PandaLabs Bulletins:

Waledac and Social Engineering

Contents

Contents 2
1.- Introduction 3
2.- Storm Worm: The beginning 4
3.- Main effects 5
4.- The many guises of Waledac 7
Resignation of Barack Obama 7
Valentine’s Day 8
Discount coupons in times of crisis 9
Explosions 10
SMS spy services 10
Independence Day 11
5.- Tips 13
6.- References 14

1.- Introduction

Email messages using social engineering techniques continue to be one of malware's main entry points into users' computers. Malware usually arrives in message attachments, passing itself off as a harmless file: pictures, Word documents, Excel spreadsheets, etc.

However, not all malware families spread in email attachments. This is the case of the Waledac family, which has been particularly active during the first semester of the year.

This malware family is characterized by the wide variety of topics it uses to spread and because it distributes itself in email messages that contain links to Web pages that download the worm.

This bulletin contains an in-depth analysis of the Waledac family of worms. We'll discuss its malicious payload, offer statistics about its activity during the first semester of the year, cover the different topics it uses to spread and give you some tips to stay protected.

2.- Storm Worm: The beginning

The origin of the so-called Storm Worm dates back to January 2007, when a series of malware-spreading emails started circulating on the storms that were sweeping across Europe at the time.

This was simply another example of social engineering. However, it was also the beginning of the Storm Worm phenomenon, which involved several malware families that used this technique even though the topics they used were very different.

The Storm Worm was at its peak in February and November 2007. This was mostly due to the great activity of various variants of the Nurech worm.

2008 was quiet, although at the end of the year the Storm Worm surged again thanks to the Waledac family of worms.

This family was different to other previous malware in that it didn't use attached files to spread, but links that download malware when accessed by users.

Creators of this type of malware use this technique to make detection by antivirus companies as difficult as possible. In the past, it was enough to detect the infected attached file to block the Storm Worm easily, as it was the same in all cases.

However, today it is necessary to monitor and carry out an in-depth analysis of the links they use, as the malware they host changes depending on various parameters: the time when they are accessed, the browser used, the origin, etc.

Cyber-crooks have realized that trying to spread a single sample is not very effective, and have turned to this technique instead.

3.- Main effects

Besides spreading through links in email messages, Waledac can do other things as well: send out spam, steal personal information from the computer, and download other malware families.

Once run and installed on the computer, it takes the following actions:

- Modifies the system registry entries, so it is run on the next system restart.
- Looks for every email address on the computer in order to use them to send spam.
- Encrypts information about email addresses, stores them on a file with a random name, and sends them to different addresses.
- Its backdoor component opens a TCP communication port that allows remote users to connect and run arbitrary commands on infected systems, acting as a botnet.

We have found some 170 domains that belong to this family. These include:

hxxp://terrorismfree.com
hxxp://antiterroris.com
hxxp://fearalert.com
hxxp://easyworldnews.com
hxxp://bestjournalguide.com
hxxp://worldtracknews.com
hxxp://virtualesms.com
hxxp://smspianeta.com
hxxp://freeservesms.com
hxxp://codecouponsite.com
hxxp://thecoupondiscount.com
hxxp://bestcouponfree.com
hxxp://funnyvalentinessite.com
hxxp://thevalentinelovers.com
hxxp://yourvalentineday.com
hxxp://greatbarackguide.com
hxxp://bestbaracksite.com
hxxp://superobamaonline.com
hxxp://newyearcardfree.com
hxxp://bestchristmascard.com
hxxp://freechristmassite.com

As you can see from the names of these Web pages, the links are related to the topics covered in the messages sent by Waledac. This way, the worm avoids raising suspicion among users. So, in the case of Barack Obama, there are domains such as hxxp://superobamaonline.com, or hxxp://yourvalentineday in the case of Valentine’s Day.

This family has been active since the end of 2008. The first specimens were detected in December that year. Since then, many variants have appeared (a total of 68), and they have kept in circulation throughout this year.

