QUARTERLY REPORT PandaLabs (APRIL - JUNE 2009)

One step ahead.

Index

Introduction

Here we present the Q2 report, which examines some of the more interesting events of this quarter.

During this time we have detected two techniques used to spread malware-infected spam: e-cards and fake notifications from messaging companies. We will take a look at the malware families distributed in these messages.

Yet if there is one family of malware which is really flexible, changing the subject of messages to suit the circumstances, it is the Waledac worm. Valentine's Day, Obama rejecting the U.S. presidency and discount coupons are just a few of the message subjects used by this family of malicious code.

In the Vulnerabilities section you will be able to check out the vulnerabilities that have appeared over the last three months.

We also analyze the most important malware trends during this quarter. BlackHat SEO techniques have become more significant this quarter. Youtube and Twitter have been targeted, specifically to distribute malicious links. The increasing popularity of these services has not gone unnoticed by cyber-crooks.

Collective Intelligence is now two-years-old. We will explain what this technology consists of and will provide figures that demonstrate just how effective this innovative technology is in combating malware.

Similarly, as in previous reports, we will outline the evolution of active malware country by country during the first half of 2009 as well as the statistics for the last quarter.

We hope you find it interesting.

Executive summary

Infection levels of adware have remained relatively stable over the last quarter (19.62%). Trojans are still the most predominant type of malware, accounting for 34.37%.

Average active malware infection rates were 12.48% during the first half of the year, a drop of around two points from the total for 2008 (14.62%).

Once more Taiwan is the country with the highest percentage of active malware (33.63%), while Turkey and Poland come next with 28.96% and 27.54% respectively.

Over the last few months, security experts have warned of the increase in the sending of fake e-cards and spoof emails from messaging companies.

In April, over one million malicious links were created to redirect users searching for Ford-related issues to malicious pages. A few days later, the same happened with Nissan.

In May, Youtube accounts were created to automatically generate comments (over 30,000) with malicious links.

In June, Microsoft corrected a record number (31) of vulnerabilities since it started with its monthly cycle of security advisories.

Collective Intelligence is now receiving 50,000 files a day, of which 35,000 are new malware samples. 99.4% of the files are automatically processed by Collective Intelligence, taking an average of six minutes per case.

In the first quarter of 2009, Collective Intelligence processed 4,474,350 files.

Second quarter figures

Distribution of new threats detected

The graph below illustrates the percentages of different types of new malware detected by PandaLabs in the second quarter of 2009:

NEW MALWARE DETECTED IN Q2

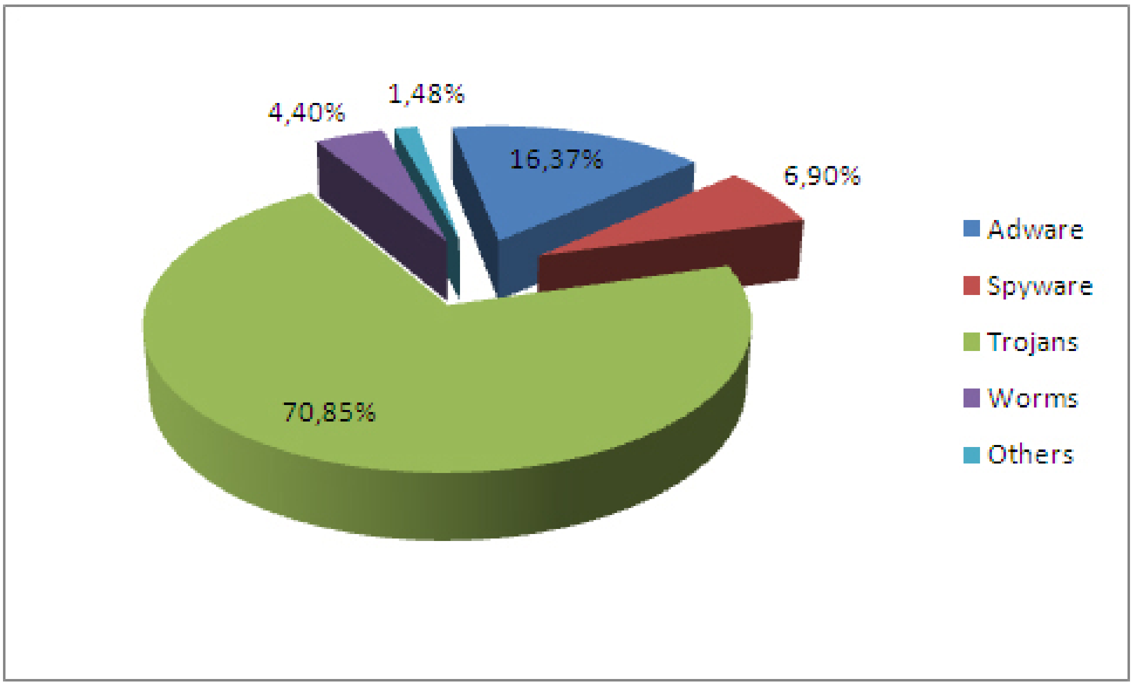


Fig. 1 Quarterly malware distribution

As illustrated in the graph, the predominant malware category throughout Q2 has been Trojans, even though the percentage (70.85%) has dropped almost three points compared to the previous quarter.

In these figures, backdoor Trojans have been included with Trojans and bots have been included either with worms or Trojans depending on their specific propagation techniques.

As for worms, their percentage has risen slightly, now accounting for 4.40% of all malware.

Malware creators are still focusing heavily on hybrid worm-Trojans, with the aim of exploiting the characteristics of both these categories to the maximum.

Second quarter figures

There has been a notable drop -more than six points- in spyware, which now represents just 6.90% of the total. In contrast, adware, rose almost eight points in Q2 2009, with a detection ratio of 16.37%.

This increase is directly related to the current vogue among cyber-crooks to create Rogue AV applications (fake antivirus), and the effectiveness that this type of malware is currently enjoying. We have grouped categories with low prevalence under the heading 'Other'.

