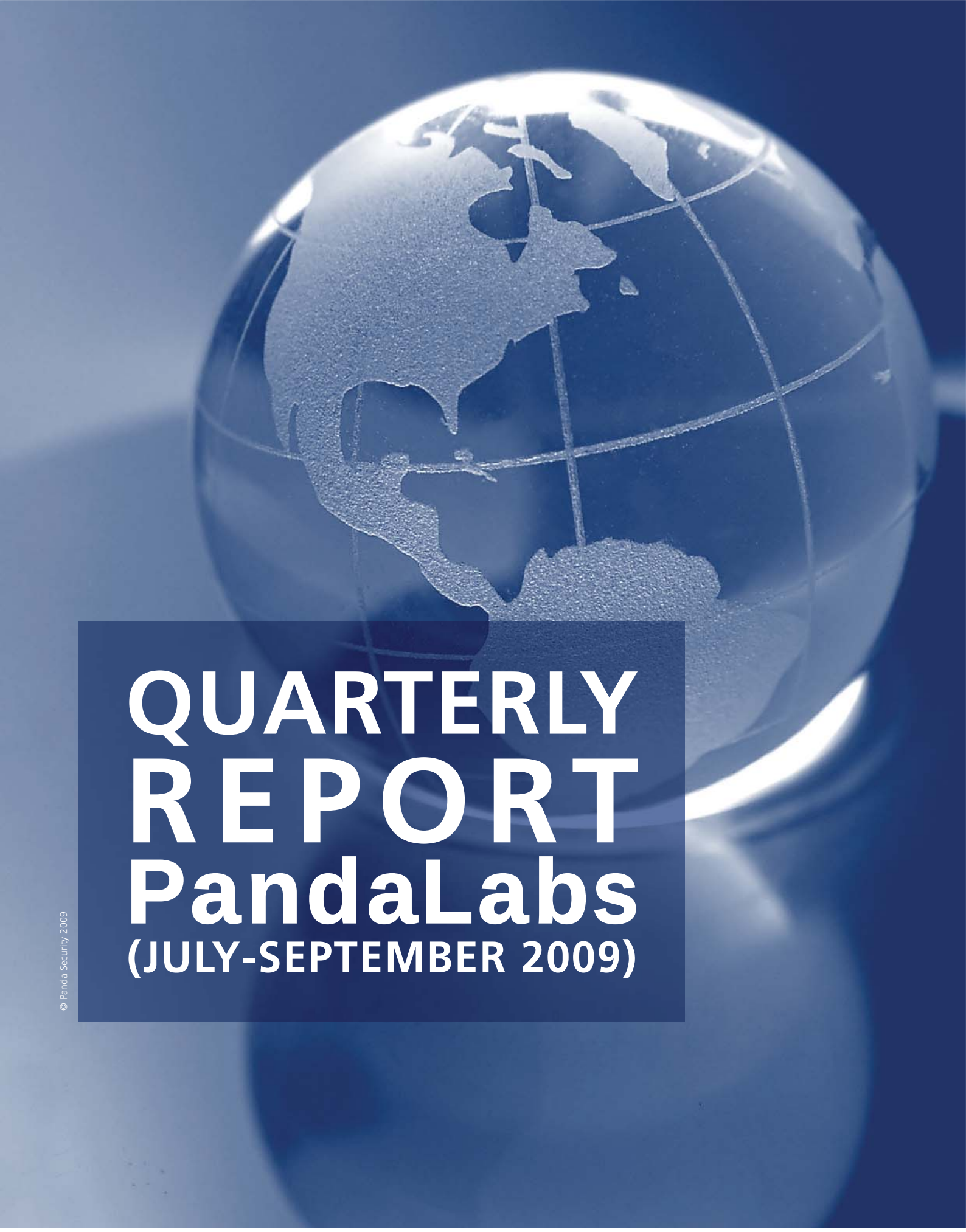

QUARTERLY REPORT PandaLabs (JULY-SEPTEMBER 2009)

© Panda Security 2009

PANDA SECURITY | 20th Anniversary 1990-2010

Index

Introduction

Here we present the Q3 report, which examines some of the most interesting events of this quarter.

As we have commented in previous reports, NDRs are being used for spamming. We will go over the current situation of NDRs and provide technological solutions to prevent malicious ones.

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

We will also analyze the most important malware trends during this quarter. As with the last quarter, several attacks using BlackHat SEO techniques have been infecting users.

Additionally, the Koobface family (a social network worm) has started using Twitter to spread by publishing malicious links from infected users' accounts.

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

We hope you find it interesting.

Executive summary

The type of malware most detected by **PandaLabs**' security sensors in the third quarter of 2009 were Trojans at 37.70%, up three points from the previous quarter.

Once again Taiwan is the country with most active malware (28.99%), followed by the U.S. (25.62%) and the U.K. (25.27%).

