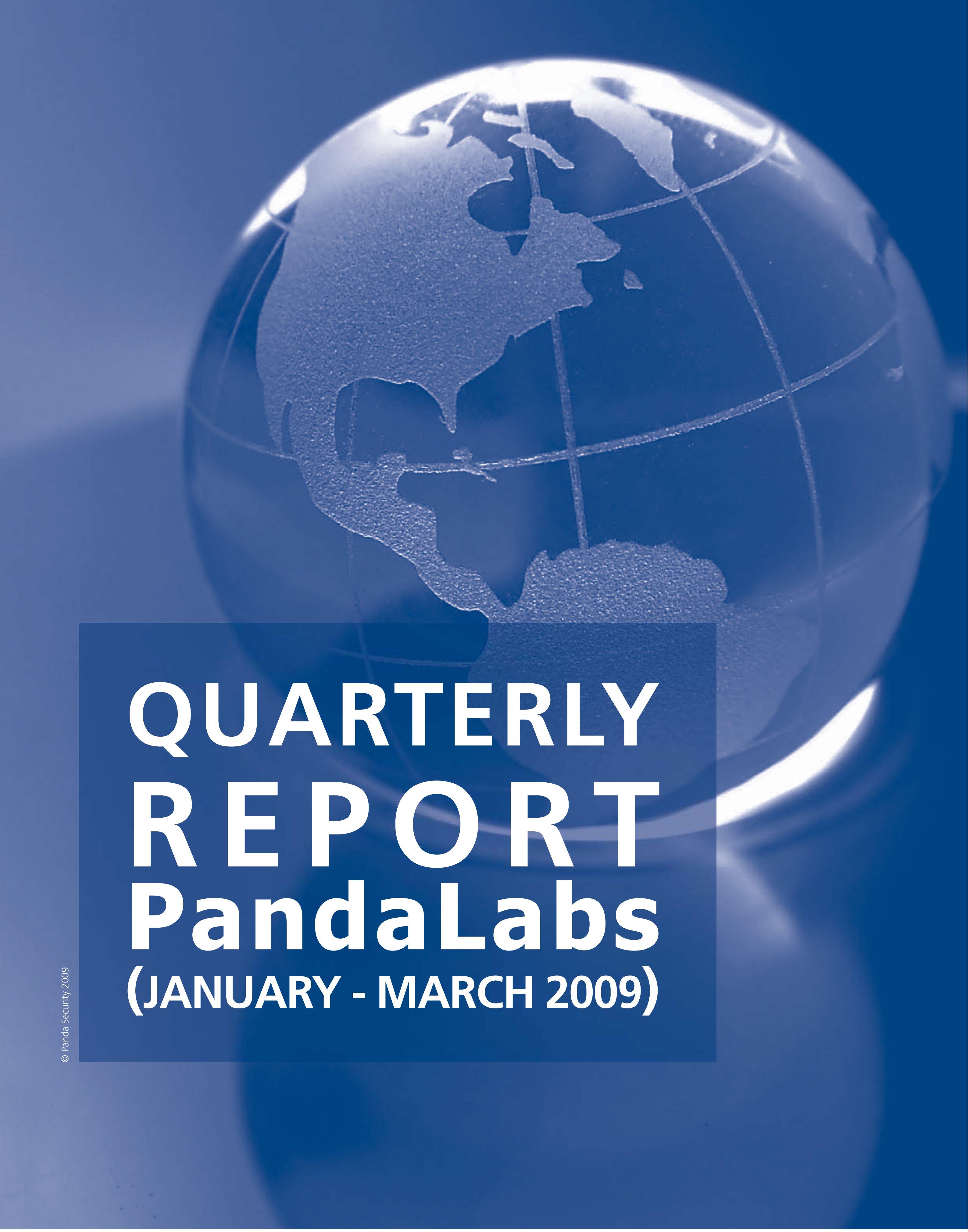


QUARTERLY REPORT PandaLabs (JANUARY - MARCH 2009)

PANDA SECURITY | One step ahead.

Index

Introduction

Here we present the Q1 report for 2009, which takes a look at some of the most interesting events of this quarter.

It seems that spam levels have stabilized over the last three months, even though the ratio is still high. We include an interesting article dealing with the main sources of spam. It is worth noting that the global financial crisis is having an impact on spam, as there has been a proliferation of messages related to job offers.

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

This quarter, two computer worms grabbed the headlines: Waledac and Conficker. Waledac is considered by some researchers as an evolved version of Storm Worm. Whatever it is, however, it is clear that Waledac used all possible means to flood users' mailboxes with Valentine's Day-related spam messages. The Conficker worm not only infected thousands of computers in a very short time, but even caused Microsoft to offer a reward to whoever was able to capture its creator.

We also analyze the most important malware trends during this quarter. It seems there is a comeback of old-fashioned viruses adapted to modern times. The Sality.AO virus is a good example of this, as it can spread across the web like the latest malware specimens.

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

We hope you find it interesting.

Executive summary

Spyware category has increased almost eleven percent, placing itself as the second most detected malware category in Q1 2009.

Taiwan leads the ranking of active malware, being over the 30% barrier. Turkey and Brazil are also noteworthy. They occupy second and third place respectively, overtaking Spain and the United States.

The amount of spam that circulates the web is stable. There have not been any considerable changes over the last few months.

The global financial crisis has caused an increase in the number of messages related to job offers or academic degrees.

Most of web pages included in spam messages are hosted in the United States, Europe and China, the main markets that spam targets at.

At present, approximately 140 domains have been used to distribute malicious codes from the Waledac family.

The extent of the Conficker attack has lead Microsoft to offer a $250,000 reward to whoever provides information about its creators.

The latest known variant will start to generate 50,000 URLs on a daily basis from April 1.

First quarter figures

Distribution of the new threats detected

The graph below illustrates the distribution of new variants by type of malware detected by PandaLabs in the first quarter of 2009:

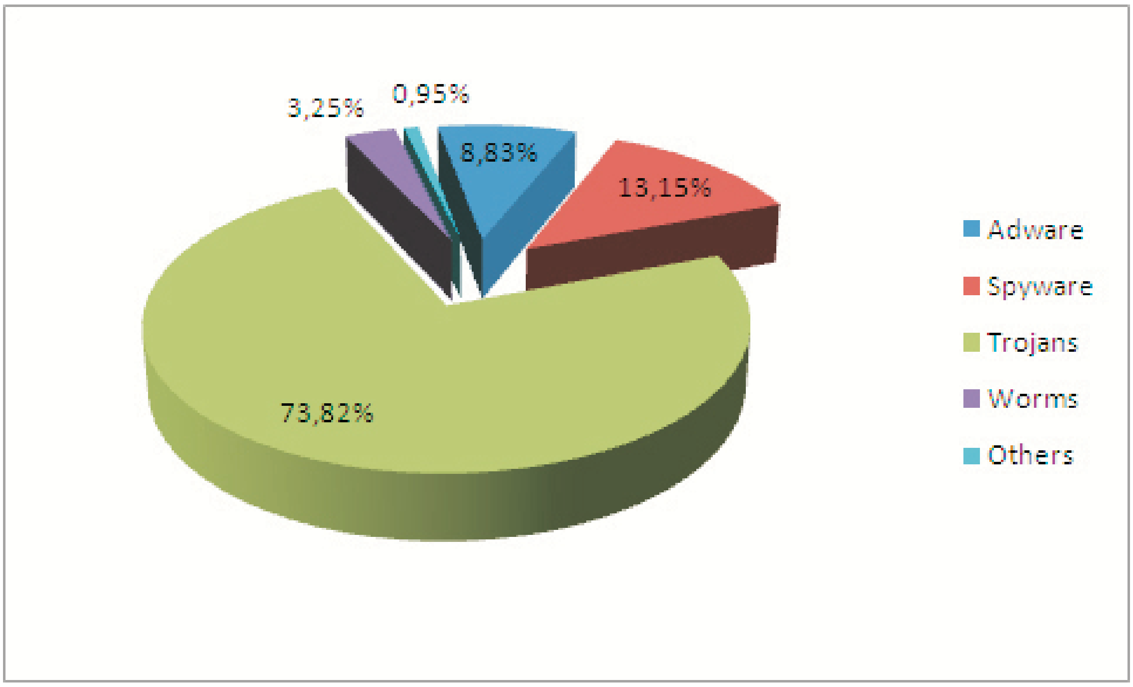


Figure 1. New malware detected in Q1.

As illustrated in the graph, the predominant malware category throughout Q1 has been Trojans, even though the percentage (73.82%) has dropped almost 4 percent (3.67%) compared to the previous quarter.

With respect to these figures, backdoor Trojans have been included in the Trojans category, and bots have been included in either worms or Trojans, depending on the type.

As for worms, their percentage has risen slightly, now accounting for 3.25% 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.

First quarter figures

The most interesting aspect has been the considerable increase of spyware, almost eleven percent (10.57%) compared to the previous quarter. Spyware has placed itself as the second most detected malware category in Q1 2009 (13.15% of all malware).

As for adware (8.83% of all malware), cyber-crooks continue to show a preference towards the 'rogue antivirus' subtype.

We have grouped categories with low prevalence under the heading 'Other'.

