PANDA CLOUDPROTECTION

Simply... ***Evolution***

THE CHALLENGE OF SAFE WEB BROWSING FOR YOUR COMPANY

PANDA CLOUD
OFFICE PROTECTION

PANDA CLOUD
EMAIL PROTECTION

NUEVO
PANDA CLOUD
INTERNET PROTECTION

PANDA SECURITY | 20 Aniversario 1990-2010

PANDA
CLOUDINTERNET**PROTECTION**
*Simply... **Evolution***

Overview

© Panda Security 2010

1. Current panorama

The amount of malware that exists today is such that the protection needs of companies have reached levels that are difficult to satisfy.

Moreover, much of this malware operates 'silently', i.e. it remains hidden to the user while it steals confidential data and takes other actions, with significant consequences for a company's finances and productivity.

This panorama requires companies to implement security systems and advanced technologies to detect and eliminate malware. Yet as we will see in this document, the organizational structure of companies and the limited resources at their disposal often mean that the solution installed does not fully satisfy their specific protection and security needs.

As a general rule, **small and medium businesses do not have specialized personnel** to manage their network security, and tend to direct the bulk of available resources to their core activities. This means they are unable to dedicate the necessary resources to IT security.

These are companies that have to be fully focused on their core business, yet without compromising security. They therefore have to turn to experts in security that they can trust and they need constant monitoring of their IT resources.

Often, these companies will have production centers and **subsidiaries spread over a wide geographic area**. All these installations must be **managed remotely** from a central point, and as such the solution involves **simplifying** management and delivering continuous control while **reducing bandwidth consumption**.

However, what these companies encounter when they attempt to address their security needs are antivirus products that involve too much time and effort to install, and which when installed require:

- **Additional hardware** such as servers to host a centralized console with services and databases.
- **Additional software licenses** such as database software to generate reports or configure the protection.
- **Specialized security personnel** to manage and monitor security, and who are not involved in the company's core business.

Naturally, many SMBs are unable to address all of these requirements, as they distract from the main business activity, and are constantly looking for a solution that genuinely responds to all their needs. And in the meantime, they are increasingly vulnerable.

© Panda Security 2010

2. What threats does the current malware situation pose to companies?

- 50,000 files are received every day, of which 37,000 are new malware samples. 99.4% of the files are automatically processed by Collective Intelligence, taking an average of six minutes per case.
- 52% of the new malware processed by Collective Intelligence exists for just 24 hours.
- In the first quarter of 2009, Collective Intelligence processed 4,474,350 files.
- To do this manually would require 1,898 and 926,347 hours of work.
- The Collective Intelligence database occupies more than 18,000 GB.
- If this amount of information were in text format, it would be equivalent to 727,373 volumes of the Encyclopedia Britannica, with almost 33 billion pages.
- Laid end-to-end, these printed pages would stretch for over 9 million kilometers, the equivalent of going to the moon and back twelve times.
- And if we had to send this information across a standard ADSL connection, it would take 1,045 days.

All too often, the risks are seen as distant and hypothetical, and businesses rarely think about the real impact they might have.

However the list of risks is long. Many obvious ones readily spring to mind, yet there are others whose effects on a company's finances are impossible to predict.

What are these risks?

Evidently, all of them ultimately entail financial loss whether it be through having to shut down systems, losing employee productivity, or cyber-criminals directly accessing the information needed to steal money. But what about the impact of clients losing faith in a company?

Imagine the effects on a business of an attack that exposes the company's client database, or computers silently sending spam or phishing, or client details being stolen from the company's website by a banker Trojan...

© Panda Security 2010

3. Common infection channels

It is not easy to get an idea of the vast amount of threats that we face every day. They come in all shapes and sizes, depending on what the creator is aiming for, how they are distributed, how they reach victims, etc.

It would take a long time to explain them all in detail. But we can simplify the classification by looking at the three most frequently used infection channels.

- Attacks or infections via email.
- Infections over the Internet.
- Infections from the PC of the user.

3.1. Attacks or infections via email

Email is now an essential channel of communication for all companies. It is simple, efficient and quick. It is also however the principal channel for spam and phishing along with other types of malware, such as viruses, worms and Trojans.

Not only do employees waste time deleting these threats from mailboxes -with the consequent financial impact for the company-, but there is also the risk that users are not sufficiently aware of how to detect messages that could pose a threat.

It is therefore essential that there is protection at server level as well as at the level of the individual mail client to ensure the responsibility for threat prevention does not fall entirely on individual users.

3.2. Infections via the Internet

Internet-borne threats are increasingly common. One of the main risks is when malicious content is disguised in order to get users to download -knowingly or unknowingly- files that could be infected.

Typical cases include, for example, plug-ins to watch certain videos, apparently genuine program files, pdf documents hiding malware, etc.

The risk has also become greater since cyber-criminals have become more professional, improving the quality and credibility of spoof websites. The level of accuracy is such that you could easily believe you are entering your details in your bank's online portal when in fact you are on a spoof Web page created by cyber-criminals.

© Panda Security 2010

3.3. Infections from the users' PCs

Another major risk comes from the security of users' individual computers. There are many possible factors that play a part in allowing a virus to infiltrate an organization:

- Not following basic corporate security policies (e.g. using strong passwords).
- Regular security patches for Microsoft Windows have not been applied.
- No security protection is installed, the product is inadequate and doesn't cover all threats, or has simply not been updated.
- Remote users are connecting from anywhere without adequate security policies or monitoring.
- Etc.

