2014 (with figures on the number of advisories or alerts published), and a review of the main threats that led to Cert-IST Alerts (or Potential Dangers).

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

Note: The blue insets enclosed all over the document are articles or announcements taken from the Cert-IST monthly bulletins published during 2014.

➢ Regarding the Cert-IST

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

2) Most significant events of 2014

2014 was rich in events. First of all, companies had to face to attacks induced by the discovery of new flaws. And these attacks generated crisis situations which were more or less severe:

- Shellshock and HeartBleed attacks against servers.
- attacks targeting workstations through new vulnerabilities in Internet Explorer, Flash, etc…
- or even infection campaign by e-mail with malware such as CryptoLocker.

But beyond these daily threats (that we develop in Chapter 3), more global trends emerge. We go through them below.

2.1 More sophisticated attacks that modify the risk level

There were in 2014 many reports describing "sophisticated" attacks. For instance:

- The « Havex » attack (as part of cyber-spying operations named « Energetic Bear » or « Dragonfly ») tried to compromise industrial systems by infecting legitimate SCADA software on the official web sites that distribute these software.
- The « Zombie Zero » attack succeeded in compromising a logistic and transport company, by delivering specifically infected barcode scanners to this company.
- The « Target » US retail chain was affected (by end of 2013) by a major intrusion in its information system that resulted in the installation of spyware on the payment terminals of the chain stores, and in the stealing of millions of payment card data.
- The Sony Pictures Entertainment company went through (end of 2014) a major intrusion that resulted in the disclosure of internal data, the delay of the release of « The Interview » movie, and a diplomatic escalade between the USA and North Korea.
- …

For a specialist, none of these attacks was really sophisticated. The techniques used are fairly simple and the exploited flaws known for a long time (sometime there is even no flaw at all, but only well known weaknesses like poorly separated infrastructures, or users trapped by social engineering techniques, etc…). Up to now, these attacks were very occasional, and no reports were released about them. But the multiplication of the incident cases published, shows that this time has changed: by now, this kind of attack is much more common. And it is even very likely that this situation will provide inspiration to others.

- Before 2010, only some governments (and some specialized private companies?) probably conducted this kind of computer attacks.
- In 2010, the APT phenomenon became public (with Google revelations about the "Aurora" attack) and every government had to ask itself to acquire this capacity.
- Today, the Target case (and probably also Sony case) shows that cybercriminals as well adopted cyber-spying techniques to take control of the information systems of their victims.

Major cyber-incident at Target stores
(Extract from Cert-IST bulletin - January 2014)

Mid-December 2013, it was discovered that the retail company Target was victim of a major incident that would have allowed attackers to steal data from 40 million credit cards. Many articles have been published since then on this incident, as the investigation advanced. To sum it up, the attackers would have illegally gained access to Target internal IT system, thanks to a remote maintenance access for the air conditioning system. They then infected multiple POS (Point Of Sale) machines with a malware that grabbed credit card data. This is a sophisticated operation demonstrating that infiltration attacks are not limited to state-sponsored cyber-espionage operations. It also highlights the fact that malwares targeting POS have become quite common in 2013. This article by Brian Krebs (among others) gives more information on this incident.

Target shows the limits of traditional security
(Headlines of Cert-IST bulletin - March 2014)

The cyber-attack that affected the retail company "Target" in late 2013 (see the "Attacks of the month" section in our January 2014 Bulletin) will probably be a typical "case study" for anyone who looks on how to improve security. It shows, but this was (almost) obvious, that:

- A security certification (PCI-DSS in this case) is not enough to prevent a major incident. Two banks have filed a complaint in March against the company that did the PCI-DSS certification of Target, but finally canceled this action.
- Technical tools (Symantec and FireEye in this case) are not enough if they are not properly configured and operated (or if they are not usable). At their hearing at the U.S. Senate in March, Target said on this topic that the alerts generated during the intrusion were lost in the flood of hundreds of alerts generated every day.