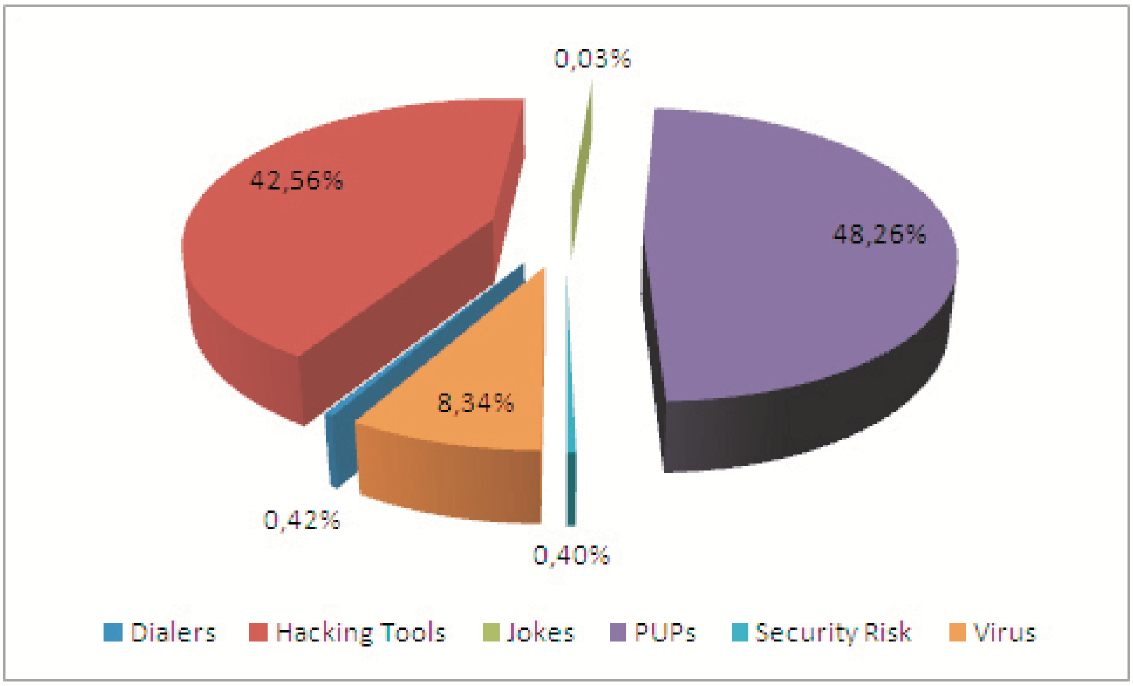


Figure 2. Other malware.

First quarter figures

Month by month

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

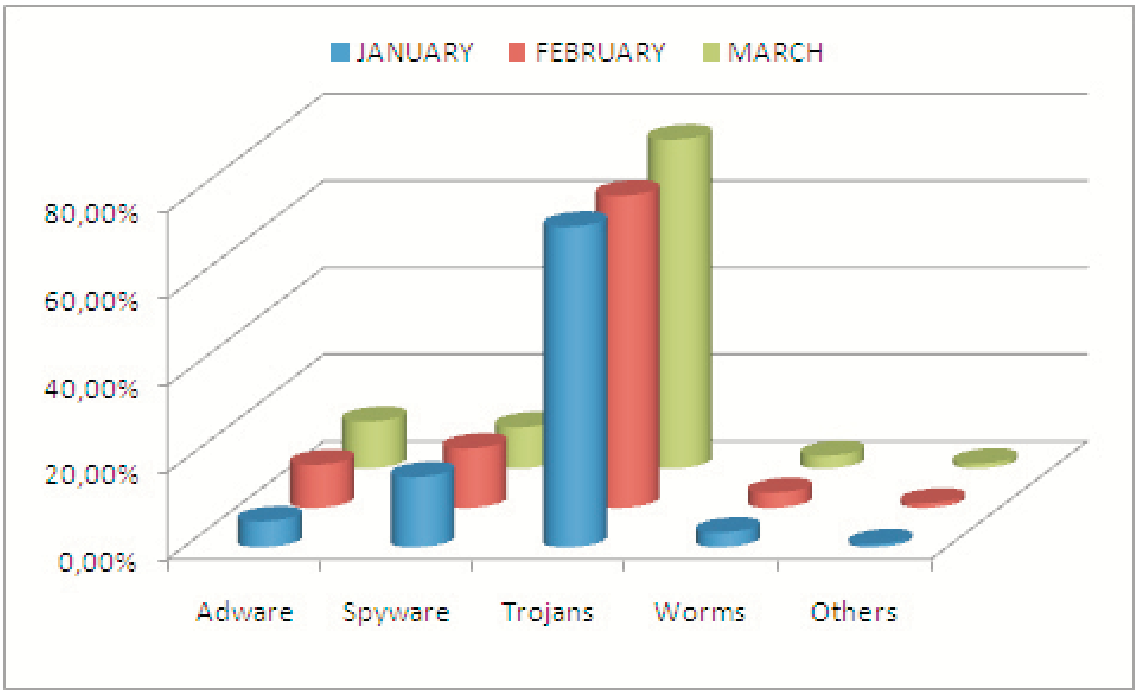


Figure 3. Evolution of the new malware.

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

First quarter figures

Threats detected by the PandaLabs sensors

The following graph shows the distribution of detections made by the Panda Security sensors throughout the fourth quarter of 2008.

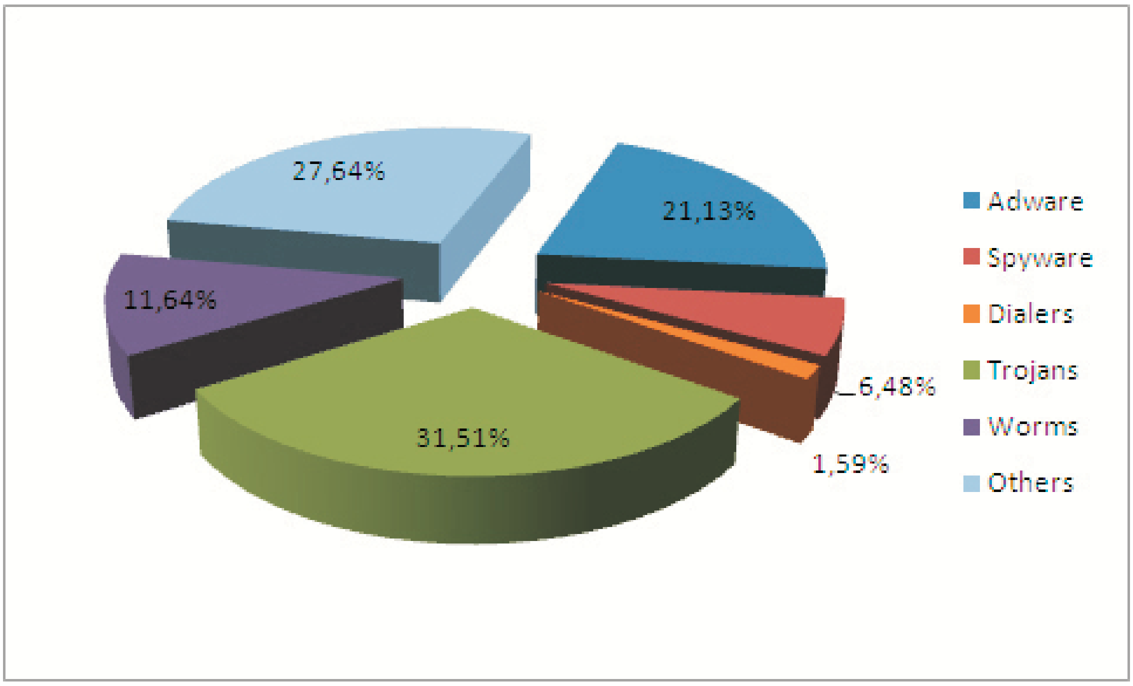


Figure 4. Distribution of detections in Q1.

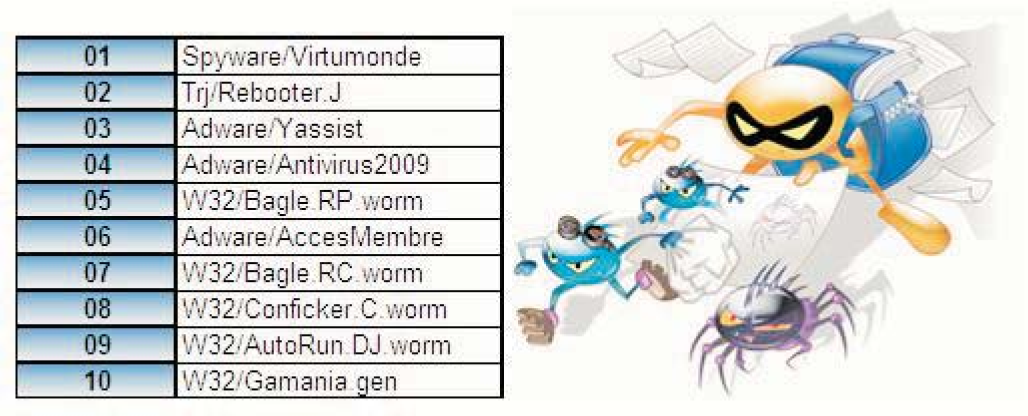
In this quarter, adware has increased slightly by half a point to 21.13%, with Trojans now in first place at 31.51%. Even though Trojans have decreased compared to the previous quarter, they remain at the top of the most widely detected malware types.

Worms are also in decline (they dropped by 0.83%) although they more or less maintain their infection ratio, which stays at 11.64%, and still represent a significant type of malicious code due to the speed with which they spread to other systems.

At 1.59%, dialers still refuse to disappear, despite their downward trend over the last few years.

First quarter figures

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



01	Spyware/Virtumonde
02	Trj/Rebooter.J
03	Adware/Yassist
04	Adware/Antivirus2009
05	W32/Bagle.RP.worm
06	Adware/AccesMembre
07	W32/Bagle.RC.worm
08	W32/Conficker.C.worm
09	W32/AutoRun.DJ.worm
10	W32/Gamania.gen

Figure 5. The 10 threats most frequently detected.

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.

PANDA activescan 2.0
Home | Give us your opinion! | Help
Are you sure your PC is not infected?
Scan now
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.
Register!
I am already registered
ENTER

Figure 6. ActiveScan 2.0 online tool

Active malware

In this graph you can see how malware has evolved so far during Q1 2009.

