Quarterly Report PandaLabs

(April - June 2005)

www.pandasoftware.com

Quarterly Report PandaLabs (April – June 2005)

Agustin Mogollon – Surveillance Department - PandaLabs

Introduction

PandaLabs, ***Panda Software's*** anti-*malware* laboratory, is pleased to offer its second quarterly report for April to June 2005.

As with the previous quarterly report, this document summarizes the most significant events with regard to *malware* and other threats during this period, always according to the point of view and under the critical eye of ***PandaLabs***.

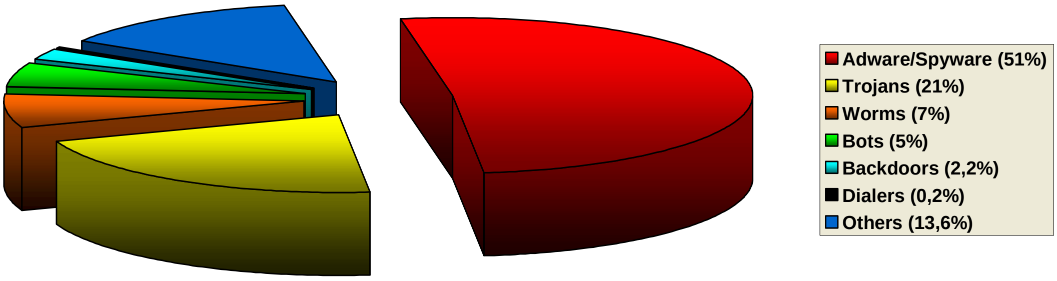
The second quarter of the year saw the logical evolution of circumstances and events that occurred during the first quarter, confirming and reinforcing certain signs that had appeared in that period. This new report will look in more depth at some common patterns, and analyze differentiating events and factors.

Significant data from the second quarter of the year

Before analyzing the main events and trends from the second quarter of the year, significant data with regard to detections recorded by ***Panda ActiveScan*** as well as new specimens and variants identified by ***PandaLabs*** are detailed below.

About ***Panda ActiveScan*** detections…

The graph below includes statistical information about ***Panda ActiveScan*** detections carried out during the second quarter of the year. The data shown is distributed between the most significant categories:



As in the first quarter of the year, ***Adware*** **and** ***Spyware*** **detections were comfortably ahead of each of the rest of the categories, accounting for 51% of the total. Consequently**, *Adware* and *Spyware* detections alone **were greater than the rest of the categories as a whole**, albeit to a lesser extent than in the previous quarter (when the percentage of *Adware* and *Spyware* detections was 60%).

The total number of ***Adware*** **and** ***Spyware*** **detections** as well as the total number of detections in other categories **has increased substantially compared to the previous quarter. In fact,** ***Panda ActiveScan*** **recorded 12% more detections than in the first quarter. This circumstance illustrates the inexistence of any signs of weakness in the epidemic of** ***malware*** **and other threats currently being suffered.**

Trojans are the second most widespread threat, representing a solid 21% of all ***Panda ActiveScan*** **detections** this past quarter (3% more than in the first quarter). **27% of detections relating to Trojans are specimens from the Trj/Downloader family**, closely related to *Adware* and *Spyware*, as explained in the previous quarterly report. Consequently, **detections attributed to the Trj/Downloader family represent a fairly substantial 6% of the** ***Panda ActiveScan*** **total.**

Worms, however, continue their downward trend, recording only **a modest 7% in the total number of** ***Panda ActiveScan*** **detections.**

For their part, bots have once again assumed a prominent role, making up 5% of the total detections recorded during this second quarter. The number of incidents generated by this type of *malware* is similar to traditional worms.

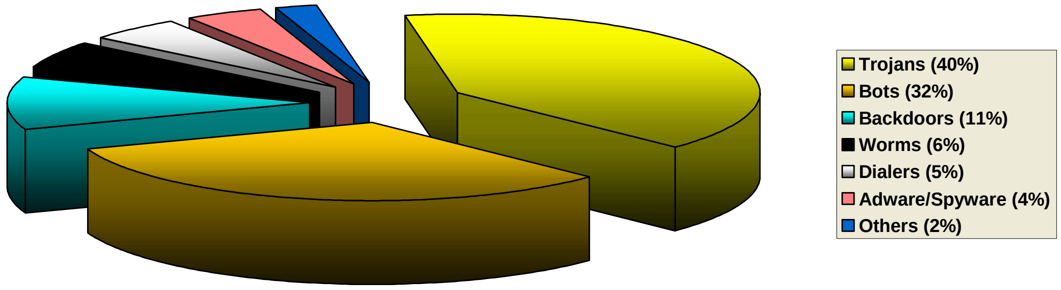
About new specimens identified by ***PandaLabs***…

The volume of new specimens and variants[1] identified by *PandaLabs* during this second quarter has experienced a spectacular increase of 60% compared to the first quarter. With regard to the number of new variants identified during the second quarter of the year by ***PandaLabs***, the increase in those linked to diverse families of instant messaging worms, spy Trojans or the ***Mytob*[3]** family of mail worms merit special mention.

> ***variants*[1]** *: throughout this document, on numerous occasions, there is mention of malware variants. Certain modifications to a specific sample of malware in particular give rise to what is known as a new variant (use of modified* ***packers*[2]** *, changes to certain code routines etc.).*
>
> ***packers*[2]** *: malware creators use encryption routines and code compression to try to avoid detection, without the need for changing the source code of their creations.*
>
> ***Mytob*[3]** *: in reality, as explained in the previous quarterly report, the Mytob family of worms is characterized by a double propagation mechanism (the sending by email of attachments and the exploitation of vulnerabilities in remote services).*

Furthermore, in line with the increase of new specimens and variants detected by *PandaLabs*, the number of those detected or blocked by *TruPrevent*™ has risen by 144%. This percentage covers all new specimens and variants discovered by the ***TruPrevent™*** advanced heuristic module or blocked in execution by the ***TruPrevent™*** behavior analysis module.

The graph below shows the distribution of the different specimens and variants identified by ***PandaLabs*** during the second quarter:



Particularly interesting is the **high percentage of new bot-type variants** (**32%** of the total recorded) detected by ***PandaLabs***, a clear indication of the interest that this type of *malware* arouses in cyber-criminals and underground communities.

Likewise, but for different reasons, both *Adware* and *Spyware* are worth mentioning. As in the first quarter of the year, these categories play only a secondary role when the data of new variants and specimens distributed are analyzed. However, the situation here is different to that applicable to Trojans, bots, backdoors or even worms, since the number of detections recorded for each *Adware* and *Spyware* specimen or variant is up to many times greater in some cases. To enter into details here as to why this is the case goes way beyond the scope of this document.

Mydoom and Bagle: has-beens in decline

There has been a reaffirmation during the second quarter of 2005 of the already evident decline in mail worms compared to other forms of *malware* and threats. This trend has been particularly noticeable in two of the most notorious families in *malware* history: ***Mydoom*** and ***Bagle***.

Diverse variants of the unpopular ***Mydoom*** and ***Bagle*** families have tried to put email users and different companies from the anti-*malware* industry in a quandary during the second quarter of the year. In spite of attempts to achieve this, none of the attacks launched by these new variants managed to reach anything like worrying levels. In fact, levels of virulence recorded were even less than the previous quarter, which in turn were a mere shadow of levels reached during 2004.

During the second quarter of the year, ***PandaLabs*** did not record any situation that could be considered as an alert due to incidents attributable to these two *malware* families (remember there were two orange alert situations during the first quarter of the year caused by ***W32/Mydoom.AO.worm*** and ***W32/Bagle.BL.worm*** respectively).

Looking at the data provided by ***Panda ActiveScan***, it is also apparent that the ***W32/Netsky.worm*** family of worms has produced a similar volume of incidents to the number generated by these other two *malware* families combined.