The report prepared for the Senate gives an interesting analysis of cyber attacks suffered by Target, and points out the shortcomings of the security systems in place. Above all, this major incident shows that security supervision is now a key component to master IT security.

Due to this evolution, it is necessary to reconsider the "cyber-intrusion" risk: it must be assumed that by now all the attacks known as “theoretically possible” are no longer “just theoretical”. Here are some examples of theoretical risks that cannot be ignored anymore:

- Eavedropping on a network link that goes outside of the company perimeter without being encrypted,
- MiTM attack (Man In the Middle) on a network flow,
- Lateral movement of the intruder, inside the company network, after an initial workstation was compromised, because internal network was not segmented and no strict limitation of privileged accounts was applied,
- Mobile user attacked via fake Wi-Fi access points,
- Attack using vulnerabilities already identified during intrusion tests, but that were not fixed.
- …

Provokingly, we may say that if 100% of the intrusive audits (penetration tests) a company performed led to an intrusion, there is thus 100% of "chance" that a real attacker may perform an intrusion if he cares about systems that have not been audited yet, or that were audited but not fixed.

In our 2011 annual review of flaws and attacks, we said that the wave of APT attacks seen that year showed a new risk (or a risk which level must be increased) and that it corresponded very likely to the beginning of a cycle of security strengthening. 2014 actuality clearly confirms this trend: **It is necessary to strengthen the company security or at least to re-asset its security level in front of the current threat.**

2.2 Many attacks targeting cryptography

The year 2014 was marked by a series of events related to cryptography:

- **Many flaws discovered in SSL and TLS protocols,**
- **Stop of the Truecrypt encryption software,**
- **Attacks aiming at breaking TOR anonymity.**

Cryptography is today an essential part for Information System security, and these events show that this central brick is actively attacked. 2014 is the first year where this trend is clearly visible.

- **Many flaws discovered in SSL and TLS**

During the year, a series of serious vulnerabilities have been discovered in SSL and TLS protocols (TLS is the successor of SSLv3; the latest version is TLSv1.2). We sum them up in the following table.

Vulnerability Date	**Editor** Comment
GotoFail March 2014	**Apple** Allows to bypass the verification of the digital certificate validity
CVE-2014-0092 (aka « Bool is not Int ») March 2014	**Unix-Linux/GnuTLS** Allows to bypass the verification of the digital certificate validity
HeartBleed April 2014	**Unix-Linux/OpenSSL** Remote reading of memory areas on a vulnerable system
Poodle October 2014	**Independent constructor** (protocol flaw) A weakness in SSLv3 allows a MiTM attacker to decrypt the flows
Schannel November 2014	**Microsoft** Remote code execution

We may see in this list that all editors are affected (Apple, Linux and Microsoft).

It is not unusual that SSL flaws are discovered (each year, the Cert-IST releases around ten security advisories on these topics), but the flaws listed above are more severe than usual. There is no real explanation to the fact that so many severe flaws had been discovered. For instance, as far as we know, there are no new techniques for searching for vulnerabilities (like « fuzzers »). We thus think that these discoveries are due to the fact that security researchers are more and more sharp and skilled in their area: when they notice an abnormal behaviour, they analyze the anomaly deeply until they find vulnerabilities which are sometimes critical. It is moreover worth noticing that researchers are also skilled for exploiting discovered vulnerabilities. For instance when HeartBleed vulnerability was first announced, it was not clear at all that the flaw could be exploited to successfully collect sensitive information: because from a flaw allowing a memory leak, to the theft of a server private key, there are many (implementation) difficulties to solve. Cloudflare launched a challenge on this topic… that was wined in less than 24 hours! (See this explanation on the Cloudflare blog).

The HeartBleed flaw
(Headlines of Cert-IST bulletin - April 2014)

The HeartBleed vulnerability in OpenSSL (see **CERT-IST/DG-2014.004**) is the most important vulnerability seen this year. This vulnerability is very serious (it allows a remote attacker to steal sensitive data on a vulnerable server, such as passwords or digital certificates), and it impacts a security component which is used on a lot of systems (at first web servers, but also any other software relying on the vulnerable OpenSSL library). It consequently triggered in all organizations, large patching campaigns to inventory and update the impacted IT servers. We describe in more details the chronology of this event (and the Cert-IST treatment for it), in the Attacks of the month section below.