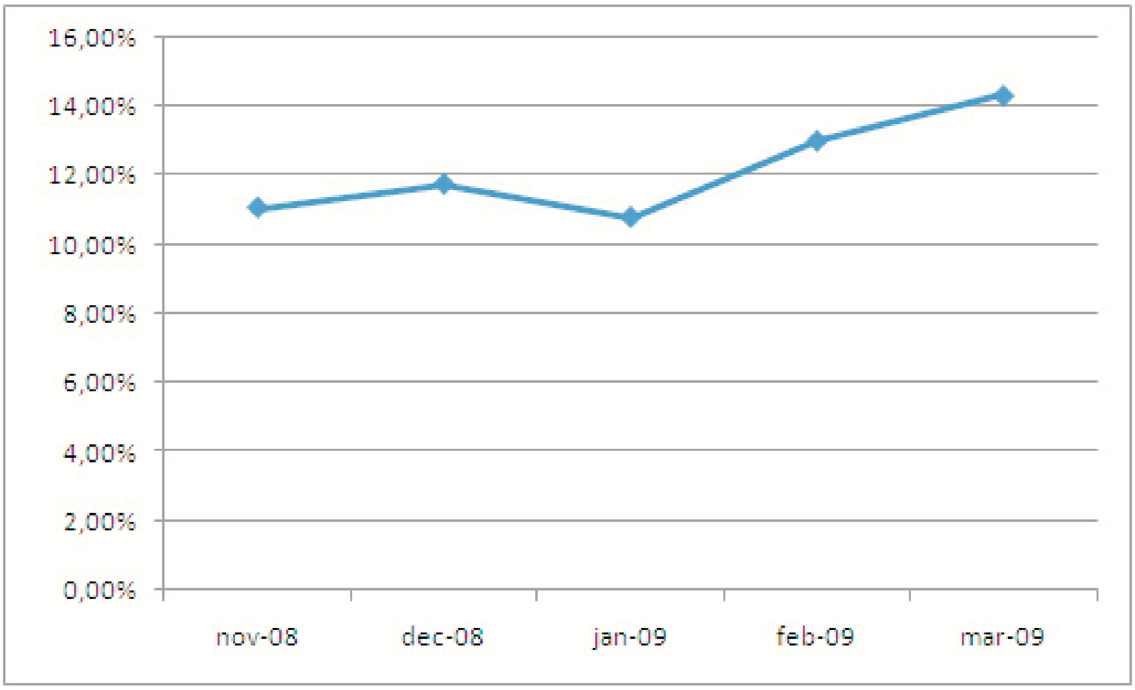


Figure 7. Active malware evolution during Q1 2009.

We have included data from the last two months in 2008 to give a better overview of the evolution of active malware.

January started off with the lowest malware ratio in Q1 2009 (10.78% of infected PCs). From then on there has been a progressive increase up to 14.33%, the highest active malware ratio since August 2008.

The average active malware ratio in Q1 reached 12.67%, a lower percentage than that registered for the whole of 2008. The data shows that this quarter's figures are higher than those in Q4 2008, so, if the current trend continues, the percentage is likely to increase in the next quarter.

This data reflects the evolution globally, but what about in each country? The graph below shows the infection percentage in the countries with most scans[1] through the Infected or Not site and ActiveScan 2.0.

[1] Countries are ordered according to the number of scans performed.

Active malware

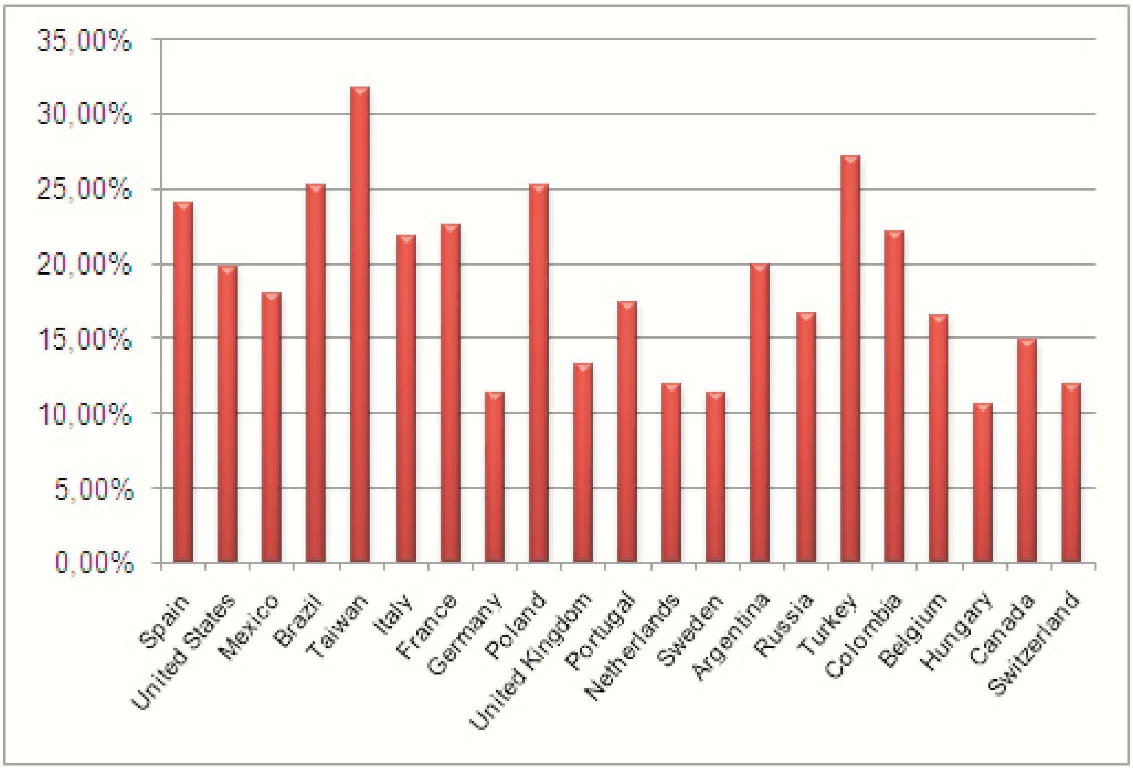


Figure 8. Countries with highest malware percentage (January-March 2009).

Taiwan leads the ranking with 31.70%, and is actually the only country that is over the 30% barrier. Turkey and Brazil are also noteworthy. They occupy second and third place respectively, overtaking Spain and the United States. Poland shares the same percentage as Brazil, but it would occupy fourth place, as it has a lower number of scans performed. Mexico, nevertheless, has witnessed a decrease in the amount of malware (17.95%), dropping almost 10% compared to the 24.87% active malware average recorded for the whole of 2008.

Quarterly Spam Report

This document analyzes the current situation of spam. The PandaLabs spam monitoring systems provide us with statistical data about the amount of spam that reaches our SpamTraps[2], our products' spam detection ratios, sources of spam, etc.

Spam traffic

In order to analyze spam traffic we have used a source that provides us with some 43,000 spam messages every day, with peaks of 68,000 daily emails. This amount of spam lets us obtain quite reliable statistics about the current spam situation.

The amount of spam that circulates the web is stable. There have not been any considerable changes over the last few months.

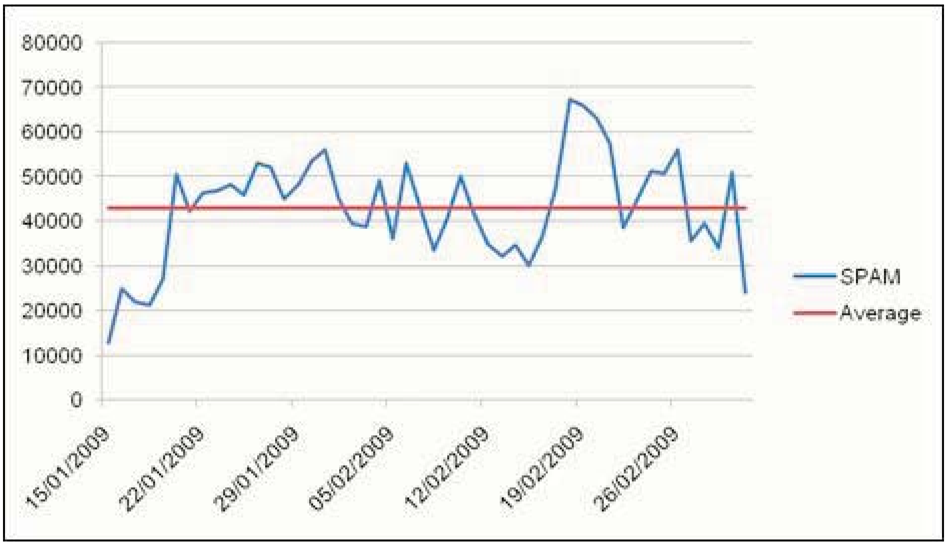


Figure 9. Spam in circulation (January-February 2009).

[2] A SpamTrap is a Web-based mail server that has certain domains associated to it with no accounts. It is configured so that it accepts all emails sent to the server. The purpose of this server is to collect spam sent by spammers. There are several techniques and configurations to facilitate the reception of spam.

Quarterly Spam Report

Regarding message subjects, the global financial crisis has caused an increase in the number of messages related to job offers or academic degrees.

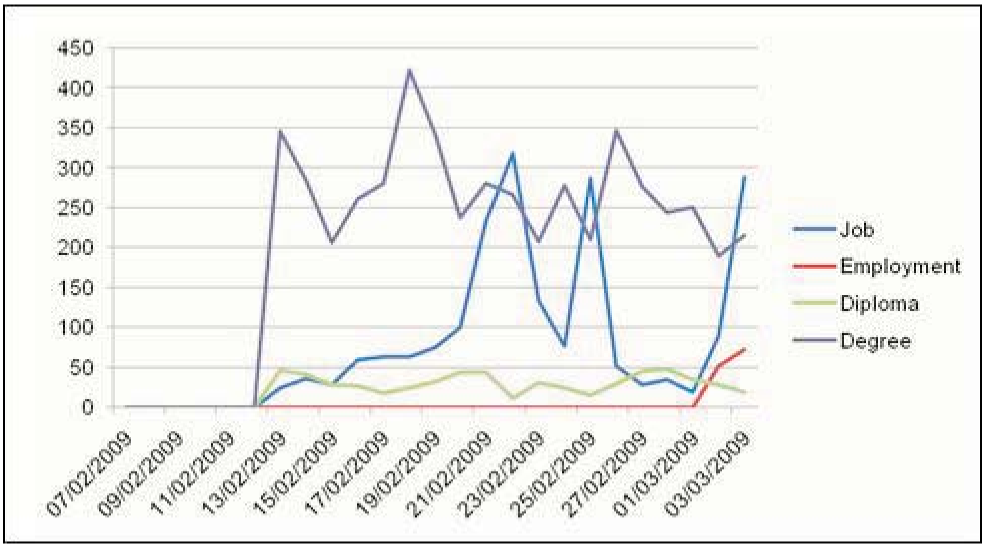


Figure 10. Subject of spam messages.

