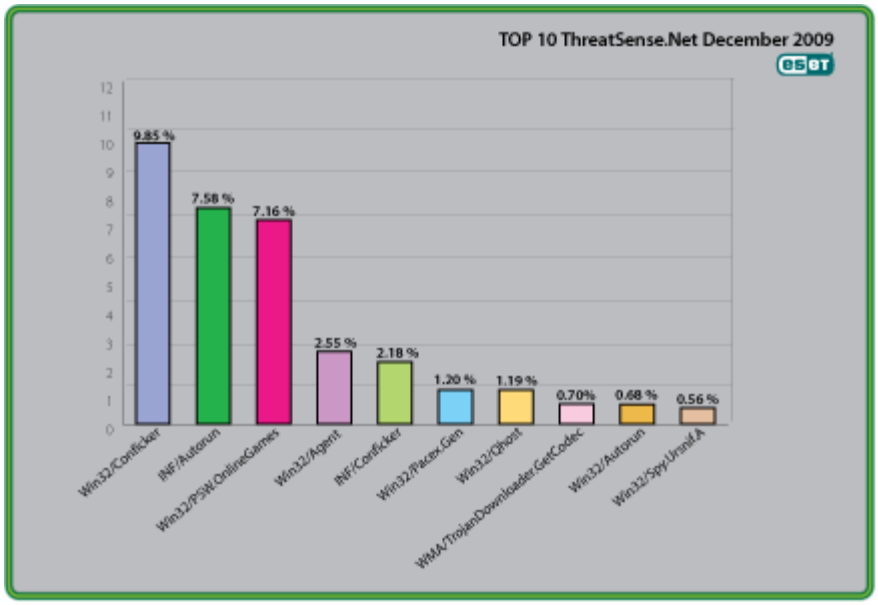
Global Threat Trends – December 2009

Figure 1: The Top Ten Threats for December 2009 at a Glance



Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 9.85% of the total, was scored by the Win32/Conficker class of threat.

More detail on the most prevalent threats is given below, including their previous position (if any) in the "Top Ten" and their percentage values relative to all the threats detected by ThreatSense.Net®.

In view of the fact that this is the last Global report of 2009, we're providing a reminder of some of the more interesting events of the past 12 months, as well as some thoughts on what's in store for 2010, so this report is quite a lot longer than usual.

1. Win32/Conficker

Previous Ranking: 1
Percentage Detected: 9.85%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the *svchost* process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

What does this mean for the End User?

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since Autumn 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: http://www.eset.com/threat-center/blog/?cat=145

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions.

2. INF/Autorun

Previous Ranking: 2
Percentage Detected: 7.58%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run

automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

What does this mean for the End User?

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (http://www.eset.com/threat-center/blog/?p=94; http://www.eset.com/threat-center/blog/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 7.16%

This is a family of Trojans used in phishing attacks aimed specifically at game-players: this type of Trojan comes with keylogging and (sometimes) rootkit capabilities which gather information relating to online games and credentials for participating. Characteristically, the information is sent to a remote intruder's PC.

What does this mean for the End User?

These Trojans are still found in very high volumes, and game players need to remain alert. While there have always been unpleasant people who will steal another gamer's credentials just for the heck of it, trading in virtual cash, treasure, avatars and so on is now a major source of illegal income for cybercriminals. It's also important that participants in MMORPGs (Massively Multi-player Online Role Playing Games) like Lineage and World of Warcraft, as well as "metaverses" like Second Life, continue to be aware of the range of other threats like griefing ranged against them. The ESET Research

team considered gaming malware in detail in the ESET 2008 Year End Global Threat Report, which can be found at http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf

4. Win32/Agent

Previous Ranking: 4
Percentage Detected: 2.55%

ESET NOD32 describes this detection of malicious code as generic, as it describes members of a broad malware family capable of stealing user information from infected PCs.

To achieve this, the malware usually copies itself into temporary locations and adds keys to the registry which refers to this file or similar ones created randomly in other operating system's folders, which will let the process run at every system startup.

What does this mean for the End User?

This label covers such a range of threats, using a wide range of infection vectors that it's not really possible to prescribe a single approach to avoiding the malware it includes. Use good anti-malware (we can suggest a good product ☺), good patching practice, disable Autorun, and think before you click.

5. INF/Conficker

Previous Ranking: 5
Percentage Detected: 2.18%

INF/Conficker is related to the INF/Autorun detection: the detection label is applied to a version of the file autorun.inf used to spread later variants of the Conficker worm.