HeartBleed threat against OpenSSL
(Extract from the « Attacks of the month » section - April 2014)

It is a critical vulnerability in the "heartbeat" feature of the OpenSSL library. It allows a remote attacker to read fragments of RAM of a vulnerable OpenSSL server. This can be used typically to read the memory of vulnerable HTTPS web servers. These memory fragments potentially contain sensitive data such as passwords, cookies, sensitive application data, etc. It has been demonstrated (via the challenge issued by CloudFlare) that it is possible to thereby steal the private key of a vulnerable HTTPS web server.
This vulnerability has been disclosed on April 7th, when OpenSSL release a patch to fix it. It was discovered on March 21st 2014 by researchers at Google, and kept secret since April 7th (see this article for further details about the vulnerability timeline).
Cert-IST has first released the **CERT-IST/AV-2014.0266** security advisory on April 8th 2014, and the day after, the **CERT-IST/DG-2014.004** Potential Danger notice. At that time we rated the Potential Danger as “Medium” risk because, while the vulnerability was obviously dangerous, effectiveness of real attacks using it was still subject to speculations. In parallel, we opened the [Heartbleed] threat in our Crisis Management Hub, to keep subscribers aware about the evolution of this threat. On April 15th, we re-issued the Potential Danger notice with a risk raised to “High” because more attack tools were available on the Internet (and the CloudFlare challenge had demonstrated that stealing web server private keys was actually possible), which resulted in a high risk of attacks raising on the Internet.
The HeartBleed vulnerability is very severe because it gives attacker (read) access to vulnerable web server memory. Several attack cases were reported, for example:

- The Canada Revenue Agency closed its web site on April 14th because of attack attempts which resulted in the theft of taxpayer’s personal data (see this article).
- On April 18th, the Mandiant company informed that it had detected HeartBleed attacks which resulted in VPN session tokens theft (see this DarkReading.com article). And it is quite worrying to see that these attacks have occurred on April 8th, just the day after the vulnerability was first disclosed.

- **Stop of the Truecrypt encryption software**

2014 is also the year where the team that developed the open-source "TrueCrypt" encryption software suddenly announced (end of May) it stopped the project. No clear explanation was given for this stop. We may think that it is due to secret NSA pressures on the development team; the only way out to avoid them might have been to abruptly stop the project.

- **Attacks aiming at breaking TOR anonymity**

We saw as well in 2014 several attacks targeting the TOR network:

- Attack of researchers inserting **fake TOR nodes** (See this Freedom-To-Tinker.com article)
- **Onymous operation** (by police forces) that led to the neutralization of illegal servers (See this article of the Tor project official blog or this 01Net.com article)
- Researchers study using **Netflow** to establish a traffic correlation (See or this ZDNet article - or this TheRegister.co.uk article).

It is clear that TOR houses many illegal traffics and that breaking the anonymity it gives is a major concern for legal entities of many countries. Breaking TOR anonymity also allows totalitarian countries to keep under surveillance their population. If the surveillance is operated without any control of a regulation entity, it then opens the door to abuse.

2.3 Cyber-spying: governments at the cutting edge of cyber attacks

Since 2010 and the progressive hype of infiltration attacks (attacks called « APT »: Advanced Persistent Threat), governments – or private agencies sponsored by governments – appear as the more advanced in cyber-intrusions and cyber-spying techniques.

We already often mentioned this in our annual reviews. And 2014 only reinforces this statement. To illustrate this point, we list below the cyber-spying affairs that were revealed in 2014. Most of them are related to operations launched several years ago and that were discovered only recently.

