2010: Cybercrime Coming of Age

Table of Contents

Overview

The Research teams in ESET Latin America and ESET, LLC put their heads together in December 2009 to discuss the likely shape of things to come in the next 12 months in security and cybercrime (and cyberwarfare, to use one of the more irritating buzzwords of the moment).

Randy Abrams, Director of Technical Education at ESET, LLC blogged the LLC Research Team's thoughts: see http://www.eset.com/threat-center/blog/2009/12/14/que-sera-sera-%e2%80%93-a-buffet-of-predications-for-2010.

ESET Latin America published its thoughts (in Spanish) at http://eset-la.com/centro-amenazas/2256-tendencias-eset-malware-2010.

This document combines the thoughts of both teams into a single paper, proposing a comprehensive vision of how the threatscape is likely to evolve in 2010.

A briefer summary of our combined thoughts was included in the December 2009 Global Threat Report at http://www.eset.com/threat-center/index.php. For a more cynical view, you might want to check out "Top Ten Trite Security Predictions" (http://www.eset.com/threat-center/blog/2009/12/30/top-ten-trite-security-predictions); however, this document takes a rather more sober standpoint.

David Harley, FBCS CITP CISSP
Director of Malware Intelligence, ESET, LLC

Introduction

As you will have guessed from the title, we believe that cybercrime is very much the "shape of things to come". ESET Latin America's document forecasts the continuing shift of the most malware attacks to the Internet. The team also predicted that during 2010, crimeware[1] will be the most commonly used attack vector. The cyberattackers' inclination to make money from their activities has found a natural ally in the criminal underworld. For this reason we expect to see a clear upward trend in malicious code created with profitability in mind.

Cybercrime is on the rise, not only in terms of the number of perpetrators and the volume of crimes committed, but also of the range of techniques employed to carry them out. In this environment, malicious code offers a valuable resource for those wishing to perform attacks through the Internet and information technology.

Crimeware

Crimeware involves a complex ecosystem, including criminal organizations and individuals, botnets (networks of Trojan-infected computers exploited by a remote attacker), and ever-increasing attacks on individuals, companies and systems.

Whether the profit is made directly (using scams or bank Trojans), indirectly (via spyware and botnets, among other approaches), or by the theft of confidential information, any of these objectives is motivation enough to create malware and endanger the user, his money and his data.

It is believed that during 2010 the highest threat based on malicious code will be crimeware: specifically, malware specially developed with the intention of making a profit and which can cause harm to the user's financial well-being or valuable information.

The term crimeware is considered here to identify any illegal activity committed using a computer or other information technologies, or when the computer or information resource is the target of the criminal activity. Many of the offenses that have existed in some form since ancient times are performed today using computer resources, but there are also crimes that are more or less specific to the online world. Malicious code may be among the most valuable resources available to a criminal, and may be applicable in both these areas.

High propagation rates, the ability to control computer systems remotely and steal information through botnets, along with the ability to modify the configuration of target systems, are among many other actions that malware may perform; all these factors make it possible to commit serious crimes, in particular those involving the theft of online data or money.

It is therefore to be expected that malware falling into this category will increase in overall quantity, but also in proportion to other types of malicious code.

Botnets

At present, botnet networks[2] are one of the most important cybercrime resources, since they allow a remote attacker to take control of infected systems, and manipulate them in order to execute malicious actions such as spam dissemination, Distributed Denial of Service (DDoS) attacks, and click fraud through the concerted use of whole populations of compromised PCs incorporated into a virtual network.

We can expect bot-compromised PCs and botnets to maintain and increase their current high volumes and malicious activity, since they offer a profitable area for malware developers. These botnets will continue to innovate in the use of technologies such as Fast-Flux and a range of communication channels such as social networks, encrypted communications or peer-to-peer networks. These trends will continue to replace previous communication channels through IRC (Internet Relay Chat) and, to a lesser extent, of HTTP communications using plain text.

Business Partners

Partnerka[3] is the name given to the Russian business networks that work together with attackers to accomplish some kind of malicious action: for example, spam distribution or malware propagation. Once the objective is defined, the attackers share resources and carry out their criminal activities through the Internet. These collaborations enable the implementation of more complex attacks, on a larger scale; furthermore, these attacks are more difficult to trace to their points of origin.

The trend toward malware administered and propagated by groups and networks of professionals will continue, while volumes of malware created by maverick individuals will continue to decline.

Malware Developed in Latin America

As a consequence of crimeware and the economic profits available to malware writers, during 2010 we expect to see even more malicious code developed in Latin America and aimed directly at Spanish-speaking victims in the region.