The number of **new variants** recorded by ***PandaLabs*** during the second quarter of the year for the ***W32/Bagle.worm*** family **increased by 26% compared to the previous quarter**. ***PandaLabs*** recorded a **sharp decrease of 64%** for the ***W32/Mydoom.worm*** family.

W32/Bagle.worm	***26% increase***	***04/01/2005 –06/30/2005***

W32/Mydoom.worm	***64% decrease***	***04/01/2005 –06/30/2005***

Symbiotic Strategies – Second take

The previous quarterly report detailed the propagation strategy in phases deployed by the ***W32/Bagle.BN.worm*** and its successors: ***Trj/Mitglieder.BO***, ***Trj/Downloader.BBN*** and ***Trj/Ruzes.A***. The ultimate aim of this approach was simply to increase the possibility of avoiding temporary detection by antivirus companies, making the most of the element of surprise.

The second quarter of the year witnessed new ***Bagle*** related incidents characterized by the same combined propagation pattern which, fortunately, did not have any more far reaching consequences than in the first quarter.

The Mytob clone war

If, fortunately, the "activity" of different variants of ***Mydoom*** and ***Bagle*** did not manage to rise to the occasion, the activity related to the numerous variants belonging to the ***Mytob*** family distributed throughout the second quarter of the year faired slightly better. This second quarter saw an authentic wave of very similar variants, which appeared to claim the dubious distinction of king of the mass mailing worms.

PandaLabs **recorded an incredible 1169% increase in the number of new variants identified for the *W32/Mytob.worm* family compared to the previous quarter**.

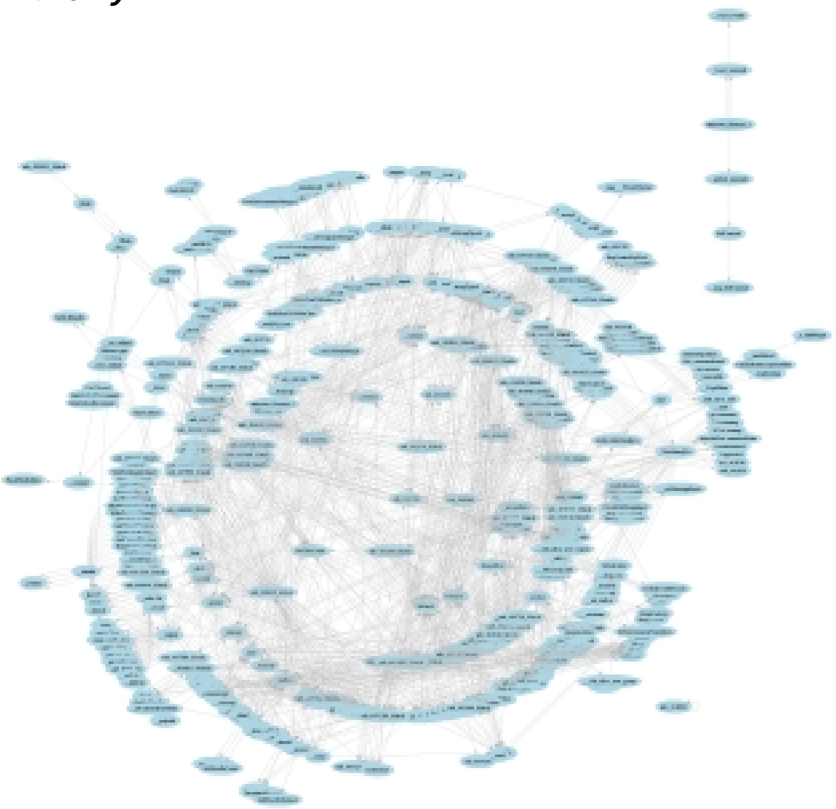
W32/Mytob.worm	***1169% increase***	***04/01/2005 –06/30/2005***

Classing these different variants from the ***Mytob*** family as clones is highly appropriate when evaluating the minimal differences that exist between them. In fact, in many cases, the only real difference is found in the combined use of different or modified packers, as well as certain variations in the composition of the propagation messages.

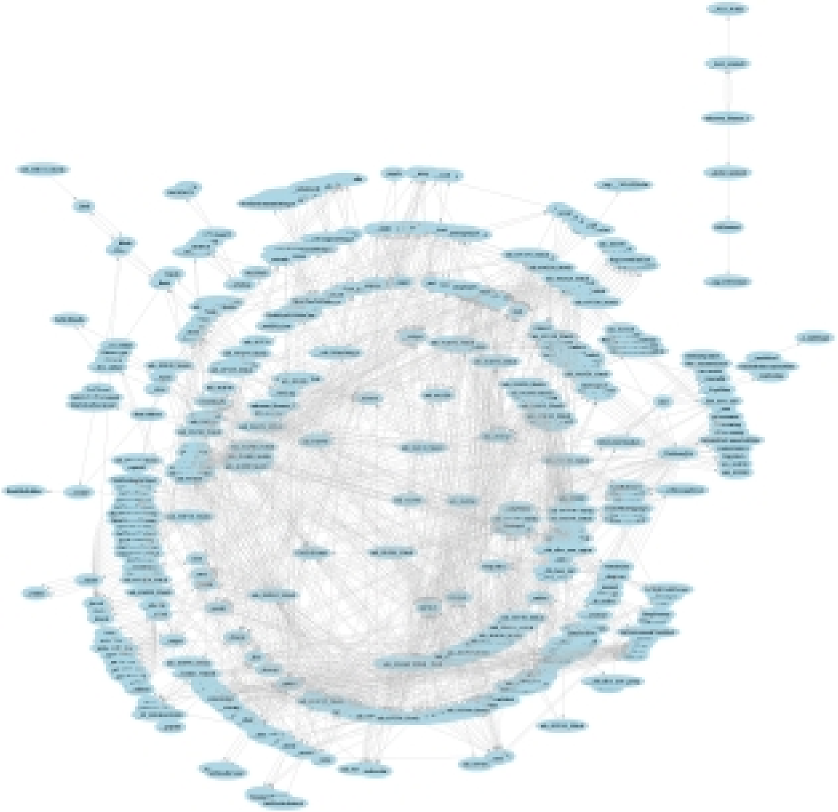
The illustrations below show the graphic representation of two different variants of the ***W32/Mytob.worm*** family. Each of the different nodes represents a code procedure or function, while the vectors show the order or hierarchy of calls between them. Naturally, both specimens were unpackaged and disassembled before being processed.

As can be seen, it is difficult even visually to notice the differences:

W32/Mytob.BA:



W32/Mytob.FX:



The list of packers used to date to "package" different ***Mytob*** specimens is very varied:

ARM	***PECompact***
Armadillo	***PE-Crypt***
ASPack	***PE-Diminisher***
Expressor	***PEncrypt***
FSG	***PE-Pack***
Kcuf	***PESpin***
MEW	***Petite***
MewBundle	***Pex***
Molebox	***UPack***
Morphine	***UPX***
Packman	***Yoda***
PecBundle	***YodaProt***

Even more significant and revealing is the fact **that the majority of Mytob variants have multi-layer packaging with up to 6 different packers added.**

War of attrition against anti-*malware* companies

The unique distribution pattern that has characterized the ***Mytob*** clone army is closely related to a fortunate circumstance that arose at the end of 2004: ***malware* creators are finding it increasingly difficult to produce global epidemics with a single *malware* specimen.**

This situation has become especially relevant among email worms, whose propagation capability depends on the success of a social engineering technique*: **after a disastrous 2004, plagued with incidents resulting from this type of *malware*, there are an increasing number of email users that take precautions before opening attachments.**

***** *On various occasions email worms have been distributed by exploiting any known vulnerability in order to infect systems without the intervention of users themselves.*

Naturally, greater user awareness has not been the only catalyst in this situation. **The role of companies in the IT security sector and their clients, who ultimately deploy the defensive measures offered, has been equally important.**

In the end the fight against *malware* is not only about continuously improving existing solutions, but also in making sure they are appropriately used.