Release date	Name of the cyber-spying operation	Supposed source country
February	Uroburos Other names: Epic Turla, Snake	Russia
February	Careto/The Mask	Spain
March	Siesta	China
March	Snowglobe Other name: Babar	France
May	Clandestine Fox	China
June	Energetic Bear Other names: Crouching Yeti, Dragonfly	Russia
June	Putter Panda	China
June	Pitty Tiger	China
July	CosmicDuke	
August	Machete	
August	Poisoned Hurricane	
October	SandWorm / BlackEnergy2	
October	Axiom	
November	DarkHotel	South Korea
November	Regin	USA

In 2000, when “the web” took the lead, Internet has appeared as a land of freedom (or even a lawlessness zone!) with a strong spirit of free-sharing and democracy (sometimes called « the global village »). States then seemed absent from this land (overtaken by events?). In fact this is not the case. Countries visibly understood several years ago the strength Internet may give them in terms of monitoring and cyber-spying, and silently developed technical capabilities in this field. Today, these practices come to light, probably because they are more and more commonly used.

There is of course legitimacy for states to operate monitoring of terrorist activities, or even necessity to be able to practice spying. But these cyber techniques also tend to generalize and go beyond the domain of the State.

2.4 Flourishing frauds

In the area of cyber-criminal activities, we noticed in particular in 2014 the following events:

- Raise of « Fake transfer orders » or « President scams » frauds
- Widespread of Crypto-ransomware,
- Wave of attacks against payment terminals (Point Of Sale systems) in the USA

There is no technical innovation here. But the magnitude of the attacks seen is amazing.

Fake transfer orders and President scams: New cases of scams impacting French companies
(Extract of the « Attacks of the month » section - January 2014)

Two new cases of the "Francophoned" attack (this is the name Symantec gave to those attacks) were revealed in the French press in January:

- A company located in the Pyrénées-Atlantiques department was stolen 800,000 Euros (see this article from Undernews website – in French),
- A company located in the Manche department was stolen 200,000 Euros (see this article from Ouest-France newspaper – in French).

We already mentioned this kind of attack in the Headlines of May and September 2013 bulletins. The modus operandi for such an attack includes the following:

- Infect a computer within the company (e.g. the computer of an executive assistant) to obtain sensitive information,
- Send an email to this assistant to request a money transfer, pretending to be from the top management of the company,
- Have a phone call to this assistant to convince her to perform the money transfers.

For more information, refer to this article from Symantec.

Crypto-ransomware
(Headlines of Cert-IST bulletin - June 2014)

Virus that encrypt user data and ask for a ransom to decrypt them, have been there for a long time (see for example PgpCoder in 2005), but CryptoLocker – that spread in October 2013 – was the first ciphering virus to cause severe impact (see our **CERT-IST/DG-2013.012** Potential Danger notice). Since that date, several other ciphering virus have been seen: CryptorBit (December 2013), CryptoDefense (Frebruary 2014, aka CryptoWall, that was very active in June with a spam campaign with mail titled « Incoming fax report »), or even Simplocker against Android (June 2014). Unlike conventional ransomware (which can be cleaned by re-installing the infected device), these "crypto-ransomware" affect user data, and if there is no backup, then the alternative is to pay or to forget about the files. As this type of scam seems pretty lucrative, there is no reason for it to stop. It is therefore recommended to remind users to make backups of their important files.

Wave of attacks against payment terminals in the USA
(Extract of the « Attacks of the month » section - August 2014)