OTHER MALWARE

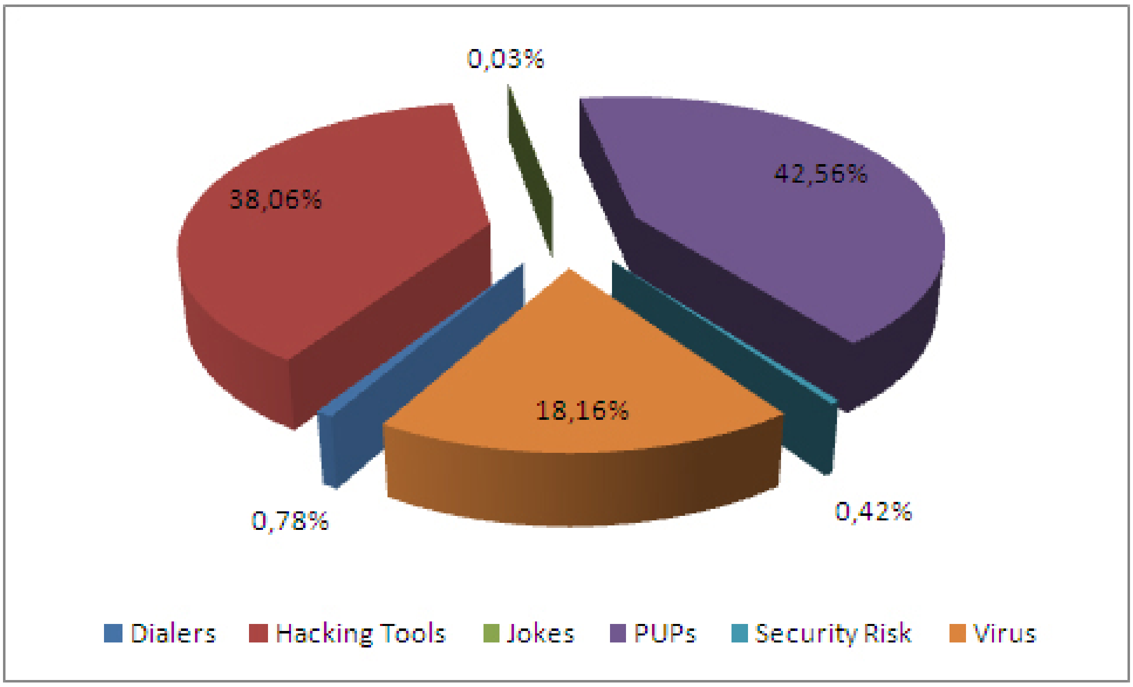


Fig. 2 Other malware

In this section it is clear that among the other types of malware, PUPs and hacking tools still predominate, with percentages of 42.56% and 38.06% respectively, despite the fact that both of these categories have fallen back slightly over this last quarter.

However, there has also been a significant rise in the number of viruses, increasing almost 10 points with respect to Q1 up to 18.6%.

Due to the steady decrease of dial-up Internet connections, the presence of dialers remains negligible (0.78%).

Second quarter figures

Month by month

Below you can see the appearance of new malware month by month, separated into the most important categories.

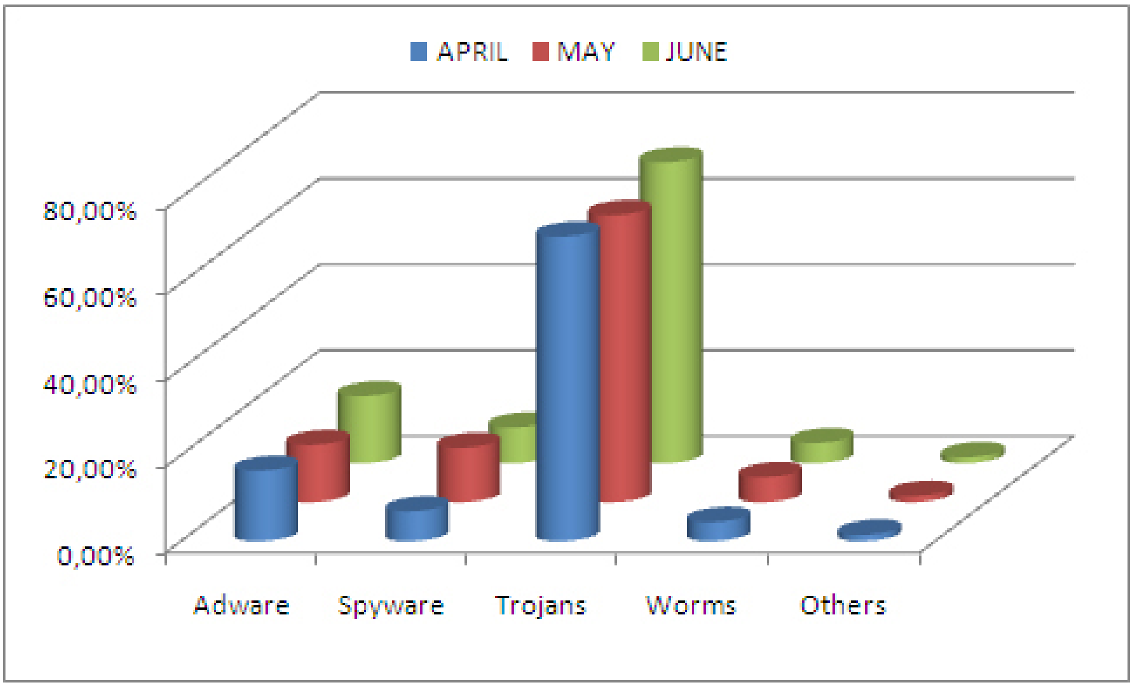


Fig. 3 Evolution of new malware

The most prevalent malware categories each month are those that provide the largest financial return to threat creators.

Second quarter figures

Threats detected by the PandaLabs sensors

The following graph shows the distribution of malware in accordance with detections made by the Panda Security sensors throughout the second quarter of 2009.

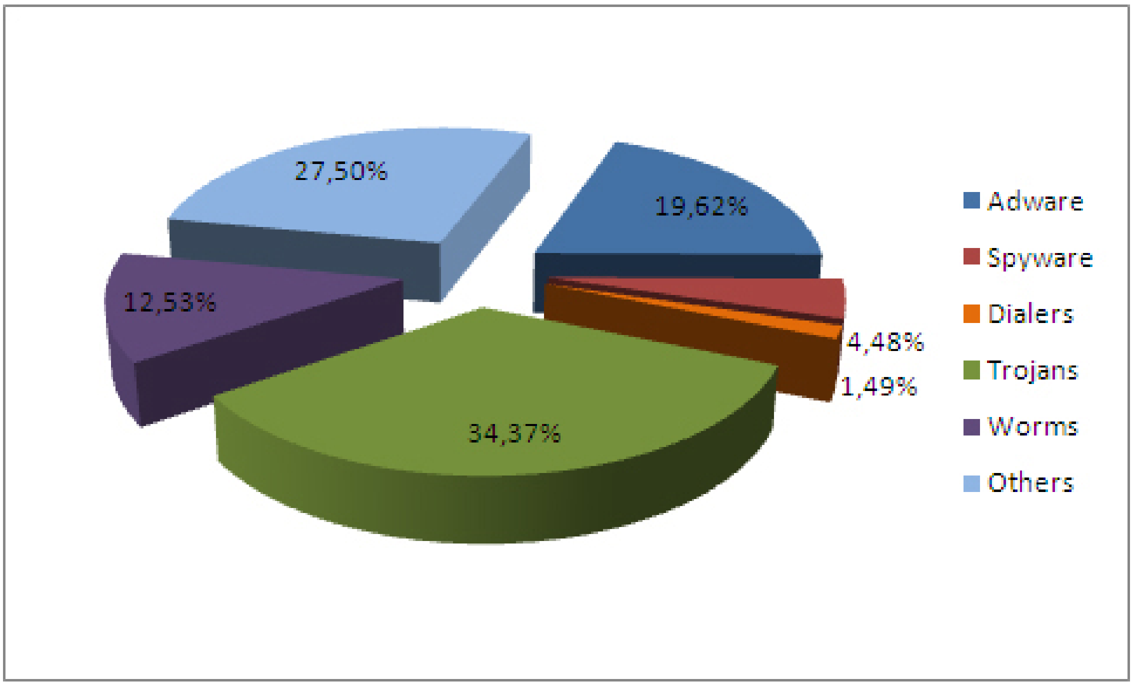


Fig. 4 Distribution of detections by PandaLabs sensors

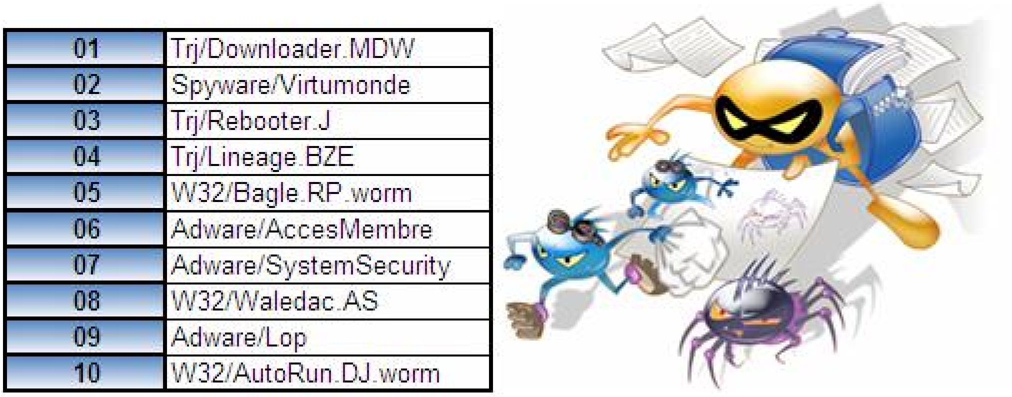
Over this quarter, adware maintained its usual levels, at 19.62%, with Trojans in first place at 34,37%, having increased 2.86% with respect to the previous quarter.