The creators of Waledac (also known as Storm Worm) used Independence Day in the USA as a ruse to infect users.

A few days later, a new 0-day vulnerability appeared which affected Microsoft Video ActiveX Control, and was exploited by several Chinese websites.

At the beginning of July, a DDoS (Distributed Denial of Service) attack was launched against several governmental, military and financial South Korean and American websites.

From August onwards, increases of up to 2000% were detected in NDR traffic used for spamming.

In September, a new 0-day exploit was detected which affected Microsoft Windows operating systems, from Vista to Windows 2008, and which could allow remote code execution.

Cyber-crooks' are trying to infect the maximum number of computers possible, exploiting vulnerabilities and using social engineering techniques in spam messages, social networks and search engines through Blackhat SEO techniques.

Distribution of the new threats detected

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

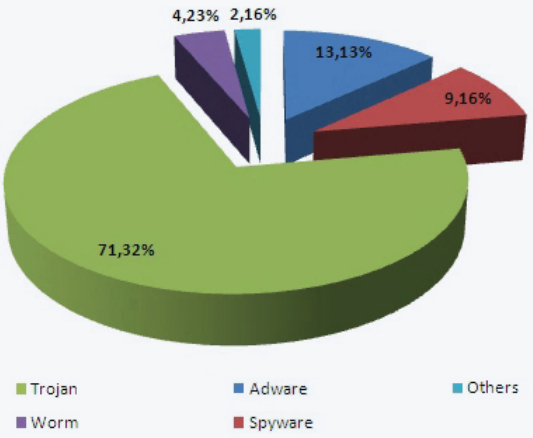

FIG.01

QUARTERLY MALWARE DISTRIBUTION

As illustrated in the graph, the predominant malware category throughout Q3 has been Trojans (71.32%), up nearly half a point 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 slightly decreased, now accounting for 4.23% as opposed to 4.40% in the previous quarter.

On the other hand, spyware has increased for the first time this year, rising from 6.90% to 9.16%. Adware however has decreased slightly from 16.37% to 13.13%, yet it was still the second most detected malware category this year.

This position 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'.

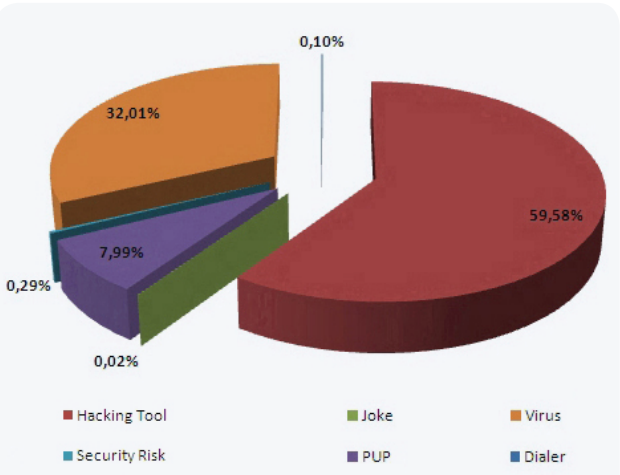

FIG.02

OTHER MALWARE

Hacking tools are the leading malware in this section, at 59.98%, followed by viruses which have significantly increased from 18.16% in the second quarter to 32.01% in the third quarter.

Month by month

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

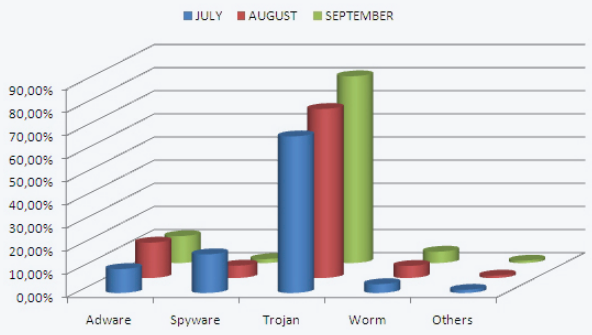

FIG.03

EVOLUTION OF NEW MALWARE

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

Threats detected by the PandaLabs sensors

The following graph shows the infection levels per malware type detected by Panda Security's security sensors throughout the third quarter of 2009:

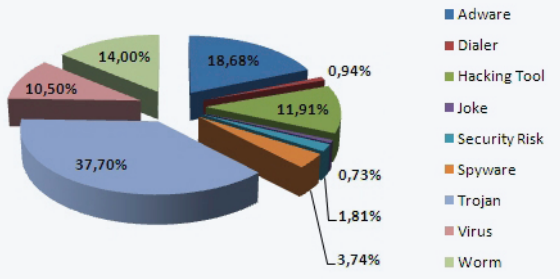

FIG.04

DISTRIBUTION (DETECTED BY PANDALABS SENSORS)

Adware infection levels have remained relatively stable over the last quarter (18.68%) due to the large volume of fake antiviruses that are currently in circulation, but are far behind the main threat detected by our security sensors, Trojans (37.70%), over three points up on last quarter's 34.37%.