During August, there was extensive media coverage about **incidents affecting payment card data in US**. All along the summer, several retail companies (and restaurant chains) have informed customers that they have detected attacks against their point-of-sale (POS) systems : UPS Stores, SuperValu, Home Depot, Goodwill Stores, Jimmy John sandwich restaurants. This kind of incident already made the news frontlines in early 2014, with the attack against Target stores (see the Attack section of our Bulletin for January, and the headline of our Bulletin for March), and later against PF Chang restaurants (see the Attack section of our Bulletin for June).
These attacks use specific malware (named Ram scrappers) that catch the payment card data just at the time they are in RAM on the POS (which runs Windows). The number of "Ram Scrapper" incidents has soared in 2013, first without any public announcement about them, but later new attacks were publically disclosed (the Target attack, in late 2013, was the first that was disclosed). US-CERT has released several documents in July and August about the "Ram Scrapper" named "Backoff" (including a Backoff description and an alert about on-going attacks). The PCI council also released recommendations on this topic.
Note : Other "Ram Scrapper" malware exist, such as JackPOS, Decebel, Soraya or BrutPOS: this Net-Security.org article, and the Trend Micro study it refers to, give further details about them.
A solution to these attacks should be to replace the regular payment cards used in US (with magnetic stripes) by smartcards (based on EMV system and used in Europe). EMV does not totally prevent "RAM Scraper" attacks (see this IEEE-USA article), because "RAM scraper" only steal general information (such as owner, card number and CVV) but not the PIN. But it makes those attacks, and the forging of fake cards, much more complex.

3) Vulnerabilities and attacks seen in 2014

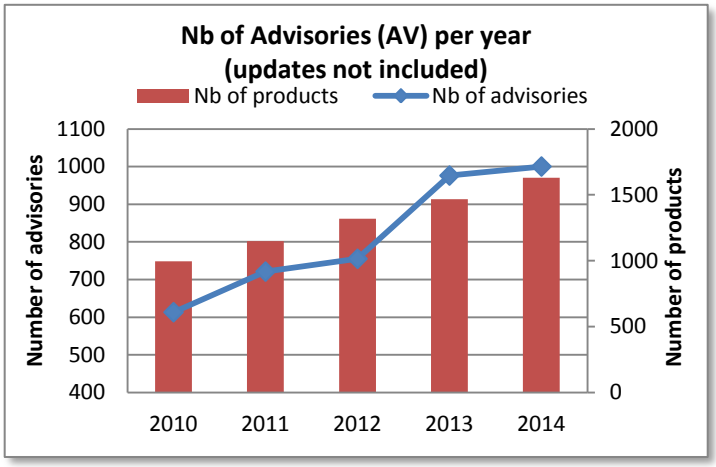
3.1 Figures about Cert-IST 2014 production

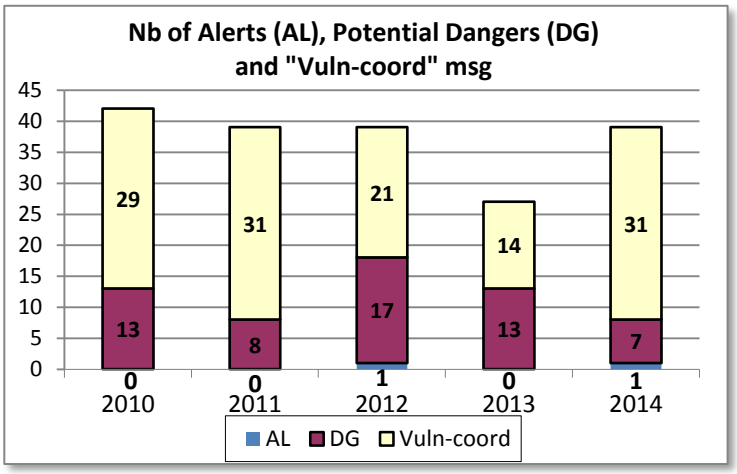
3.1.1 Daily monitoring on vulnerabilities and threats

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

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

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





Therefore, during 2014, the Cert-IST published:

- **1000 security advisories** continuously followed during the year with 2931 minor updates and 68 major updates. The number of advisories has been in constant increase for several years (see the curve above), and this trend greatly increased in 2013 (+29% compared to 2012). This continuous raise shows that the discovery of vulnerabilities is a trend that does not dry up: invariably, from year to year, vulnerabilities are discovered in products that constitute the Information System of a company. Therefore, holding the security level then requires a regular application of the security patches on these products. On the 31st of December 2014, Cert-IST follows vulnerabilities concerning 1 655 products and 13 010 product versions.