The strategists responsible for orchestrating the activity of the *Mytob* army were very aware of this change of panorama, assuming from the outset a limited amount of hits for each of their ***Mytob*** 'soldiers' and, in particular, **a very limited lifetime for each of the different variants.**

The ultimate aim is to create a network of *zombies*[1] with a large enough volume to launch other activities which, in all likelihood, will have financial gains.

> ***zombies*[1] :** *this name is used to identify systems which, once taken over, are at the mercy of a third party obeying their every order without the real user being aware of this. Bots are the malware par excellence for these types of functions.*

Heavily committed to their aim, executors of these waves of attacks have been remorseless with companies from the sector, continually distributing new variants of the ***Mytob*** family in order to compensate for casualties suffered in anti-*malware* system detections.

Mytob: a Mydoom substitute

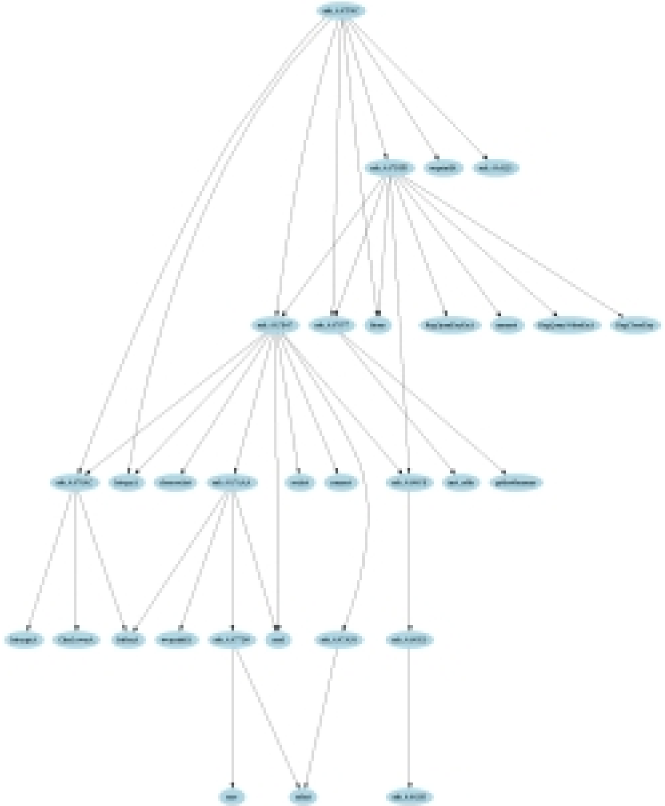
Several months after the appearance of the first variant of the ***W32/Mytob.worm*** family, on 28th February, the high degree of similarity between this *malware* family and the veteran ***W32/Mydoom.worm*** is now common knowledge.

The people responsible for this wave of ***Mytob*** variants appear to have recycled the code of some of the ***Mydoom*** family specimens, making minimal changes to integrate the module that enables propagation via remote exploit. While ***Mydoom*** is a pure email worm, ***Mytob*** is a hybrid able to spread via email and exploit vulnerabilities in remote services (LSASS, fundamentally: *MS04-011*).

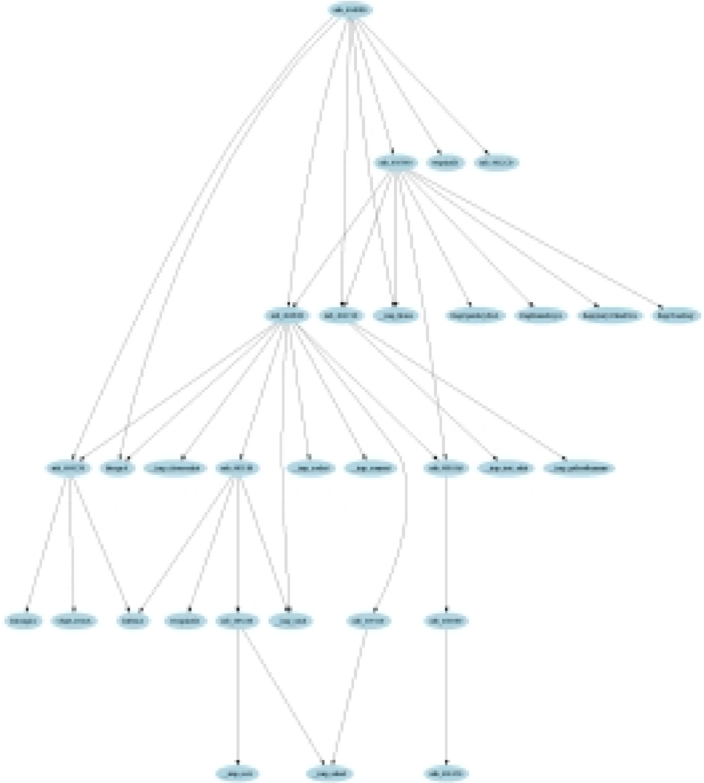
When carrying out a comparative study on the unpackaged and disassembled code of some of the different specimens belonging to the ***Mytob*** and ***Mydoom*** families, the above-mentioned circumstance is apparent.

To reflect this visually, two graphs are included below in which each node represents a different function or procedure and the vectors show the order or hierarchy in each of their calls. The representation of each of these graphs is restricted to the email propagation module and is practically the same in both cases.

W32/Mydoom.A:



W32/Mytob.A:



The return of Sober

It's a case of the proverbial bad penny, as they say. During the second quarter of this year, ***PandaLabs*** recorded a reasonable number of new variants for the ***W32/Sober.worm*** family. Although the volume in itself was not significant, it was enough for the puppeteers that operate in the shadows to achieve substantial "success". As a result, ***PandaLabs*** ordered a state of Orange Alert on May 3rd due to the increasing number of detections of the ***W32/Sober.V.worm*** specimen. This state of alert continued for various days.

W32/Sober.V.worm	***ORANGE ALERT***	***05/03/2005***

It should be pointed out that the ***W32/Sober.V.worm*** was initially blocked proactively using the ***TruPrevent™*** behavioral analysis module. Consequently, clients with this technology were protected even before ***PandaLabs*** had the opportunity to prepare the relevant "vaccine".

PandaLabs detected the first ***W32/Sober.V.worm*** sample on May 2nd:

W32/Sober.V.worm	***05/02/2005***

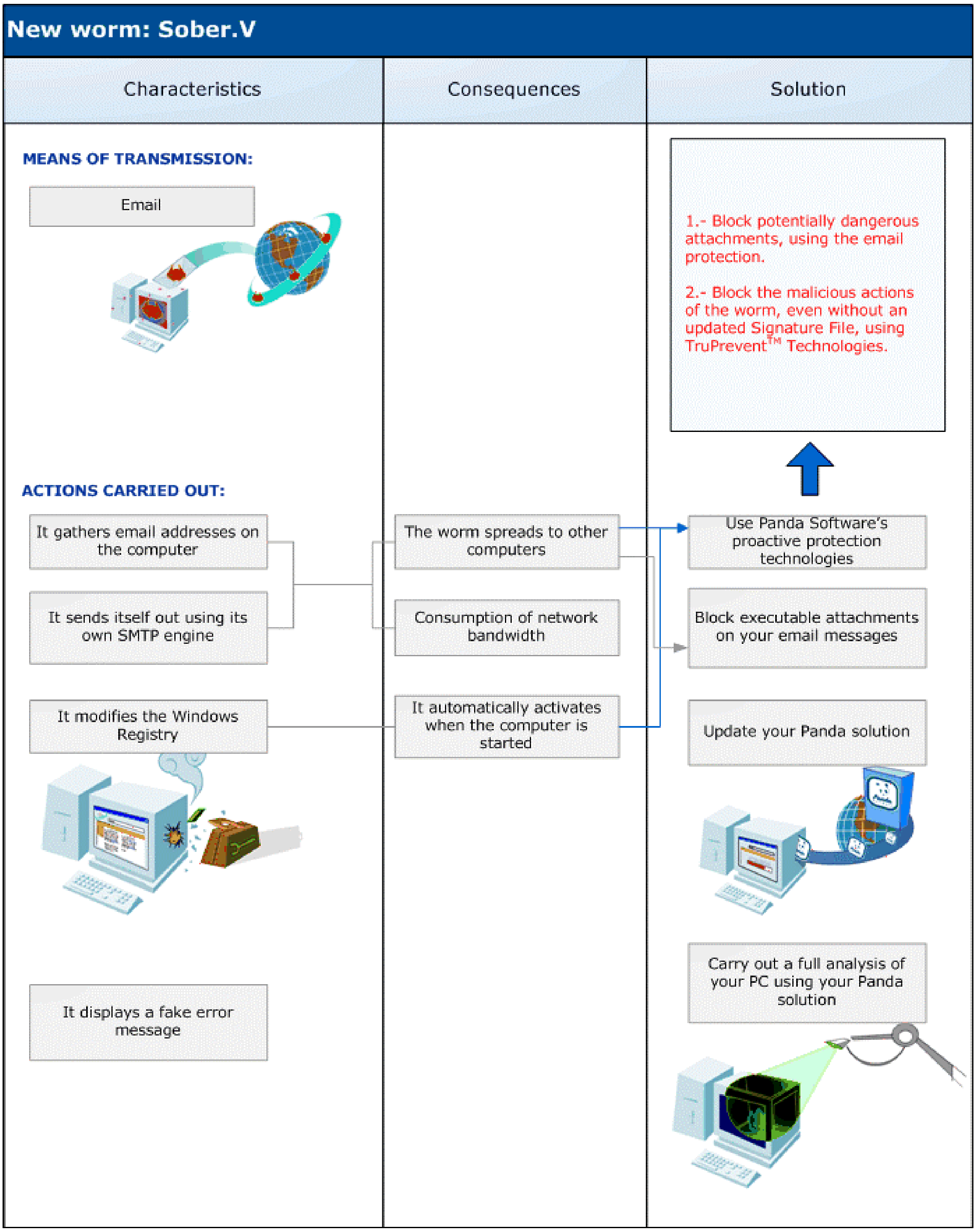
All of the details about ***W32/Sober.V.worm*** can be found in the Panda Software Virus Encyclopedia.

More than just one headache…

W32/Sober.V.worm presented companies from the anti-*malware* sector with additional problems: the specimen in question is capable of blocking access to the executable file that contains it, making detection and elimination tasks by anti-*malware* solutions more difficult. It would not be appropriate here to go into more detail on this matter, but certainly more than one security analyst will remember themselves scowling while they analyzed ***W32/Sober.V.worm***.

Furthermore, a week after the appearance of ***W32/Sober.V.worm***, ***PandaLabs*** detected a new variant named ***W32/Sober.W.worm***, which was being downloaded actively from workstations previously infected by ***W32/Sober.V.worm***. **Curiously, *W32/Sober.V.worm* did not include a predefined list of urls from which to attempt the download. Instead of this, the list of urls was entered dynamically through an integrated backdoor**. The objective, as one would expect, is to complicate analysis and prevention by AV companies.

Unlike its first-born, ***Trj/Sober.W.worm*** does not spread; it sends huge amounts of SPAM instead.



New worm: Sober.V

Characteristics

MEANS OF TRANSMISSION:

Email

ACTIONS CARRIED OUT:

It gathers email addresses on the computer

It sends itself out using its own SMTP engine

It modifies the Windows Registry

It displays a fake error message

Consequences

The worm spreads to other computers

Consumption of network bandwidth

It automatically activates when the computer is started

Solution

1.- Block potentially dangerous attachments, using the email protection.

2.- Block the malicious actions of the worm, even without an updated Signature File, using TruPrevent^{TM} Technologies.

Use Panda Software's proactive protection technologies

Block executable attachments on your email messages

Update your Panda solution

Carry out a full analysis of your PC using your Panda solution

Strengthening of instant messaging worms

If, during the first quarter of the year, there was clear evidence of a increase in the use of instant messaging as a way of distributing *malware* and other threats, the second quarter has provided visible signs that such evidence is a tangible reality.

Instant messaging worms have consolidated their presence with a continuous trickle of new variants which have caused a constant but sustained number of incidents during the period.

Of note is the role performed by *W32/Kelvir.worm*, whose number of incidents has comfortably surpassed those caused by other instant messaging worm families. The arrival on the scene of two new families should also be mentioned: ***W32/Prex.worm*** and ***W32/Oscarbot***, the latter designed for the AOL messaging network.

W32/Prex.worm	***36 new variants***	***04/01/2005 – 06/30/2005***

W32/Oscarbot.worm	***52 new variants***	***04/01/2005 – 06/30/2005***

The disproportionate increase recorded by *PandaLabs* in the number of variants belonging to the ***W32/Kelvir.worm*** family stands out: a massive **1280% increase compared to the previous quarter**. The explosion of the *W32/Kelvir.worm* family is in stark contrast to the sharp decline of 71% in the ***W32/Bropia.worm*** family.

W32/Kelvir.worm	***1280% increase***	***04/01/2005 – 06/30/2005***

W32/Bropia.worm	***71% decrease***	***04/01/2005 – 06/30/2005***

As indicated in the previous quarterly report, instant messaging worms, in contrast to their email counterparts, have been driven from the beginning by motives that transcend mere demonstrations of ego or power: the different variants of these *malware* families exploit each "conquest" to install a bot in the infected system.

The omnipresent bots are a very useful tool for hackers and cyber-criminals: authentic Swiss Army knives with which to perpetrate all types of actions. When a "tool" of this type is installed in a system, it is left at the mercy of the hacker or cyber-crook, opening up a whole range of possibilities: installation of all types of *Adware*/*Spyware*, carrying out of dDoS attacks, sending of SPAM etc. In fact, various cases of the fraudulent installation of *Adware* and *Spyware* using bots spread by these instant messaging worms have been recorded.

As in the first quarter of this year, the ***TruPrevent™*** behavioral analysis module managed to satisfactorily block some of these bots installed by instant messaging worms. This circumstance allowed ***PandaLabs*** to rapidly and cleanly obtain samples to perform adequate detections and incorporate them in the signature file.

A notable example is the ***W32/Gaobot.EYP*** bot, downloaded by the ***W32/Kelvir.M.worm***, of which ***PandaLabs*** received numerous copies reported automatically by ***TruPrevent™*** on April 13th.

W32/Gaobot.EYP.worm	***04/13/2005***

All the details about ***W32/Gaobot.EYP.worm*** can be found in the Panda Software Virus Encyclopedia.

Trojans in the service of phishers

Phishing is one of the fastest growing threats since its emergence became clear at the end of 2003. Of the all the types of phishing in existence, the one that creates most fear is the one that targets online banking clients. In fact, it is so worrying that financial institutions offering online services have now decided to step in.

Furthermore, phishers appear to have found a perfect ally in specialist Trojans to carry out far more silent and difficult to identify attacks:

- Installing this type of *malware* in the system of a potential victim means social engineering is no longer necessary in order to obtain the desired information (bank details, access credentials to online services etc), which results in greater precision and possibilities of success.