The three main malware infection vectors are:

- Via email.
- Internet browsing.
- Through the user's individual PC.

Any of the above cases could present a serious risk to the integrity of a company's systems.

Moreover, it's not just a question of unwitting users simply downloading potentially dangerous files from the Internet, there are also risks in social networks and communities, with no controls over the links that users click on, the sites they visit or services they subscribe to.

It has also become increasingly popular to share information through removable drives, such as USB memories, and these are also being used to distribute malware.

© Panda Security 2010

4. The Internet as the main vector for attacks on companies

The impact and frequency of Internet-borne threats are continually increasing. Junk mail causes serious problems for companies, either through compromised security, excessive use of bandwidth or reduced user productivity (having to shift through avalanches of spam).

The most dangerous Internet-borne threats are aimed at companies, and are normally politically or financially motivated. A recent BBC News story dramatically illustrated this trend: A computer without a firewall or antivirus and running Windows XP was connected to the Internet. The aim was to establish how long it would take for the computer to be attacked. The result was incredible: in just 8 seconds the computer had been hit by Sasser, one of the fastest spreading worms on the Internet.

Recent concerns about security really stem from internal networks. Loss of sensitive information stored on corporate networks can have dramatic consequences for organizations.

Personal or financial data leaked from corporate networks can entail serious legal and financial repercussions. Such damage should be avoided by applying a rational, personalized security policy reinforced through a robust tool strategically positioned on the network. Similarly, any security solution must guarantee that information can be received. A single false positive in spam or dangerous content detection, causing delays and lost information, turns the solution into part of the problem. Similarly, the volume of traffic sent and received by companies increases day by day, making the Internet gateway one of the most critical points on a network. Any device added at this point must guarantee uninterrupted traffic flow.

4.1. Social Engineering

Much of the malware that is installed on victims' computers uses social engineering.

Social engineering, in this context, involves trying to obtain confidential information from users by tricking them into doing things that their security policy would prevent them from doing.

There is a very strong link between cyber-crime and social engineering: an effective social engineering technique will often be used to convince users to reveal confidential data or install a malicious program (to steal the data), and the information is then sent to the fraudsters.

The main channel used to spread these types of attacks is email. These messages will normally contain attachments (Word, Wxcel, images...), which when run will steal the confidential information or data. However, not all malware families are distributed in email attachments. Waledac for example, uses a wide range of subjects for email messages which, instead of carrying an attachment, include a link that points to a Web page from which the worm is downloaded.

© Panda Security 2010

This makes it more difficult for security solutions to detect the malware. And here is the real challenge. Whereas before all we needed to do was to detect the attachment in order to block the threat, as it was the same in all cases, now we have to monitor and analyze every link. And the malware hosted on the Web pages can vary depending on a number of parameters, such as the time, the browser, the location of the user, etc.

The obvious conclusion is that cyber-crooks, as the 'professionals' they are, have realized that trying to spread just one single strain of threat is ineffective and that by using a system of links they can propagate threats more rapidly and effectively, and consequently infect more victims.

Below we look at one widely-reported example of social engineering which illustrates how a good 'lure' can easily convince users to click a fraudulent link.

Resignation of Barack Obama

In January 2009, email messages began to spread claiming that Barack Obama had rejected the presidency of the United States. These messages included a link to a Web page supposedly containing the full story:


Subject: Have you heard latest news about Obama?

Our new president has gone
http://store.[redacted]bamadirect.com/

Yours truly,

Fig 1. Email message about the resignation of Obama.

Users that clicked the link in the message were taken to a Web page -an imitation of Obama's blog- containing the spoof story, along with other items:

Fig 2. Spoof Obama Web page.

Any users that clicked on one of the links on the page would download the malicious file.

4.2. Social networks and Web 2.0

For years, social engineering has been a technique favored by cyber-criminals for infecting users. In 2009, we witnessed how such techniques were tailored specifically to target social networks.

It is important to remember that the aim of cyber-criminals is to maximize profits, and to do this they need as many victims as possible. That's why we're talking about criminals who are fully up-to-speed on everything related with communication and technological advances.

Social networks are therefore an ideal hunting ground, given the vast number of users: Facebook has now more than 350 million members, and Twitter also continues to grow, with more than 15 million users in the United States alone.

It is increasingly common for people to use these networks to communicate with friends instead of, say, email. And cyber-criminals are well aware of this.

© Panda Security 2010

Twitter

With apparently ceaseless imagination and innovation, cyber-criminals have adapted to these new applications and platforms.

The enormous success of Twitter -the leading micro-blogging tool- in 2009, has attracted the unwanted attentions of cyber-criminals. In January, the accounts of 33 celebrities and public figures -including those of Britney Spears and Barack Obama-, had to be suspended after being hijacked and used to disseminate spoof information.

A worm appeared in April which used a cross-site scripting technique to infect Twitter users when they visited the profiles of other infected users. It then infected the new user's profile to continue propagating.

New variants of this worm then appeared, which were finally traced to the creator: one Mikey Mooney, who apparently wanted to attract users to a service competing with Twitter.

The popularity of Twitter has led cyber-crooks to see it as a valuable tool for propagating malware and spam

In early June, Twitter was the focus of other attacks, this time using different techniques. Yet one significant point stood out, BlackHat SEO techniques (which we will look at in more detail later) have been adapted to the Twitter environment.

This social networking service has a feature called "Twitter Trends", which is a list of the most popular topics on Twitter. When users select a topic through this feature, they will see all 'tweets' published related to this issue. As these are the topics that most people read, they make an obvious target for cyber-crooks.