We also observed that worms increased slightly (0.89%), staying in the picture due largely to the effectiveness with which they spread.

At 4.48%, dialers still refuse to disappear, despite their downward trend over the last few years.

Second quarter figures

Below you can see the 10 threats most frequently detected by these sensors:



01	Trj/Downloader.MDW
02	Spyware/Virtumonde
03	Trj/Rebooter.J
04	Trj/Lineage.BZE
05	W32/Bagle.RP.worm
06	Adware/AccesMembre
07	Adware/SystemSecurity
08	W32/Waledac.AS
09	Adware/Lop
10	W32/AutoRun.DJ.worm

Fig. 5 Top Ten threats

Active malware

In this section we will be looking at how malware has evolved so far during 2009.

In order to understand what active malware is, we must first define the two possible status for malware: active and latent.

Latent malware is malware that is on a PC but not taking any action. It is waiting to be executed, either directly by the user or remotely by an attacker.

Once it is run, it starts to take the damaging action for which it has been programmed. In this case, the status changes from latent to active.

We have been monitoring the evolution of active malware month by month on our website: www.pandasecurity.com/infected_or_not/, and through our online tool ActiveScan 2.0.

This service allows any users to run free online scans of their computer, and check whether they are infected or not.

Are you sure your PC is not infected?

23% of PCs with antivirus are infected

Create a free account to enjoy the benefits of:

- Disinfection of viruses, worms and Trojans.
- Custom scans.
- Scan history.

I am already registered ENTER

Fig. 6 ActiveScan 2.0 online tool

Active malware

In this graph you can see how malware has evolved so far during the first half of 2009:

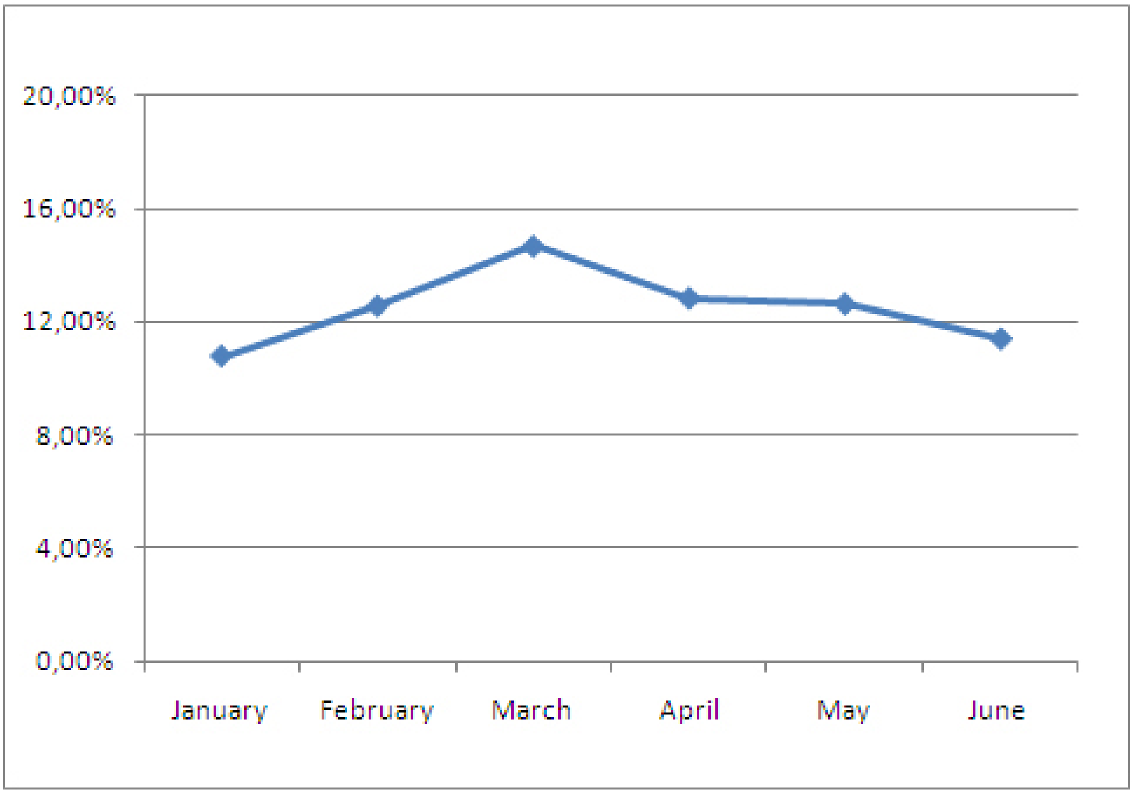


Fig. 7 Active malware evolution during the first half of 2009

January began with the lowest malware ratio in Q1 2009 (10.78% of PCs infected). The malware ratio continued to rise over the next few months, reaching 14.68% in March, the highest rate in the first half of 2009. After this it slowly began to decrease reaching 11.39% in June.

The average rate of active malware so far this year has been 12.48%, lower than the average rate in 2008 (14.62%).

This data reflects the evolution globally, but what about in each country? The graph below shows the infection rate in those countries that most used the Infected or Not website and ActiveScan 2.0 during the first half of 2009.