- **1 Alert, 7 Potential Dangers and 31 "Vuln-coord" messages.** We give an overview of these 2014 publications in the 3.2 chapter below.

3.1.2 Monitoring watch

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

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

3.2 Alerts and Potential Dangers released by the Cert-IST

The table below lists the most important threats for the year 2014 (by decreasing order), and the associated Cert-IST publications.

We find at the top the massive attacks that targeted web servers: **Shellshock and HeartBleed**. Then, we gathered in a single category (line 3) all the attacks aiming at infecting **the user workstation** via documents (received by e-mail) or infected web sites. We may also note in the rest of this « top 10 »:

- In line 5 the **Kerberos and Active Directory vulnerabilities** affecting Windows: we analyze this trend in the 3.3 section.
- The large amount of **cryptographic flaws** in the news: HeartBleed (line 2), Windows/SChannel (line 6), Poodle (line 8) and TrueCrypt (line 10). We already have analyzed this trend in the 2.2 section.

1	**ShellShock**	
		CERT-IST/AL-2014.001 **Alert:** Expected attacks against Unix/Linux web servers through the "Bash/Shellshock" vulnerability **- September 25, 2014**
		VulnCoord-2014.020 **Message:** Bash vulnerability in Unix/Linux **- September 25, 2014**
2	**HeartBleed**	
		CERT-IST/DG-2014.004 **Danger**: Expected exploitation of the “Heartbeat/Heartbleed” vulnerability in OpenSSL **- April 9, 2014**
3	**Targeted attacks via crafted documents or web sites**	
	Internet Explorer	
		CERT-IST/DG-2014.001 **Danger**: Expected attacks for a 0-day vulnerability (CVE-2014-0322) in Internet Explorer 9 and 10 **- February 14, 2014**
		VulnCoord-2014.008 **Message:** New vulnerability in Internet Explorer 8 (CVE-2014-1770 / ZDI-14-140) **- May 22, 2014**
		VulnCoord-2014.006 **Message:** Internet Explorer CVE-2014-1776 vulnerability exploited in the wild **- April 28, 2014**
	Flash	
		CERT-IST/DG-2014.002 **Danger**: Expected attacks for the CVE-2014-0502 vulnerability in Adobe Flash **- February 21, 2014**
	Word	
		CERT-IST/DG-2014.003 **Danger**: Expected attacks for a 0-day vulnerability (CVE-2014-1761) in Microsoft Word **- March 25, 2014**
	0-days: PowerPoint, IE and Windows(TTF)	
		VulnCoord-2014.024 **Message:** About Microsoft 0-days and the SSLv3 Poodle vulnerability **- October 16, 2014**
	PowerPoint	
		VulnCoord-2014.026 **Message:** New vulnerability in the handling of OLE objects on Microsoft Windows (3010060) **- October 23, 2014**
4	**Web: Drupal CMS**	
		CERT-IST/DG-2014.005 **Danger**: Expected automated attacks against Drupal 7 servers (CVE-2014-3704) **- October 30, 2014**
5	**Windows: Kerberos authentication and Active Directory**	
	PyKEK	
		CERT-IST/DG-2014.007 **Danger**: Expected attacks for the Kerberos (CVE-2014-6324) vulnerability in Microsoft Windows (MS14-068) **- December 19, 2014**
	Pass-the-Ticket	
		VulnCoord-2014.015 **Message:** Vulnerability in Microsoft’s Active Directory authentication mechanism **- July 16, 2014**