- Another major factor which tips the balance in favor of phisher-type *malware* is the possibility of capturing data of diverse nature and origin with each specimen. It should not be forgotten that in the case of traditional phishing, each message is personalized to obtain very specific data. The same message cannot be used at the same time to steal data from clients of two different financial institutions.

During the second quarter of 2005, *PandaLabs* recorded a large increase in the number of new variants detected for these types of Trojans; highlighting those designed to **steal bank information** (with a major **increase of 113%**). Of particular relevance is a significant increase in certain families of Trojans specialized in **stealing online multiplayer games** (with an **increase of 58%**).

The main players in the financial scene…

Families such as ***Trj/Banbra***, ***Trj/Bancos***, ***Trj/Banker***, ***Trj/Bancodor*** or ***Trj/Banpaes*** are the leading types of *malware* specialized in bank data theft.

The overall growth of these *malware* families is around 113% according to ***PandaLabs*** data, which means that **the number of new variants identified is comfortably double that of the previous quarter**.

There is no doubt that Trojans specializing in the theft of financial information is alarming. This concern has spread not only to end users but also to financial institutions.

This situation is especially difficult in countries like Brazil, where these types of threats are increasingly prevalent. *PandaLabs* would like to acknowledge the magnificent effort being made by members of the Brazilian CERT[1] in their particular struggle against these types of threats, and takes this opportunity to send them our most sincere congratulations.

CERT*[1] *: *this term is short for **C**omputer **E**mergency **R**esponse **T**eam. A CERT is responsible for receiving, reviewing and responding to all types of warnings related to security incidents that occur within its jurisdiction (a network or network of networks, a company or even a country).*

A very ambitious Trojan "phisher"

During the second quarter of the year, ***PandaLabs*** detected a Trojan-type phisher which exploited to the full one of the main advantages that this type of *malware* possesses compared to traditional phishing: ***Trj/Bancos.NL*** includes a list made up of various thousands of domains which, once visited by the affected user, activate a mechanism that makes it possible to steal data entered there (for example, all types of access credentials to online services). This enormous list includes hundreds of banks and financial institutions.

Trj/Bancos.NL	***04/27/2005***

All the details about ***32/Bancos.NL.worm*** can be found in the Panda Software Virus Encyclopedia**.**

The irrestible temptation of online games

The success that some online role-playing games are having is incredible, with large sums of money offered for objects and characters auctioned. This success has undoubtedly attracted the attention of *malware* creators, leading to the appearance of certain very peculiar and specialist threat families.

Families such as ***Trj/Legmir*** or ***Trj/Lineage*** are *malware* specimens whose objective is to steal the credentials necessary to access the "Legend of Mir" and "Lineage" games, respectively.

The *Trj/Legmir* family has experienced a 68% increase in new variants compared to the previous quarter.

Trj/Legmir	***68% increase***	***04/01/2005 – 06/30/2005***

***PandaLabs* has identified a 50% increase in new variants for the *Trj/Lineage* family during the second quarter.**

Trj/Lineage	***50% increase***	***04/01/2005 – 06/30/2005***

Other relevant events

More attacks against DNS servers in the Internet

As reflected in the previous ***PandaLabs*** quarterly report, diverse cyber attacks against Internet DNS servers occurred during the first quarter of this year. These attacks displayed a technique known as DNS cache poisoning and aimed to redirect legitimate web traffic to illegal servers from which a whole host of *malware*, *Adware* and *Spyware* are installed.

DNS cache poisoning incidents intensified in the Internet at the beginning of the second quarter of this year. This circumstance led to the rapid intervention of the security analyst community who were enraged at the prospect of this growing threat.

Once again, the work carried out by the team at the ***Internet Storm Center*** ***(ISC)*** deserves special mention, with their analysts reminding people of the weaknesses of Windows NT and Windows 2000 servers against these types of attacks (there is a document about this problem in the Microsoft Knowledge Database).

The **ISC** has an excellent report which details the particulars of the numerous DNS cache poisoning incidents produced during the first six months of the year.

New worm for mobile devices with double the propagation capability

The first quarter of the year, March specifically, witnessed an unprecedented *malware* event: the first worm for mobile devices with short and long-range propagation capabilities (***SymOS/Comwar.A.worm***). This *malware* specimen is capable of sending itself through Bluetooth (to nearby devices within a limited range) and also through multimedia or MMS messages (using the list of contacts from the device itself).

There was a reoccurrence at the beginning of the second quarter this year (on April 7th) and ***PandaLabs*** had the opportunity of detecting the second worm for mobile devices with double the propagation capability: ***SymOS/Cabir.J.worm***.

SymOS/Cabir.J.worm	***04/07/2005***

All the details about ***SymOS/Cabir.J.worm*** can be found in the Panda Software Virus Encyclopedia.

The name chosen for this new *malware* specimen stems from the high degree of similarity its code has to the rest of the ***SymOS/Cabir.worm*** family members. There is evidence to show that its author reused the code of one of the old ***SymOS/Cabir.worm*** variants, adding the modules necessary for propagation via MMS. Until then, members of the ***SymOS/Cabir.worm*** family could only be spread through Bluetooth.

Curiously, it should be pointed out that in contrast to the ***SymOS/Comwar.A.worm***, which sends copies of itself via an MMS to contacts stored in the device affected, ***SymOS/Cabir.J.worm*** responds to messages received through an MMS which includes a copy of itself.

The reaction principle applied to instant messaging

On April 8th, Microsoft published the seventh version of its popular instant messaging client MSN Messenger. This new version includes some modifications designed to counteract certain security deficiencies caused by numerous incidents attributed to new instant messaging worms. As commented, diverse families of worms with instant messaging propagation capabilities dominated the first quarter of the year, and have become increasingly relevant over the past three months.

MSN Messenger 7	***04/08/2005***

One of the measures implemented is the filtering of URLs linking to remote files with the .PIF extension, which satisfactorily prevents the propagation of certain variants of the ***W32/Bropia.worm*** or ***W32/Kelvir.worm*** family. It is worth remembering that many variants belonging to these *malware* families send messages that include links to remote .PIF files hosted in previously deployed web servers. The aim of these messages is to trick recipients that receive them into executing the .PIF file, which naturally includes a copy of the worm.

Another of the various restrictions included in the new MSN Messenger version is the blocking of certain executable files transferred.

The Kelvir family reacts and counterattacks

A few days after Microsoft released its new MSN Messenger version, ***PandaLabs*** detected a new variant of the ***W32/Kelvir.worm*** instant messaging worm family. The creators of this new specimen (***W32/Kelvir.L.worm***) appear to have taken careful note of the restrictions imposed by the Redmond multinational, using a new propagation mechanism which managed to effectively evade these measures.

W32/Kelvir.L.worm	***04/13/2005***

All the details about ***W32/Kelvir.L.worm*** can be found in the Panda Software Virus Encyclopedia.

In contrast to many of its closest relations, the ***W32/Kelvir.L.worm*** does not send messages with links to .PIF files hosted in remote web servers. Its strategy consists in including links to PHP forms (hosted in the same way in remote web servers) which return the file with the copy of the worm in question. These links include, as an argument for the PHP form, the email address of the mail user (the address used for the MSN Messenger service).

As a result, ***W32/Kelvir.L.worm*** achieves a twofold aim: on the one hand it manages to evade the security restrictions of the new MSN Messenger version and, on the other, makes it possible to compile lists of email addresses belonging to "curious" users (do not forget that the email address is only sent if the sender visits the url inserted in the message received). These lists are highly attractive to *malware* creators and especially to their distributors.