In any event, messages having to do with sexual enhancers or pharmaceuticals are still predominant, as shown by the graph below:

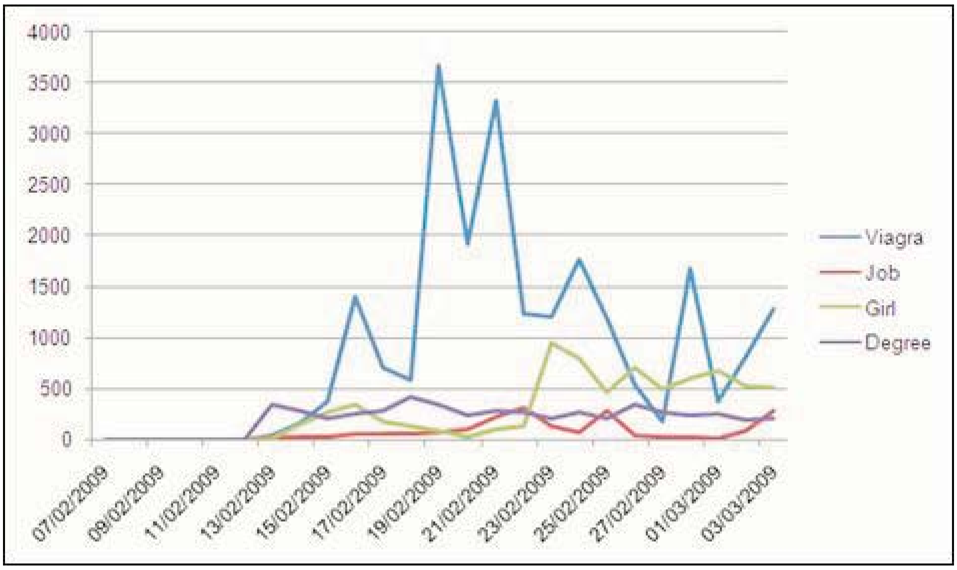


Figure 11. Comparative among the main subjects of spam.

Quarterly Spam Report

Sources of spam

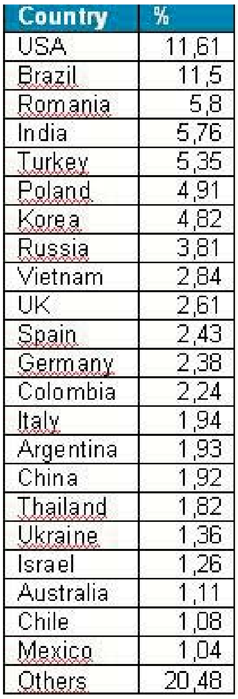
Regarding spamming countries, before drawing any conclusions it is important to bear in mind the possible sources of spam:

- SPAMMERS
- BOTNETS (Malware)

On one hand, we have ISPs that host computers for tracking addresses and massively sending spam to them. On the other hand, we have malware-infected computers controlled remotely for sending out spam.

It must also be taken into account that, in the case of spammers, they host their computers in ISPs in countries where spam control regulations are poor or simply don't exist.

Next is a series of figures that show the geographical distribution of spam sources:



Country	%
USA	11,61
Brazil	11,5
Romania	5,8
India	5,76
Turkey	5,35
Poland	4,91
Korea	4,82
Russia	3,81
Vietnam	2,84
UK	2,61
Spain	2,43
Germany	2,38
Colombia	2,24
Italy	1,94
Argentina	1,93
China	1,92
Thailand	1,82
Ukraine	1,36
Israel	1,26
Australia	1,11
Chile	1,08
Mexico	1,04
Others	20,48

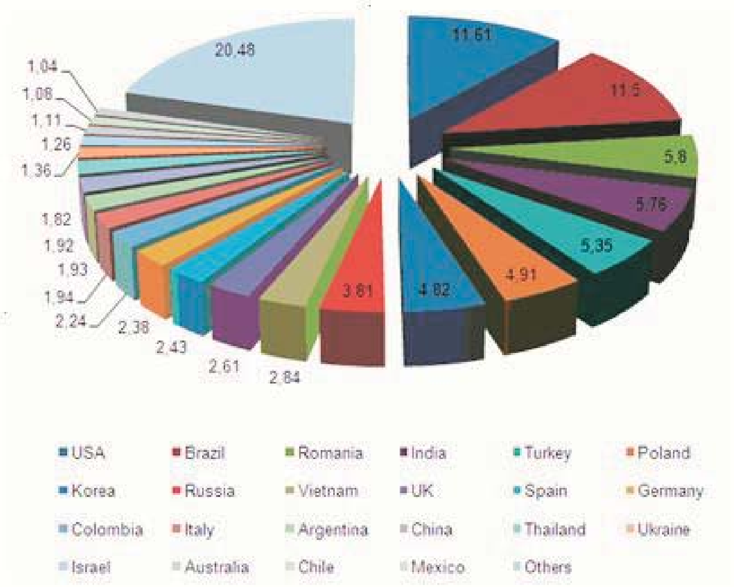


Figure 12. Geographical distribution of spam sources.

Quarterly Spam Report

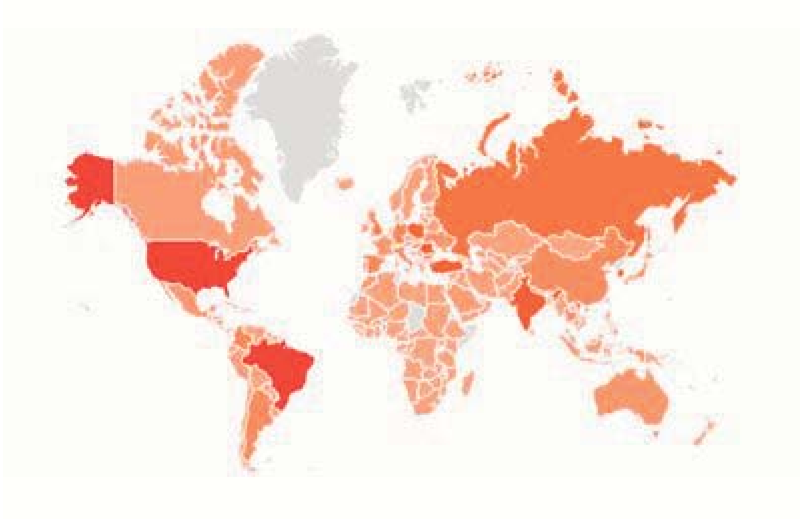


Figure 13. Geographical distribution of spam
(the deeper the color, the higher the spam level).

The figure below shows the location of the top spamming regions according to the source IP address. Green shows moderate spammers, orange shows moderate-high spammers and red indicates massive spammers.

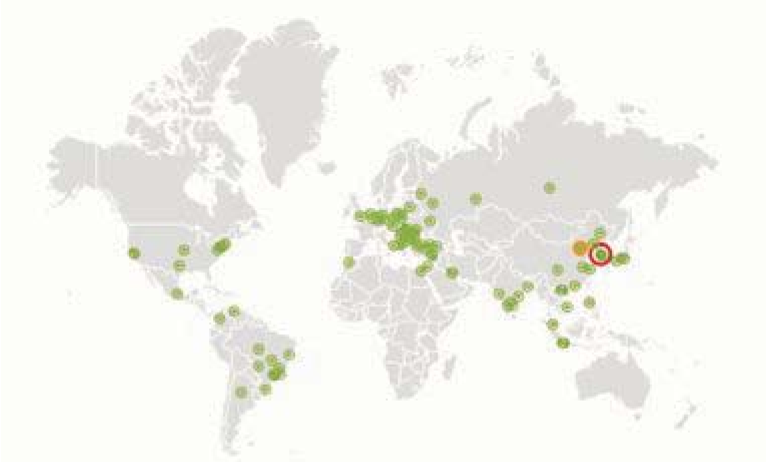


Figure 14. Spamming centers by IP address.

Quarterly Spam Report

Two IP addresses are particularly noteworthy: 58.211.75.8, with over 1,000 emails sent out and based in Beijing, and 211.234.119.69, with almost 3,400 emails sent out, and based in Seoul.

As shown in the image below, the highlighted points also show circles in different colors. This indicates that several important spammers coexist in those cities.

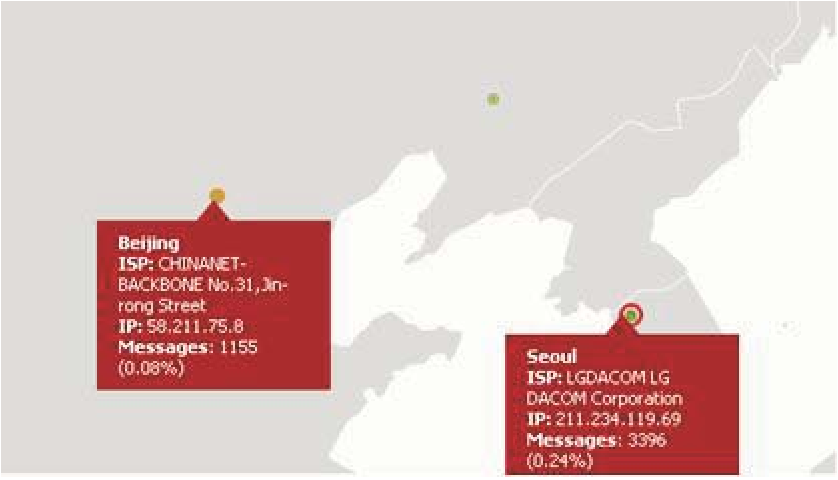


Figure 15. Other important spamming centers.

Quarterly Spam Report

In Europe, it is Eastern countries that concentrate the vast majority of spamming centers.