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

1	Generic Trojan
2	Generic Malware
3	Trj/Lineage.BZE
4	Trj/Downloader.MDW
5	W32/AutoRun.APJ.worm
6	Adware/AccesMembre
7	Spyware/Virtumonde
8	W32/Bagle.RC.worm
9	Trj/Rebooter.J
10	Generic Worm

FIG.05

TOP TEN THREATS

Active malware

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

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

Latent malware is malware that is on a PC but not taking any action. It is waiting to be run, 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 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.

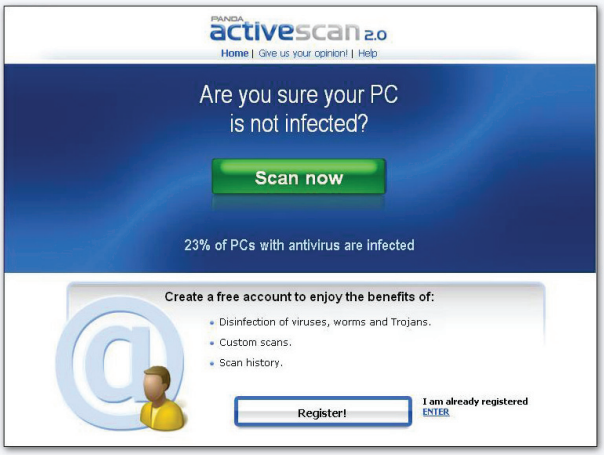

FIG.06

ACTIVESCAN 2.0 ONLINE TOOL

In this graph you can see how malware has evolved so far during Q3 2009.

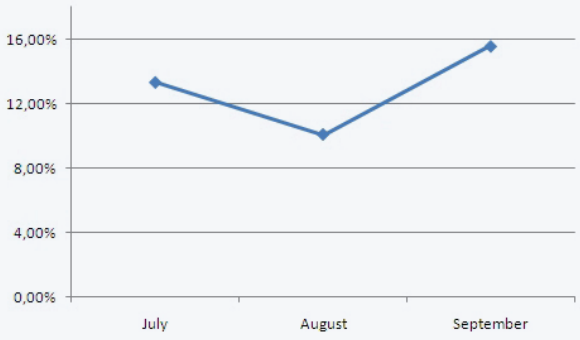

FIG.07

EVOLUTION OF ACTIVE MALWARE THROUGHOUT THE THIRD QUARTER OF 2009

As you can see in the graph above, although malware rates decreased during the summer, September holds the highest ratio of PCs infected with active malware, not only in the third quarter, but throughout the whole year (15.57%).

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 ActiveScan 2.0 in Q3.

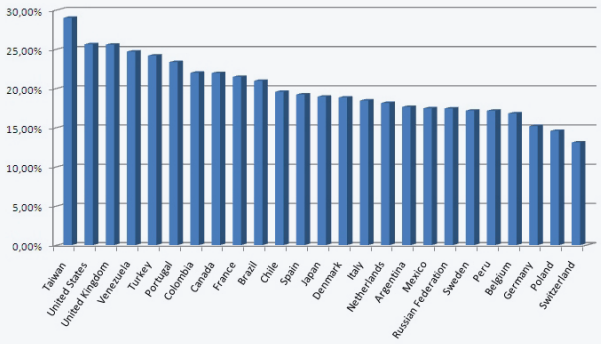

FIG.08

COUNTRIES WITH THE HIGHEST MALWARE PERCENTAGE (JULY-SEPTEMBER 2009)

Once again Taiwan is the country with most active malware (28.99%), followed by the U.S. (25.62%) and the U.K. (25.27%).

We must highlight Switzerland, which was among the least infected countries in the second quarter, and has managed to decrease its active malware rate (from 15% to 13.10%).

An NDR (Non Delivery Report) is an email automatically sent by mail systems to advise senders of problems delivering their messages.

In **previous reports** we have already explained what 'illegitimate' NDRs are (for our purposes we will refer to them simply as NDRs), and we have also mentioned that combating these threats is one of the priorities of our perimeter security solutions.

This article focuses on the current situation of NDRs and the technological improvements included in our products[1] to keep them at bay.

Current situation

NDRs have become a recurrent threat over the last few years as a result of the DHA[2] techniques used by spammers to send spam or detect valid email accounts. However, NDR circulation has increased up to 2000 percent from August this year.

This type of attack is usually carried out by botnets comprising infected computers. Therefore, the bandwidth and economic cost borne by spammers is very small. Also, these attacks have become more indiscriminate as the success/failure ratio does not have any impact on cost. This is increasing the collateral damage to users everywhere.