Active malware

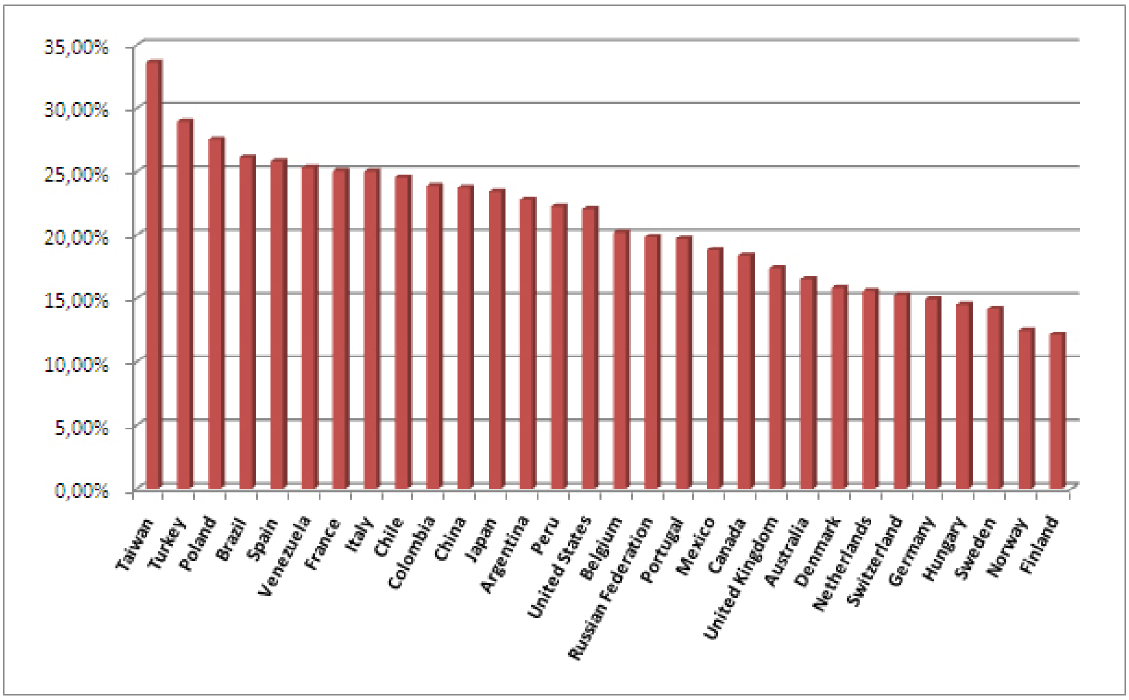


Fig. 8 Countries with the highest malware percentage (January-June 2009)

Once again, Taiwan has the highest percentage of active malware (33.63%). Turkey and Poland come next, with just under 30%. Three Scandinavian countries, Sweden (14.2%), Norway (12.48%) and Finland (12.17%), are the countries with the lowest number of computers infected by active malware during the first half of 2009.

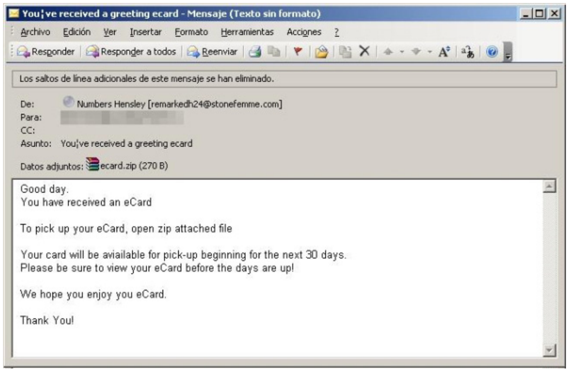
Different trends in sending malware via spam

Emerging threats are increasingly sophisticated and complex to detect. They are capable of infecting computers using vulnerabilities which are very difficult to identify. However, social engineering that uses emails to spread is still one of the most widely-used techniques and one of the main malware entry points on computers.

In the last few years, security experts have highlighted the sending of e-cards and of fake emails from messaging companies (e-cards have generated most traffic).

The message content is usually short and in plain text. E-cards inform recipients that they have received a 'Thank You' card from an acquaintance or a family member, while emails from messaging companies inform the recipient that an order could not be delivered and attach a follow-up sheet.

Below are examples of these messages:



Los saltos de línea adicionales de este mensaje se han eliminado.

De: Numbers Hensley [remarkedh24@stonefemme.com]
Para: [redacted]
CC:
Asunto: You¦ve received a greeting ecard

Datos adjuntos: ecard.zip (270 B)

Good day.
You have received an eCard

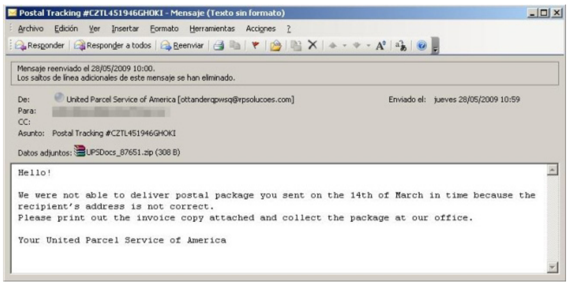
To pick up your eCard, open zip attached file

Your card will be aviailable for pick-up beginning for the next 30 days.
Please be sure to view your eCard before the days are up!

We hope you enjoy you eCard.

Thank You!

Fig. 9 E-card message



Mensaje reenviado el 28/05/2009 10:00.
Los saltos de línea adicionales de este mensaje se han eliminado.

De: United Parcel Service of America [ottanderqpwsq@rpsolucoes.com] Enviado el: jueves 28/05/2009 10:59
Para: [redacted]
CC:
Asunto: Postal Tracking #CZTL451946GHOKI

Datos adjuntos: UPSDocs_87651.zip (308 B)

```
Hello!

We were not able to deliver postal package you sent on the 14th of March in time because the
recipient's address is not correct.
Please print out the invoice copy attached and collect the package at our office.

Your United Parcel Service of America
```

Fig. 10 Messaging company message

Different trends in sending malware via spam

We have monitored a small mail server to check the traffic these messages generate, and have detected several peaks:

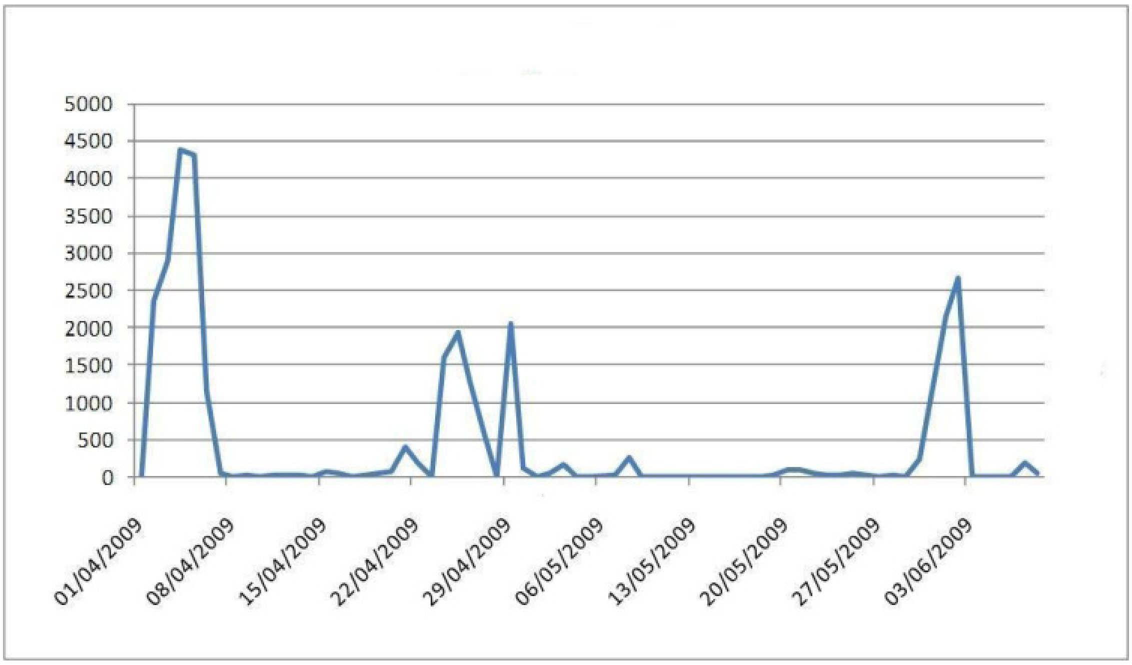


Fig. 11 Number of e-card messages and messages from messaging companies (last two months)

These 'waves' of messages are controlled by the mafias that own botnets[1] and that are responsible for sending this type of spam. Consequently, these messages are sent according to the botnets' owners' strategies and needs.

