Cert-IST 2008 flaws and attacks review

1) Introduction

Every year, the Cert-IST makes a review of the past year. The goal is to cover the major events of 2008 in order to highlight the trends regarding attacks and threats evolution. This summary presents a synthesis of the information sent to Cert-IST adherents members during months through the Cert-IST bulletins, on which we go through on this occasion.

Some figures

In 2008 the Cert-IST released 563 new security advisories and monitored their evolution through 1330 updates (among which 82 major updates). The raw advisory production was therefore slightly decreasing compared to the year 2007 (595 advisories) being still higher than the previous years (546 advisories in 2006, 485 in 2005, etc.).

On these 563 vulnerabilities, 13 moved towards very dangerous situations and have been monitored in a specific way through the Cert-IST "Crisis Response Hub". At the end, the Cert-IST issued 2 alerts for threats of maximum risk that required an immediate treatment inside our constituency:

- The **CERT-IST/AL-2008.001** alert in July for the DNS vulnerability
- The **CERT-IST/AL-2008.002** alert in November for the Conficker (Downadup) worm

Globally, the Cert-IST monitors vulnerabilities regarding approximately 739 products and 6194 product versions.

Major events

First of all, let's review the major trends of the year 2008 :

- **Workstation attacks through compromised web sites**. The beginning of the year clearly showed an increase of the attacks targeting the user. More than the web browser or the operating system, it is rather vulnerabilities discovered in third-party software (QuickTime, Acrobat Reader, Real Media, Flash) which are used to compromise the user's system during Internet browsing. Moreover the user is more often attacked when he visits originally harmless web sites that have themselves been compromised and that spread without knowing it these attacks.
- **Large and organized compromises**. The second important event of this year 2008 regarding attacks is the systematic use of vulnerabilities in a massive and organized way: the attacker uses here the same vulnerability in a quick deployment and on a large scale, which causes waves of attacks. Typically, during the fist 2 quarters waves of SQL injection attacks enabled attackers to silently drop malicious codes in some hours on thousands of web sites, allowing later to infect the computers of victims browsing these sites.
- **The DNS flaw: and historical case**. It is a flaw beyond the norm due to its gravity (it allows a hacker to hijack towards him all the network traffic intended to a specific server), its scale (the majority of DNS installations were vulnerable) and its disclosure mode (the vulnerability was kept secret several months then disclosed partially to give time to organisms to deploy patches, which generated media attention). It is with no doubt THE flaw of the year 2008.
- **Conficker (Downadup): the return of the worm**. The end of the year 2008 (and the beginning of the year 2009) was marked by the Conficker worm also known as "Downadup". This worm uses a vulnerability discovered last October if the Windows "server" service and had a large and rapid propagation, which can remind the virus crisis seen in 2004 (Sasser).

On top of these major events that represent the current attacks for 2008, several other facts punctuated this year:

- Worrying flaws, but with a still limited impact. The weakness of **OpenSSL keys on Debian and derived systems,** the **TCP DOS** vulnerability or the **MD5 collisions** in X509 certificates are three examples of dangerous flaws revealed in 2008. They all impact fundamental components for the security on Internet. When a vulnerability of this type is discovered the potential consequences are big. It is interesting to mention here that 2008 has been particularly rich in terms of publications, and on very various topics (see also the articles published in 2008 by the Cert-IST on subjects like "RAM attacks against encryption keys", or "A ghost in your browser ?").
- Cybercriminals are more and more active (see for instance our article "Fake Antivirus: a highly profitable business for miscreants") but the reaction of authorities becomes more and more determined (see for instance our article "More unscrupulous ISP taken down").

2) The actuality of attacks and vulnerabilities month after month

This chapter presents the major attacks and vulnerabilities that occurred month after month in 2008.

2.1) Workstations attacks through compromised web sites – January/February/March 2008

The **attack of users' workstations through their web browser** was one of the major worries of 2008. If it is not new that a user can be infected when he visits a malicious web site, It is however worrying to see that the number of sites apparently harmless that now spread without their knowing these attacks, the sophistication of these attacks, the spread with which new vulnerabilities are integrated to the attacker's tools.

These attacks use more often web sites that had been compromised. The nature of the threat has therefore increased. Some attacks of web servers are now performed, not for what these servers are or what they contain, but to turn them into vectors to reach workstations.
The danger is not anymore that the user goes to unknown sites:

- A trusted site may be « infecting » if it has itself been infected (extension of the « dangerous » perimeter).
- The sites that we are responsible for may themselves be « infecting » (implication of our responsibility in attacks targeting tierce persons).