A hypothetical MSN Messenger user (***user@domain.com***) included in the contacts of a victim infected with ***W32/Kelvir.L.worm*** would, before long, be approached with the following message, supposedly sent by the user affected:

its you!
http://hydr0.net/pictures.php?email=user@domain.com

Conversion of worms to Trojans…

During the second quarter of the year, ***PandaLabs*** witnessed the birth of a new family of Trojans derived "genetically" from the ***W32/Kelvir.L.worm*** worms. Their creators have reused the code of one of the numerous variants of this *malware* family to breed a new "race" of Trojans with identical functionality, but now without the propagation capability they had.

So, as an example, ***Trj/Kelvir.AS*** sends messages to members of the MSN Messenger list of contacts of the user affected. These messages contain links to what ***PandaLabs*** detects as ***W32/Sdbot.DKE.worm***, in the hope that it is executed by one of the message addressees. It can therefore be said that ***Trj/Kelvir.AS*** acts as a medium for distributing copies of the bot ***W32/Sdbot.DKE.worm***.

Trj/Kelvir.AS	***05/10/2005***

W32/Sdbot.DKE.worm	***05/10/2005***

The Gookle case

A very peculiar malicious website was identified at the end of April. At first it seemed that a new Internet domain very similar to the famous Google search engine had been registered, as a way of obtaining easy hits from unwary users.

When a user entered this domain in their browser, the web server showed what appeared to be the genuine Google search engine web page; however, nothing could have been further from the truth. While the browser loaded the content of the bogus Google site, different types of *malware* tried to interfere with the system without prior warning by exploiting known vulnerabilities.

The type of *malware* that Gookle tried to install in the system of unfortunate "victims" included backdoors, trojans and even ***Adware***/***Spyware***.

The Gookle case was given broad coverage in the specialist press, in spite of the fact that **it was not the first time that these types of virtual traps were set** in the Internet. **It is likely that these sorts of situations will reoccur in the future**. There is a sample list below of similar cases recorded to date as proof of this:

gfoogle.com
ghoogle.com
msnm.com
googfle.com
msn1.com
passpport.com
gizoogle.com
luycos.com
xcnn.com

Winding up of COAST

The Register published an interesting article on April 13th: the controversial anti-*Spyware* consortium COAST will cease operations on Friday April 14th. The COAST website announced:

NOTICE: *C.O.A.S.T. has ceased operations, and this website will be taken down permanently on April 15, 2005.*

As discussed in the previous quarterly report, the credibility of this consortium was significantly damaged and called into question after numerous *Adware* development companies were accepted as COAST members. This loss of confidence led to numerous casualties among its ranks, reaching a stage where anti-*malware* companies became an "overwhelming minority".

Whatever the reasons, it appears that major internal and external pressures on the consortium ultimately resulted in its collapse.

A void to be filled…

Protecting users' workstations against any type of unwanted *Spyware* and *Adware* has proven to be a complex task where a lot of different types of factors come into play (mainly theoretical, technical and legal).

This difficult situation has led to a major change in perspective for companies from the anti-*malware* sector, accustomed to issuing conclusive and decisive verdicts that differentiate *malware* from all other software.

This is why, more than ever, cooperation and collaboration between the different representatives from the anti-*malware* sector is crucial. This step will be vitally important when establishing the guidelines for a more than necessary strategic action plan. Paving the way and obtaining general consensus and support on some basic principles may prove decisive.

Where to start? Undoubtedly, the definition and determination of what can and must be considered as *Adware* or *Spyware* should appear as one of the top priorities in the agenda of any new initiative, coalition or alliance.

In fact, at the end of the second quarter of the year, a new coalition (**Anti-*Spyware* Coalition** or **ASC**) which ***Panda Software*** forms a part of and which promises to deal with some of these needs was formed. ***PandaLabs*** hopes to be able to announce in the next quarterly report the implementation of new, solid cooperation projects within the framework of this new alliance.

Malware capable of detecting simulated environments

The practice of using virtual environments designed for *malware* analysis is becoming increasingly widespread. Systems such as VMWare or VirtualPC are the order of the day when carrying out *malware* tests. The use of virtual environments for real-time execution of samples provides *malware* analysts with very valuable, additional data on information obtained through the static analysis of unpackaged and disassembled code.

This situation is very familiar nowadays to *malware* creators and, as to be expected, in their desire to make the work of security analysts as difficult as possible, they have not taken a long to set the anti-*malware* community new tests.

During the second quarter of the year, ***PandaLabs*** detected diverse specimens of the **Gaobot** and **Sdbot** families capable of altering their behavior when executed in VMWare environments, hiding their true intentions and actions carried out in real environments.

PandaLabs has also identified variants of the **Gaobot** and **Sdbot** families packaged with modified packers so that they only unpackage the code after checking that they are not being executed in VMWare or VirtualPC environments.

This practice is added to the already considerable list of obstacles deployed by *malware* creators in their creations, with the sole objective of hindering their detection and analysis by security analysts.

Self-destructive *malware* "against piracy"

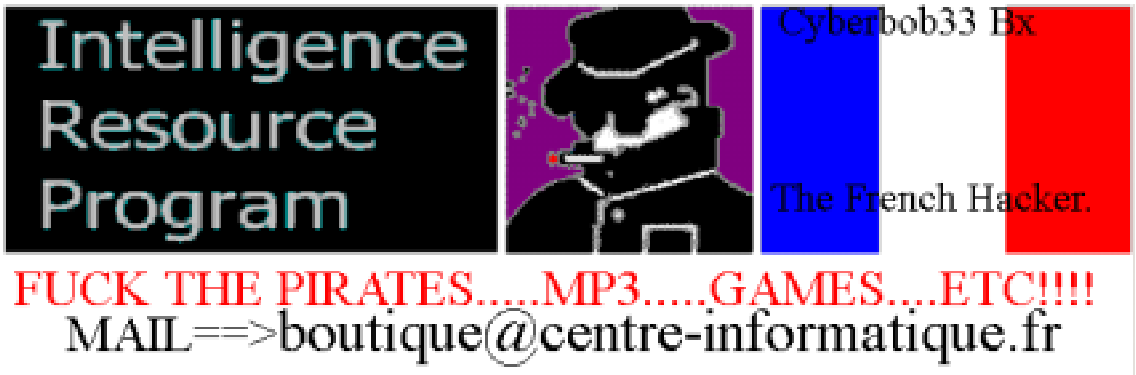
It is well known that self-destructive *malware* will shortly become extinct, that is why the appearance of new specimens of this type is worth mentioning.

The term "self-destructive" has been chosen deliberately to exclude all types of *malware* capable of causing damage to systems other than those in which they are in. After all, when a *malware* specimen decides to inflict damage on the system sheltering it, not only does it run the risk of being discovered, but it may also place its own survival in serious danger (≈ self-destructive *malware*).

During the second quarter of the year, ***PandaLabs*** detected two new *malware* specimens with this type of destructive behavior. In both cases, the motive and pretext chosen were identical in nature: activism against piracy. Consequently, as difficult as it might be to believe, these two *malware* specimens took their own particular revenge on software pirates by eliminating files in the system affected.

W32/Nopir.A.worm

In April, ***PandaLabs*** detected a new P2P worm named **W32/Nopir.A.worm**, which would have passed unnoticed if it had not been for the fact that it was one of the few destructive specimens recorded recently. The worm in question eliminates all *.MP3* and *.COM* type files found in the affected system, showing the following image when executed:


Intelligence
Resource
Program
Cyberbob33 Bx
The French Hacker.
FUCK THE PIRATES.....MP3.....GAMES....ETC!!!!
MAIL==>boutique@centre-informatique.fr

W32/Nopir.A.worm	***04/27/2005***

All the details about ***W32/Nopir.A.worm*** can be found in the Panda Software Virus Encyclopedia.