The graph below shows the volume of Waledac variants detected by our products. This can give you an idea of the number of Waledac samples that have been circulating and affecting users over the last few months.

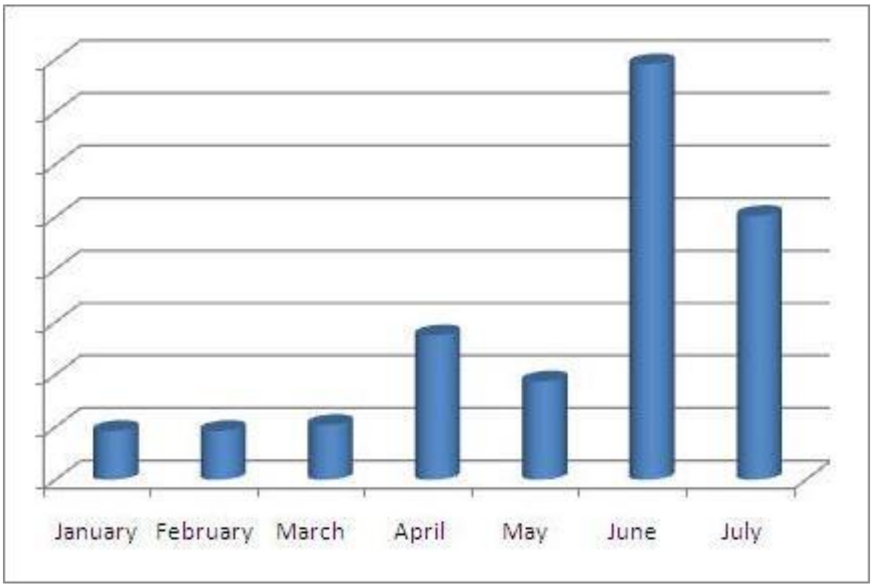


Fig. 1 Detections reported by our products (January-July 2009)

As you can see, the family's activity was constant during the first five months of the year, with a small increase in April. However, its activity has risen notably over the last two months (June and July).

4.- 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."

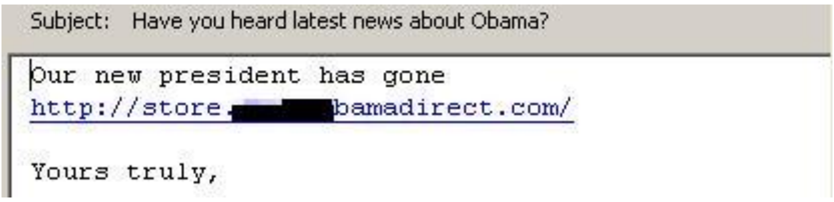
If there is one factor that characterizes the Waledac family it is the diversity of the subject matter used to spread it. Yet the choice of subjects is not random, it has been carefully calculated in order to exploit:

- 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:



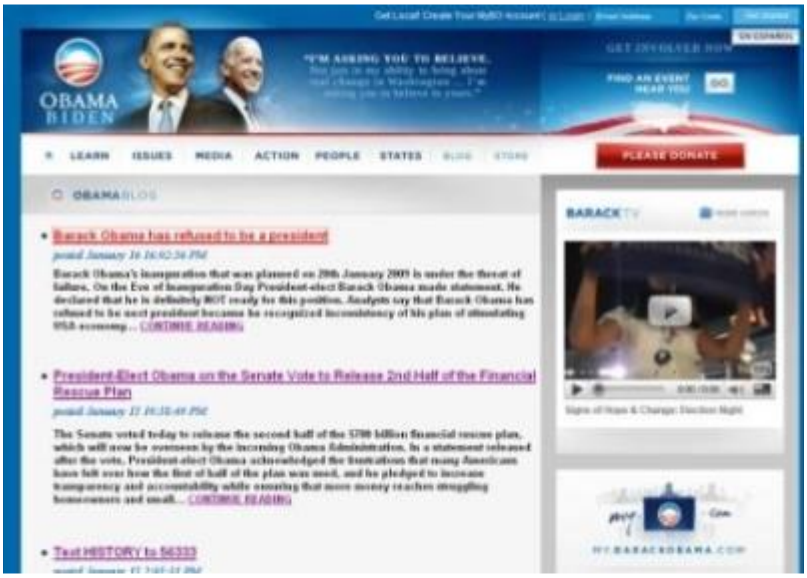
Subject: Have you heard latest news about Obama?