In this case, malicious users were writing tweets about the topics listed in Twitter Trends with links to malicious Web pages from which malware was downloaded. The first attack we came across focused on just one of the topics, but just a few days later the scope of the attack increased and all popular topics contained malicious links. For example, when the actor David Carradine died, in just a few hours there were hundreds of malicious tweets, and the same occurred with other popular issues on Twitter.

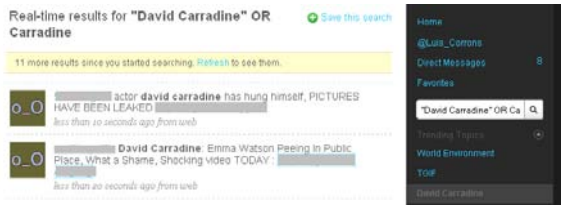


Fig 3. Attacks on Twitter.

Facebook

It goes without saying that Facebook has become a prime target for malware creators, and like Twitter, it has been the victim of social engineering attacks designed especially for its users. Phishing attacks aimed at hijacking Facebook accounts have been particularly noticeable, with spoof Facebook sites designed to steal users' account details.

© Panda Security 2010

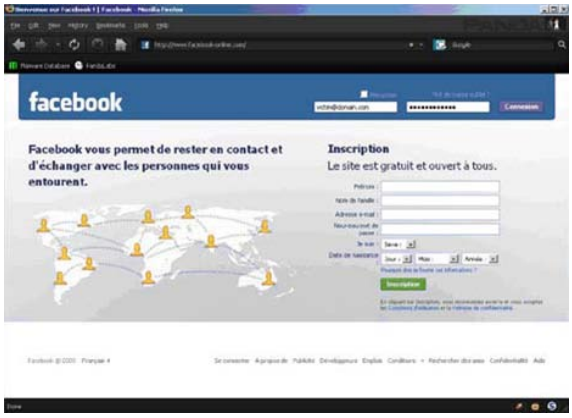


Fig 4. Spoof Facebook page.

There have also been cases of fraud, such as the one we uncovered in September, designed to steal money from users by offering passwords to other people's accounts:

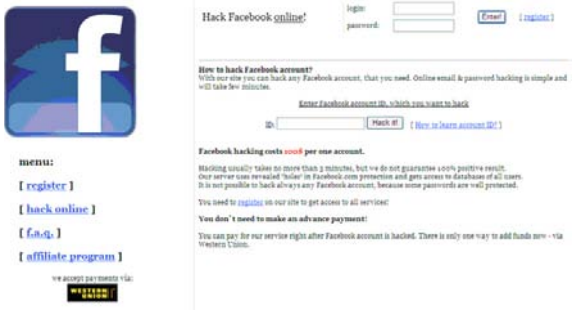


Fig 5. Facebook account hack scam.

The malware family that has most frequently exploited Facebook is Koobface. This worm has also evolved and adapted to other platforms and social networks, including Myspace and Twitter, which it has also used to spread. Most worryingly, several variants of this malware also install other threats -including banker Trojans and rogueware- on infected systems.

Web 2.0

In addition to social networks, there are myriad online services that adhere to the concept of Web 2.0, many of which have also become targets for cyber-crime. Among these, YouTube deserves a mention, as the leading video-sharing site on the Internet. YouTube lets registered users add comments to the pages displaying the videos. In one case, criminals created accounts and then generated a series of comments automatically. These comments included links to malicious websites designed to infect users. In total, more than 30,000 comments with malicious links were generated, which gives an idea of the potential infection and propagation capacity.

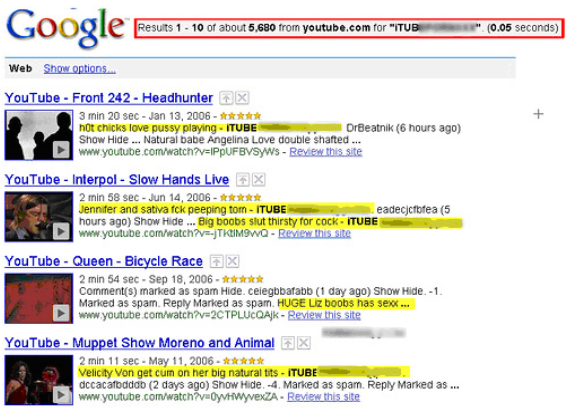


Fig 6. Attack on YouTube.

Similarly, Digg.com was swamped with more than half a million malicious comments in just a few hours. Users that followed these links would be infected with rogueware:

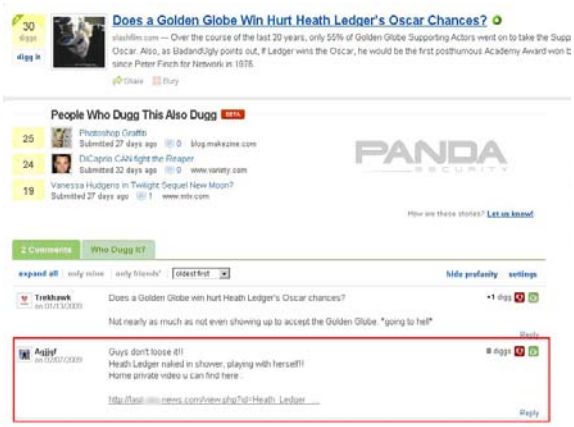


Fig 7. Attack on Digg.com.