Although the attacks are sporadic, they require numerous system resources due to their size and volume. The malware types concealed in the messages vary depending on the family and family variants. It is therefore necessary to monitor these threats to update security systems with the latest versions.

[1] Botnets are a group of computers infected by some type of "bot" malware installed on the computer without the user's knowledge, and are remotely controlled to take different actions (usually send spam and attack other computers).

Different trends in sending malware via spam

The graphs below show the main families that have been sent using these types of messages.

E-cards contain a larger variety of malware, the two main types being those of the spammer family (Spamta and Spamtaload) and banker malware (Banker and Goldun).

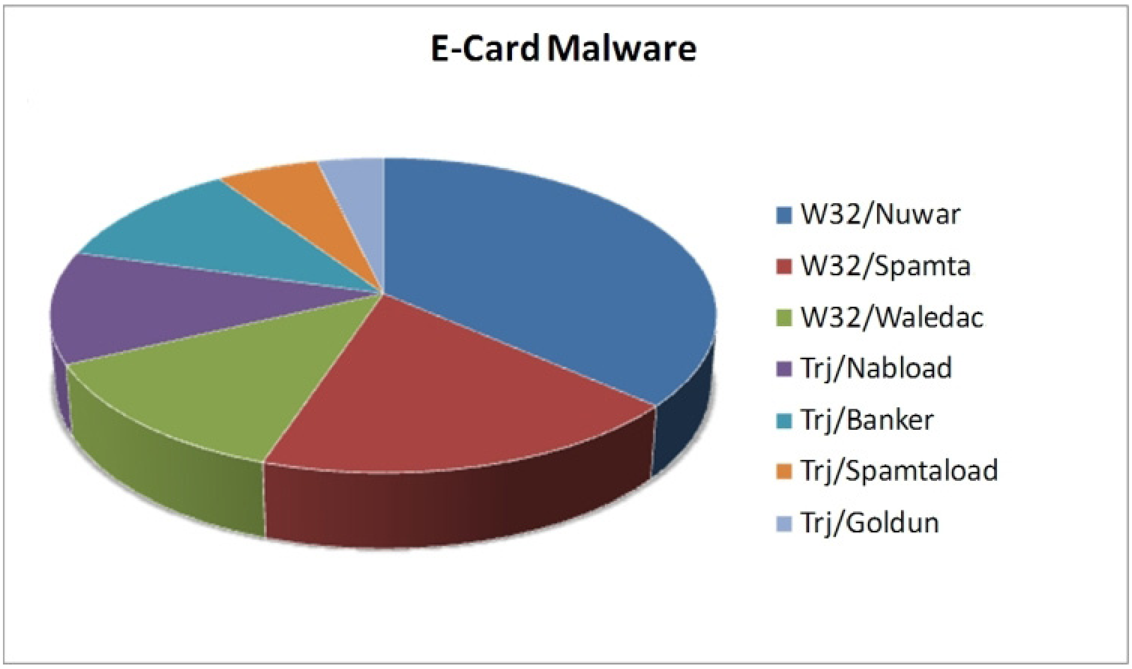


Fig. 12 E-card malware types

The latest e-card waves indicate that a new type of malware has been sent in the last few days (PrivacyCenter, rogueware-type adware). It is not included in the graph, as very few samples have been collected compared to older samples.

In the case of messaging company messages, most of the malware sent is of the banker type, mainly Sinowal and, to a lesser extent, Buzus.

Different trends in sending malware via spam

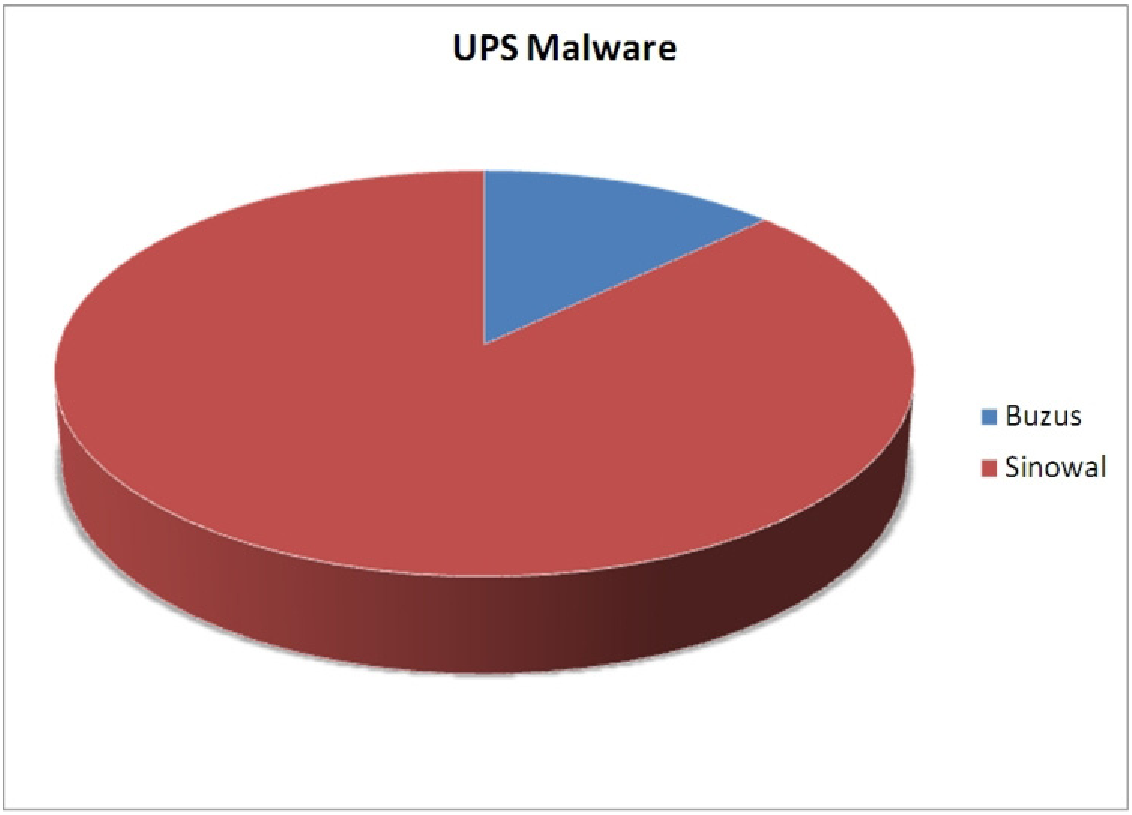


Fig. 13 UPS malware types

The malware is usually password-protected to avoid arousing suspicion and prevent antivirus systems from detecting the file content.

In short, it is not only important to have good security software, but also to be alert and cautious, bearing in mind that many threats distributed in these emails are of the banker type. Their objective is to profit from stealing banking information.

Vulnerabilities in Q2 2009

In April, Microsoft published eight security bulletins (MS09-009 to MS09-016). As is the norm nowadays, some of the new vulnerabilities affected the Microsoft Internet Explorer browser. These security flaws allowed remote execution of code on computers when users visited a malicious Web page. This simple flaw could lead to a user's system being completely compromised.

Internet Explorer was not the only Web browser affected. Mozilla launched a new version of its Firefox Web browser (3.07) to solve eight security flaws (six of them critical), which also allowed remote code execution using the same technique.