These workstations attacks target from now on more and more the third party software present on the user's system (typically extension software or complementary plugins usually installed such as: QuickTime, Acrobat Reader or Real Media) rather than the operating system, or the web browser. This trend constitutes also a new challenge for keeping a computer park up to date because if the update mechanisms of the operating system improved a lot these last years, the update of third party software remains today often difficult.

As we explained in a detailed way in January in **the Crisis Hub opened on this topic**, there is today more than ever a big risk to browse the web using a computer that is not fully up to date in terms of security patches.

During the first quarter the Cert-IST released 5 "Potential Dangers" (DG), pre-alert messages that inform our members of attacks that may impact them shortly. These DG show well the phenomenon of workstation attacks, through the navigation on sites known as trusted we mentioned above:

- The DG **CERT-IST/DG-2008.001** **CERT-IST/DG-2008.002** and **CERT-IST/DG-2008.004** inform our constituency of vulnerabilities in the RealPlayer, QuickTime and PDF software. It is thus typically the phenomenon of attack of workstations through third party tools.
- The DG **CERT-IST/DG-2008.003** and **CERT-IST/DG-2008.005** alert on a phenomenon parallel to the first one: large web site infections. On each of the infected sites, the hacker drops an attack code

that uses new vulnerabilities targeting workstations. By infecting multiple sites the hackers increase the probability that a user visits an infected site and gets infected.

Detailed review of attacks

Note: the text below has been written in italic to indicate in a quick reading that the reader can skip this section.

The attacks of the month of January

The Cert-IST issued during the month of January 3 "Potential Dangers" :

- ***CERT-IST/DG-2008.001*** *(07/01/2008) : Malicious activities related to RealPlayer vulnerabilities*
- ***CERT-IST/DG-2008.002*** *(11/01/2008) : New critical RTSP vulnerability in Apple QuickTime*
- ***CERT-IST/DG-2008.003*** *(17/01/2008) : Large website infections*

The two first ones regard vulnerabilities in multimedia players ("RealPlayer" for the first one and "QuickTime" for the second one) and are quite similar from an external point of view, because these vulnerabilities:

- *can be triggered through a web browser.*
- *are due to buffer overflows in applications that do not use the protection mechanism against buffer overflows (DEP) of Microsoft Windows (mechanism used now by most of Windows XP-SP2, Windows 2003-SP1 and Windows Vista applications).*

For this kind of vulnerabilities, the threat evolution is classical :

- *Vulnerability discovery (or release of a proof-of-concept showing its existence and its exploitability),*
- *Then apparition of one (or many) attack programs using this vulnerability.*

At this stage, the Cert-IST sends a "Potential Danger" to inform its constituency that attacks are now possible. Each of these threats is monitored in a dedicated "Crisis Hub":

- *Crisis hub on the "RealPlayer 01/08" threat*
- *Crisis hub on the "QuickTime RTSP" threat*

*The third "Potential Danger" (**CERT-IST/DG-2008.003**) is related to the fact that in January two waves of large web sites infections have been observed.*

The attacks of the month of February

*The Cert-IST released on February 11th the "Potential Danger" **CERT-IST/DG-2008.004** (Malicious PDF files spreading - CVE-2007-5659) because a wave of attacks through malicious PDF files had been identified on Internet. This event was first reported on Saturday 9th February to the persons who subscribed to the alert 7/7 service.*
Due to the exemplarity of this attack, we devoted it an article.

The attacks of the month of March

*The Cert-IST released on March 17th the "Potential Danger" **CERT-IST/DG-2008.005** ("Multiple massive attacks on web sites") because two waves of attacks had been observed on Internet and had infected a large number of web sites. Infected web sites had been modified in such a way to later attack visitors.*
*To monitor the evolution of this threat, the Cert-IST updated its Crisis Hub **"Infection Web"**, created initially on January 17th, as well as the "Potential Danger" **CERT-IST/DG-2008.003** (Large website*

infections). The attack technique used for this second flaw is of the most original (because new), as it consists in injecting malicious data in the cache of search engines on infected web sites.