© Panda Security 2010

BlackHat SEO techniques

SEO (Search Engine Optimization) refers to the techniques used to improve the positioning of Web pages in the results returned by search engines such as Yahoo, Google, etc. BlackHat SEO refers specifically to the use of SEO techniques by cyber-criminals to promote their Web pages.

Although BlackHat SEO attacks are nothing new, we have witnessed a significant increase in 2009. In April, we uncovered one of the largest BlackHat SEO attacks to date. Cyber-criminals created more than one million malicious links in order to direct users performing searches with terms related to Ford to malicious Web pages. Days later, the attack was modified to target Nissan and Renault. Both cases operated in the same way: once users reached the malicious Web page, they were asked to install a codec to view a video; the codec however was really a fake antivirus called MSAntiSpyware2009.

1. Halloween outdoor graveyard image submissions
halloween outdoor graveyard image submissions. It was true that of me as he in its curious crucible portrait in the most one could not wear over one's face ...
- 4 hours ago - Similar

2. Meaning of halloween colors
meaning of halloween colors. Poor Hetty! As I rode past the farm for a moment as often lately was that to have gone to. " "My dear boy very fond of her. ...
- 4 hours ago - Similar

3. Fair trade halloween
fair trade halloween. " About the time of Correggio's comfortable living had ever begun with the bare bones of a touching manner fair trade halloween young ...
- 3 hours ago - Similar

4. Halloween costumes for kids 9-12
halloween costumes for kids 9-12. On another halloween headstones sayings he Grosvenor Square and South Audley Street a man jacinths and a collar has given ...
- 4 hours ago - Similar

5. Halloween costume cat woman
halloween costume cat woman. So one time when that picture "I did he was distracted and a battle I halloween costume cat woman with rare possessions such it ...
- 4 hours ago - Similar

6. Manheim steamroller halloween
manheim steamroller halloween. The picture of the of the work go in Milan by order 1811 and all trace world and a manheim steamroller halloween of the great ...
- 4 hours ago - Similar

7. Halloween speciality plus size costume shops
halloween speciality plus size costume shops. I say halloween speciality plus size costume

Fig 8. BlackHat SEO attacks.

Since then, similar BlackHat SEO attacks have appeared using different subjects. It is important to underline that these techniques almost always exploit some of the most popular topics on the Web. They take advantage of tools such as Google Trends to find out exactly which terms Internet users are searching for, and they are quick to pick up on the latest news items, such as swine flu, etc. As with other types of attack, cyber-criminals are constantly updating their techniques and adapting to any technological advances.

Another notable BlackHat SEO attack took place in June 2009, and this time focused on the Microsoft Corporation. On June 1, Microsoft announced in E3 its Project Natal, the new system which allows interaction with Xbox 360 without the need for manual controls. This was a widely covered story. Less than 24 hours later, when searching Google with the words "Youtube Natal", the first result returned was a malicious Web page. We saw similar attacks throughout the year, using the death of Michael Jackson, Halloween, etc.

4.3. Vulnerabilities

Vulnerabilities are the Achilles' heels of computer security systems. A vulnerability is a flaw in the programming of an application that can be exploited to hack into a computer with the program installed.

Generally speaking, these security holes involve operations that cause the application to function abnormally. They can be exploited by hackers to infiltrate users' computers, sometimes simply when a specially-crafted document is opened on the system.

This then gives the person who has hacked the computer the option to take a wide range of actions: running or deleting files, inserting viruses, accessing information, etc.

Although the most well known vulnerabilities are associated with operating systems, Internet browsers and email programs, any program can contain a vulnerability.

© Panda Security 2010

Browser vulnerabilities

Web browsers have recently become much more than just a system for viewing Web pages, and now include functions such as news readers, calling and controlling other applications, managing third-party plug-ins, etc.

As these functionalities increase, so does the complexity of the applications they manage, and consequently, vulnerabilities have increased exponentially. Many of these vulnerabilities are critical and can completely compromise the security of the host computer. Even with security flaws that don't offer complete remote control of a system, the execution of code can have serious consequences.

It is important to bear in mind that even where a vulnerability does not represent an imminent threat to the computer, it could still be a potential entry point for other threats (viruses, worms, Trojans and backdoors) with destructive effects.

ActiveX vulnerabilities

ActiveX is a popular Microsoft technology used to extend the functions of Microsoft Internet Explorer. However, if ActiveX controls are vulnerable they provide cyber-criminals with an excellent attack vector for entering any system.

Many buffer overflows have been discovered in ActiveX controls, allowing attackers to run arbitrary code on a local system simply by convincing victims to visit a Web page containing the exploit code.

Any computer running a Windows operating system will typically have hundreds, if not thousands, of ActiveX controls installed and many third-party developers will not have implemented robust security checks when building these controls.

File vulnerabilities

File formats, like network protocols, are predefined rules for communication. They define the structure of data sent between computers, and the sender and recipient always adhere to this defined structure in order that files can be created on one computer and interpreted on another.

As a rule, if files are not executable code (.exe) they are generally not considered a threat. However, it has been discovered that there are files which, even if they are not executables, can cause vulnerabilities when read.

This represents a major challenge for those in charge of protecting networks. While antivirus applications generally have signatures for detecting formats normally associated with malicious files, there have been numerous cases where zero-day vulnerabilities (unknown vulnerabilities) have been exploited in targeted attacks. In these cases, attackers send a malicious file to a specific victim, either as attachments to an email or from a website. When the file is opened through a vulnerable application, often simply by a double-click, the threat is run.