6	**Windows: Schannel**	
		CERT-IST/DG-2014.006 Danger: Expected attacks for the "Schannel" vulnerability in Microsoft Windows (MS14-066) **- November 18, 2014** *Note:This threat is further described at the end of section 3.3*
7	**Crypto-Ransomware**	
		VulnCoord-2014.029 Message: Cryptolocker malware campaign **- December 4, 2014**
8	**Poodle (faille SSLv3)**	
		VulnCoord-2014.024 Message: About Microsoft 0-days and the SSLv3 Poodle vulnerability **- October 10, 2014**
9	**Windows (privilege escalation)**	
		VulnCoord-2014.025 Message: Exploit for MS14-062 available on XP **- October 17, 2014**
10	**Miscellaneous**	
	TrueCrypt stop	
		VulnCoord-2014.010 Message: TrueCrypt software stopped **- June 12, 2014**
	Computrace hidden software	
		VulnCoord-2014.009 Message: Hidden "Computrace/Lojack" feature embedded in various BIOS **- May 22, 2014** *Note:This threat is further described at the end of section 3.3*

3.3 Zoom on some flaws and attacks

- **Kerberos and ActiveDirectory**

Since 2012, we have seen more papers published regarding Microsoft about:

- Active Directory compromising,
- Vulnerabilities in Kerberos authentication features.

These two components (Active Directory and Kerberos) are closely linked and are central elements of Windows authentication:

- Kerberos is the native authentication mechanism in Active Directory environments.
- Active Directory stores all the encryption keys used to implement Kerberos authentication (and in particular the machines and KDC secret keys).

Publishing papers about the analysis of an AD that was compromised is quite logical because, after the wave of infiltration attacks that occurred in 2010 (see the APT phenomenon already mentioned in chapters 2.1 and 2.3), Active Directory analysis has became a recurrent topic in forensics investigations.

Here are the main elements to sum-up this topic:

- The Windows security model has clearly its limits: when a domain account is compromised, it is then difficult to prevent all the Windows domain resources from being progressively compromised (see for instance this presentation of the JSSI-2014 conference: Est-il possible de sécuriser un domaine Windows ? - in French). This observation leads companies to set up Windows accounts partitioning solutions, in particular for privileged accounts.
- The Active Directory is a complex component and permission handling may easily shift towards a situation difficult to control. The audit of this aspect is a complex task but it enables to identify and limit the drifts.
- If an AD has been compromised during an attack, it is impossible to correctly clean it (changing the KDC secret key is today impossible). A new AD must be rebuilt.
- Kerberos is vulnerable and flaws are progressively discovered in this component.

On the topic of Kerberos vulnerabilities, we may note in particular thiese items published in 2014:

- The presentation on this topic during the SSTIC-2014 conference: Secrets d'authentification épisode II : Kerberos contre-attaque - in French (June 2014),
- The Pass the ticket attack released in July 2014,
- The PyKEK (MS14-068) attack released in December 2014.

- **New threats: Air-gap attacks**

- Is it possible to secretly talk to a machine if this machine is not linked to any network (we then say that the machine is isolated by an « air gap »)?
- Yes: with ultrasounds.

End 2013, a researcher named Dragos Ruiu announced having discovered a malware called BadBIOS able to talk through ultrasounds to another computer (see this ErrataSec article, October 2013). This allegation left many experts sceptical (including the Cert-IST): if the principle of hiding a signal in a sound is totally possible, its set up seemed much more problematic. For instance, we could doubt that the speaker and the microphone of a basic computer were efficient enough to do it.
In 2014, the feasibility of this technique has been clearly demonstrated. For instance, during the SSTIC 2014 conference, a demonstration has been made with a transmission over a distance of about 12 meters between a smartphone (playing an inaudible ultrasound) and a laptop (receiving this sound on its standard microphone): see the video "J'ai cru voir un grosminet" available in section 7 of the Rumps session of the SSTIC 2014 conference.

- **2014: year of open-source software vulnerabilities?**

(Headlines of Cert-IST bulletin - September 2014)

HeartBleed vulnerability in OpenSSL, **TrueCrypt** tool stopped, **Shellshock** vulnerability: 2014 seems to be a bad year for open-source software.
Speculate on these events to claim a trend on vulnerabilities in open-source software is probably unfounded (as Bruce Schneier said). But these events show that (of course) there are bugs in open-source software, and that (of course) source codes availability does not mean that someone actually had a look at these sources (see this Robert Graham's article on code review).
To conclude, we can state that open-source software:

- Pay the price of its success: it is everywhere and some open-source components are universally used.
- Is not less buggy than the "closed" source but is more adaptable and versatile, and can be used to build its own solutions (rather than relying on the solutions designed by a vendor).
- Has less support and is more difficult to maintain than a commercial solution. Open-source software (which are most of the time given for free) therefore require a significant investment in terms of human resource and expertise to deploy and maintain the solutions implemented.