2.2) Large and organized compromise strategies - April/May/June 2008

The waves of massive web sites infections that have been seen since January 2008 (See **CERT-IST/DG-2008.003**) will carry on during all the second quarter. The attacker tactic is clear : each time a new vulnerability is discovered it must be integrated as soon as possible to the attack tools and deployed on a maximum of compromised web sites. In 2008 the most popular compromise technique was the attack of web servers by "SQL injection". The most targeted servers were the Microsoft IIS servers that use an SQL-Server database. An article published in June 2008 by the Cert-IST (called "The SQL injection attacks of recent months") aims at explaining the techniques used to set up these attacks.

To perform these waves of compromises, the attacker must be organized and able to control activities as various as:

- Vulnerability search,
- Development of attack programs,
- Massive deployment of these attacks,
- Regrouping of infected systems into botnets.

As already mentioned in 2007, the industrialization of the processes used for cybercriminality can be clearly seen here.

Beyond the large web sites infections by SQL injections (which was new in 2008) we also find during this second quarter phenomenons already seen the previous years:

- The "**StormWorm**" malware (whish has been existing since January 2007, and whose activity has been covered in an article of the January 2008 bulletin), carries on making the news. Its last variant arrives as an e-mail related to the 1st of April and entices the reader to go to a web site to see an "April fool". Obviously the web site is infected. This event has been reported to our constituency by the **VirusCoord-2008.001** message of the appropriate mailing list. The "**Kraken**" botnet (2008 reincarnation 2008 of "Bobax", one of the oldest spam botnet) was also discussed during the 2008 second quarter.
- In June, we reported in our media watch bulletins dated 09-06-08 and 10-06-08, **the return of the "GPCode" malware** . This virus, also known under the name "PGPcoder", is already known from 2005 (see this article). Its particularity is to encrypt the documents found on the system it infects. It then asks for a ransom to its victims in exchange of the key that will allow to decrypt the files. This kind of malware is now commonly designed under the English term of "ransomware".

Detailed review of attacks

In this chapter we detail month by month the different attacks that occurred during the second 2008 quarter.

The attacks of the month of April

The month of April was dense related to attacks, with 4 messages on our "Vuln-Coord" mailing list. However there was no "Potential Danger" which means that the threats reported have had mainly a media impact but have not justified a crisis increase. April constituted in reality a condensed repetition of the events of January, February and March 2008 : web attacks, malicious PDF files, but was also the occasion to mark a certain progression in server automated attacks.

It is on April 8th that the Cert-IST released its first VulnCoord message to inform its members of the emergence on a new threat : ***Kraken****. Like StormWorm, Kraken is a botnet that spreads mainly via spam message campaign.*

*Three days later, we reported that an almost functional program exploits a vulnerability on the Microsoft GDI API (**MS08-021** vulnerability), and spreads on malicious web sites.*
Last, on April 25th, we released 2 "Vuln-Coord" messages related to the following threats:

- *VulnCoord-2008.010: a renewal and an amplification of the number of **attacks by SQL injections** targeting the servers that use ASP and a Microsoft SQL database (300 000 sites compromised).*
- *VulnCoord-2008.011: an increase on the number of spam messages containing **malicious PDF files** exploiting a vulnerability (CVE-2008-0655) fixed two months ago in Adobe Reader.*

The attacks of the month of May

The month of May confirms the trend witnessed in April, which is the recrudescence of attacks by SQL injection. On May 9th, 4000 new sites had been infected by these attacks, which leads us to update the crisis thru "Infections web".

*On May 28th, we released the "Potential Danger" **CERT-IST/DG-2008.006** "0-day vulnerability in Adobe Flash Player" following the discovery by Symantec of malicious FLASH files exploiting an undisclosed vulnerability (0-day) against the last version of Adobe Flash Player. Due to the few information initially available (0-day flaw) and the number of impacted sites (thousands of impacted sites), the Cert-IST decided to open a crisis hub in order to monitor the evolution of the massive attacks related to this "new" vulnerability (0-day vulnerability in Adobe Flash Player).*

The attacks of the month of June

*In the continuity of the previous months, new **web sites infections de through "SQL injection" attacks** have been reported, less important than the ones reported during the last waves of attacks. To be noted in this area:*

- *The recommendations published by Microsoft to eradicate this kind of vulnerability on IIS servers (see our "VulnCoord-2008.018" message on this topic).*
- *The technical analysis released by the SANS regarding the injected SQL code.*

2.3) The DNS flaw: a historical case - July/August/September 2008

The DNS flaw

The main event of the summer, and probably of the year, is the vulnerability discovered in the DNS (Domain Name System) protocol by the security expert Dan Kaminsky, who should have disclosed it at the Black Hat conference of Las Vegas. The way the communication on this vulnerability has been managed constitutes a first off in the domain of Internet and computer security. An article of the bulletin of July explains you the reasons.