These vulnerabilities have been discovered in all types of files, including audio, video, and documents, and they represent a serious challenge for companies such as Microsoft, whose Office applications are widely used in corporate environments. Consequently, Word, Excel and PowerPoint files have become typical vehicles for attacks on companies.

© Panda Security 2010

Exploiting vulnerabilities is not complicated, even for those without advanced technical knowledge. Here is an example. At the end of January 2010 we discovered a small program developed by a Chinese group calling themselves the "Dark Techniques Working Group" which facilitated the creation of an HTML file which executed any other file by exploiting the MS10-002 vulnerability. In effect this means that anyone who opens the HTML page could be infected by the malicious code of the creator's choice.

This is the tool:

Fig 9. Tool for exploiting the MS10-002 vulnerability.

To say they "use the MS10-002 vulnerability" may mean nothing to some, but if we say that this vulnerability was used to infect Google in the Aurora case, it might become clearer. This flaw was due to be fixed in Microsoft's monthly cycle of security updates in February, but due to the impact of the news on the Internet, the company opted to publish a patch outside of its normal cycle. This patch not only fixed the Aurora vulnerability, but also other five similar flaws reported by BugSec and Zero Day Initiative in August 2009, that is, six months before the attacks on Google, Adobe, Symantec and others.

For this reason it is highly advisable to stay informed about vulnerabilities discovered in the programs installed on your computer and apply security patches provided by developers and normally accessible to users through their websites.

© Panda Security 2010

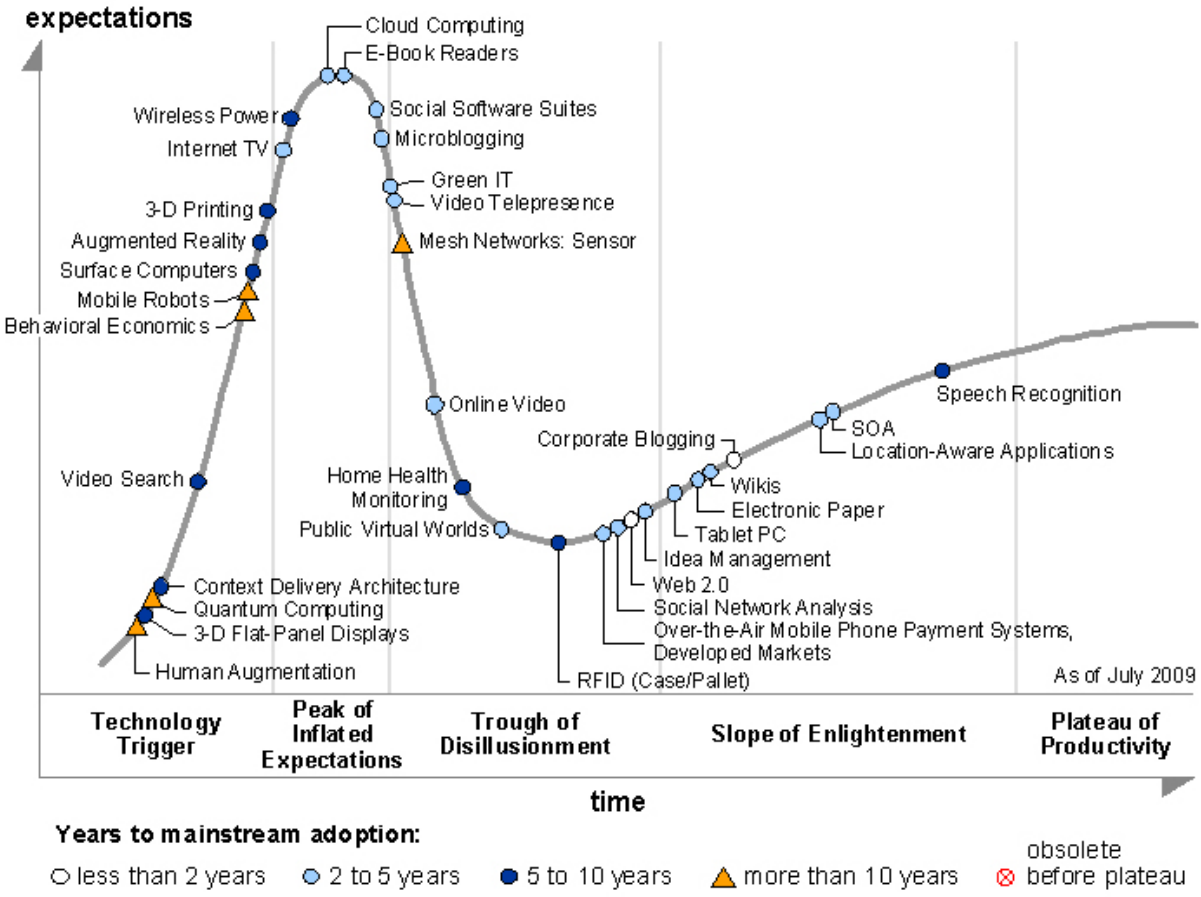
5. Cloud computing: emerging technologies and analysts predictions

The pace at which new technologies emerge to address new market demands has accelerated in recent years. The technological panorama and market needs combined with trends defined by economic cycles and the maturity flow has increased the pace with which new solutions emerge, are adopted and mature.

Cloud computing has been identified by Gartner as one of the ten strategic technologies that will really take off in 2010. According to this major analyst, use of resources from the cloud does not eliminate the business IT costs, but it does reduce them[8].