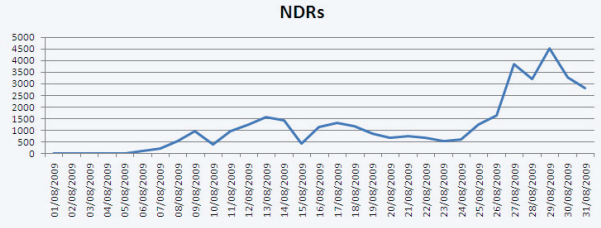

FIG.09

NUMBER OF NDRS RECEIVED AT ONE OF PANDALABS' SERVERS

Panda Security is using two techniques to combat this threat: BATV and NDR restriction.

BATV

BATV or Bounce Address Tag Validation is an anti-NDR technique consisting of adding tags to outbound messages so that in the event that an email message cannot be delivered, the NDR generated includes the relevant tag and can be recognized as a valid NDR generated as a result of the non-delivery.

Email messages that do not include these tags will be considered as illegitimate NDRs and rejected.

The way to include these tags in outbound messages and NDRs varies depending on how the BATV technology is implemented, even though the basics are essentially the same in all cases.

Tags are inserted in the sender's address during the SMTP connection. These tags identify messages unequivocally and can be checked in the event that an NDR is generated. For example if, during an SMTP connection, ***sender@pandasecurity.com*** is sent in the MAIL FROM command, the following tag is added: ***prvs=xxxxxxx=sender@pandasecurity.com***, where xxxxxxx is a unique code generated dynamically that identifies the message.

If the message is incorrectly delivered, a reply message will be sent to the sender's address with the tag of the original message: ***prvs=xxxxxxx=sender@pandasecurity.com***. Consequently, when the message goes through our solution, it will check the tag ***prvs=xxxxxxx*** and will deliver the message to the address ***sender@pandasecurity.com***.

---

1 Panda GateDefender Performa 3.2.00.

2 Directory Harvest Attack: A technique used by spammers to send email messages to combinations of common names and valid domains in order to discover existing accounts in certain domains and send spam to them. Out of all the various combinations tried by spammers, only a small percentage of them reach their objective, therefore, failed attempts will generate NDRs. Also, if you consider that spammers forge valid email addresses, these NDRs may reach users that have not sent any messages in the first place.

The following question may arise: If the message is correctly delivered, will the tags appear in the message sender field? The answer is no, as mail clients get a message sender's address from the "From" field (in the previous example, ***sender@pandasecurity.com***), which never changes. The use of these tags doesn't affect users.

Is it possible that a spammer sends a message with a valid tag, and our solution lets the NDR through? The code included in tags is generated from random values and keys unknown to spammers. Therefore, it is very difficult for spammers to generate valid values. Also, sending NDRs is not the spammers' primary intention, but a side effect derived from their actions. Therefore, it is very unlikely that spammers try to exploit this possibility.

Next, we will explain how BATV works in our products from a more technical point of view.

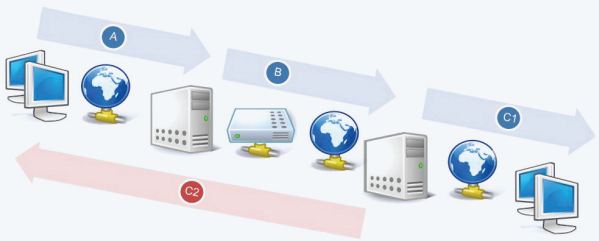

FIG.10

SMTP TRAFFIC AND NDR GENERATION AND DETECTION

A. Let's suppose you send a message from your account ***sender@pandasecurity.com*** to ***receiver@destination.com*** through your mail server.

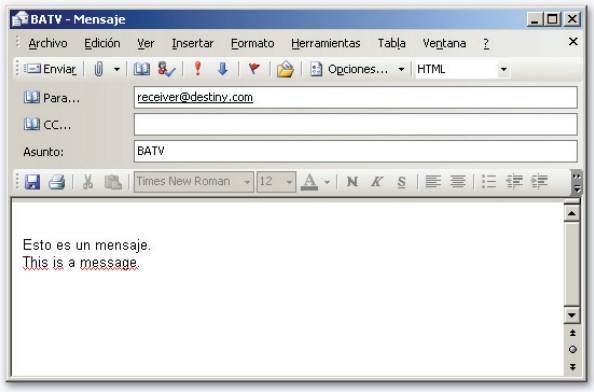

FIG.11

TEST EMAIL MESSAGE

B. Your server starts a SMTP connection with the destination.com server. The product (in this case Gate Defender Performa 3.2.00) intercepts the SMTP connection and modifies the "MAIL FROM" parameter (see *TABLE.01*).

C. There can be two situations during the third step:
1) The ***receiver@destination.com*** account exists and the message is delivered or
2) The ***receiver@destination.com*** account does not exist and an NDR is generated.