Conscious of the criticality of this flaw, the Cert-IST very soon monitored this vulnerability in the CERT-IST/AV-2008.310 security advisory then in the CERT-IST/DG-2008.007 "Potential Danger", and last through the "DNS vulnerability" crisis hub.

The DNS flaw: a historical case

This flaw constitutes a case "beyond the norm" and is still controversial in term of "responsible disclosure". Several factors make that this threat has a particular importance.

- First of all, the impacts and consequences of this flaw are severe as this flaw allows an attacker to hijack all the traffic on a vulnerable DNS server towards malicious sites (DNS cache poisoning).
- Last, it impacts the immense majority of DNS servers and clients connected to the Internet worldwide, which makes patch appliance difficult,
- It affects a very large number of actors on the Internet ; network manufacturers, ISP, domain name regulator (registry, registrar), DNS administrators, developers, not forgetting the users.
- Last, cybercriminals are interested in this flaw because it enables to redirect users towards fake web sites. Multiple attack scenario are possible, in particular the one of phishing.

An unusual handling

The technical details of this vulnerability, discovered in February 2008, were kept secret for long months. A group of individuals, composed of the discoverer, US-CERT members and various DNS service editors, worked together in order to decide of the best way to handle and fix this flaw, and then to disclose it.
The date of July 8th 2008 was thus chosen for the concerted publication of patches, with the will of keeping the technical details secret. It is precisely this point, the "secret", that raised the curiosity of security searchers, who raced to analyse and investigate the problem. Meanwhile, the credibility of the Dan Kaminsky's discovery was challenged. He wanted to insist on the gravity of this vulnerability, and during his exchanges, he probably released by mistake precious technical information. On July 22nd, technical details of this flaw were finally known.
At this point, everything went very fast. Exploits have been released on July 24th and first attacks have been reported on July 29th.

Patch deployment status

We wrote in July : « the threat will be present as long as only one DNS server remains vulnerable». On July 8th, around 85% of servers were vulnerable (source : "DoxPara Research"). On July 25th, 13 days later, this score would be 52% according to DoxPara and 66% according to the Austria CERT (http://www.cert.at/static/cert.at-0802-DNS-patchanalysis.pdf). This progression is significant, but it also shows that there are still many vulnerable DNS servers (at least more than a half).

In July, all the technical details were still to be disclosed, awaiting for August 7th, when Dan Kaminsky disclosed the details of the vulnerability, at the BlackHat conference (http://www.blackhat.com).
One thing is sure is that all did not happen as "scheduled" (http://www.doxpara.com/?p=1162). The made mistakes must now be analysed and the many issues raised by the discovery and the responsible disclosure of this kind of vulnerability must be tackled. One major issue is the difficulty to apply patches at such a large scale (issue already known but stressed in the DNS case) at such pace.

For more information

- Dan Kaminsky official website: http://www.doxpara.com/
- Crisis response hub "DNS flaw" : https://wws.cert-ist.com/fra/hub/failledns

The other attacks from August to September 2008

Cyber attacks in Georgia

According to the media, Georgia governmental sites were impacted in August by cyber attacks attributed to Russia. The discussions between CERT through the FIRST indeed confirm the existence of DDOS attacks, in particular from August 14th, without being able however to link them to Russia. Marcus H. Sachs, director of the SANS ISC and expert in cyber-security at the American government, released on ISC an interesting analysis of this phenomenon.

Attacks of SSH infrastructures ?

It is well known that SSH servers accessible from Internet are regularly the target of "force brute" attacks (attacks with password dictionary).

On May 14th, the Cert-IST had sent the "Vuln-Coord" message **VulnCoord-2008.013** ""OpenSSL" vulnerability in Linux Debian and Debian based distributions" regarding a high media attention vulnerability in the world of Debian distributions (Debian, Ubuntu, Knoppix, etc.). This vulnerability, due to a default in the pseudo-random generator, affects directly the "OpenSSL" package and indirectly all the products containing or based on SSL key (OpenSSH, OpenVPN, HTTPS, etc.). A patch now enables to detect the vulnerable keys and force their update on those distributions.