What does this mean for the End User?

As far as the end user is concerned, this malware provides one more good reason for disabling the Autorun facility: see the section on INF/Autorun above.

6. Win32/Pacex.Gen

Previous Ranking: 6
Percentage Detected: 1.20%

The Pacex.Gen label designates a wide range of malicious files that use a specific obfuscation layer. The .Gen suffix means "generic": that is, the label covers a number of known variants and may also detect unknown variants with similar characteristics.

What does this mean for the End User?

The obfuscation layer flagged by this detection has mostly been seen in password-stealing Trojans. However, as more malware families appear that don't necessarily use the same base code but do share the same obfuscation technique, some of these threats are being detected as Pacex.

However, the increased protection offered by multiple proactive detection algorithms more than makes up for this slight masking of a statistical trend: as we discussed in a recent conference paper, it's more important to detect malware proactively than to identify it exactly. ("The Name of the Dose": Pierre-Marc Bureau and David Harley, Proceedings of the 18th Virus Bulletin International Conference, 2008 - http://www.eset.com/download/whitepapers/Harley-Bureau-VB2008.pdf; "The Game of the Name: Malware Naming, Shape Shifters and Sympathetic Magic" by David Harley - http://www.eset.com/download/whitepapers/cfet2009naming.pdf)

7. Win32/Qhost

Previous Ranking: 7
Percentage Detected: 1.19%

This threat copies itself to the %system32% folder of Windows before starting. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker. This group of trojans modifies the host's file in order to redirect traffic for specific domains.

What does this mean for the End User?

This is an example of a Trojan that modifies the DNS settings on an infected machine in order to change the way that domain names are mapped to IP addresses. This is often done so that the compromised machine can't connect to a security vendor's site to download updates, or to redirect attempts to connect to one legitimate site so that a malicious site is accessed instead. Qhost usually does this in order to execute a Man in the Middle (MITM) banking attack. It doesn't pay to make too many assumptions about where you are on the Internet.

8. WMA/TrojanDownloader.GetCodec.Gen

Previous Ranking: 8
Percentage Detected: 0.70%

Win32/GetCodec.A is a type of malware that modifies media files. This Trojan converts all audio files found on a computer to the WMA format and adds a field to the header that includes a URL pointing the user to a new codec, claiming that the codec has to be downloaded so that the media file can be read.

WMA/TrojanDownloader.GetCodec.Gen is a downloader closely related to Wimad.N which facilitates infection by GetCodec variants like Win32/GetCodec.A.

What does this mean for the End User?

Passing off a malicious file as a new video codec is a long-standing social engineering technique exploited by many malware authors and distributors. As with Wimad, the victim is tricked into running malicious code he believes will do something useful or interesting. While there's no simple, universal test to indicate whether what appears to be a new codec is a genuine enhancement or a Trojan horse of some sort, we would encourage you to be cautious and skeptical: about any unsolicited invitation to download a new utility. Even if the utility seems to come from a trusted site (see http://www.eset.com/threat-center/blog/?p=828, for example), it pays to verify as best you can that it's genuine.

9. Win32/AutoRun

Previous Ranking: 9
Percentage Detected: 0.68%

Threats identified with the label 'AutoRun' are known to use the Autorun.INF file. This file is used to automatically start programs upon insertion of a removable drive in a computer.

What does this mean for the End User?

The general implications of this particular threat for the end user are much the same as for malware detected as INF/Autorun.

10. Win32/Spy.Ursnif.A

Previous Ranking: 23
Percentage Detected: 0.56%

This label describes a spyware application that steals information from an infected PC and sends it to a remote location, creating a hidden user account in order to allow communication over Remote Desktop connections. More information about this malware is available at http://www.eset.eu/encyclopaedia/win32-spy-ursnif-a-trojan-win32-inject-kzl-spy-ursnif-gen-h-patch-zgm?lng=en

What does this mean for the End User?

While there may be a number of clues to the presence of Win32/Spy.Ursnif.A on a system if you're well-acquainted with the esoterica of Windows registry settings, its presence will probably not be noticed by the average user, who will not be able to see that the new account has been created. In any case it's likely that the detail of settings used by the malware will change over its lifetime. Apart from making sure that security software (including a firewall and, of course, anti-virus software) is installed, active and kept up-to-date, users' best defense is, as ever, to be cautious and proactive in patching, and in avoiding unexpected file downloads/transfers and attachments.