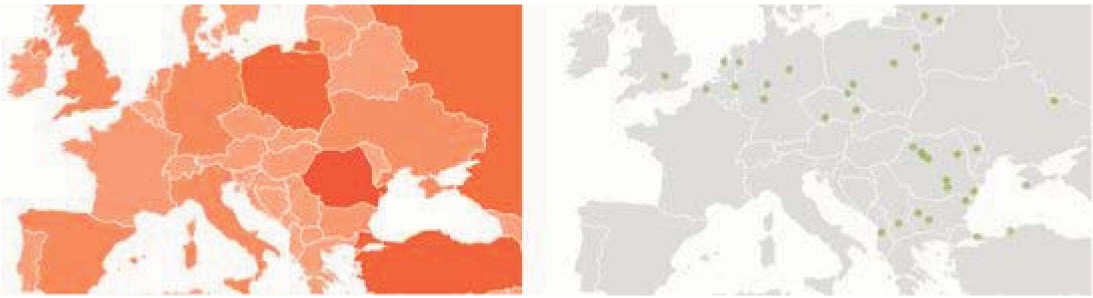


Figure 16. Spam sources in Europe.

Spam URLs

After analyzing the source of spam we will now analyze the servers that host the web pages that spam messages point to. As previously mentioned, spam sending is prosecuted in certain countries, whereas in countries like the United States some prison sentences have been issued for spammers. However, in the case of the web pages that spam points to it is almost impossible to identify who is behind them. That's why the map of spam sources changes considerably with regard to Western countries.

Quarterly Spam Report

Most of these web pages are hosted in the United States, Europe and China, the main markets that spam targets at.

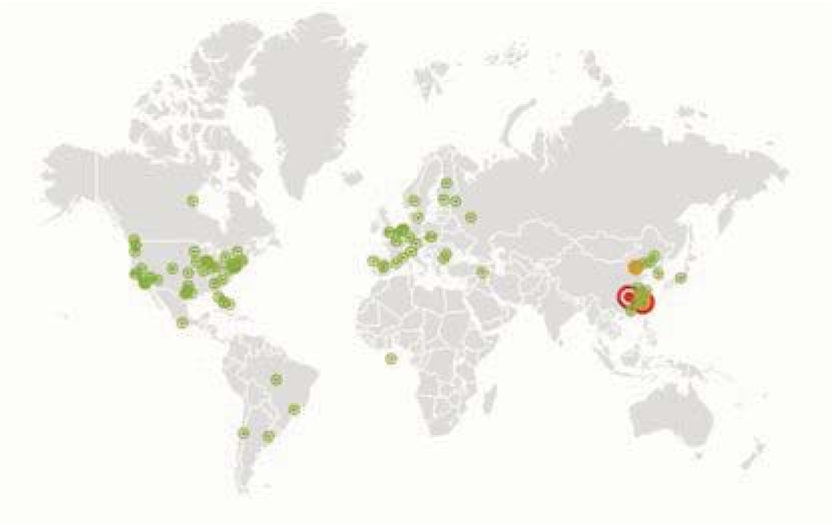


Figure 17. Hosting of spam URLs.

Conclusion

The conclusion that can be drawn from this data is that the anti-spam policies implemented by certain governments and specially ISPs have caused botnets to become spammers' weapon of choice. As they are low-intensity sources, they don't draw people's attention and are less likely to be listed on DNSBLs[3]. Also, they allow spammers to escape any accountability.

It is worth mentioning that the shutdown of McColo, the ISP that controlled the largest botnet in the world, in November last year made spam traffic decline by 75%. It is very important to raise awareness among users of the need to keep their systems free of malware. This will not only help keep the integrity of their IT systems and data, but will also reduce possible sources of spam.

[3] DNSBL are lists of possible IP addresses used to send out spam. These IP addresses have been identified either because some SPAMTRAP network has received spam from them, or because users have received spam from those addresses and have reported them, or because they are considered IP addresses from which no such volume of emails should be sent (home connections). These IP addresses are collected and updated by institutions such as SpamHaus and used by several email servers to reject emails sent from those IP addresses.

Vulnerabilities in Q1 2009

MS09-001, the first security bulletin issued by Microsoft in 2009, included several critical updates for all Windows systems. These updates fixed two privately reported vulnerabilities and one publicly disclosed vulnerability in Microsoft Server Message Block (SMB) Protocol. An attacker who successfully exploited these vulnerabilities could run code on unpatched Windows systems. This way, affected computers were completely compromised.

The second bulletin of the year, MS09-002, addressed several vulnerabilities in Internet Explorer. This browser is probably Microsoft's application most affected by security flaws.

Microsoft Exchange and Microsoft SQL Servers were subject to attacks in February. Two critical vulnerabilities were discovered in Microsoft Exchange Server, whereas one was detected in Microsoft SQL Server. The latest affected the stored procedure sp_replwritetovarbin and even though it was first discovered in December 2008, it wasn't finally resolved by Microsoft until February 2009. These three vulnerabilities were corrected in the MS09-003 and MS09-004 bulletins respectively.

Security researchers have also turned their attention to office applications. In February, a 0-day vulnerability was discovered in Microsoft Excel that was being used to install malware in governmental organizations in Asia. So far, Microsoft has not published any patches to fix this vulnerability. It has, however, given some recommendations in its security advisory 968272. We have published a post on the PandaLabs blog informing how the TruPrevent tehnologies included in our antivirus programs have protected our clients right from the appearance of the first vulnerable .xls files.

Besides Microsoft Excel, Microsoft Office Visio has also been affected by several vulnerabilities. However, this time, Microsoft published a security bulletin -MS09-005- including the patches that fixed the three vulnerabilities that could be exploited to run code on affected computers.

Vulnerabilities in Q1 2009

Several critical flaws were also revealed that affected PDF files, turning Adobe Acrobat and Adobe Reader vulnerable. Even the Foxit Reader free application was found affected by a flaw similar to the others. This is probably due to the fact that more and more users are turning to this free application to view PDF files, which has caused malware writers to include it on their hit list.

Finally, Microsoft has published a number of security updates in March: MS09-006, MS09-007 and MS09-008. The flaw covered in MS09-006 is due to incorrect validation of input passed from user mode parsed through the kernel component of DGI. This vulnerability is highly critical and affects all Windows versions. The 2 remaining vulnerabilities are of the spoofing type. The first one was addressed in bulletin MS09-007 and affected the Secure Channel (SChannel) security package in Windows. The other vulnerability affected Microsoft's WINS and DNS servers. We have published a post on the PandaLabs blog that shows an analysis conducted in our laboratory on Microsoft's update for fixing this vulnerability detected on the Windows DNS server.

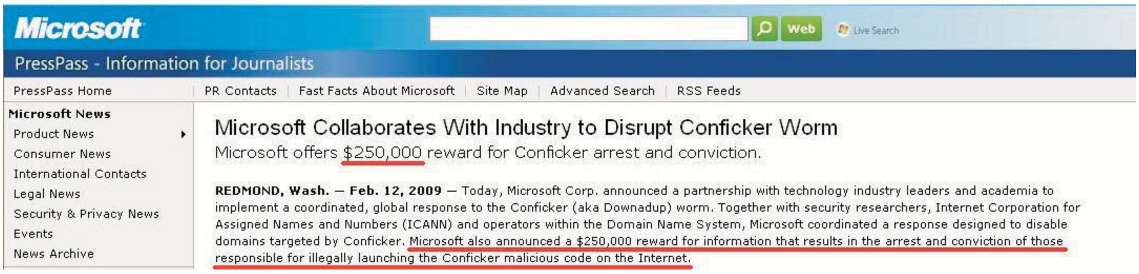
At Panda Security we are continuously improving our products to protect our clients against new vulnerabilities. We'd like to recommend users to install the updates made available in Microsoft's security bulletins as soon as possible, as well as other security updates that may affect other products installed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

The most significant malicious codes in Q1

Conficker

Having affected approximately 10 million computers (including computers belonging to British and French military organizations), the Conficker worm is the most important malware strain of this last quarter.

The extent of the attack has lead Microsoft to offer a $250,000 reward to whoever provides information about its creators.



Microsoft Collaborates With Industry to Disrupt Conficker Worm

Microsoft offers $250,000 reward for Conficker arrest and conviction.