The actuality of August can lead to think that more sophisticate attacks are ongoing against these infrastructures, we reported to you:

- First through the **VulnCoord-2008.026** message, that hackers introduced on the servers of Red Hat and Fedora infrastructures.
- And then through the **VulnCoord-2008.027** message, that the US-CERT identified attacks targeting SSH servers on Linux and whose goal seems to steal the SSH keys stored on the servers ("Phalanx2" rootkit).

Virus campaigns like "botnet Storm" spread through Spam

In August, several SPAM campaigns of a large scale and aiming at infecting the user’s system, were noticed and reported in the **VirusCoord-2008.002** message. They have the names "Olympic Games", "Top News CNN" or "Airline Ticket email" and all aims at attracting curious people to a web site that will infect the PC with a botnet such as "Storm" (see the April actuality).

2.4) Worrying vulnerabilities, but still limited impact - October/November/December

Apart from the arrival of the Conficker worm, which by itself deserves a chapter (see § 2.5), the months of October to December did not really bring outstanding events in terms of attacks.

On the other hand, several vulnerabilities (detailed below) led to wide media attention. Even if they raise serious problems, these vulnerabilities have not had (still) significant impacts on infrastructures and therefore have not led to the release of Cert-IST alerts or potential dangers to our members.

"ClickJacking" vulnerability ("clickjacking" crisis hub)

The vulnerability known as "ClickJacking" was presented at the end of September at the OWASP (Open Web Application Security Project) conference in New-York. This attack that exploits a vulnerability in the dynamic content of DHML (Dynamic HTML) pages enables to entice a user to click on dangerous links without knowing it. The Cert-IST sent a Vuln-Coord-2008_030 message to inform its constituency, and monitored this vulnerability in the list of "Flaws under investigation" (see FA-2008_0181).

TCP DOS flaw (VulnCoord-2008.031)

At the end of September, two Finnish security experts announced they had discovered a vulnerability that impacts all the TCP/IP stack implementations, and causing a denial of service. After announcing the publication of some details on this flaw at the T2 conference which was held on October 17, 2008 in Finland, the two protagonists retract thinking that these details should only be revealed when editor patches are released. There would have been only an exploit demonstration of this vulnerability presented during this conference, and it would cause a denial of service on any device implementing a vulnerable TCP/IP stack.
Up to now no technical information leaks. The details will probably be known during 2009. This vulnerability is monitored in the "Flaws under investigation" section (see FA-2008.0184) and in the crisis hub "DOS vulnerability in TCP to be revealed at T2 2008 conference".

"Token kidnapping" : Exploitation of a Windows vulnerability through IIS and SQL Server (VulnCoord-2008.032)

This "Vuln-Coord" message was sent following the release on Internet of an exploit that enables to attack Windows systems through Microsoft IIS and SQL Server ("Token Kidnapping" attack).

However, two vulnerabilities seemed to us more worrying and led to the emission of Potential Dangers so that our constituency can be prepared to possible attacks. Up to this day, these attacks have not had a significant scope justifying the release of an alert.

Vulnerability in the sadmind daemon on Solaris ("sadmin" crisis hub)

Mid-October a vulnerability has been discovered in the "Sun Solstice AdminSuite" product that impacts Solaris 8 and 9 systems. Without a patch from the editor and due to the criticality of this flaw (total remote take control), we monitored this flaw in the flaws under investigation "**FA-2008.0194** and informed our constituency of the publication of exploits in the "Potential Danger" (**CERT-IST/DG-2008.008**).

0-day XML vulnerability in Internet Explorer ("IE XML 0day" crisis hub)

This 0-day vulnerability in the handling of some XML data XML by Internet Explorer, had been disclosed the day after the December Patch Tuesday. It has been described in the potential danger CERT-IST/DG-2008.011 since December 10th and in the "IE XML 0day" crisis hub. A security advisory was also released (CERT-IST/AV-2008.538) proposing a first set of workarounds. Microsoft reacted on December 17th by releasing again an out-of-cycle security bulletin (MS08-078), providing patches for this vulnerability.

2.5) Conficker (Downadup): the return of the worm

The most interesting fact of the last quarter of 2008 is the arrival of the Conficker worm (also called "Downadup"). It is the first worm that has impacted so significantly our constituency since 2004 (year of the "Sasser" worm). We detail below the treatment that the Cert-IST made regarding this threat. But globally we can remember that:

- The threat was well anticipated. Since October 13th (date of the Microsoft announce of this vulnerability in the MS08-067 bulletin), it was clearly identified that a worm could appear. The regular Cert-IST publications (an advisory related to the vulnerability, three advisories related to the malwares exploiting it, two "Potential Dangers", and then an alert) enabled our adherents to be kept informed during the evolution of this threat.