1. The destination.com server delivers the message to ***receiver@destination.com*** with the following format:

```
Return-Path: prvs=abcdefgh=sender@pandasecurity.com
From: sender@pandasecurity.com
To: receiver@destination.com
Date: Wed, 2 Sep 2009 12:49:31 +0200
Subject: BATV

Esto es un mensaje.
This is a message
```

FIG.12

FORMAT OF THE DELIVERED MESSAGE

Original SMTP Connection	Modified SMTP Connection
220 ESMTP	220 ESMTP
helo pandasecurity.com	helo pandasecurity.com
250 mail.destination.com	250 mail.destination.com
mail from: sender@pandasecurity.com	mail from: ***prvs=abcdefgh=sender@pandasecurity.com***
250 Ok	250 Ok
rcpt to: receiver@destination.com	rcpt to: receiver@destination.com
250 Ok	250 Ok
Data	Data
354 Enter mail, end with <CRLF>.<CRLF>	354 Enter mail, end with <CRLF>.<CRLF>
From: sender@pandasecurity.com	From: sender@pandasecurity.com
Subject: BATV	Subject: BATV
Esto es un mensaje.	Esto es un mensaje.
This is a message.	This is a message.
.	.
250 ok: queued as B028343F94	250 ok: queued as B028343F94
quit	quit
221 Bye	221 Bye

TABLE.01

ORIGINAL AND MODIFIED SMTP PROTOCOL

As the message is stored in the target server, the SMTP connection MAIL FROM parameter is saved as Return-Path. As previously mentioned, the mail client gets the sender address from the FROM field. The delivered message will look like this:

As you can see, added tags do not affect the way email messages are sent/received and are transparent to users.

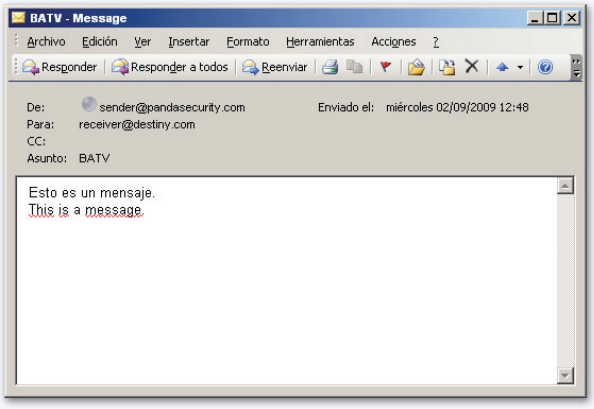

FIG.13

TEST EMAIL MESSAGE

2. If the target server accepts the connection but finds out that the target email account doesn't exist, it will send an NDR notice to the email address identified as the sender in the SMTP connection, i.e. to the address specified in MAIL FROM.

   In other words, an NDR will be returned to your server, to the address ***prvs=abcdefgh=sender@pandasecurity.com***.

   In this case, the SMTP connection will be analyzed again by our product (GateDefender Performa), restoring the original address, i.e. it will replace ***prvs=abcdefgh=sender@pandasecurity.com*** by ***sender@pandasecurity.com***, and ensure that the tag is correct and corresponds to an NDR generated from a message you have sent. (see *TABLE.02*).

   If the tag does not exist or is invalid, the NDR message will be rejected.

NDR restriction

Rather than an anti-NDR feature included in our products, this is more a policy that users can enable if they want to. Enabling this policy implies that all NDRs not received from a list of IP addresses defined by the user will be rejected. Users can add to that list relay servers or other trusted servers they want to receive NDRs from.

To illustrate how useful these policies can be, we will explain how legitimate NDRs are generated under two different configurations:

Configuration 1

A. The user sends an email message through their Email Server.
B. The email server connects to the email server that hosts the account the message has been sent to, informing it that it wants to deliver the message to that account.

Original SMTP Connection	*Modified SMTP Connection*
220 ESMTP	220 ESMTP
helo destination.com	helo destination.com
250 mail.pandasecurity.com	250 mail.pandasecurity.com
mail from: postmaster@destination.com	mail from: postmaster@destination.com
250 Ok	250 Ok
rcpt to: ***prvs=abcdefgh=sender@pandasecurity.com***	rcpt to: sender@pandasecurity.com
250 Ok	250 Ok
Data	data
354 Enter mail, end with <CRLF>.<CRLF>	354 Enter mail, end with <CRLF>.<CRLF>
Subject: Message Delivery Failure	Subject: Message Delivery Failure
This is the mail system at host destiny.com.	This is the mail system at host destiny.com.
I'm sorry to have to inform you that your message could not be delivered to one or more recipients…	I'm sorry to have to inform you that your message could not be delivered to one or more recipients…
.	.
250 ok: queued as B028343F94	250 ok: queued as B028343F94
quit	quit
221 Bye	221 Bye

TABLE.02

ORIGINAL AND RESTORED SMTP PROTOCOL

C. The server hosting the target account replies indicating that the account the message has been sent to doesn't exist.
D. The sender's server sends an NDR to the user indicating that the message could not be delivered since the account that the message was sent to does not exist.