Perhaps the most significant bulletin was MS09-009, a critical vulnerability in Microsoft Excel used by malicious users to install malware on vulnerable systems. Additionally, bulletins MS09-012 and MS09-015 solved several vulnerabilities that allowed local privilege escalation.

In April, Adobe reported a "0-day"[2] issue in its Acrobat and Reader products for all platforms (Windows, Linux and MacOS). The flaw was in the "getAnnots" function. Attackers could create a specially-crafted PDF to exploit this vulnerability and run malicious code on the system of users who tried to view the document.

In May, Adobe solved the critical vulnerability mentioned earlier, while Microsoft published a security bulletin (MS09-017) to solve 14 vulnerabilities detected in Microsoft PowerPoint. These vulnerabilities have also been exploited by malicious users to install malware on vulnerable systems. PowerPoint files are becoming a popular channel for propagating infections as in addition to being used to create presentations, PowerPoint is also used on the Internet to share interesting stories, view photos, etc. Consequently, most users trust PowerPoint documents and are curious about their content even if the sender is unknown.

In June, a serious vulnerability affecting the Microsoft Internet Information Server (IIS) was published (MS09-020). The features and exploitation method of this new "0-day" resembled old vulnerabilities detected a few years ago in the Microsoft Web server. For example, the "Web Server Folder Traversal" vulnerability detected in 2000 was widely used to infiltrate numerous Web servers.

[2] New vulnerability yet to be patched.

Vulnerabilities in Q2 2009

The successful exploitation of this new vulnerability allowed hackers to access private information, avoiding authentication in the IIS server. Malicious users with the corresponding permissions could even load a file to the server using this vulnerability. The problem stems from the WebDAV protocol, more specifically the "Translate: f" header and the unicode characters in the URL of the user's request to the server.

On May 28, Microsoft published a new security warning (971788), reporting a new vulnerability in DirectX which was being used to install malware on vulnerable systems using multimedia files.

The good news was that Windows Vista and Windows Server 2008 were not vulnerable. The same applied to other vulnerabilities detected. The vulnerability severity is much lower -sometimes even nonexistent- in these two operating systems than in Windows XP and Windows 2000. It would seem at least that Microsoft's efforts to improve the security of its Windows Vista and Windows Server 2008 operating systems have not been in vain.

Finally, in June Microsoft published ten security bulletins that solved 31 vulnerabilities: the mentioned IIS Web Server vulnerability, 11 Microsoft Office vulnerabilities, eight Microsoft Internet Explorer vulnerabilities, two Microsoft Active Directory vulnerabilities, three Windows print queue service vulnerabilities, one Windows Search vulnerability and one vulnerability regarding Remote Procedure Calls (RPC) which affects all Windows versions including Windows Vista and Windows Server 2008 and allows local privilege escalation. However, regardless of the number of vulnerabilities solved in June, Microsoft has been unable to solve the vulnerability detected in DirectX on May 28.

To protect computers from this vulnerability our products include technologies to protect against unknown threats.

At Panda Security we are continuously improving our products to protect our clients against new vulnerabilities. However, we'd like to recommend users to install the updates made available in Microsoft's security bulletins as soon as possible, as well as other security updates that may affect other products installed on their systems (Adobe, Mozilla, Google and Microsoft Office).

The many guises of Waledac

Social engineering is still one of the techniques most often used by malware to spread, and this is the case with the Waledac worm. It can be defined as "a collection of techniques used to trick users into taking certain actions, such as sending personal information, downloading files, etc."

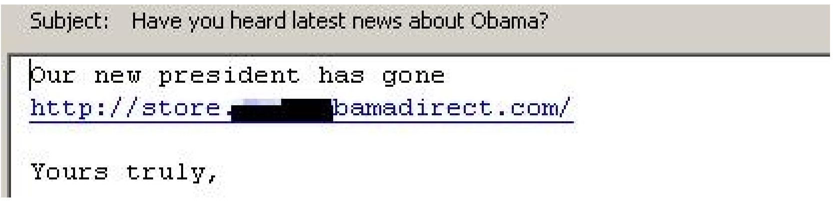
If there is one factor that characterizes the Waledac family it is the diversity of the subject matter used to spread it. Yet the choice of subjects is not random, it has been carefully calculated in order to exploit:

- Significant events or dates such as Christmas or Valentine's Day.
- Spoof news stories, such as the resignation of Barack Obama or explosions in certain cities.
- Bogus offers of discount vouchers or even services for spying on other people's text messages.

The first examples of this worm emerged around Christmas 2008 using seasonal greetings as bait to trick users and propagate.

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?

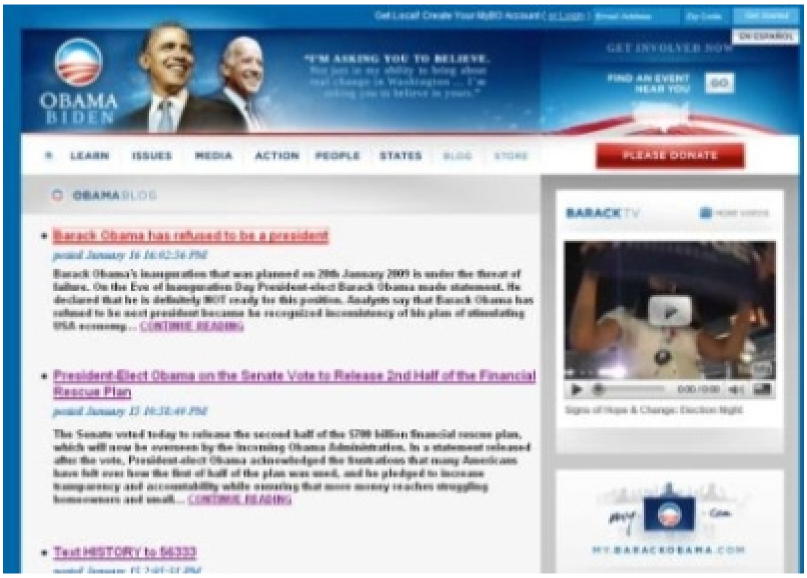
Our new president has gone
http://store.[redacted]bamadirect.com/

Yours truly,

Fig. 14 Email message about Obama's resignation

The many guises of Waledac

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:



- Barack Obama has refused to be a president
  posted January 16 16:02:56 PM
  Barack Obama's inauguration that was planned on 20th January 2009 is under the threat of failure. On the Eve of Inauguration Day President-elect Barack Obama made statement. He declared that he is definitely NOT ready for this position. Analysts say that Barack Obama has refused to be next president because he recognized inconsistency of his plan of stimulating USA economy... CONTINUE READING
- President-Elect Obama on the Senate Vote to Release 2nd Half of the Financial Rescue Plan
  posted January 15 16:58:49 PM
  The Senate voted today to release the second half of the $700 billion financial rescue plan, which will now be overseen by the incoming Obama Administration. In a statement released after the vote, President-elect Obama acknowledged the frustrations that many Americans have felt over how the first of half of the plan was used, and he pledged to increase transparency and accountability while ensuring that more money reaches struggling homeowners and small... CONTINUE READING
- Text HISTORY to 56333