Bank trojans – first seen developed locally in Brazil and then spreading to Mexico and Argentina – will be particularly noticeable. Malware and phishing attacks will continue to be detected arising from across the region. In addition, the operation of botnet networks designed and administered from Latin America is likely to be more frequent, performing malicious actions that specifically target Latin American countries.

Targeted Attacks

Threats aimed at CIOs, CSOs, managers, directors, owners or the holders of other high-ranking corporate positions in companies are clearly intended to obtain money or marketable intelligence. Companies should be on the alert for targeted email messages sent to high-ranking executives. These are likely to carry highly malicious file attachments, or incorporate information requests based on deceptive social engineering. This is sometimes referred to as "whaling," by analogy with phishing. You might say it has the same relationship to phishing that real whalers have to riverside anglers.

Since they are not reported on a massive scale, such attacks are not normally included or stressed in campaigns to raise awareness of security issues, but their impact can be greater than more frequently observed attacks on less "important" individuals.

Targeted attacks (spear-phishing, whaling) will continue to be a significant (though currently underestimated) threat. At the moment, we're seeing such attacks moving away from Microsoft Office document formats toward Adobe formats, especially PDFs. This trend is likely to continue, at least until Adobe's patching and updating standards are as high as Microsoft's are nowadays.

There will also be an increase in the type of attack often called APT (Advanced Persistent Threat). These attacks usually rely on targeting rather than innovative technology. Among other tools, they frequently use malicious code specially designed to persist over time in the affected systems, without being detected. In general, their targets are large corporations, and their purpose is to steal confidential and valuable information.

Security Trends

New threats will have a major impact on security, and it will be extremely important, where possible, to have access to the tools necessary for dealing with them.

First, it is important to consider the current controversies concerning the effectiveness of Cloud Computing security solutions. Although it has been shown that a Cloud Computing-based security solution offers as many questions as answers regarding user protection [4] it is a safe bet that the debate will continue throughout 2010.

Secondly, the anticipated high volumes of adware, rogue software, and other types of potentially unwanted and potentially unsafe applications will continue to generate legal confrontations between security researchers and cybercriminals, as pointed out by Jurach Malcho,[5] the head of ESET's Virus Lab, in his very popular paper for 2009's Virus Bulletin conference. The attackers behind these threats and nuisances are no longer individuals, but organized networks of professionals who have recruited lawyers to confront security companies.

Various kinds of threat reference listing will be used more frequently in security solutions. Blacklisting (the blocklisting of malicious files or sites), whitelisting (lists of known legitimate files/sites), and greylisting (dynamic blacklist creation through heuristic methods) will be widely used to detect threats such as spam or malicious web sites in contexts such as HTTP traffic.

Social Engineering: Public Enemy Number One

Many existing computer threats have complex technical components. However, the use of social engineering [6] has been a hugely successful strategy for malware developers – and will continue to be so.

As operating systems and eventually applications become more secure through sound patching implementation, the easiest way to steal money or install malicious software will be to trick people into taking dangerous actions.

Hot Topics

A very common use of social engineering in the context of malware is to attract the attention of the potential victim sitting in front of the computer. A particularly effective way of achieving this is to make use of topics that have importance in people's lives, or which currently preoccupy the media, or even to invent eye-catching stories.

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, as ever, be used as hooks on which to hang social engineering attacks.

During 2010, threat propagation through social engineering will, as usual, make use of special occasions such as Valentine's Day and Halloween, and national holidays such as Independence Day. At the same time, gangs spreading malware will take advantage of particular hot topics to cover up their real objectives. Characteristic topics in 2009 included software updates, the election of President Obama in the U.S., and Fidel Castro's health. In 2010, malware designers will continue to take advantage of topics like the economy, money, countries facing crisis, job opportunities (http://www.eset.com/threat-center/blog/2010/01/10/bbc-click-net-scams-and-jobseekers) and other similar issues in order to persuade victims to execute infective files through social engineering techniques.

However, economic crises and global recession are still much used as social engineering hooks for phishing [7] attacks and other instances of fraud and theft.[8]

In June 2010, one of the most popular regular sports events, the soccer World Cup, will take place in South Africa. We can expect that this will be a widely exploited topic in social engineering attacks, due to the great interest it will inspire in many users. Fake news, holiday trip promotions, thematic gifts for special occasions and videos are just a few of the other topics we expect to see used to pique the interest of potential victims.