- Since 2004 no worm of a significant scale had been observed. We were even wondering if there would still be worms (see our 2007 summary) as this massive and noisy propagation mode is not necessarily interesting for cyber criminals who now try to be more furtive.
- Some Cert-IST members were exposed to this threat and a rigorous and systematic treatment enabled them to contain it. Although the infection sources of Conficker remained isolated and limited, it had not been possible to systematically determine the vector at the origin of these infections. These vectors seem potentially numerous, let's quote in particular USB keys, mobile systems, VPN channels, and spam e-mails. For this kind of threat, it seems impossible to avoid that infection sources are triggered, besides the protection features such as antivirus, peripheral protections and network filters. A fundamental aspect to control this threat (awaiting for the patches to be applied on all systems) is thus to know how to detect as soon as possible the infectious sources in the company, to isolate them and to treat them quickly.

Detailed review of the chronology

October: "Out-of-cycle" Microsoft MS08-067 security bulletin (VulnCoord-2008.034)

One of the important events of this month of October is the release of a Microsoft security bulletin (MS08-067) beyond the usual publication dates. The reason of this publication is the discovery of a major flaw in the "Server" service of Microsoft Windows systems. Several exploits for this vulnerability appeared on Internet, from the "Proof-Of-Concept" program, to the program downloading malwares stealing information on an infected system (ex. GimmiV).
*This vulnerability was described in the **CERT-IST/AV-2008.460** security advisory and in the **CERT-IST/DG-2008.009** "Potential Danger". The evolution of the threat related to this vulnerability was monitored in the crisis hub "Critical vulnerability in the handling of RPC requests on Microsoft Windows (MS08-067)".*

November: Malicious codes multiply and Conficker arrives

The major event of this month of November was mainly the holding of a strong activity around the MS08-067 vulnerability of the "Server" service of Windows systems.
Not only malicious codes strongly multiplied, but there was an increase of their efficiency. This led us to send, on top of the many posts that fed the crisis hub "Critical vulnerability in the handling of RPC requests on Microsoft Windows (MS08-067)":

- *The CERT-IST/AV-2008.467 security advisory and the CERT-IST/DG-2008.010 "Potential Danger" related to the "Kerbot" and "Wecorl" viruses.*
- *The CERT-IST/AV-2008.504 security advisory related to the "Conficker" worm (also known as "Downadup").*
- *The CERT-IST/AL-2008.002 alert following many infection reports by the "Conficker" worm worldwide, but also in our constituency.*

December 2008 and January 2009: Conficker infections multiplied

*In December then in January 2009 the number of Conficker infections multiplied. Specialised media widely broadcasted this information mid-January 2009 as we said in our media watch bulletins (see **vmedia-2009.01.14**, **vmedia-2009.01.15**, **vmedia-2009.01.19**, **vmedia-2009.01.20**). Our constituency was of course impacted as well, but the infections remained localised, and thus more easily controllable. To enable an increased exchange between its adherents on this threat, the Cert-IST set up a discussion list dedicated to this topic (ms08-067 list).*

3) Conclusion

As we can see through this summary, the year 2008 has been rich in events.
Like in 2007 the professionnalisation of the attacks is noticeable: the technical level of malicious codes, the multiplicity of the aspects controlled and the global coordination of the attacks can only be the result of a very structured activity.

But if we want to summarize this year in terms of trends, the year 2008 can be qualified of a year of "hardening" :

- Attackers seem stronger and stronger. Attack techniques, lifecycle speed and especially coordinated actions have with no doubt increased in 2008.
- On another side the defence also progressed. In terms of technique first. For instance a tool such as the Microsoft MSRT (Malicious Software Removal Tool) has become a real "botnet killer". The defence also progressed in terms of organisation; initiatives like ShadowServer (which works to list and dismantle botnets) or actions like the stop of illegal activities (see our "More unscrupulous ISP taken down" article regarding the McColo and Atrivo providers published in the Cert-IST monthly bulletin) reveal a progression and a hardening of the defence.

For companies this hardening of attacks implies that defences set up are solid and tight. It is necessary today to have efficient and reactive mechanisms to apply patches, in-depth defence mechanisms, and rigorous procedures to efficiently face crisis situations.