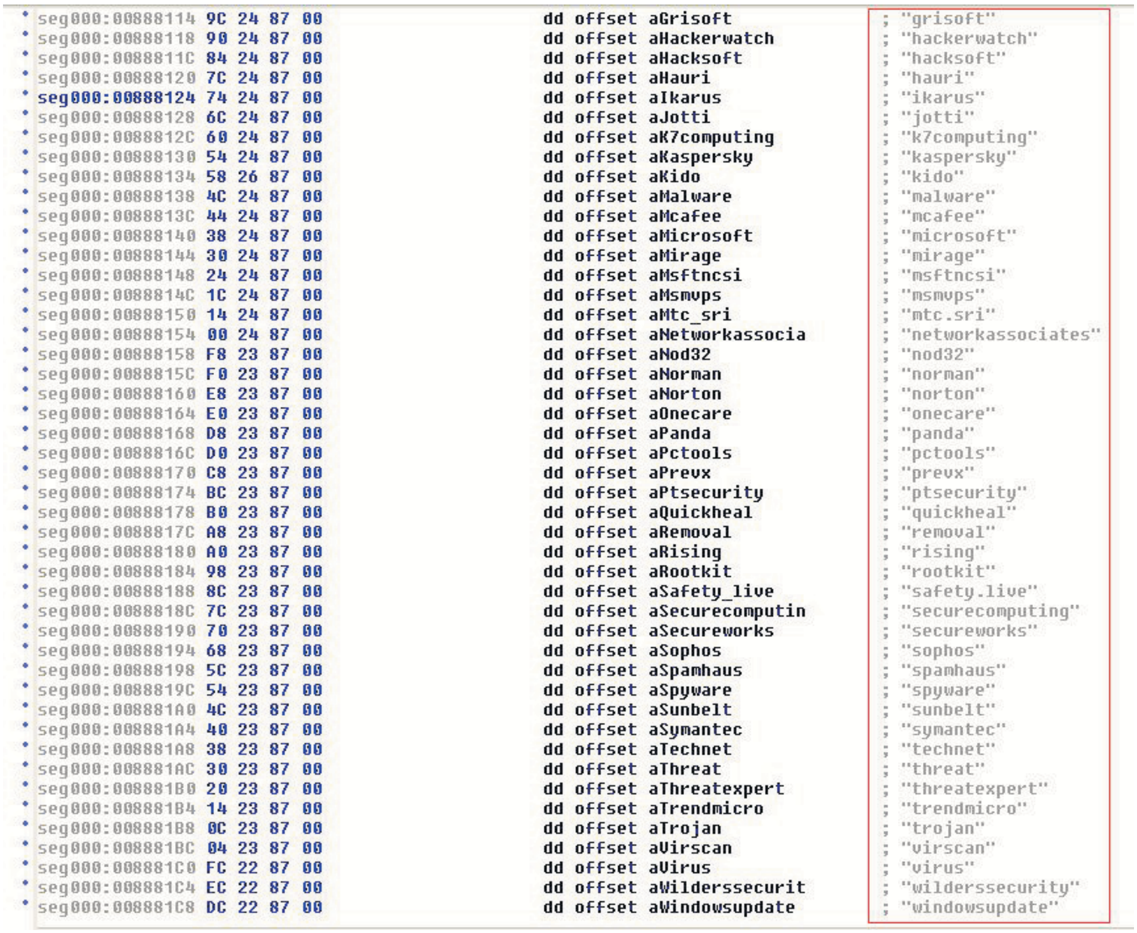
REDMOND, Wash. — Feb. 12, 2009 — Today, Microsoft Corp. announced a partnership with technology industry leaders and academia to implement a coordinated, global response to the Conficker (aka Downadup) worm. Together with security researchers, Internet Corporation for Assigned Names and Numbers (ICANN) and operators within the Domain Name System, Microsoft coordinated a response designed to disable domains targeted by Conficker. Microsoft also announced a $250,000 reward for information that results in the arrest and conviction of those responsible for illegally launching the Conficker malicious code on the Internet.

Figure 18. Article published by Microsoft offering a reward.

The most significant malicious codes in Q1

Here are just a few examples of common passwords: 123456, qwerty, admin., password, login, default, etc.

Malicious actions carried out by this worm include monitoring active system processes to eliminate those corresponding to security applications and reduce the computer's protection level, and preventing web access to the most important software domains and security forums.



```
seg000:00888114 9C 24 87 00          dd offset aGrisoft           ; "grisoft"
seg000:00888118 90 24 87 00          dd offset aHackerwatch       ; "hackerwatch"
seg000:0088811C 84 24 87 00          dd offset aHacksoft          ; "hacksoft"
seg000:00888120 7C 24 87 00          dd offset aHauri             ; "hauri"
seg000:00888124 74 24 87 00          dd offset aIkarus            ; "ikarus"
seg000:00888128 6C 24 87 00          dd offset aJotti             ; "jotti"
seg000:0088812C 60 24 87 00          dd offset aK7computing       ; "k7computing"
seg000:00888130 54 24 87 00          dd offset aKaspersky         ; "kaspersky"
seg000:00888134 58 26 87 00          dd offset aKido              ; "kido"
seg000:00888138 4C 24 87 00          dd offset aMalware           ; "malware"
seg000:0088813C 44 24 87 00          dd offset aMcafee            ; "mcafee"
seg000:00888140 38 24 87 00          dd offset aMicrosoft         ; "microsoft"
seg000:00888144 30 24 87 00          dd offset aMirage            ; "mirage"
seg000:00888148 24 24 87 00          dd offset aMsftncsi          ; "msftncsi"
seg000:0088814C 1C 24 87 00          dd offset aMsmvps            ; "msmvps"
seg000:00888150 14 24 87 00          dd offset aMtc_sri           ; "mtc.sri"
seg000:00888154 00 24 87 00          dd offset aNetworkassocia    ; "networkassociates"
seg000:00888158 F8 23 87 00          dd offset aNod32             ; "nod32"
seg000:0088815C F0 23 87 00          dd offset aNorman            ; "norman"
seg000:00888160 E8 23 87 00          dd offset aNorton            ; "norton"
seg000:00888164 E0 23 87 00          dd offset aOnecare           ; "onecare"
seg000:00888168 D8 23 87 00          dd offset aPanda             ; "panda"
seg000:0088816C D0 23 87 00          dd offset aPctools           ; "pctools"
seg000:00888170 C8 23 87 00          dd offset aPrevx             ; "prevx"
seg000:00888174 BC 23 87 00          dd offset aPtsecurity        ; "ptsecurity"
seg000:00888178 B0 23 87 00          dd offset aQuickheal         ; "quickheal"
seg000:0088817C A8 23 87 00          dd offset aRemoval           ; "removal"
seg000:00888180 A0 23 87 00          dd offset aRising            ; "rising"
seg000:00888184 98 23 87 00          dd offset aRootkit           ; "rootkit"
seg000:00888188 8C 23 87 00          dd offset aSafety_live       ; "safety.live"
seg000:0088818C 7C 23 87 00          dd offset aSecurecomputin    ; "securecomputing"
seg000:00888190 70 23 87 00          dd offset aSecureworks       ; "secureworks"
seg000:00888194 68 23 87 00          dd offset aSophos            ; "sophos"
seg000:00888198 5C 23 87 00          dd offset aSpamhaus          ; "spamhaus"
seg000:0088819C 54 23 87 00          dd offset aSpyware           ; "spyware"
seg000:008881A0 4C 23 87 00          dd offset aSunbelt           ; "sunbelt"
seg000:008881A4 40 23 87 00          dd offset aSymantec          ; "symantec"
seg000:008881A8 38 23 87 00          dd offset aTechnet           ; "technet"
seg000:008881AC 30 23 87 00          dd offset aThreat            ; "threat"
seg000:008881B0 20 23 87 00          dd offset aThreatexpert      ; "threatexpert"
seg000:008881B4 14 23 87 00          dd offset aTrendmicro        ; "trendmicro"
seg000:008881B8 0C 23 87 00          dd offset aTrojan            ; "trojan"
seg000:008881BC 04 23 87 00          dd offset aVirscan           ; "virscan"
seg000:008881C0 FC 22 87 00          dd offset aVirus             ; "virus"
seg000:008881C4 EC 22 87 00          dd offset aWilderssecurit    ; "wilderssecurity"
seg000:008881C8 DC 22 87 00          dd offset aWindowsupdate     ; "windowsupdate"
```

Figure 19. List of addresses of security companies.

The most significant malicious codes in Q1

Conficker disables services such as Windows Automatic Update, Windows Security Center, Windows Defender and Windows Error Reporting, leaving the system vulnerable to other malicious codes.

It also checks the system date and compares it to that of websites such as google.com, yahoo.com, ask.com, etc. If the latter is later than January 1 or another predefined date, it generates an algorithm, depending on the current system date, to access a web page and download other malicious codes.

Additionally, Conficker enables remote access through a backdoor with "self-update" features, allowing it to keep up-to-date on its creator's instructions.

Although a critical security patch has been released, there is a vulnerability window from the moment until the patch is actually applied by most users. Cyber-crooks use that vulnerability window to collect confidential information from the infected systems.

Even four months after Microsoft has published the patch there are computers that have been infected and that are unprotected due to administrators' or owners' neglect.

The most significant malicious codes in Q1

Waledac in Valentine's Day

Spammers tend to become more active as specific dates such as Christmas, New Year and Valentine's Day approach. During these periods, users are bombarded by annoying and occasionally malicious spam.

In the last two years, the Storm worm botnet accounted for the majority of spam sent around these dates. However, it is the Waledac family of malicious code that has most exploited Valentine's Day.

More annoying than malicious, the first malicious Valentine-related messages appeared long before February 14, and used a range of social engineering techniques to deceive users. Simply viewing their content makes cyber-crooks' activity viable.

The image below shows a typical page that users are redirected to when clicking one of the initial Valentine's Day spam messages:

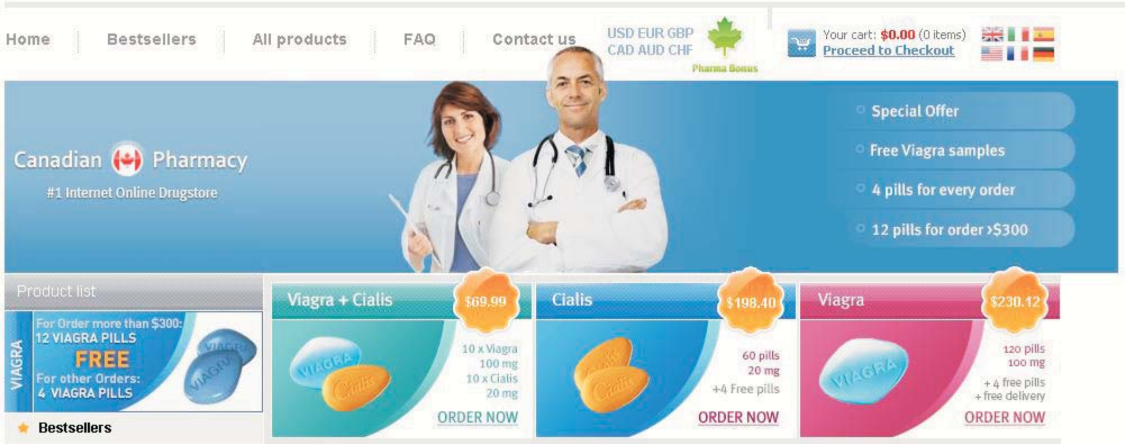


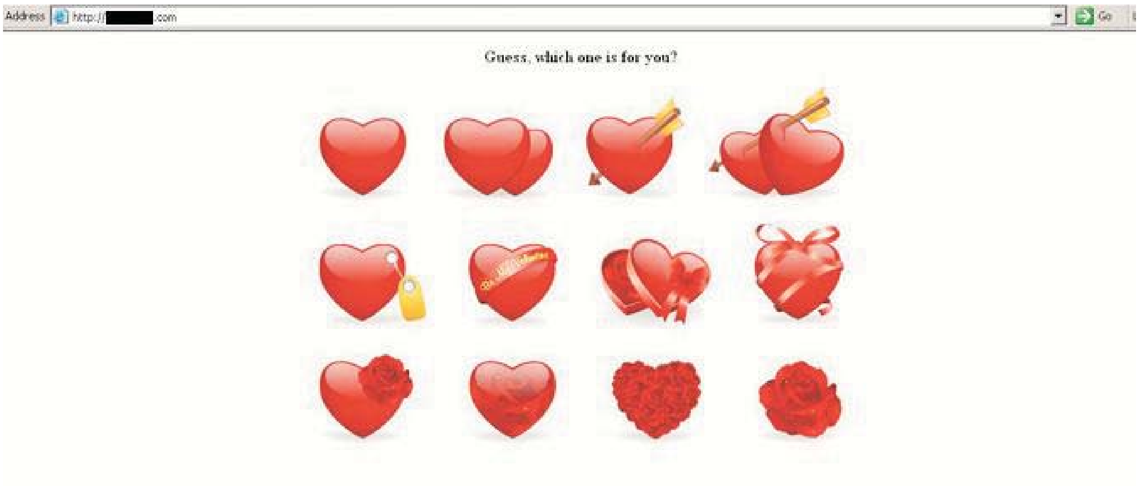
Figure 20. Website to which the first malicious Valentine's Day messages redirect users.