Despite those who say that user education is ineffective, it remains an under-explored option for mitigating social engineering.[9] It's unlikely that a psychological attack can be totally eliminated by technical means. On the other hand, it's always easy and resource-non-intensive to push responsibility back to the user and say "just be careful!" There are signs that user education in some areas is being taken more seriously, though: in anti-phishing education, for instance.

Vulnerabilities: OS Versus Application

Patch management will continue to challenge IT departments trying to strike a balance between the need to apply patches as quickly as possible for defensive purposes, and the risks of implementing insufficiently sound change testing and management.

At the moment, vulnerabilities in applications are a serious threat (arguably more so than operating system vulnerabilities). Third-party applications will continue to bear the brunt of vulnerability attacks as improvements in the security of operating systems will continue to drive vulnerability research toward applications like Safari, iTunes, Adobe Flash, Adobe Reader, many IM clients and other applications. Unfortunately, users are far less savvy about patching third-party applications than they are about patching the operating system. This vector will also decline in impact as mainstream application vendors learn to tighten their quality control and patching methodologies.

Part of this trend will be driven by adoption of Windows 7.
Computers that were sold with Windows XP (with a few exceptions, such as newer netbooks) are beginning to age and will be replaced with PCs that are supplied with Windows 7. The increased security in Windows 7 means that, for most criminals, tricking the user is far more viable than exploiting the OS. For example, Windows 7's move away from the misconceived, much misused Autorun facility will contribute to a gradual decline in INF/Autorun and related threats.

Windows 7

Toward the end of 2009, Microsoft launched the latest version of its operating system, Windows 7. This incorporates security improvements to counterattack the malware currently in existence. However, it is probable that in 2010 new malicious code specially developed with the intention of circumventing these measures will start to appear.

The appearance of this type of malware will grow slowly but steadily as the number of Windows 7 users increases, and potential victims abandon Windows XP, at the moment the most widely used version and the one most favored by attackers in recent years.

Expect also the emergence of multi-version malware capable of affecting users of both Windows XP and Windows 7, as is the case with bootkits,[10] a threat that allows infection in different versions of Microsoft operating systems.

Fair Game

Phishing and related attacks on online gamers will continue to be big business, though attacks on gaming consoles are likely to meet with limited success due to the restricted nature of their Internet connectivity. Online games, however, are a tempting source of targets, as virtual assets such as in-game currencies such as Linden Dollars or other valuable in-game resources can be re-sold for real money, especially in Asia.

Advertising and Malvertising

Online advertising allows the promotion of malicious sites on various web pages. The popularity of this attack among cybercriminals is demonstrated by the increasing appearance of malicious code advertised on legitimate web pages or flagged by popular search engines.

Also known as malvertising, the abuse of advertising to promote malicious content will increase during the next year. In 2009, this technique was most frequently used in the purchase of publicity material made with Adobe Flash, using malicious scripts to exploit vulnerabilities in certain versions of the Flash Player.

Broadly speaking, malvertising consists of placing publicity material on web sites or social networking sites incorporating a direct or indirect link to the installation of malicious software. In this way, each person visiting the web site where the online advertisement was placed becomes a potential victim.

Randy Abrams, in a recent blog at http://www.eset.com/threat-center/blog/2010/01/06/malvertising, tried to answer the question: "If these attacks are being propagated through known and trusted web sites, what constitutes the best line of defense, particularly in the face of rapidly changing threats that may be unrecognized by security software?"

He suggested that in addition to being very picky about what you believe, download or run, it is important to keep your operating system and all third-party applications patched. Programs like iTunes, QuickTime, Flash and Acrobat are not Microsoft products, but frequently have had vulnerabilities that can result in the compromise of your computer just as surely as an operating system vulnerability. He recommends regular scans at http://www.secunia.com for home users, to make sure they know what they need to patch.

He continued: "Sometimes these attacks are propagated through trusted web sites. The advice to stick with known and trusted web sites is still excellent advice, but you have to realize there is always some degree of risk. It's great advice not to drink and drive, but it doesn't mean that you avoid all accidents by following that advice. Keep in mind that when you visit a trusted site and click on an advertisement, you are leaving the trusted site. Keeping informed about the latest threats and how to avoid them makes a lot of sense."

Jailbreaking: Breaking for the Border

While attacks on jailbroken iPhones may increase, they are likely to affect fewer people as potential victims become aware of the primary current attack vector, as this is a single, high-visibility vulnerability in a (significant) minority of systems. Additionally, in many cases, the affected user incurs data charges, and so they are motivated to do things like changing default passwords. Those who have flat rate data plans will be far more likely to continue to neglect security.