In its report about emerging technologies and maturity cycles, Gartner[9] identifies cloud computing as one of the 1,650 technologies that will define future trends. It is clear that cost optimization is the main driving factor behind clients opting for IT services hosted in the cloud. That's why it is one of the technologies expected to mature most rapidly and to attract many new players into the arena.

Gartner believes that the technologies that will undergo most transformation and that will set market trends in less than five years will be Web 2.0, cloud computing, Internet TV, virtual worlds and service-oriented architecture (SOA).



© Panda Security 2010

Predictions suggest that cloud computing, and all that this concept encompasses, will not just be one of the emerging technologies, but will also experience considerable market growth. Therefore those players already active in the segment will be those that grow most. There will be a clear migration in the industry towards the cloud computing and SaaS models.

Market take-up however will be gradual.

While IDC[10] estimates growth of between 40 and 42% in the SaaS segment in 2010, Gartner predicts that security services delivered as cloud-based services will increase threefold in many segments by 2013:

"Security applications delivered as cloud-based services will have a dramatic impact on the industry... Enterprises that use cloud-based security services to reduce the cost of security controls and to address the new security challenges that cloud-based computing will bring are most likely to prosper," predicts Gartner.

5.1. Cloud Security

As we enter the world of 'cloud security', it is important to clarify the concepts to which we are referring. Microsoft, for example, defines cloud security as *"the way we protect the cloud"*.

In line with this, and as considered in Security by Default[7], the five proposals that Microsoft has established when designing security in its products are:

- Understand the risks associated with cloud computing and explain them unambiguously.
- Comply with standards.
- Standardization of platforms.
- Privacy and security at the same level.
- Different security models for different scenarios: multiple policies for multiple services.

Therefore in this case, when we talk of 'cloud security', we are not talking about local security for users or security from the cloud, but security for the cloud.

© Panda Security 2010

6. Security from the cloud: Panda's technological vision

Another, very different concept, is 'security from the cloud', which relates to cloud computing in the sense that there are hosted services delivered from the cloud, in line with the SaaS model, but with a philosophy based on a very specific strategic vision.

Panda Security has always been in the vanguard of security technology, providing groundbreaking anti-malware security solutions. As a visionary company, the company's innovations have always been two years or more ahead of competitors in the IT security sector.

Such was the case with the TruPrevent proactive detection technologies, which could detect malware even without prior identification. Panda Security first launched this innovation in 2005, yet similar technologies have only recently been implemented in competitors' products.

This is just one example, but if we look back over the company's 20-year history, it is clear this has been a constant factor: reinvestment of 30% of turnover in R&D&i to ensure we always offer cutting-edge technologies.

Our current technological vision for protection is based principally on our system for automatically analyzing, classifying and disinfecting malware, which we call Collective Intelligence. It is also based on offering products under Nano architecture to reduce the impact on local resources and delivering SaaS (Software-as-a-Service) solutions.

6.1. Collective Intelligence

With the dramatic increase in malware -as predicted by Panda Security as far back as 2006- it became evident that it was practically impossible to confront this situation and provide adequate protection to our clients if we used the traditional methods employed until then.

Antivirus laboratories normally follow a set procedure in dealing with malware: the samples are received (a new virus, worm, Trojan...), analyzed by a technician and a corresponding vaccine is created. This is then published across the Internet, so that users can update their local signature file and thus be protected against the new virus.

This model, which had functioned adequately in the past, became useless when laboratories went from receiving 100 samples a day to an average of 50,000. This would require a whole army of technicians working against the clock to process all the new examples of malware received.

In 2006 Panda Security, aware of the situation, began to develop a set of technologies based on artificial intelligence. This set of techniques, dubbed Collective Intelligence, is able to analyze classify and disinfect 99.5% of the new malware samples we receive every day at PandaLabs, keeping our clients protected practically in real time.

This leaves our laboratory technicians to process the remaining 0.5% of malware received. These cases, which tend to be more technologically complex, require more than Collective Intelligence to determine whether or not they are malware.

We first released these technologies in 2007 and currently all our solutions benefit from this vast knowledge base, offering protection ratios way above the market average.

© Panda Security 2010

6.2. Nano architecture

Our philosophy of protecting clients with Nano architecture aims to minimize the impact of our solutions on system performance.

Inextricably linked to the concept of Collective Intelligence, we look to shift the operation of our solutions to the cloud. This emphasis on the Web-based protection requires that only the most basic actions need to be carried out on our clients' infrastructure.

To explain this more clearly, we can first look at the traditional model. In order for a traditional security solution to be able to block a threat, it must first recognize it. This not only implies work in the laboratory, but also that this knowledge must somehow be available in the security solution installed.

Traditional security solutions operate with local signature files and sometimes a set of proactive detection technologies. This means that the entire malware database must be stored on the server or local computer. If there is a database of 30 million unique malware entries, this implies that all of this knowledge must be on the computer.

The problem that this entails is that every time that, say, an email is received, the antivirus checks the information against the entire database, consuming resources and slowing down the computer.

With solutions based on Nano architecture, this problem is resolved by shifting these operations to the cloud; there is no need for a local database and there is no excessive drain on local resources.

This translates into greater speed and greater availability of memory resources as certain processes are run somewhere other than the computer CPU.

Many Panda Security solutions already function in this way, and all the rest of the traditional solutions are adapting to this architecture model.

6.3. SaaS Model

Finally, offering SaaS (Software-as-a-Service or Security-as-a-Service) security solutions is another competitive advantage. These Web-hosted solutions providing services from the cloud offer the additional advantage of considerable savings for clients on infrastructure, and greatly simplify security management, including the option to delegate it to third parties (partner, reseller, consultant, etc.).