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

Yours truly,
```

Fig. 2 Email message about Obama's resignation

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

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

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. 3 Spoof Obama Web page

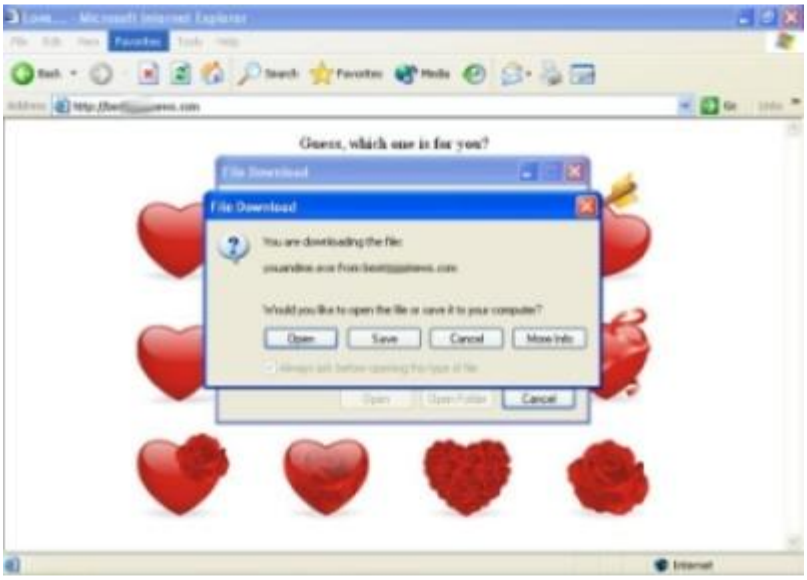
Any users that clicked on one of the links on the page would download the malicious file.

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.

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 as the file was, in fact, a copy of the worm.



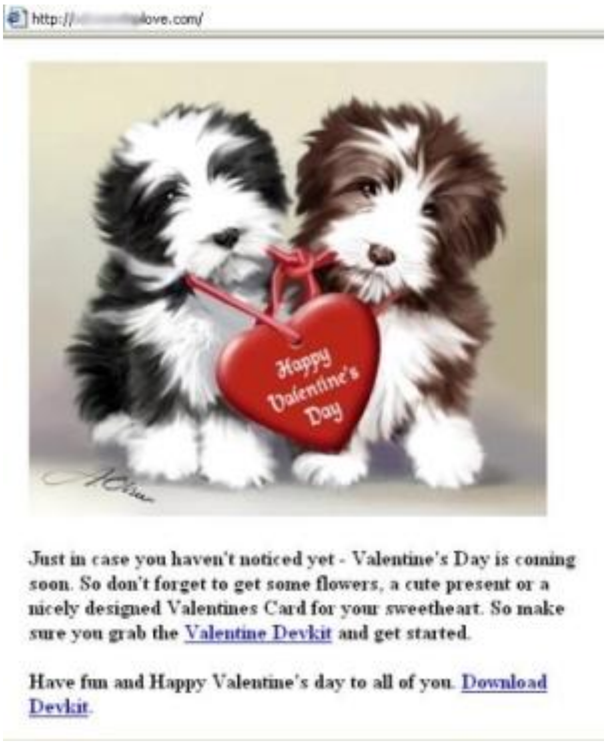
Guess, which one is for you?

You are downloading the file:

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

Fig. 4 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.



http://[redacted]love.com/

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.

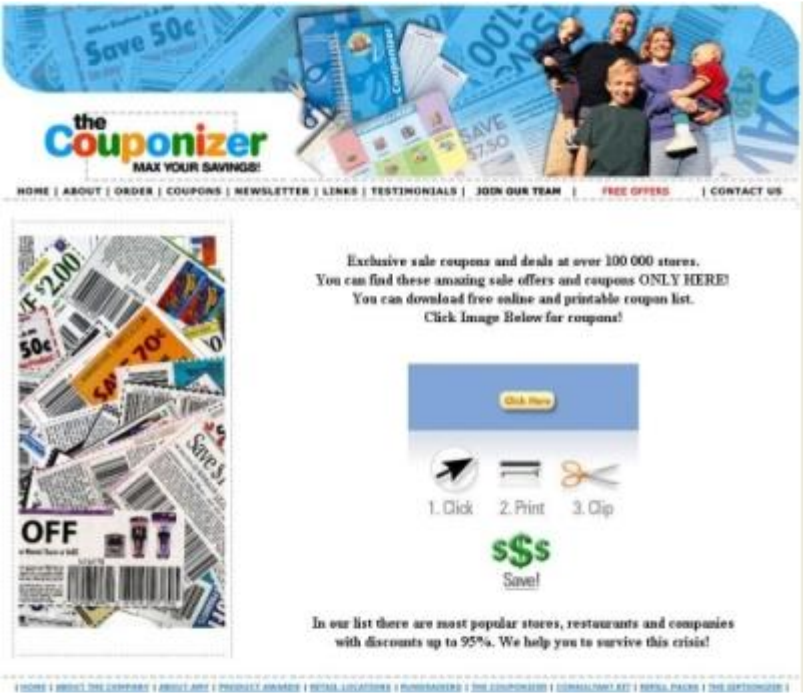
Have fun and Happy Valentine's day to all of you. Download Devkit.

Fig. 5 Web page for designing romantic 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.

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 | TESTIMONIALS | JOIN OUR TEAM | FREE OFFERS | CONTACT US
Click Here
1. Click
2. Print
3. Clip
$$$
Save!

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. 6 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.

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.

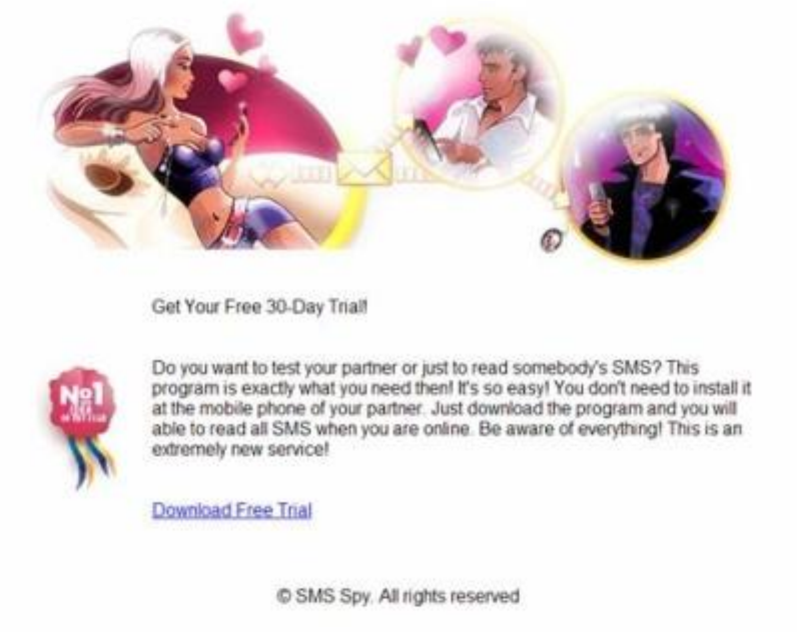
Links in the messages led to a Web page with the full story and, supposedly, a related video. Waledac used the logo of Reuters to gain users confidence.