Nevertheless, there will be increased probing of mobile devices, in general, for exploitable vulnerabilities and for opportunities to make use of social engineering as described above. After all, many smart phones have somewhat comparable functionality to low-power systems such as netbooks, and, in many cases, are used as a supplement to larger systems. Why break out your laptop at an airport to log into Facebook if you can do it on your phone?

Indeed, phones and iPods are even used by many nowadays as their "primary" system, so these devices are an obvious target. Even in the corporate sector, however, where a smart phone is less likely to be the executive's only mobile device (let alone his or her only computer) the use of high-end mobile devices or smart phones is rising. These devices usually enable access to confidential corporate information and systems that may not be protected from less obvious vectors.

In general, iPhone attacks will probably be a blip rather than an increasing trend. However, attacks on smart phones as a general class of device are likely to increase as long as providers rely on a closed system whitelisting model that encourages jailbreaking/rooting. The rising interest in "rooting" other types of smart phone such as the Motorola Droid, thus breaking the whitelisting, will be examined closely by bad guys in search of a way in. Hopefully, the efficacy of whitelisting will probably be reviewed eventually, even by Apple, which seems content to rely on it absolutely at the moment.

A Question of Quarantine

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

ISPs will increasingly implement technologies to identify users who are infected and take measures to block their access to the Internet until their machines are cleaned up. It will probably be a few years before these ISPs are the norm, rather than the exception, but we still expect the prevalence of such practices will increase.

Data: the Breach and the Observance

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 between providers. Data breaches/losses will grow in scope as people put their data in the cloud. Cloud systems security is still fairly immature, but the aggregation of data will make many Cloud service providers attractive targets. We've already seen this as web-hosting providers and credit card-processing businesses have been targeted.

Data mining (legitimate and criminal) will have a wider and by no means automatically beneficial range of effects on individuals. The arch example is Facebook's lack of commitment to a realistic security model, which counts more for some people than its security center advice. Essentially, Facebook is encouraging its users to share as much information as possible, while essentially making them responsible for the security of their own data. This isn't unique to Facebook, of course, or even to Web 2.0 providers in general. But such actions are grooming us to accept that it's legitimate for an ever-wider pool of data to be used to monitor our behavior, and makes it harder to distinguish between legitimate and criminal data mining.

Privacy tends to diminish where it's in the way of commercial rather than political interests. So, ironically enough, there will be particular and ongoing interest in data leakage where it affects public bodies, but selling on information at the backdoor by more or less legal means will continue as it always has, though it's starting to attract some attention. This may be less true in Europe, where data protection and other directives *already* give some formal weight to the principle that organizations should only hold as much personal data as they *need*, rather than what they *want*.

Rogue Mail[11] (and Pop-ups, and Redirects, and...)

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. There will be an increase in rogue software or extortion software, probably fake memory optimization tools and so on. Rogue malware[12] has been — and in 2010 will continue to be — a particularly effective form of malware used by attackers as a multi-platform infection tool.

Spam and other manifestations of unwanted messages will continue to increase during 2010, as will the propagation of unsolicited adware through channels other than email, such as social networks, instant messaging systems or weblogs.

Malware as a Service (MaaS) will, more than ever, reflect the models of cooperation seen between specialists in the legitimate business world. There will be more specialization from malware gangs, and more exchange of services and roles between them.

There is likely to be more use of high-level languages (especially scripting languages) so as to repurpose malicious code across multiple platforms. More malware will target alternative operating systems like OS X and Linux as they increase their market shares. This probably means an increase in malware written in high-level languages and scripting environments are found on more than one OS, such as bash, perl and python. Platforms other than Microsoft Windows (more precisely Mac OS X and Linux) will be targeted by new variants of malicious code. In particular, the number of users of Apple's OS X operating system has multiplied during 2009, and this trend will continue.

Internet as Infection Platform

It is likely that the shift forecasted by ESET Latin America's team in the report[13] called "Tendencias 2009: Internet como plataforma de infección" (Trends for 2009: Internet as Infection Platform) will continue and become more noticeable during 2010.

The rise in connectivity rates will convince attackers to persist in the use of the Internet as their preferred medium for malware propagation and the infection of systems. At the same time, cybercriminals will also take advantage of the Internet to control and administer their organizations. There will be larger teams of attackers working in unison, taking advantage of the opportunities offered by dynamic, anonymous and safe communication through the Internet. As already described, legitimate but insecure web sites will continue to provide an effective propagation channel for malware creators.