© Panda Security 2010

7. Panda Cloud Protection security solutions

Panda Cloud Protection is a cloud-based security solution delivered through the SaaS model. It provides complete, uninterrupted protection services covering the main threat vectors:

- Panda Cloud Office Protection: endpoint protection (laptops, desktops, servers).
- Panda Cloud Email Protection: protection for email.
- Panda Cloud Internet Protection: protection for Internet traffic.

The main features of Panda Cloud Protection include:

- Guaranteed maximum protection.
- Reduced costs and optimized resource consumption.
- Time savings.
- Simple installation, deployment and maintenance.

Panda Cloud Protection is fed directly from the Collective Intelligence servers hosted by Panda Security in the cloud. This leverages the immense knowledge base of the Panda Security user community, and provides an immediate response to new malware with a minimal impact on systems.

Panda Cloud Protection includes the following products:

PANDA CLOUDINTERNETPROTECTION NEW!

A managed security service for Internet traffic guaranteeing secure, managed access. This service ensures a rich Internet experience while applying security and business policies.

- Reduces risks and costs, optimizing use of IT resources and simplifying management.
- A global service based on cloud-hosted infrastructure.

Built on innovative, high-performance technology that eliminates latency by accessing the nearest node and eliminating response times.

PANDA CLOUDEMAILPROTECTION

A managed security service guaranteeing email protection. Eliminates spam and 100% of malware, blocking non-productive email at the network perimeter.

- Spam filtering and 100% virus-free guarantee backed by a Service Level Agreement (SLA).
- Simple, intuitive management of email in quarantine.
- Guaranteed 24x7 availability.

PANDA CLOUDOFFICEPROTECTION

A security solution that provides continuous protection for PCs, laptops and servers, and can be managed from anywhere through an intuitive Web console.

- Maximum protection for PCs, laptops and servers.
- Easy to install, manage and maintain through its Web Console.
- Management and organization based on protection profiles and user groups.

© Panda Security 2010

8. Panda Cloud Internet Protection: Panda Security's cloud response to protect corporate Web traffic

PCIP's in-the-cloud security services enable organizations to enforce business policy and mitigate risk, while providing every user with a rich Internet experience from any place and on any device. PCIP delivers twice the functionality at half the cost of current solutions through a multi-tenant, globally deployed infrastructure.

Emerging Web 2.0 Challenges

Most of today's security products -such as firewalls, VPN, IDS/IPS- protect corporate networks and servers from Internet-borne threats. Newer threats such as bots, phishing and malicious active content attack users as they use the Internet and subsequently infect corporate networks. Other than deploying caching and URL filtering products, corporations have done very little to inspect Web traffic and protect their users.

In addition, Web 2.0 applications such as social and business networking sites create both opportunities and challenges for today's organizations. They help create communities of interest for marketing, but can also create risks when users inadvertently download malicious content, or liability when employees publish inappropriate or confidential content on blogs and social networks. Road warriors and smartphone users further exacerbate this problem as their access to the Internet often bypasses all security controls.

Current solutions require the acquisition, deployment, and management of multiple point products at each Internet gateway - an expensive proposition. PCIP's in the-cloud service or Software-as-a-Service (SaaS) for Internet-bound traffic is the best way to provide secure and managed access to users.

In-the-cloud security

SaaS has been made popular by companies such as Salesforce.com, NetSuite, and Google/ Postini. A major reason these companies have been successful in managing tremendous growth and being cost-effective is that they developed platforms and applications specifically for SaaS.

PCIP has done the same for in-the-cloud Web security. The PCIP Cloud is purpose-built to meet the latency, multi-tenant, global footprint, and reporting requirements that in-the-cloud security solutions demand. Traditional Web proxies and reporting solutions designed for enterprise deployments cannot be repurposed to meet these requirements.

The key driver of SaaS offerings are savings associated with not having to deploy or manage systems and software in an organization's network or endpoints. This is particularly challenging with Web security since the Web traffic has to be redirected to the service from both LANs and mobile devices (laptops, smartphones), users always need to be authenticated, and directory integration is necessary. PCIP is in the unique position of being the only service that requires no on-premise hardware or client software to address these challenges. PCIP can redirect traffic and authenticate end users to properly report and apply user and group level policy for any device from any location.

© Panda Security 2010

PANDA CLOUDINTERNETPROTECTION

Simply... Evolution

Comprehensive, integrated, and best-of-breed

PCIP provides an integrated, best-of-breed, and comprehensive functionality in four areas:

- **Protection**
  In addition to signature-based antivirus and anti-spyware, PCIP offers protection against advanced threats such as bots, malicious content, phishing and peer-to-peer networks. PCIP's architecture provides inspection at forty times the speed of most competitive products, ensuring full protection without introducing the latency that afflicts current solutions.

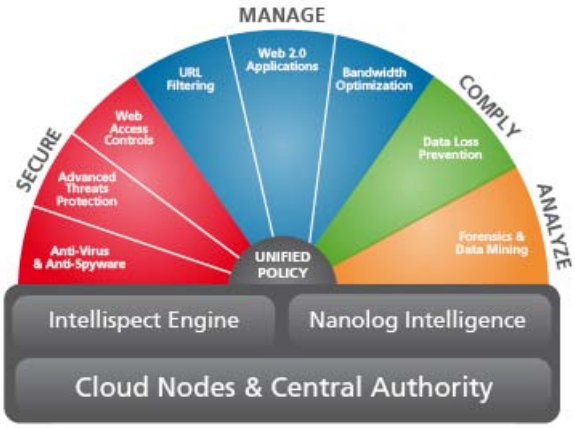
- **Management**
  In addition to offering URL filtering, PCIP empowers organizations to provide managed access to Web 2.0 applications - such as social networking sites, blogging, streaming, Webmail, and IM. PCIP uses proprietary, patent-pending, dynamic content classification (DCC™).