Configuration 2 "Open Relay"

A. The user sends an email message through their Email Server.
B. The email server connects to the email server that hosts the account the message has been sent to, informing it that it wants to deliver the message to that account.
C. The server that hosts the target account accepts the connection, receives the message and ends the connection to the sender's server. It then checks the email's recipient and, should the account not exist, sends an NDR to the sender indicating that the account the message is sent to does not exist.

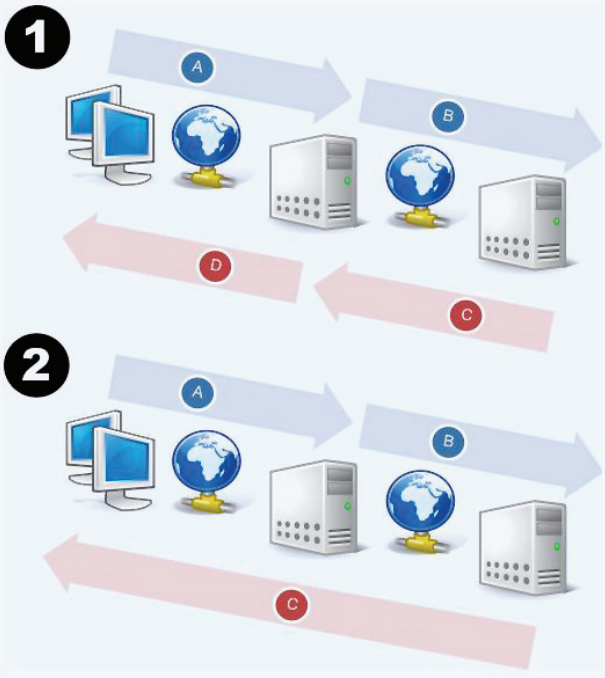

FIG.14

POSSIBLE CONFIGURATIONS IN EMAIL SERVERS

Configuration 1 is the standard configuration of an email system. You send an email message through your mail server or relay server, the mail server or relay server communicates with the target server, and it checks whether the account that the message is sent to exists. If it doesn't, you get an NDR generated by your mail server or relay server. So, according to this configuration, you should only receive NDRs from your mail server or relay server, which will always send legitimate NDRs. You could then reject all other NDRs not received from your mail server or relay server.

There could be problems with the servers that work with **Configuration 2**, which, even though considered an "incorrect" configuration, is used by users that want better performance as it allows you to manage larger traffic volumes with the same devices. In this case, the target server accepts all connections. It is not checked whether the corresponding target account exists for every message. If then, the target server finds out that the account does not exist, it sends the corresponding NDR indicating so. Using the NDR restriction policies you would reject legitimate NDRs generated by these "wrongly"[3] configured servers.

With the second configuration type users can choose from three options:

- Use the policy with their mail server and/or relay server and accept the possibility of losing certain NDRs from "wrongly" configured servers.
- Use the policy with their mail server, relay server and a series of "wrongly" configured servers that they want to receive NDRs from, despite running the risk of receiving illegitimate NDRs from those servers.
- Use BATV technology.

3 In this article we describe this configuration as wrong as most experts do not recommend it for being one of the causes of unwanted traffic.

In July, Microsoft published six security bulletins (MS09-029 to MS09-035). As is the norm nowadays, some of the new vulnerabilities affected the Microsoft Internet Explorer browser. These security flaws could allow remote code to run on computers when users visited a malicious Web page. This simple flaw could lead to a user's system being completely compromised. Microsoft also had to publish two additional updates (MS09-34 and MS09-035) to resolve critical vulnerabilities affecting the ATL (Active Template Library).

One of the most striking vulnerabilities published in the July bulletin (MS09-029) was a vulnerability reported by an anonymous researcher to iDefense, which could allow arbitrary code to be run remotely through a heap overflow when processing and interpreting source files. Microsoft had been aware of this vulnerability since 2008, according to the information provided by the Verisign subsidiary.

During July, other software companies released corrections for several vulnerabilities. On July 30, for example, Adobe published a bulletin addressing 12 remotely exploitable vulnerabilities, which affected popular products such as Flash Player and Acrobat Reader. Flaws resolved in this bulletin included the CVE-2009-1869 vulnerability which affects the ActionScript virtual machine. This bug, an integer overflow, affected versions 9 and 10 of Adobe Flash Player (practically all Adobe Flash Player installations).

In August, also affected by an integer overflow, Java's virtual machine had to be updated to solve the CVE- 2009-2675 vulnerability, which could allow a remote attacker to run arbitrary code simply by users visiting a malicious Web page.