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.



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

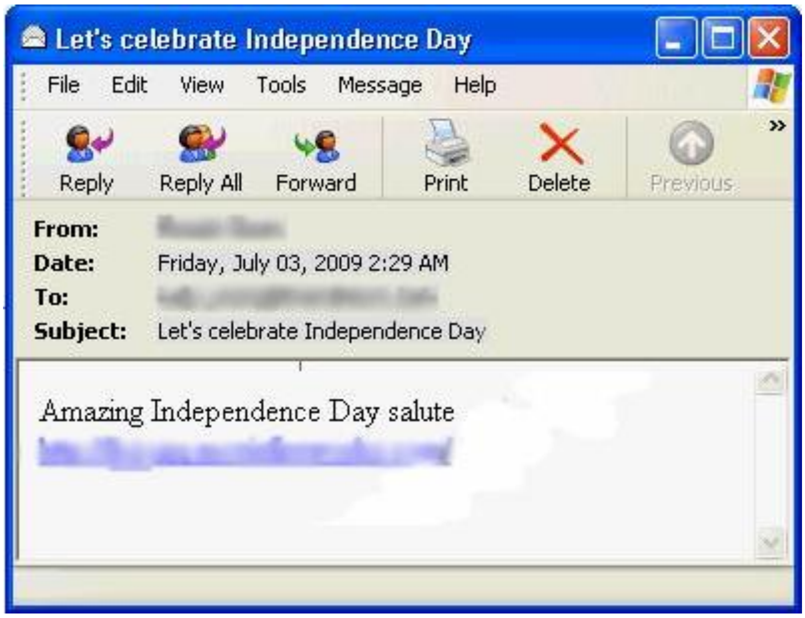
Fig. 7 Spyware download page

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

Independence Day

The latest topic to be used by this family of worms to spread is the U.S. Independence Day (July 4). The email messages related to this event started circulating some days before the actual festivity.

In this case, the messages contain a link to a video that supposedly shows Independence Day celebrations:



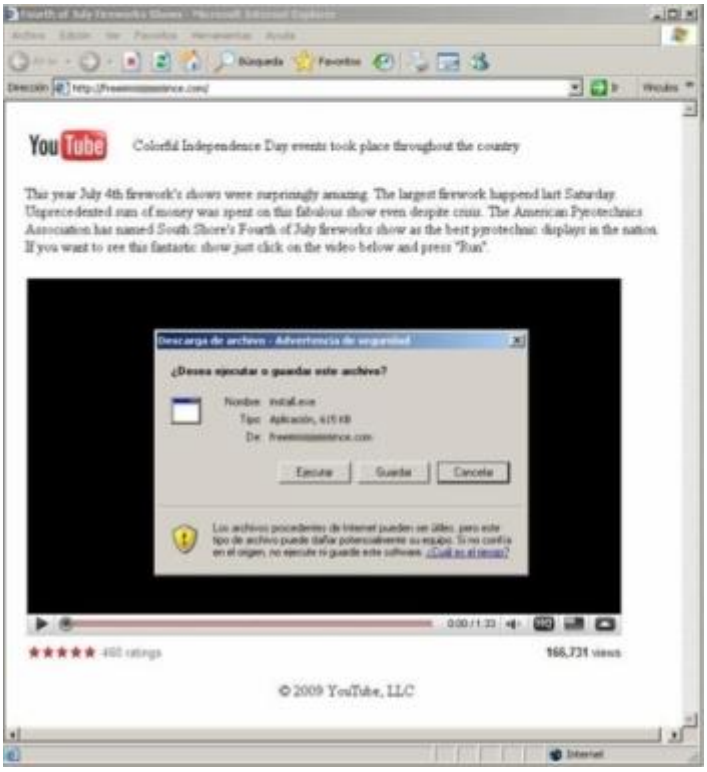
From: [redacted]
Date: Friday, July 03, 2009 2:29 AM
To: [redacted]
Subject: Let's celebrate Independence Day

Amazing Independence Day salute
[redacted]

Fig. 8 Independence Day message

If the user clicks the link, a Web page similar to YouTube opens. The page contains an article about the event and a fireworks video.

In order to watch the video, the user is asked to install a file. However, the file is in reality a copy of the worm.


Fourth of July Fireworks Shows - Microsoft Internet Explorer
Búsqueda
Favoritos
YouTube
Ejecutar
Guardar
Cancelar
0:00 / 1:33

Colorful Independence Day events took place throughout the country

This year July 4th firework's shows were surprisingly amazing. The largest firework happend last Saturday. Unprecedented sum of money was spent on this fabulous show even despite crisis. The American Pyrotechnics Association has named South Shore's Fourth of July fireworks show as the best pyrotechnic displays in the nation. If you want to see this fantastic show just click on the video below and press "Run".