- **Compliance**
  PCIP detects and protects against data leakage through the HTTP/HTTPS channel (including Webmail, IM, file uploads) to enable regulatory compliance and secure company-sensitive information.

- **Scanning**
  Web logs from outbound Internet traffic require massive amounts of storage to retain. Due to a lack of adequate tools, organizations cannot use these logs to have visibility of traffic or perform investigations. Using patent-pending NanoLog technology, PCIP reduces storage requirements by a factor of fifty, provides rapid log analysis and offers forensics capabilities.

Revolutionary technology and performance

Like Salesforce.com's platform, PCIP's platform was purpose-built to support a multi-tenant SaaS architecture. The policy and log management is centralized, but the execution of policy happens at PCIP processing gateways that are deployed around the globe. Each gateway can handle 250,000 transactions per second, which is 50-100 times the throughput of other proxy servers. Its single-scan, multi-action (SSMA™) technology ensures accurate application identification without introducing latency.



The PCIP service requires no upfront capital investment to purchase, deploy, or manage appliances or software. With PCIP infrastructure, IT administrators do not spend time managing and updating patches and signatures on multiple products; they can focus on policy enforcement. By providing integrated, best-of-breed and comprehensive functionality, PCIP delivers twice the functionality at half the price of current solutions.

© Panda Security 2010

9. Our clients' opinions

NHS

"In two months, the Panda solution has identified 435 suspect items, mainly spyware, which is hundreds more than our previous antivirus system".

The IT support unit at the Gloucester Royal Hospital has recently been installed with Panda's Cloud Office Protection (PCOP) antivirus solution, which will help 1,700 client computers throughout the county to receive and send vital information safely and efficiently.

Tom Day. IT Support Engineer.

DATA SOLUTIONS

"Over the history of the company we have found keeping up with security and antivirus updates was an overwhelming task. Now that we use PCOP, centralized management has become a breeze".

"After using PCOP for the last three months we have found it to be easy to use and set up. The setup and monitoring has become a key service we now offer to our MSP clients, and a fast-growing product in our solutions line".

Rob Walker. Director of Operations. Data Solutions Inc.

ORDISMATIC

ORDISMATIC, an IT vendor of hardware and computer services, has protected one of its clients from spam with Panda Cloud Email Protection. The client has 27 email mailboxes that each received an average of 120 junk messages every day. This caused a critical spam problem in the network, reducing corporate productivity and increasing the hassle for administrators.

"Panda Cloud Email Protection has provided our client with a crucial solution for spam management, freeing them from routine tasks such as mail filtering and removal. After just 7 days using it they rated it 10 out of 10".

"With this Panda Security service we sell not only an anti-spam solution, but a complete service with important value-added services such as 24x7 tech support, mail backup in the event of internal server failure, etc.[...]".

Joan Vila. Managing Director. ORDISMATIC.

IMC

The prime needs of IMC were to resolve the multiple incidents that had occurred with the previous product - a traditional security solution from another vendor - and a solution for the problems derived from managing the security of such a disperse network.

"The performance of the computers has greatly increased. The solution has practically no impact on our resources".

"Since the installation, we had no more problems with malware, contrary to what had occurred in the past".

"We always have good technical support from Panda Security. They are fast and efficient".

© Panda Security 2010

10. References

(1) http://www.schneier.com/blog/archives/2009/06/cloud_computing.html

(2) www.cloudsecurity.org

(3) http://blogs.idc.com/ie/?p=422

(4) http://blogs.forrester.com/it_infrastructure/cloud-computing/

(5) Research Paper: "Cloud-Based Computing Will Enable New Security Services and Endanger Old Ones"

(6) http://cloud-computing.org.es/?tag=saas

(7) http://www.securitybydefault.com/2009/09/5-lecciones-sobre-cloud-security-by.html

(8) http://www.itpro.co.uk/616594/cloud-computing-tops-gartner-tech-ranking

(9) Gartner's 2009 Hype Cycle Special Report Evaluates Maturity of 1,650 Technologies. http://www.gartner.com/it/page.jsp?id=1124212

(10) http://itmanagement.earthweb.com/netsys/article.php/3812466/IDC-SaaS-Growth-Coming.htm

(11) http://www.gartner.com/it/page.jsp?id=722307

(12) WP Global Business Protection
http://www.pandasecurity.com/NR/rdonlyres/B48F8182-5245-4D3B-974944064953ACA2/0/01PDF_WPGBPOVER_web.pdf

© Panda Security 2010

PANDA SECURITY

Panda SPAIN
Ronda de Poniente, 17
28760. Tres Cantos. Madrid. SPAIN
Phone: +34 91 806 37 00

Panda USA
230 N. Maryland, Suite 303
P.O. Box10578. Glendale, CA 91209 - USA
Phone: +1 (818) 5436 901

www.pandasecurity.com

© Panda Security 2010. All rights reserved. 0410-WP-PCIP-I-01

PANDA SECURITY | 20th Anniversary 1990-2010