Also in August, Microsoft published eight security bulletins (MS09-036 to MS09-042), including security updates for numerous Microsoft products: Microsoft Office, Media Player, Microsoft Active Template Library (ATL), ASP.NET, etc.

In the same month, Adobe resolved more Adobe Flash Player vulnerabilities, many of which were reported by companies such as iDefense and Tipping Point. Most of the vulnerabilities allowed arbitrary code execution when users visited a malicious Web page.

At the time of writing this article (September), a new, alarming 0-day exploit has appeared affecting Microsoft Windows operating systems from Vista to Windows 2008. According to Microsoft, the only operating system not affected is the retail version of Windows 7. However, the beta versions of the product are vulnerable.

The vulnerability was reported by Laurent Gaffie on September 7 through the popular "Full Disclosure" IT security list. The person who uncovered the vulnerability incorrectly believed it was simply a denial of service (more of a nuisance than a real problem). However, once the researcher Ruben Santamarta analyzed the bug, he realized it could allow arbitrary code to run.
At present there is no solution for this vulnerability, only a workaround involving the disabling of SMB2 (the new version of the Microsoft Windows protocol to share files and printers). In any event, the complexity of exploiting the bug at kernel level greatly reduces the risks of it being used by malware in the future as a means of propagation (as **Conficker** did in the past with the MS08-067 vulnerability).

To safeguard computers from these vulnerabilities, 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. Nevertheless, we strongly advise 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, e.g. Adobe, Mozilla, Google and Microsoft Office.

Once again, this year cyber-crooks took no vacations during the summer.

At the beginning of July, the creators of **Waledac** –a.k.a. Storm Worm– took advantage of the Independence Day celebrations in the US to launch a campaign to infect users. This time, potential victims were tricked into visiting a fake YouTube Web page showing what was supposed to be a 4th of July celebration video. As is usually the case with this type of attack, users that wanted to watch the video were displayed a message informing them that they had to install a codec to do so. However, this codec was in reality the Waledac worm. Once infected, the victim's computer sent out email messages aimed at causing other users to fall into the same trap.

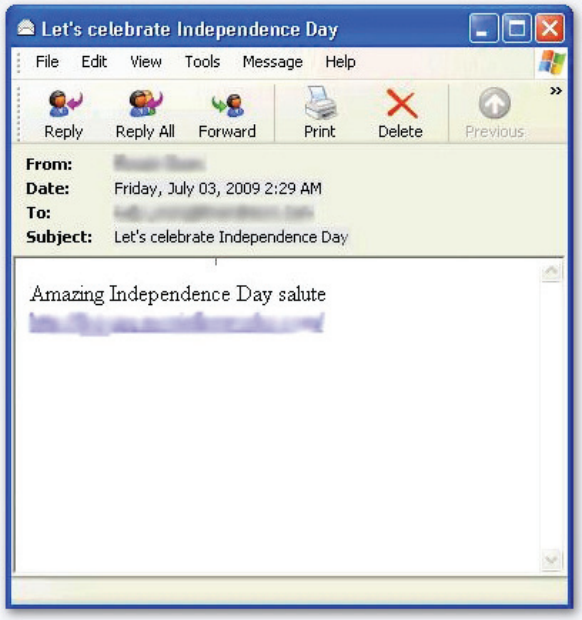

FIG.15

INDEPENDENCE DAY EMAIL MESSAGE

Some days later, a new **0-day vulnerability** was discovered which affected the Microsoft Video ActiveX Control. We found a dozen China-based Web pages that exploited this vulnerability. Soon after the vulnerability was revealed, Microsoft published a fix for the flaw.

This **video** shows how the vulnerability is exploited by cyber-hackers to run code on systems and how the TruPrevent preventive technologies block it without needing to have the security patch installed.

During the first days of July there was also a **DDoS (Distributed Denial of Service) attack** aimed at several Web pages in South Korea and the United States. Most of these sites belonged to governmental, military and financial institutions. The Mydoom worm, which installed several components on the infected computer, sent commands to other computers to launch the attack. Even though there was speculation that the attack originated from North Korea, this could never be proven.

These are some of the targeted Web pages:

www.president.go.kr
www.whitehouse.gov
www.faa.gov
www.dhs.gov
www.defenselink.mil
www.nasdaq.com
finance.yahoo.com
www.usbank.com
www.ftc.gov
www.nsa.gov
www.amazon.com
www.washingtonpost.com

Some **new variants of the Koobface worm** were also in circulation during this quarter. These new variants not only used Myspace and Facebook to spread, but also Twitter by posting malicious links from infected users' accounts:

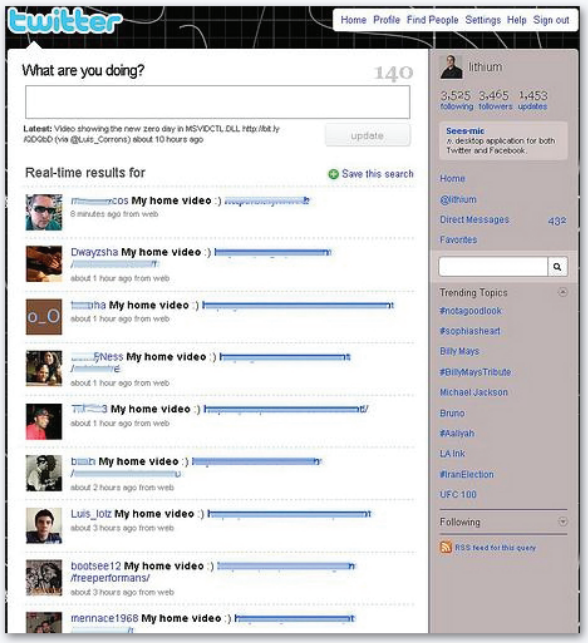

FIG.16

MALICIOUS LINKS ON TWITTER

Besides spreading, this variant of Koobface also installed the InternetAntivirusPro fake antivirus to profit from it.

Using social engineering techniques to trick users is also a common strategy of hackers. In this sense, they are increasingly using the latest news stories to attract users' attention. What's new about this technique is that they not only use international stories, but are also turning to local news in order to launch more targeted attacks. This is the case of a small fire at **Angeles Crest National Forest**. The first results displayed by Google when searching for information about the fire were malicious pages placed by cyber-crooks by using Blackhat SEO[4] techniques:

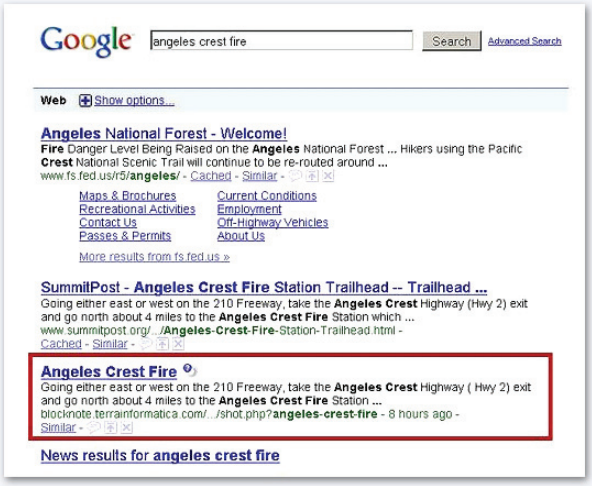

FIG.17

RESULTS SHOWN USING BLACKHAT SEO TECHNIQUES

These attacks have been repeated massively. Just a few days after the attack, we realized it was part of a much larger campaign. The figure below shows a series of search terms that were used by cyber-crooks for their Blackhat SEO attacks:

4 SEO stands for Search Engine Optimization. Basically, it refers to techniques used to improve the positioning of Web pages in search engines (Yahoo, Google, etc.). BlackHat SEO refers specifically to the use of SEO techniques by cyber-criminals to promote their Web pages.

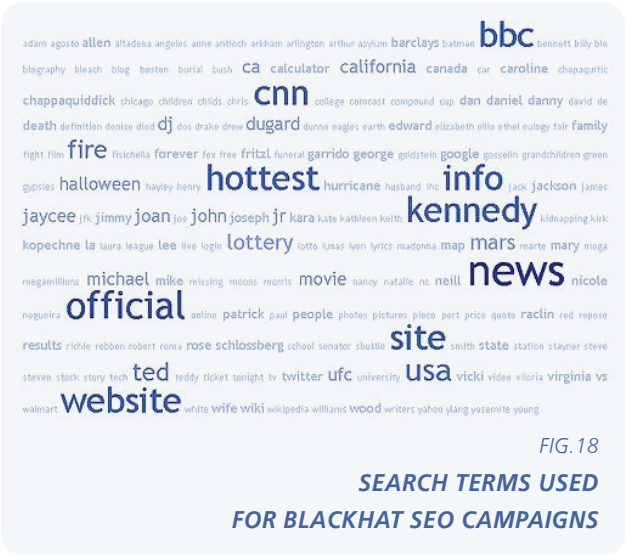

FIG.18

SEARCH TERMS USED FOR BLACKHAT SEO CAMPAIGNS

These attacks have continued in September. Below is a list of the most-searched terms used by cyber-criminals this month:

- Obama Speech
- GM group enterprises
- Apple
- Beatles
- America
- White House
- Jon Gosselin
- Live Interview
- School Season

As you can see, cyber-crooks are trying to increase the number of potential victims by exploiting vulnerabilities and social engineering techniques, both through spam messages and social networks, as well as through search engines with Blackhat SEO techniques. Our advice to protect yourself from these infections is to have your computer's software always up-to-date and avoid clicking links of unknown origin.

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/*