The most significant malicious codes in Q1

As well as distributing 'inoffensive' messages, cyber-crooks have used Valentine's Day to spread numerous malicious codes from the Waledac family through emails with malicious urls.

The *modus operandi* is similar to that of the first spam messages advertising pharmaceuticals, as they are distributed via email, in this case using Valentine-related messages informing recipients that someone has sent them a virtual card. The message contains a link that is redirected to a malicious domain in order to view the card.

Below is an example of a malicious domain:



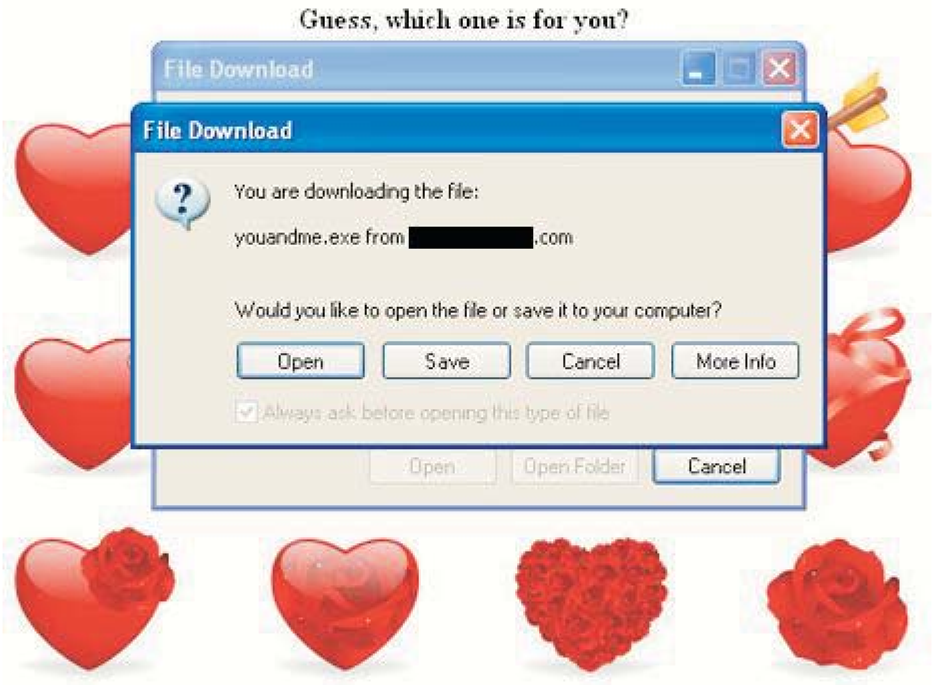
Address http://[redacted].com

Guess, which one is for you?

Figure 21. Malicious Waledac domain.

The most significant malicious codes in Q1

The worm is downloaded to the computer (automatically or through user interaction). However, for the download to be successful, users must agree to it:



Guess, which one is for you?

File Download

You are downloading the file:

youandme.exe from [redacted].com

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

☑ Always ask before opening this type of file

Figure 22. Download of the malicious file.

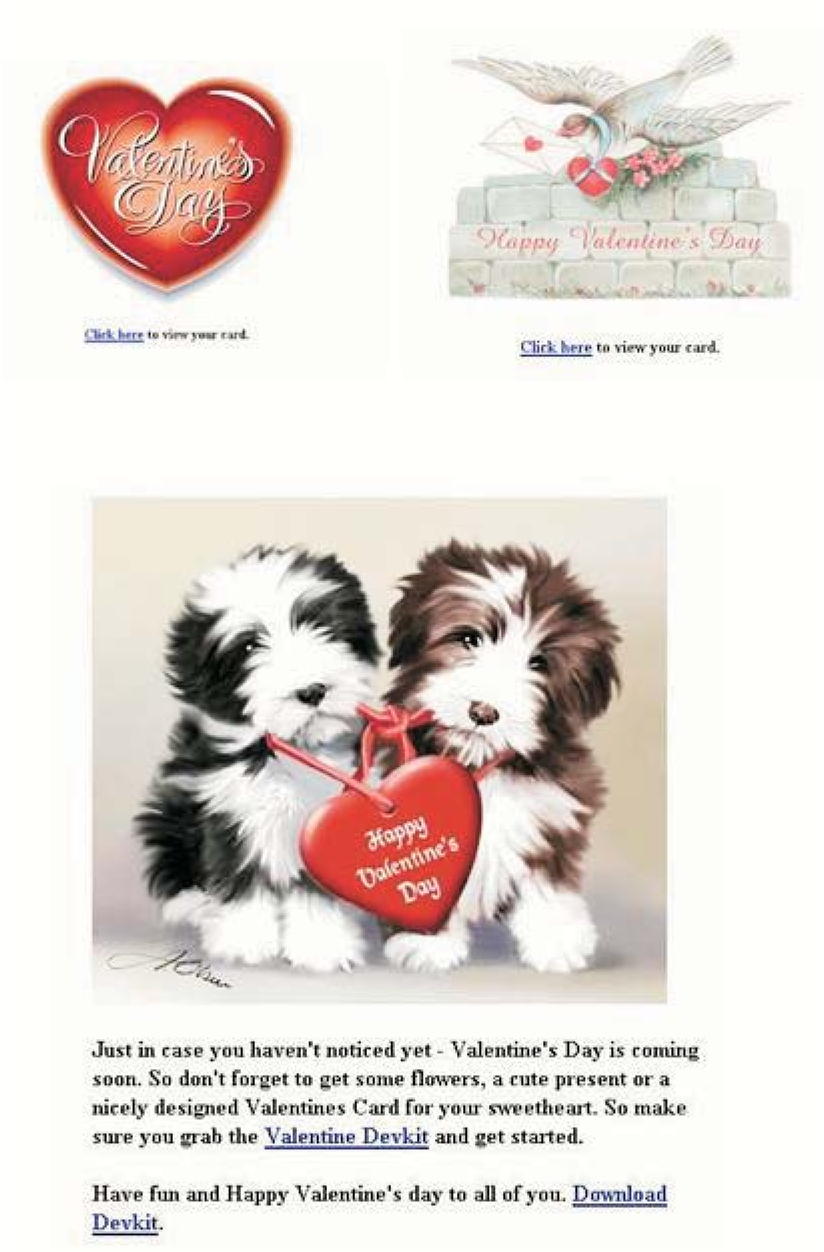
Cyber-crooks created numerous domains to distribute the Waledac worm using inoffensive names such as card.exe, ecard.exe, love.exe, loveyou.exe, meandyou.exe, etc.

Some of these domains were designed to modify the file to be downloaded in order to distribute different malicious codes and prevent security companies from detecting them. This idea of numerous small infections is known as a silent epidemic.

The impact of domains distributing malicious Waledac codes was so great that some domains were even highly-ranked in search engines. This could cause users trying to locate virtual cards to access malicious domains by accident.

The most significant malicious codes in Q1

Below are a few examples of malicious domains related to virtual Valentine cards:



Click here to view your card.

Click here to view your card.