Trj/Whiter.F

On 11th May, ***PandaLabs*** detected a very destructive new Trojan: ***Trj/Whiter.F***. This *malware* specimen replaces all files recursively with the content of a text file called WXP, which includes the message "***You did a piracy, you deserve it***". It then eliminates them.

Trj/Whiter.F	***05/11/2005***

All the details about ***Trj/Whiter.F*** can be found in the Panda Software Virus Encyclopedia.

A Trojan extortioner

During the second quarter of the year, ***PandaLabs*** detected a very peculiar new Trojan. This *malware* specimen called ***Trj/PGPCoder.A**** searches for and encrypts files with certain extensions *(ASC, DB, DB1, DB2, DBF, DOC, HTM, HTML, JPG, PGP, RAR, RTF, TXT, XLS and ZIP)*, with the only aim being to demand a ransom: $200 in exchange for obtaining the decryption key.

> ***** *In spite of what its name might suggest, the algorithm of the encryption used by this Trojan has nothing to do with the complex arsenal of the famous PGP (PrettyGoodPrivacy).*

Trj/PGPCoder.A	***05/25/2005***

All the details about ***Trj/PGPCoder.A*** can be found in the Panda Software Virus Encyclopedia.

Given the behavior of ***Trj/PGPCoder.A***, ***PandaLabs*** considered the inclusion of additional routines necessary in order to detect and decrypt files used by this Trojan. Consequently, ***Trj/PGPCoder.Crypt*** matches a detection prepared by ***PandaLabs*** designed to identify and decrypt files previously encrypted by ***Trj/PGPCoder.A***.

Trj/PGPCoder.Crypt	***05/25/2005***

This incident led to some of the media talking about ***ransomware*** as a term linked to this type of hijacker *malware*. In fact, there is an entry in the free encyclopedia WikipediA which includes a definition of this new term.

Approximately one month later, ***PandaLabs*** detected a second variant of this particular Trojan: ***Trj/PGPCoder.B***.

Trj/PGPCoder.B	***06/29/2005***

Trj/PGPCoder.B.Crypt	***06/29/2005***

All the details about ***Trj/PGPCoder.B*** can be found in the Panda Software Virus Encyclopedia.

Rogue anti-*Spyware*

Adware and *Spyware* type threats are now reaching epidemic levels and proportions. There is an increasing level of awareness and knowledge about this reality, and it is arousing all sorts of interest for financial gains.

The "latest trend" appears to be the development and distribution of anti-*Spyware* tools that show false results, identifying supposedly real *Spyware* specimens which are in fact not detected at all. The aim is to sell licenses of the product in question. Some of these tools are distributed fraudulently through websites that install them, without the consent or knowledge of the users affected.

The renowned *Adware/Spyware* analyst Eric Howes has an exhaustive *list of rogue anti-Spyware*.

During the second quarter, ***PandaLabs*** detected various new specimens that showed this dishonest behavior. Particularly noteworthy were ***Adware/SpywareNo*** and ***Adware/SpySheriff*** .

Adware/SpywareNo	***05/26/2005***

All the details about ***Adware/SpywareNo*** can be found in the Panda Software Virus Encyclopedia.

Adware/SpySheriff	***06/21/2005***

All the details about ***Adware/SpySheriff*** can be found in the Panda Software Virus Encyclopedia.

PandaLabs also detected a new *Spyware* specimen (***Spyware/SmitFraud***) at the beginning of June, with similar behavior: once it enters the system it displays bogus warning messages about non-existent *Spyware* infections, installing and executing an anti-*Spyware* tool of dubious origin without notification.

Spyware/SmitFraud does not just install a supposed anti-*Spyware* tool, but also exploits each "conquest" to make its own contribution, modifying one of the system's libraries (*WININET.DLL*) to capture urls entered by users affected in their browser.

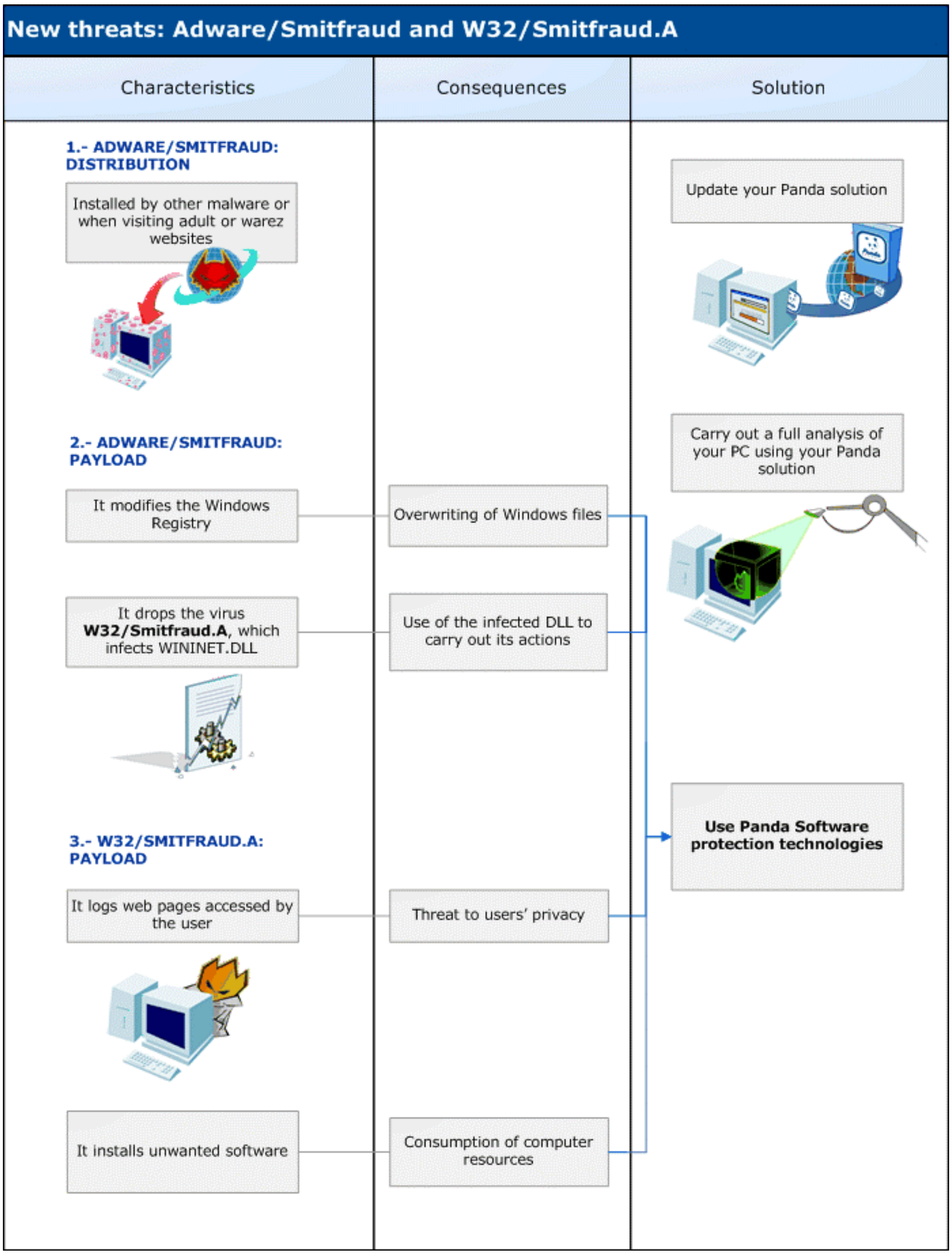
Altered versions of *WININET.DLL* such as ***W32/SmitFraud*** and ***W32/SmitFraud.B*** created by ***Spyware/SmitFraud*** were detected by ***PandaLabs*** .