2009 In Retrospect

This is the section in which we normally look back over the events of the previous month. However, since this is the last Report of 2009, it seems appropriate to look back over the whole year, rather than just December.

January

Over the new year in 2009, we ran a series of tips on self protection (see http://www.eset.com/threat-center/blog/2008/12 and http://www.eset.com/threat-center/blog/2009/01). (A revised version of those tips is likely to come out as a white paper shortly.) A major threat that month (as always) was INF/Autorun. There was a renewal of interest in the association of that class of threat and digital photo-frames that month, too, perhaps to do with the volume of such devices given as Xmas gifts?. Most of the top ten entries for that month were advanced heuristics rather than a single malware family, but the pernicious Virtumonde adware Trojan was also present in high volumes. Twitter phishing gained a high profile because celebrity Stephen Fry admitted he'd fallen for one such scam. David Harley, ESET's Director of Malware Intelligence, started to look in earnest at Twitter. 12 months later, he says he's still no expert, but has almost as many Twitter accounts as he does blog accounts. (You can follow the San Diego Research Team as http://twitter.com/esetresearch, if you're so inclined.)

In the UK, there was concern about extended powers given to the police: this was one of the issues addressed by Craig Johnston and David Harley in a presentation at AVAR 2009

(http://www.eset.com/download/whitepapers/Please_Police_Me.pdf). Randy Abrams, ESET's Director of Technical Education, posted a blog on (un)sound password practice that was later incorporated into a paper by Randy and David at http://www.eset.com/download/whitepapers/EsetWP-KeepingSecrets20090814.pdf.

Win32/Conficker was prominent in the top ten list and there was a lot of media attention paid to guesswork as to how many machines were actually infected. Of course, Conficker is very much a live issue today, and a translation of a paper by Sebastián Bortnik, Security Analyst at ESET Latin America which we call "Conficker by Numbers" should be available shortly on the ESET White Papers page at http://www.eset.com/download/whitepapers.php. IRS and government grant scams were rife, but then fraud is a consistent visitor to most Internet mailboxes. Google accidentally flagged every site on the Internet with the message "This site may harm your computer." Which I suppose is, in an abstract sense, not altogether untrue in an age of injection attacks and cross-site scripting, but not very helpful, either to end users or to Google's reputation. Apparently it's not only anti-virus products that can generate false positives.

February

As usual, INF/Autorun (and related detections) and password stealers continued to dominate, though the name on everyone's lips was "Win32/Conficker". Adware, Possibly Unwanted Applications and so on were (and still are) both prominent and annoying. Phishers started to use the Stimulus program as a hook for tricking people into revealing passwords: we suppose that health insurance legislation is likely to generate social engineering in 2010. The gang behind Win32/Waledac used Valentine's day as an opportunity to disseminate "greetings cards" that were really malware. Curiously, someone mailed out a "Bill Gates is sharing his fortune" hoax to a wide range of antivirus people, who are not usually naïve enough to fall for such things. Adobe was forced to flag a severe PDF-related vulnerability: unfortunately for Adobe, their products have been exploited in a number of ways this year, and ESET's bloggers spent much time flagging some of those problems. Fake security software continued to increase in scope and impact. Nostalgically, there was a significant wave of malware exploiting Microsoft Excel.

March

The first week in March was National Zombie Awareness Week in Australia, but of course it's always a good week to be aware of botnets and zombie systems. (http://www.eset.com/threat-center/blog/2009/03/03/zombies-down-under) We noted an upsurge in scams aimed at selling domains to people worried about cybersquatting. Gossip and rumor blew a minor error by Symantec (releasing an unsigned diagnostic patch) into a fabulous tale of rootkits and backdoors. We use the term fabulous in its original sense: there was no truth in the rumors. The BBC dipped a toe into criminal

activity by buying a 22,000 PC botnet and used it to demonstrate how spam and DDoS attacks work. While there was really no need to put money into a criminal's pocket in order to illustrate this, they managed to avoid prosecution under the UK's Computer Misuse Act. David Harley and Randy Abrams were goaded by a spate of "missing child" hoaxes and semi-hoaxes into writing a paper for Virus Bulletin 2009 on the topic: http://www.eset.com/download/whitepapers/Harley-Abrams-VB2009.pdf. Google's (non-)handling of abuse complaints received a lot of attention. Virus Bulletin started to do anti-spam testing. Psyb0t pushed the botnet envelope a little by targeting routers and DSL modems rather than PCs. There was much speculation about what would happen on April 1st when Win32/Conficker.C was expected to do *something*, though it wasn't possible to predict what. In fact, it didn't do anything dramatic like bringing down the Internet, but it did change communication protocols. And after practically the entire AV industry blogged for weeks saying "don't panic", some commentators, including (SC)2, claimed it was all vendor hype.