- **"Computrace/Lojack" hidden function in some BIOS**

(Extract of the « Attacks of the month » section - May 2014)

Kaspersky has identified that the BIOS of some PC computers includes an hidden feature which installs, without the user consent, an antitheft software developed by the Absolute.com company, and named "Computrace". This software is installed each time the computer is booted, and there is no way to remove this BIOS feature. Moreover this software might be illegally used by a malicious third party to spy on the PC.
For further information, refer to our VulnCoord-2014.009 message.

- **"Schannel" vulnerability in Microsoft Windows - MS14-066**

(Extract of the « Attacks of the month » section - November 2014)

On 18-Nov-2014, we released the **CERT-IST/DG-2014.006** Potential Danger notice (titled “Expected attacks for the ‘Schannel’ vulnerability in Microsoft Windows (MS14-066)”). It is about a vulnerability in the “S-Channel” component of Windows; this component implements SSL/TLS secure network connections.
This vulnerability is very severe because:

- Schannel is used by a large number of Windows services, such as IIS, OWA, RDP, Active Directory, etc...
- The vulnerability allows remote attacker to execute arbitrary code on a vulnerable system and could be used without authentication on some services.

A lot of press articles immediately announced that this vulnerability was at least as severe as the HeartBleed vulnerability and that attacks will occur soon. Although the flaw is indeed serious, this type of reaction is excessive and seems driven by sensationalism than by rational analysis (see for example this article announcing that attacks will occur for sure in less than a week).

Following are the key dates for the evolution of this threat:

- 11-Nov-2014: Microsoft discloses the vulnerability and provides patches to fix it with its MS14-066 bulletin. We release the CERT-IST/AV-2014.873 advisory.
- 14-Nov-2014: A private exploit program (not available on Internet) is published by the Immunity company. It seems to be a prototype, available only for Immunity's customers.
- 18-Nov-2014: After observing the evolution of the threat, we believe that other attack programs could appear and lead to attacks. We issue the Potential Danger, and assign it a "Medium" risk.

The situation has not changed significantly since that date and no attack has been reported yet. Several researchers published analysis (see for example this blog post on securitysift.com). **The danger is still real and attack tools could appear soon**. As we recommended in our Potential Danger, it is mandatory to ensure that patches have been applied. IIS web servers and RDP (Remote Desktop Protocol) seems to be the most probable attack targets.

Note: On 09-Dec-2014 Microsoft has released a new version of the patches for Vista and Server 2008 platforms because previous patches might induce malfunctions. The CERT-IST/AV-2014.873 advisory was updated consequently.

4) Conclusions

Companies must deal with a complex situation.

On one hand:

- Computer sciences took a central place in our day to day life, both on professional and personal aspects,
- And the evolution of technologies leads to disseminate information in multiple places around the web (with for instance technologies like Cloud and BYOD) and seeks for making always easier the access to this information.

On the other hand, intrusion risk significantly increased over the 5 last years. And new attackers, who are specifically targeting companies (with cyber-spying or cyber-vandalism attacks), have been identified.

2014 confirms the increase of cyber risks:

- Attacks are more and more frequent,
- "Cyber" is now a strategic stake for states. We discover that states are very active on offensive aspects and actually use attack techniques we considered until recently as unlikely.
- Research for vulnerabilities and attacks now turns towards encryption solutions, and tries to break their security. Vulnerabilities therefore tackle a key element on which security solutions are based.

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

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

- Assess their exposure to this kind of attacks,
- Reinforce their defences,
- Develop their capacity to detect and react to cyber-intrusions.

End of document