Fig. 15 Spoof Obama Web page

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

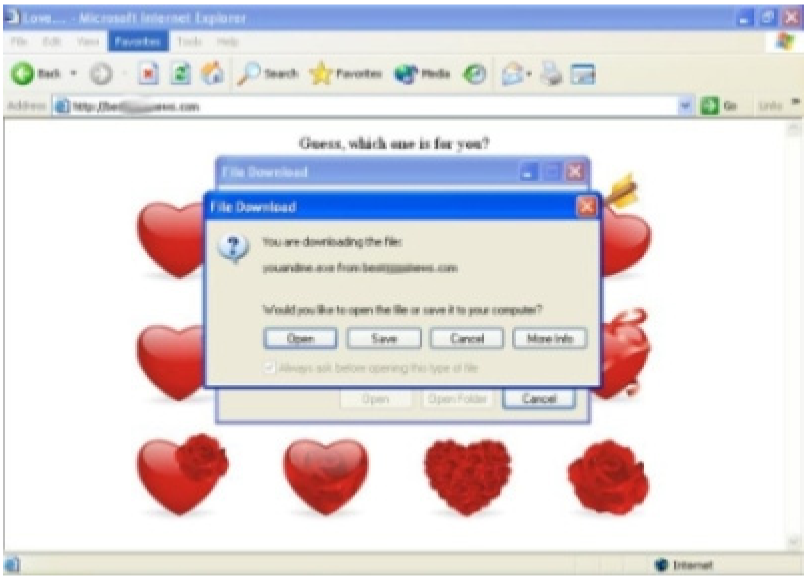
Valentine's Day

Valentine's Day has always been popular among malware creators. This year, however, messages relating to this family of worms were distributed long before the day itself.

In fact, on January 26, we published a post on the PandaLabs blog warning of a wave of Waledacs using Valentine's Day as bait.

The many guises of Waledac

In this case, the email contained a link to a Web page with images of hearts. Users were then prompted to click one of them. Needless to say, this would result in the malicious file being downloaded onto their computers.


Love... - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://bed[redacted]news.com
Go Links
File Download
Open Save Cancel More Info
Always ask before opening this type of file
Open Open Folder Cancel
Internet

Guess, which one is for you?

File Download

You are downloading the file:

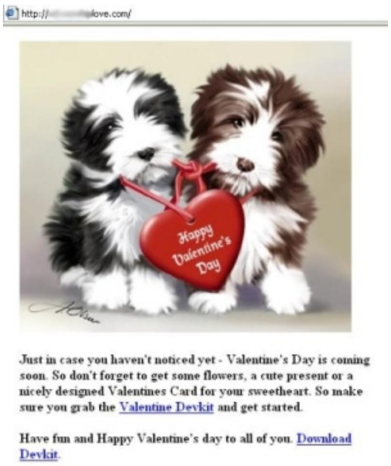
youandme.exe from best[redacted]news.com

Would you like to open the file or save it to your computer?

Fig. 16 Web page from which Waledac was downloaded

A few days before Valentine's Day, a similar wave of emails appeared. In this case the messages contained a link to a malicious page offering a tool for designing Valentine's cards.

Once again, users were encouraged to click links on the page to download this tool. The real download however was a variant of Waledac.



Just in case you haven't noticed yet - Valentine's Day is coming soon. So don't forget to get some flowers, a cute present or a nicely designed Valentines Card for your sweetheart. So make sure you grab the Valentine Devkit and get started.

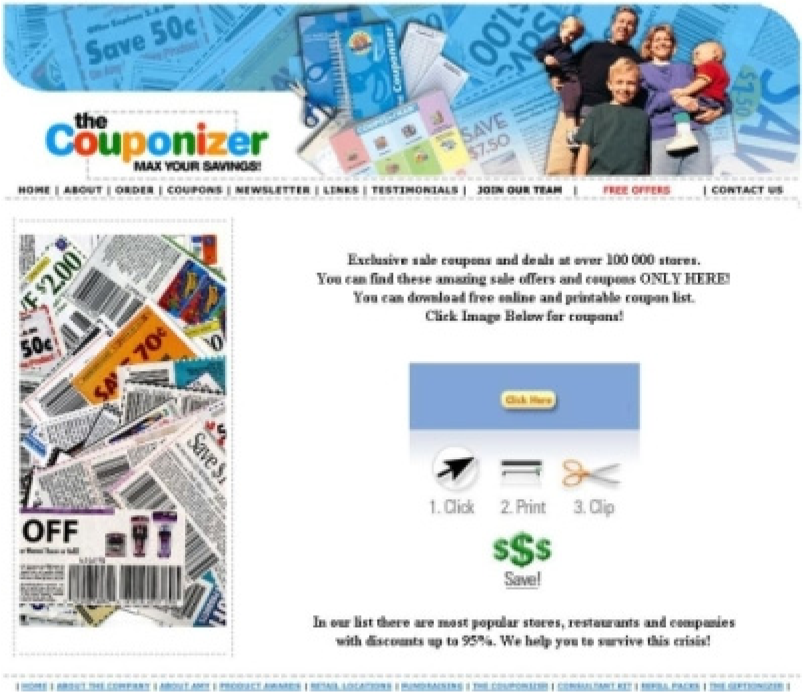
Have fun and Happy Valentine's day to all of you. Download Devkit.

Fig. 17 Web page for designing romantic cards

The many guises of Waledac

Discount coupons in times of crisis

Cyber-crooks have also been doing their bit to 'help' users mitigate the effects of the economic crisis. The messages in this case contained links pointing to a Web page offering discount vouchers for numerous stores.


the Couponizer
MAX YOUR SAVINGS!
HOME | ABOUT | ORDER | COUPONS | NEWSLETTER | LINKS | TESTEMONIALS | JOIN OUR TEAM | FREE OFFERS | CONTACT US
Click Here
1. Click
2. Print
3. Clip
s$s
Save!
| HOME | ABOUT THE COMPANY | ABOUT AMY | PRODUCT AWARDS | RETAIL LOCATIONS | FUNDRAISING | THE COUPONIZER | CONSULTANT KIT | REFILL PACKS | THE GIFTONIZER |

Exclusive sale coupons and deals at over 100 000 stores.
You can find these amazing sale offers and coupons ONLY HERE!
You can download free online and printable coupon list.
Click Image Below for coupons!

In our list there are most popular stores, restaurants and companies with discounts up to 95%. We help you to survive this crisis!

Fig. 18 Web page supposedly offering discount coupons

Users that tried to download these coupons by clicking the links on the page would actually be downloading files with plausible names such as couponlist.exe, coupons.exe, list.exe or print.exe. Yet again, the files were actually copies of the worm.

The many guises of Waledac

Explosions

A few weeks later, we started to see a new subject being used to distribute Waledac. Another spoof news story, but this time about explosions in certain cities.

Links in the messages led to a Web page with the full story and, supposedly, a related video. Waledac used the logo of Reuters to gain users confidence.

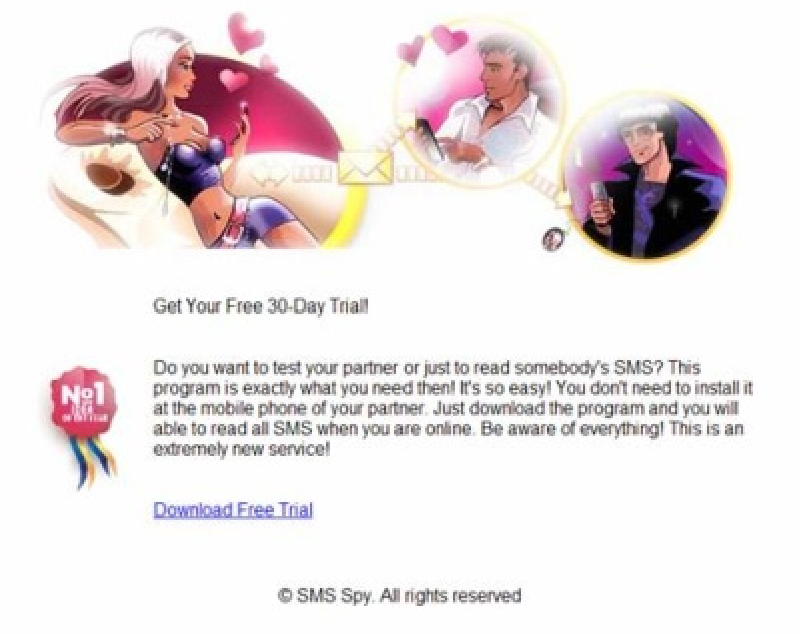
The Web page claimed that users had to download a Flash Player update to see the video. This update was none other than a copy of the worm.