April

This month saw an undramatic but nevertheless fully functioning Mac botnet that was actually used in a DDoS attack. There was an upsurge in the use of Office software to deliver targeted malware, though Microsoft seemed to think that targeted malware is a minor issue and took their time producing fixes. A Russian news site claimed that Conficker was carrying out DDoS attacks, but we, working with other researchers, found no evidence of Conficker involvement at all. There were claims that Russia and China were penetrating the US power grid. The malware we call W32/Conficker.AQ exhibited some interesting characteristics. Following a spate of Twitter worms by exhibitionist Loony Mooney, an irritated David Harley exhorted "on your bikeyy, Mikeyy!" (http://www.eset.com/threat-center/blog/2009/04/14/twit-of-the-year) The Hexzone botnet was associated with some unpleasant ransomware.

May

The merry month of May saw significant events in Budapest – a CARO workshop on exploits and vulnerabilities and the second AMTSO workshop of the year, where the Review Analysis Board procedures were approved, as were papers on sample validation and "In the Cloud" testing. The EICAR conference, where David and Randy presented a paper on testing, also included a panel on testing with representatives of EICAR, AMTSO and ICSALabs. ESET Senior Malware Researcher Pierre-Marc Bureau attended the Confidence conference in Krakow, and recommended it highly. In San Diego, "Securing our eCity", a community initiative co-sponsored by ESET, ran some highly successful free presentations on cybercrime. In the UK, the National Health Service's problems with data leakage attracted unfavorable attention from the Information Commissioner.

June

In the UK, phone scammers were targeting senior citizens in Scotland, and there was widespread concern about the widespread lack of understanding of the Data Protection Act, inspiring a new British Standard (BS 10012). MSN described Salford University's Masters Degree in Social Media as an "MA in Facebook and Twitter". There was a spate of scammers hijacking email accounts and asking contacts to send them money to get home after being mugged. People started to predict that Microsoft's free antivirus would be the death of the antivirus industry. Reports of that death have been greatly exaggerated… A survey reported that a third of workers have sent "explicit" emails, dumped a partner, or applied for a job from a work PC, indicating a worrying inability to distinguish between the work and social contexts. Michael Jackson died and inspired a slew of miscreants to use his name for social engineering, for spreading scams and malware.

July

ESET researchers played a significant part in reducing the impact of the Waledac botnet Independence Day spam campaign. The wife of the head of MI6 (one of the UK's intelligence services) put much, much too much information on a Facebook page. Sebastián Bortnik, from ESET Latin America, produced some interesting figures on how much spam a Waledac-infected PC might send (his experiments indicated about 150,000 spam emails per day from a single machine). There was speculation that US government web sites were being DDoS-ed (multiple machines used to carry out a Distributed Denial of Service attack) by North Korea. That speculation was, however, not convincingly verified. Security bloggers, exploit publication sites and exploit distributors were threatened with "deletion" by someone or something called "Anti-sec" but we're still here so far. (http://www.eset.com/threat-center/blog/2009/07/11/orwell-double-think-and-anti-sec)

The perils of (mis)using Social Security Numbers as authentication were pointed out by David Harley, among others, and Jeff Debrosse commented at length on the fact that 85% of U.S. organizations were reported in a Ponemon Institute survey to have experienced data breaches. Win32/TrojanDownloader.Bredolab.AA made a serious impact on end users, especially in Europe, as information from ESET in Slovakia (where our main labs are) made clear. (http://www.eset.eu/encyclopaedia/win32-trojandownloader-bredolab-aa-inject-abnx-x-spy-agent-bw?lng=en) ESET in Europe also came up with a nice article on the dangers of surfing on free wi-fi: http://www.eset.eu/press/summer-surfing-on-free-wifi. Adobe and Microsoft patches were big news, and Apple complained about the dangers of jailbreaking iPhones.