Descarga de archivo - Advertencia de seguridad

¿Desea ejecutar o guardar este archivo?

Nombre: install.exe
Tipo: Aplicación, 615 KB
De: [illegible]

Los archivos procedentes de Internet pueden ser útiles, pero este tipo de archivo puede dañar potencialmente su equipo. Si no confía en el origen, no ejecute ni guarde este software. ¿Cuál es el riesgo?

★★★★★ 460 ratings
166,731 views

© 2009 YouTube, LLC

Fig. 9 Web page that downloads the worm

The file names used are *fireworks.exe*, *install.exe*, *patch.exe*, *run.exe*, *setup.exe* and *video.exe.*

5.- Tips

Social engineering continues to be users' *Achilles' Heel*, as, out of curiosity, they keep falling prey to email messages that spread this family of malicious codes.

One of the characteristics of the Waledac family is that they use links to Web pages in order to spread. To do this, they create malicious Web pages similar to legitimate ones in order not to raise suspicion among users. This is the case of the YouTube Web page, which has been exploited by cyber-crooks to create similar, apparently harmless pages.

If you are taken to a Web page that looks exactly the same as a legitimate one, such as YouTube, for example, make sure that the URL displayed in the address bar is the official one.

If you don't know what the official address is, find it out by performing a search in any of the search engines that you normally use. Generally, the first result corresponds to the official site.