Spyware/SmitFraud	***06/08/2005***

All the details about ***Spyware/SmitFraud*** can be found in the Panda Software Virus Encyclopedia.

W32/SmitFraud	***06/07/2005***

W32/SmitFraud.B	***06/28/2005***



New threats: Adware/Smitfraud and W32/Smitfraud.A

Characteristics	Consequences	Solution
1.- ADWARE/SMITFRAUD: DISTRIBUTION		
Installed by other malware or when visiting adult or warez websites		Update your Panda solution
2.- ADWARE/SMITFRAUD: PAYLOAD		Carry out a full analysis of your PC using your Panda solution
It modifies the Windows Registry	Overwriting of Windows files	
It drops the virus **W32/Smitfraud.A**, which infects WININET.DLL	Use of the infected DLL to carry out its actions	
3.- W32/SMITFRAUD.A: PAYLOAD		**Use Panda Software protection technologies**
It logs web pages accessed by the user	Threat to users' privacy	
It installs unwanted software	Consumption of computer resources	

Focused attacks with *a la carte malware*

During the second quarter of the year, various cases of espionage came to light about the use of *malware* especially designed for such purpose.

These types of threats represent a real risk which should not be underestimated and which justifies, even more, the creation of proactive solutions capable of detecting or blocking unknown *malware*.

It is worth commenting on the scandal in Israel, where various companies, including some of the most important from the telecommunications sector, as well as three major private agencies from this same country, were involved in an alleged case of industrial espionage. On May 29th Haaretz published an article detailing the particulars of this thorny matter.

There were various arrests under the accusation of organizing and implementing industrial espionage which, in the words of police spokespersons, was the most important such case in Israel's history. Those arrested formed part of the top management of companies that would have benefited from the plot (spying on their competitors), as well as the body of private detectives that would have enabled this.

Apparently the espionage plot centered on a piece of *malware* especially designed for the task which would have been distributed selectively through carefully personalized email messages and CD Roms.

PandaLabs was able to detect the supposed *malware* specimen implicated (***Trj/Rona.A***), as well as seven variants.

Trj/Rona.A	***04/31/2005***

All the details about ***Trj/Rona.A*** can be found in the Panda Software Virus Encyclopedia.

We would like to take this opportunity to publicly thank the company 2BSecure for swiftly providing ***PandaLabs*** with a copy of the original sample of ***Trj/Rona.A***.

Drawing boundaries: *Adware*, *Spyware* and spy *malware*

During this second quarter of the year, debates have intensified over a matter which is threatening to become rather rhetorical: the definition and determination of the terms *Adware* and *Spyware*.

These terms currently display a high degree of ambiguity and ambivalence, both characteristics being the result of a clear lack of consensus. The problems increase when trying to draw boundaries between *Spyware* and traditional *malware*.

Spyware and spy *malware*

The term *Spyware* was originally used for a particular type of *malware*. This type of *malware* was characterized by its specialization in stealing information about the browsing tastes, preferences and habits of affected users. It is installed without the user's knowledge in the system as an Internet Explorer parasite, normally using the omnipresent BHO's (Browser Helper Objects) or plugins for the Microsoft browser. As a result, ***Spyware* was created as a very specific *malware* category, with a series of certain characteristics and even a technology different to other *malware***.

The theft of confidential and personal information is not a new *malware* practice, with a multitude of specimens especially designed for this purpose. The most recent and dangerous include Trojans designed to capture bank and financial data.

There is, however, a growing trend in the use of the term *Spyware* to refer to any type of *malware* which carries out an assault on user privacy, confidentiality or identity. It is, on the other hand, understandable that the term itself has been adopted, since *Spyware* results from the joining together of the words 'spy' and 'software'.

At *PandaLabs* we believe it is important to not forget the original and strictest meaning of the term *Spyware*, although at the same time we do consider logical the new use coming into practice now.

It is highly probable that something similar will happen to what occurred in the past with the term virus, which continues to have a double meaning today: the original and strictest referring to *malware* with file infection capabilities, as well as a more popular meaning referring to *malware* in general.

Adware and *Spyware*

The term *Adware* is produced from the union of the two words "Advertisement" and "Software". *Adware*, as the name suggests, is designed with the sole aim of promoting or advertising services and products. This type of software was included initially in freeware or shareware type programs (in exchange for its free use) and started to become linked to all types of websites that invited, fooled or even forced users into installing it.

It was not too long before the next step with respect to *Adware* followed: personalized advertising… and with it the first indications of the current *Spyware* identity problem.

Personalized advertising is achieved by studying user's browser tastes and habits. This is where the dilemma lies, since **personalized advertising makes it very difficult to distinguish between *Adware* and *Spyware* in some cases**.

Adware…software or *malware*?

It will probably not have escaped the attention of some readers that *Spyware* has been mentioned in the same terms as *malware*, while *Adware* is seen as just another form of software.

However, by concentrating excessively on the aim pursued by *Adware*, it is easy to lose sight of some important connotations: it is clear that there are major differences between the voluntary use of a free application that includes well-defined advertising software and the forced installation through some vulnerability of the same software without the user's knowledge. The list of possible connotations widens: installation method, facilities offered for its uninstallation, existence or absence of a user license (EULA) etc.

It is not surprising therefore that *Adware* is sometimes closer to traditional *malware* and *Spyware* than promotional software. This circumstance is leading to some promotional software developers feeling uncomfortable when finding out that their products are classed as *Adware*. In fact, **this situation is being exploited by some of these developers to demand that companies from the sector put an end to detecting their supposedly non-*Adware***.

Risk capital + *Adware* = explosive cocktail

Personalized advertising appears to have aroused the interest of diverse investors prepared to finance some of the most well-known companies in the *Adware* and consumerware market, as some of them proclaim to be.

Capital contributions that these types of companies enjoy are in some cases enormous, bringing back memories of the height of the cybernetic gold rush and .com fever before the Internet bubble burst. Will these same companies who are likely to have witnessed the consequences of Internet speculation go the same way? Only time will tell.

The renowned *Adware/Spyware* analyst Benjamin Edelman has a curious list with the most significant capital contributions to date.

Conclusions

The second quarter of the year clearly shows the "good run of form" being enjoyed by creators and distributors of all types of *malware* and threats such as *Adware* or *Spyware*.

Although there is a distinct lack of alert situations attributable to specific specimens, the "cake" is now being shared between many different variants and specimens. **No one should be fooled; the Internet is infested with *malware* and other threats, without any signs of this waning presently.**

It is true, however, that the current situation does reveal a loss of effectiveness in traditional mail worms, which are now making way for **other types of *malware* such as Trojans and in particular *Adware* and *Spyware* threats** (normally distributed from websites). This circumstance **also justifies the use of instant messaging as a means for the propagation and distribution of *malware*** (including the increasingly common instant messaging worms).

Special mention must be made of the **spy-type Trojans** and particularly those specializing in financial data theft (Trojan phishers), which are in rapid ascendancy.

To sum up, it is clear that *malware*, *Adware* or *Spyware* creators and their distributors are not going to cease in their efforts to complicate the work of security analysts, with new movements in this arena to be expected.

About *PandaLabs*

PandaLabs is ***Panda Software's*** anti-*malware* laboratory and the company's nerve centre when it comes to tackling *malware*:

- ***PandaLabs*** prepares in real time and continuously the countermeasures necessary to protect ***Panda Software*** clients from all types of malicious code worldwide.

- ***PandaLabs*** is also responsible for carrying out a detailed analysis of all types of *malware* in order to improve the protection offered to ***Panda Software*** clients, as well as to inform the general public.

- ***PandaLabs*** constantly monitors very closely the different trends and developments occurring in the *malware* and security field. The objective is to provide warnings and alerts about imminent dangers and threats, as well as prepare future forecasts.