August

ESET Latin America noticed that Slideshare (http://www.slideshare.net) was being used to share fake slide decks that actually diverted users to sites offering fake security software (kudos to Slideshare for responding so quickly and positively in removing the

bad account). Anti-malware researchers joined forces to counter an ugly Trojan downloader commonly called Delf or Doneltart. The UK's Cabinet Office issued a surprisingly useful template document for government departments wanting to use Twitter, though it was well over 140 characters long, and Win32/Induc.A turned out to have evaded detection by AV companies for several months by using a compiler to infect subsequently compiled programs, a concept most commonly associated with a presentation by Ken Thompson that goes back to 1984 ("Reflections on Trusting Trust"). Microsoft published a technique for disabling Autorun (the facility misused by INF/Autorun) as a default. Aryeh Goretsky, Distinguished Researcher at ESET LLC, drew attention to the growing number of OS X threats, as even Apple have started to notice (a theme developed at some length in subsequent blogs by David Harley).

September

Inevitably, some Mac fans assumed that the minimal anti-Trojan facility in Snow Leopard was all the protection they needed, or more than they needed. Pierre-Marc published a blog (http://www.eset.com/threat-center/blog/2009/09/03/more-infections-a-lot-more-malware) summarizing malware statistics gleaned from ESET's free online scanner at http://www.esetonlinescan.com/. Aryeh published a blog on self-protection in the context of social networking at http://www.eset.com/threat-center/blog/2009/09/08/armor-for-social-butterflies. David Harley's CFET conference paper on malware naming was posted on the white papers page (http://www.eset.com/download/whitepapers/cfet2009naming.pdf). A 19-year-old burglar in Virginia was caught because he took time out to access his Facebook account on the victim's laptop and didn't think to log out. Virus Bulletin's 2009 conference at Geneva included papers by Juraj Malcho, Jeff Debrosse, Randy Abrams and David Harley

October

The 6th Cybersecurity Awareness Month saw a number of events and initiatives intended to raise the level of awareness and self-protection in the US. SEO (Search Engine Optimization) poisoning (or Index Hijacking) is far from a new attack, but has reached new levels of sophistication this year, and ESET Malware Researcher Tasneem Patanwala blogged an excellent analysis of one such attack (http://www.eset.com/threat-center/blog/2009/10/01/seo-poisoning-what%e2%80%99s-in-the-news-today). Sebastián Bortnik flagged an issue with HTTPS in his blog at http://blogs.eset-la.com/laboratorio/2009/10/02/mito-https and subsequently produced a video demonstrating it, while ESET LLC's research team picked up the theme in some follow-up blogs that also addressed issues with SSL. Windows 7 was released. In the light of comparative testers claiming to be "AMTSO compliant" or similar, there was heated discussion at the Anti-Malware Testing Standards Organization meeting in Prague about ways of preventing other organizations from subverting or misrepresenting the AMTSO "brand". (Similar issues are likely to predominate at the next workshop in February.) Fake Windows updates are nothing novel, but there was something of a "spike" this month: of

course, such fakes tend to be associated with malicious URLs rather than malicious attachments nowadays.

November

The attempted use of the "Some Other Dude Did It" (SODDI) or "Trojan Defense" as a way of avoiding culpability for breaking computer-related laws came under some scrutiny, particularly in the context of pedophilia. A series of malware attacks on "jailbroken" iPhones exploited a vulnerability that affected the users of some such phones. In the long term, though, perhaps Apple's "not our problem" attitude will be seen as having more serious implications for the community as a whole. A PC vendor in Australia offered "virus-proof" PCs: while the company was evasive about the nature of this virus-proofing, it seemed to refer to a "hardened" partition using a non-Windows OS rather than the Windows partition which users were likely to find both necessary and vulnerable for many routine Windows operations.

A survey commissioned on behalf of "Securing our eCity" uncovered some disquieting findings about community perceptions of cybercrime and security issues. ESET did rather well in a performance test commissioned by another vendor, and would have done even better if a more realistic approach to measuring memory usage had been used, as Andrea Kokavcova pointed out at http://www.eset.com/threat-center/blog/2009/11/16/what-a-performance. Google's Chrome OS, still under development, attracted some attention for its potential in terms of mitigating some kinds of malware attack. A patent by Qinetiq was hailed by "New Scientist" as the end of the "virus" problem. Closer examination suggests that while there are some interesting ideas there, we at ESET won't be out of work for a while.