In order to avoid checking these addresses manually, you can use security software which carries out this task. For example, *Identity Protect*, a module included in the latest Panda security solutions. This program blocks suspicious or malicious URLs and displays a warning message informing users of the risk of accessing them.

If you don't have any solution that provides this service or you still don't know if the page displayed is the official one, you can still avoid being infected. You need to agree to the file download for the malicious code to download and install on the computer.

Scan every file with a security solution before running it.

6.- References

PandaLabs Blog

http://pandalabs.pandasecurity.com/archive/New-Alanchun.aspx

http://pandalabs.pandasecurity.com/archive/Nurech.A.worm-Alert.aspx

http://pandalabs.pandasecurity.com/archive/Nurech.A.worm-Alert-II.aspx

http://pandalabs.pandasecurity.com/archive/Malware-Campaign-Impersonates-Barack-Obama_2700_s-Website.aspx

http://pandalabs.pandasecurity.com/archive/Waledac-Storm-worm_2E002E002E00_-New-Target_3A00_-Valentine_1920_s-day.aspx

http://pandalabs.pandasecurity.com/archive/San-Valentine_B400_s-day-is-close.aspx

http://pandalabs.pandasecurity.com/archive/New-waledac_2700_s-campaign.aspx

http://pandalabs.pandasecurity.com/archive/New-Storm-Worm_3A00_-Waledacs.aspx

Malware Encyclopedia

http://www.pandasecurity.com/homeusers/security-info/

Press releases

http://www.pandasecurity.com/enterprise/media/press-releases/viewnews?noticia=9530