SMS spy services

The most recent ruse used by Waledac has been to pass itself off as an application for spying on other people's text messages.

Encouraging users to see if their partners are cheating on them or simply read someone else's SMS, the message invites them to download a special application.

However, there is no such application, just a copy of a Waledac worm which will infect users' computers if they decide to download it.



Get Your Free 30-Day Trial!

Do you want to test your partner or just to read somebody's SMS? This program is exactly what you need then! It's so easy! You don't need to install it at the mobile phone of your partner. Just download the program and you will able to read all SMS when you are online. Be aware of everything! This is an extremely new service!

Download Free Trial

© SMS Spy. All rights reserved

Fig. 19 Site from which the spy program is downloaded

2009 Q2 Trends

This quarter has seen a major drive by cyber-crooks to distribute malware using BlackHat SEO techniques and exploit Web 2.0 services, from Youtube to Twitter, by taking advantage of vulnerabilities both in these services as well as popular applications such as Microsoft PowerPoint or Adobe Acrobat Reader.

Vulnerabilities

On April 2, Microsoft published a security advisory outside its normal cycle to release a patch for PowerPoint, due to a security hole affecting versions for Windows and Mac. Throughout this quarter we have seen a growing number of vulnerabilities affecting applications from various vendors. The security bulletins published by Microsoft in June set a record in terms of the number published since the company first started its monthly cycle; these bulletins fixed a total of 31 vulnerabilities.

BlackHat SEO techniques

BlackHat SEO techniques are not new, although we have seen a major increase in their use over the second quarter of 2009. SEO stands for Search Engine Optimization and basically refers to the techniques used to improve the ranking of websites in search engines (Yahoo, Google, etc.). BlackHat SEO refers specifically to the use of SEO techniques by cyber-criminals to promote their Web pages.

In April, PandaLabs discovered a new case of BlackHat SEO. This was particularly interesting, as it targeted a single brand (the US car manufacture Ford). More than 1 million malicious links were created in order to direct users performing searches with terms related to Ford to malicious Web pages. Several days later the same strategy was applied to Nissan. Both cases operated in the same way: Once users had accessed the malicious page, they were asked to download a codec, which was really the fake antivirus Adware/MSAntiSpyware2009.

Since then, similar cases have appeared using different subjects. It is important to underline the emphasis that cyber-criminals have given these techniques. They always use the very latest topics, taking 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.

2009 Q2 Trends

To illustrate this situation, on June 1 Microsoft announced in E3 it's "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. When searching for malicious pages created by the same cyber-criminals, we found the following pages with the corresponding subjects:

16,000 links "**TV Online**"
16,000 links "**YouTube**"
10,500 links "**France**" (Airline Crash)
8,930 links "**Microsoft**" (Project Natal)
3,380 links "**E3**"
2,900 links "**Eminem**" (MTV Awards/Bruno Incident)
2,850 links "**Sony**"

Youtube has also been a major target for cyber-crooks this quarter. Basically, Youtube lets registered users add comments to the pages displaying the videos. In this case, criminals have been creating accounts and then generating a series of comments automatically; these comments include links to malicious websites designed to infect users. In total, more than 30.000 of such malicious comments have been created.

Malicious use of Twitter Trends

Another target of cyber-criminals has been Twitter. A worm appeared in April which used a cross-site scripting technique to infect users when they visited the profiles of other infected users. It then infected the new user's profile to continue propagating. New variants soon appeared of this worm, created by one Mikey Mooney, who apparently wanted to attract users to a service competing with Twitter.

In early June, Twitter was the focus of other attacks, this time using different techniques: basically a variation of BlackHat SEO for Twitter. 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, you 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.

2009 Q2 Trends

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 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. 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.

Finally, on the subject of trends, we have to mention that this quarter has seen the second anniversary of Collective Intelligence.

Two years of Collective Intelligence

In 2007, Panda Security launched Collective Intelligence: This is a suite of technologies that can automatically analyze, classify and disinfect all files received every day at PandaLabs. This strategic initiative has helped to position Panda as The Cloud Security Company, as it now offers the first cloud-based security solution: Panda Cloud Antivirus.

The existence of a highly profitable cyber-business model, orchestrated by criminal mafia, saw security laboratories inundated by an avalanche of new malware, with a tenfold increase in the number of new malware samples. This in turn made users more vulnerable, and there were only two possible solutions: rapidly expanding resources available to the laboratories in order to process these waves of malware manually, or automate processes and equip the teams adequately so that disinfection routines could be generated rapidly and automatically.

PandaLabs chose the most innovative yet most difficult path, deciding to front up to the challenge that no other company had taken on: The development of a system based on artificial intelligence which would be able not just to recognize new malware, but to learn and adapt to the new techniques of cyber-criminals.

And this is how Collective Intelligence came about. It was first put on the market in 2007 in the form of a small, free online scanner, called NanoScan, which could identify active malware in memory in just a few seconds. Given its effectiveness and the highly positive reception, Panda's 2009 retail products leveraged this greater detection capacity by connecting to the cloud.

2009 Q2 Trends

In April 2009, on the second anniversary of these technologies, the user community around the world has effectively become our laboratory, with the launch of the **first ultra-light, cloud-based antivirus on the market: Panda Cloud Antivirus**.

Now, Panda's Collective Intelligence system allows the correlation and processing of new malware in just six minutes, thanks to the thousands of files sent via the community every day. This knowledge is then shared to provide greater detection capacity for all Panda users.

Collective Intelligence is now receiving 50,000 files a day, of which 35,000 are new malware samples. Of these, some 99.4% are processed automatically, leaving just 0.6% to be resolved manually. The Collective Intelligence database now has more than 26 million malware samples, occupying more than 18,000 GB.

If all this information were stored on a PC, you would have the perfect antivirus, but the computer would not be able to do anything else. That's why Collective Intelligence is not just our answer to the exponential increase in malware, but it also allows us to offer maximum detection with a minimal impact on users' computers.

Collective Intelligence in numbers

- 50,000 files are received every day, of which 35,000 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 technicians 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.

More information about Collective Intelligence is available in the PandaLabs blog.

About PandaLabs

PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment:

- **PandaLabs** creates continually and in real-time the counter-measures necessary to protect Panda Security clients from all kind of malicious code on a global level.
- **PandaLabs** is in this way responsible for carrying out detailed scans of all kinds of malware, with the aim of improving the protection offered to Panda Security clients, as well as keeping the general public informed.
- Likewise, **PandaLabs** maintains a constant state of vigilance, closely observing the various trends and developments taking place in the field of malware and security. Its aim is to warn and provide alerts on imminent dangers and threats, as well as to forecast future events.
- For further information about the last threats discovered, consult the **PandaLabs** blog at: http://pandalabs.pandasecurity.com/