December

Randy sent PayPal a note pointing out that some of the mail they send out is far too much like phishing. They must have agreed, since they "confirmed" that their own mail was a phish. While they tried to dismiss the whole issue as the bee in one researcher's bonnet, subsequently, a sizeable proportion of the security community agreed with him. ESET released public beta versions of its products for OS X and Linux desktop, and the 150th episode of its Malware Report Podcast, as blogged by Randy at http://www.eset.com/threat-center/blog/2009/12/04/malware-report-podcast-marcus-sachs%e2%80%99-take-on-cybersecurity. David Harley also celebrated a somewhat low-key anniversary – twenty years involvement in the anti-malware industry. The Motorola Droid was "rooted", a technique for circumventing the vendor's whitelisting of applications in a similar fashion to iPhone/iPod "jailbreaking". Yet more questions were asked about Facebook and privacy, and others were raised about the use by financial institutions of "publicly available" data for authentication as well as information given directly to those institutions by their customers. (http://www.eset.com/threat-center/blog/2009/12/14/your-data-and-your-credit-card). Researchers from ESET Latin

America and ESET LLC joined forces (as they often do) to discuss and analyze a wave of malware masquerading as videos of the attack on Italian Prime Minister Silvio Berlusconi (http://www.eset.com/threat-center/blog/2009/12/15/fake-videos-of-berlusconi-attack). Randy reminded us to upgrade to XP SP3 if we want to benefit from Microsoft support past July 2010, and commented on the appointment of Howard Schmidt to the role of Cybersecurity Coordinator for the White House. And the "SODDI" defense resurfaced, this time in the context of the hacking of Sarah Palin's email account (http://www.eset.com/threat-center/blog/2009/12/24/grasping-at-straws-did-malware-hack-palins-email-account).

What's in Store for 2010?

The Research teams in ESET Latin America and ESET LLC put their heads together to discuss the likely shape of things to come in the next twelve months in security and cybercrime (and cyberwarfare, to use one of the buzzwords of the moment. Randy blogged some of those thoughts at http://www.eset.com/threat-center/blog/2009/12/14/que-sera-sera-%e2%80%93-a-buffet-of-predications-for-2010 and ESET Latin America published some of their thoughts (in Spanish) at http://eset-la.com/centro-amenazas/2256-tendencias-eset-malware-2010. however, here's a summary of the conclusions we came up with between us. (A paper on "2010: Cybercrime Comes of Age", combining both resources in English is in preparation at the moment and should be available at http://www.eset.com/download/whitepapers.php in the next few weeks.)

1. Social engineering attacks will continue to predominate, while attacks based on operating system vulnerabilities will continue to decline as more people move to more secure operating systems. While at the moment vulnerabilities in applications are a serious threat, this will decline as application vendors learn to tighten their quality control and patching methodologies. Windows 7 will contribute to a gradual decline in INF/Autorun and related threats.

2. Hot topical issues such as public holidays, current news items (real or fabricated), high-profile events such as the World Cup, and persistent preoccupations such as the national and global economy will be used as hooks on which to hang social engineering attacks.

3. While attacks on jailbroken iPhones may affect less people as they become aware of the primary current attack vector, there will be increased probing of mobile devices in general for exploitable vulnerabilities as well as opportunities to make use of social engineering as described above.

4. There will be increasing emphasis on the isolation of the owners of infected systems until they take remedial action.

5. Data breaches will continue to grow in importance, and the efficacy of security as implemented in "In the Cloud" data processing will, at least in the short term, vary widely.

6. There will be more use of rogue software to extort money, and the scope of such fakery is likely to widen beyond fake security software.

7. Malware as a Service will, more and more, reflect the models of cooperation between specialists seen in the legitimate business world.

8. There is likely to be more use of high-level languages (especially scripting languages) so as to re-purpose malicious code across multiple platforms.

9. Social networks will be targeted even more, both for social engineering attacks and in terms of probing for vulnerabilities.

10. There will be further research into and attacks on virtualized environments, though their effectiveness is likely to be limited.

11. Phishing and related attacks on online gamers will continue to be big business, though attacks on gaming consoles are likely to be meet with limited success.

12. Attacks that manipulate wireless connections will continue to flourish.

13. Criminals and legitimate businesses will mine data from a widening range of resources, exploiting interoperability between social networking providers. Sharing of data in the private sector will be an increasing threat until the need is accepted for more data protection regulation on similar lines to that seen in the public sector, especially in Europe.

14. Out-and-out crimeware will be the most common and successful form of malware, because of its potential for generating illegal profit.

15. The subversion of legitimate web sites and social networks as an attack vector will continue to be a highly successful criminal activity. We're likely to see more use of such networks as a means of administering the illicit infrastructures used by organized business networks (such as botnets), as well as more direct exploitation such as malvertising.

16. Targeted attacks (spear-phishing, whaling) will be a significant but underestimated threat.