Attacks that manipulate wireless connections will continue to flourish. Increased research into attacks on wireless networking (802.11n Wi-Fi, WiMAX, cellular broadband data connections) and SSL interception will make it more risky to conduct online shopping and banking over wireless connections (for example Man-in-the-Middle or MITM attacks for the theft of credentials).

Continued research into weaknesses in virtualization will lead to new attacks, but these will remain largely impractical to implement on a large scale, as the attacker needs direct access to a server's hardware in order to perform the attack.

Anti-Social Networks

Social networks will be targeted even more, both for social engineering attacks and in terms of probing for vulnerabilities. Targeted networks will include Facebook, LinkedIn, Twitter in the U.S., Orkut and Hi5 in South America, making use of cross-site scripting and worm attacks on those sites and their APIs (Application Programming Interface).

Social networks constitute an ideal means of malware propagation for cybercriminals. Computer users spend more and more time on this kind of activity (even work time), inviting attackers to use such networks in order to advertise malicious links.

The subversion of legitimate web sites and social networks[14] 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).

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 private sector.

References and Further Information

1. Crimeware, el crimen del Siglo XXI (Crimeware, the Crime of the 21st Century)
   http://www.eset-la.com/centro-amenazas/2219-crimeware-crimen-siglo-xxi;
   http://www.eset.com/threat-center/blog/2009/11/23/some-demographics-of-cybercrime-risk
2. Botnets, redes organizadas para el crimen (Botnets, Organized Crime Networks)
   http://www.eset-la.com/centro-amenazas/1573-botnets-redes-organizadas-crimen; "Net of the Living Dead: Bots, Botnets and Zombies" by David Harley and Andrew Lee
   http://www.eset.com/download/whitepapers/Net_Living_Dead.pdf
3. Partnerka: redes organizadas de negocios (Partnerka: Organized Business Networks)
   http://blogs.eset-la.com/laboratorio/2009/10/09/partnerka-redes-organizadas-de-negocios/;
   "The partnerka - what is it, and why should you care?" by Dmitry Samosseiko in Virus Bulletin International Conference Proceedings, 2009
4. ¿Nube o humo? (Cloud or Smoke?):
   http://blogs.eset-la.com/laboratorio/2009/09/29/computacion-nube-o-niebla/;
   Dissipating the Cloud, Randy Abrams: http://www.eset.com/threat-center/blog/2009/09/24/dissipating-the-cloud
5. Is there a lawyer in the lab? http://www.eset.com/download/whitepapers/is-there-a-lawyer-in-the-lab.pdf;
   http://www.eset.com/download/whitepapers/Lawyer_in_the_lab.pdf
6. El arma infalible: la Ingeniería Social (Social Engineering: The Infallible Weapon)
   http://www.eset-la.com/centro-amenazas/1515-arma-infalible-ingenieria-social;
   "Social Engineering" by Cristian Borghello, translated by Chris Mandarano:
   http://securingourecity.com/resources/whitepapers/Social_Engineering_Borghello.pdf
7. http://www.eset.com/download/whitepapers/Phish_Phodder.pdf;
   http://www.eset.com/download/whitepapers/Pretty_Kettle_of_Phish.pdf
8. http://www.eset.com/download/whitepapers/Harley-Debrosse-VB2009.pdf;
   http://www.eset.com/download/whitepapers/From_Fun_To_Profit.pdf
9. People Patching: Is user education of any use at all" by David Harley and Randy Abrams, at
   http://www.eset.com/download/whitepapers/People_Patching.pdf
10. Nueva generación de rootkits (New Generation of Rootkits):
    http://blogs.eset-la.com/laboratorio/2009/09/25/nueva-generacion-rootkits/; Building malware defenses: From rootkits to bootkits - Noah Schiffman: http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1270250,00.html
11. http://en.wikipedia.org/wiki/Rogue_Male_(novel)
12. "Free but Fake: Rogue Anti-malware" by Cristian Borghello
    http://www.eset.com/download/whitepapers/Free_but_Fake.pdf
13. Tendencias 2009: Internet como plataforma de infección
    http://www.eset-la.com/centro-amenazas/2001-tendencias-eset-malware-2009;
    http://www.eset.com/threat-center/threat_trends/Global_Threat_Trends_December_2009.pdf
14. Utilizando redes sociales para propagar malware (Using Social Networks for Malware Propagation)
    http://www.eset-la.com/centro-amenazas/2034-utilizando-redes-sociales-propagar-malware

www.eset.com

ESETRCAWP20100127