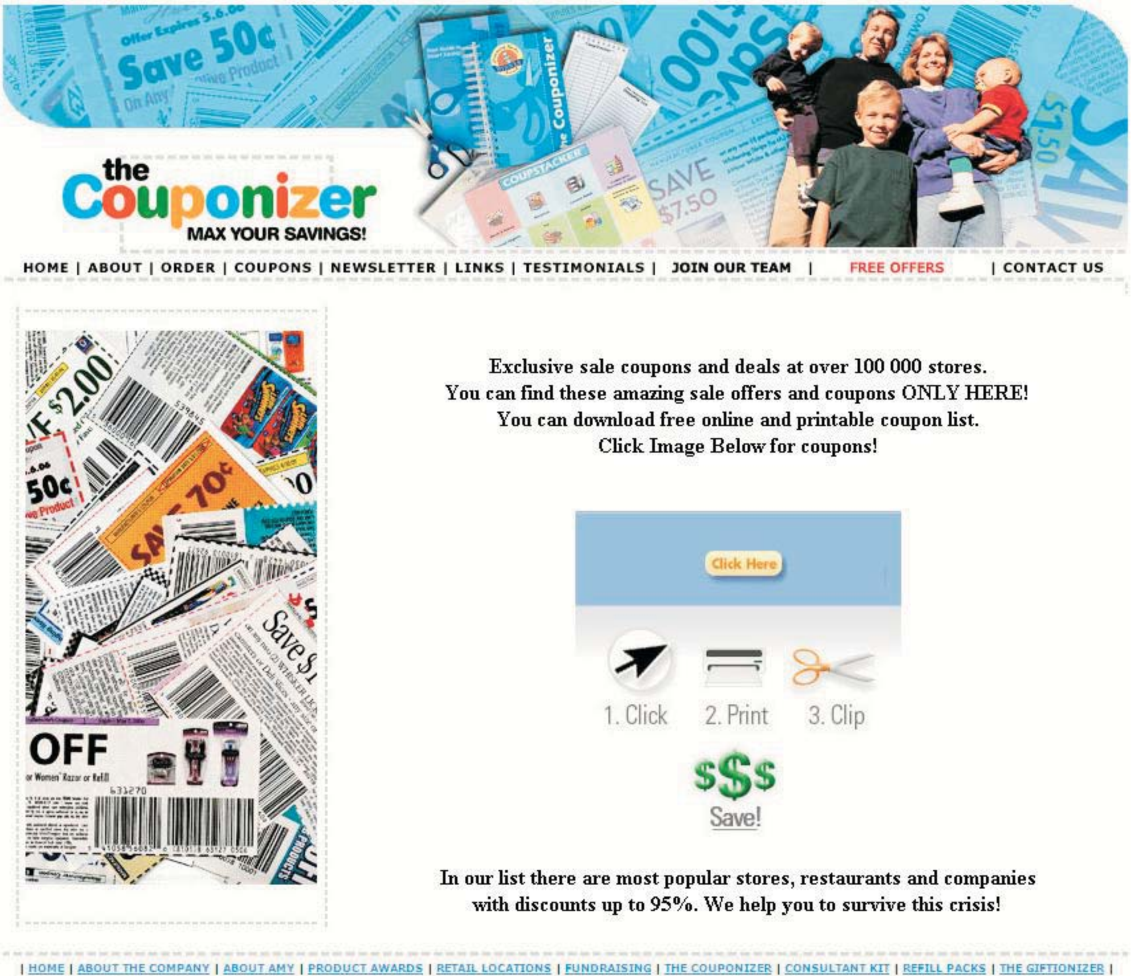
Just in case you haven't noticed yet - Valentine's Day is coming soon. So don't forget to get some flowers, a cute present or a nicely designed Valentines Card for your sweetheart. So make sure you grab the Valentine Devkit and get started.

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

Figure 23. Examples of malicious domains related to Valentine's Day.

The most significant malicious codes in Q1

Waledac has not only been active before Valentine's Day; some weeks later, the domains used to distribute malware were still offering exclusive discount coupons.


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

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!

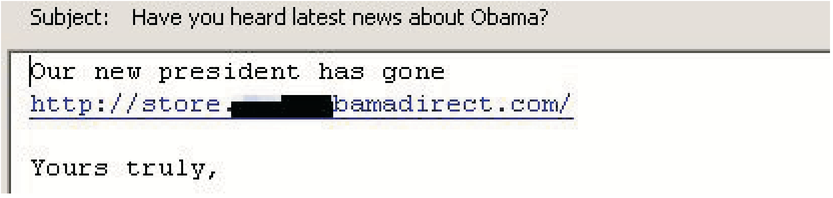
Figure 24. Website offering discount vouchers.

The most significant malicious codes in Q1

These coupons also correspond to Waledac, but use different names: couponlist.exe, coupons.exe, list.exe or print.exe; in short, same dog, different collar.

At present, approximately 140 domains have been used to distribute malicious codes from the Waledac family.

Waledac has not only used Valentine-related issues, but also other important events such as the election of the US president. Cyber-crooks used a story about Barack Obama turning down the presidency to attract users' attention.

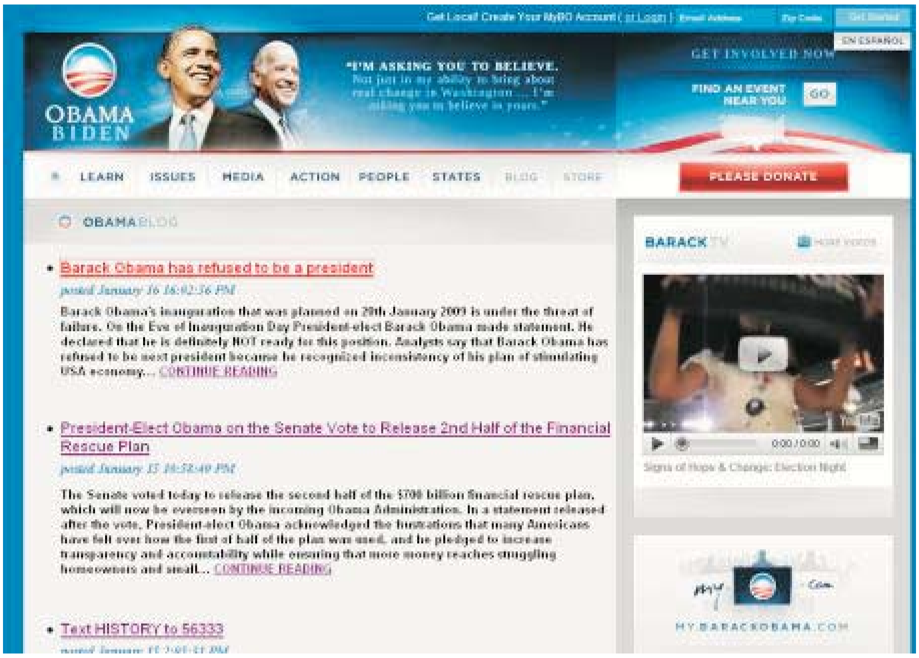


Subject: Have you heard latest news about Obama?

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

Yours truly,
```

Figure 25. Email about Barack Obama turning down the presidency.


Get Local! Create Your MyBO Account (or Login) | Email Address | Zip Code | Get Started
EN ESPAÑOL
OBAMA BIDEN
"I'M ASKING YOU TO BELIEVE. Not just in my ability to bring about real change in Washington ... I'm asking you to believe in yours."
GET INVOLVED NOW
FIND AN EVENT NEAR YOU
GO
LEARN
ISSUES
MEDIA
ACTION
PEOPLE
STATES
BLOG
STORE
PLEASE DONATE
OBAMABLOG
BARACKTV
MORE VIDEOS
0:00 / 0:00
Signs of Hope & Change: Election Night
MY.BARACKOBAMA.COM

- 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 16:52:40 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

  posted January 15 2:01:11 PM

Figure 26. Website displaying spoof news about Barack Obama.

The most significant malicious codes in Q1

Here are some of the most significant actions these malicious codes take on entering computers:

- They modify the system registry entries, so they can run on the next system restart.
- The worm searches for email addresses in the hard disk drives, removable drives and on shared networks.
- They encrypt the information collected, store it on a file using a random name, and send it to different addresses.
- The system spreads new spam messages to infect as many people as possible.
- The backdoor component opens a TCP communication port that allows remote users to connect and run arbitrary commands on infected systems.

At present, there are still different opinions on whether Waledac is an evolution of Storm worm, or Storm worm itself, as it has many similarities regarding its distribution and malicious effects on the system. Regardless of this, together with the Conficker worm, it is one of the most significant malicious codes this quarter.

2009 Q1 Trends

If the Trends section in this report partly coincides with our 2009 expectations, it demonstrates we have done a good job. And this is so, as we predicted specific viruses would re-emerge and Sality.AO is such an example.

Sality.AO

Sality.AO uses old techniques, i.e. EPO and Cavity. Both techniques are related to the way in which the original file is modified to be infected, making the infection more difficult to detect and consequently more difficult to disinfect. The EPO technique allows the legitimate file to run before beginning the infection, making its detection more difficult. The Cavity technique on the other hand, consists in using the blank spaces of the code in the legitimate file to insert the malicious code.

These techniques differ significantly from those obtained through automatic malware creation tools, which have been responsible for the significant increase of threats in recent years. They also require greater skill as well as an extensive knowledge in programming malicious code. In addition, Sality.AO implements extra features such as the possibility to connect to an IRC channel to receive instructions from its creator. This way, the creator can take control of the computer.

As well as infecting files using older techniques, Sality.AO also uses more modern mechanisms to spread across the Internet. For example, it infects PHP, ASP and HTML files on a computer with an iFrame tag. When one of these files is run, the browser is redirected to a malicious page which launches an exploit on the computer (without the user's knowledge) to download new malware samples.

If the infected files are loaded to a web page (the extensions of the infected files are typical of the types of files loaded to the web), users that visit or download from those pages will be infected.

The file downloaded through this technique is a Trojan infected by a virus (an older variant of Sality). Additionally, the Trojan has downloader functions to continue downloading new malware onto the computer.

2009 Q1 Trends

Social networks

Security companies have been warning users about social networks, informing them that their personal data could be accessed by third-parties and that these networks are sometimes used to spread malware.

In 2008 we detected isolated events affecting social networks. However, in the first quarter of 2009 there have been numerous incidents. Apart from typical malware such as Boface (also known as Koobface) that uses social networks to spread, we have detected social networks with links that direct users to malware (in the form of comments), trying to trick them into becoming infected.

This in itself is not new; it is something they have always done: exploiting users' curiosity to fool them and redirect them to advertisements or infect them. The difference is they are starting to do it massively on popular websites: digg.com, YouTube, Facebook, Twitter...

Conficker

We must not forget to include Conficker in the 2009 Q1 summary, as it has caused millions of infections over a very short period. Although the situation is currently under control, this worm is able to generate URLs to which it connects in order to download malicious code. The latest known variant will start to generate 50,000 URLs on a daily basis from April 1. We believe hackers will use it to infect users with new Conficker variants or other malicious codes.

USB VACCINE

Removable drives have become a major channel for the propagation of malicious code, due to the increasing use of memory sticks and portable hard disks to share information (in households and corporate environments).

Nowadays, most companies have perimeter protection (firewall, etc.), but this does not prevent employees from taking their memory sticks to work, connecting them to the workstation and spreading the malicious code across the network. Panda Research has developed a free tool that allows users to protect their removable drives from malware: USB vaccine.

2009 Q1 Trends

AMTSO

The next AMTSO meeting will take place in Budapest in May, where we will validate a series of documents we have worked on in the last few months. We will offer you further details in the next report.

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/.