

MALWARE INFECTIONS IN PROTECTED SYSTEMS

Research study of **PandaLabs**
pandalabs.pandasecurity.com

Table of contents

1 Abstract	3
2 Introduction to the Research Study	4
3 Methodology	5
4 Consumer Study	7
4.1 Evolution of Malware Infections	7
4.2 Statistical Sample Information	8
4.2.1 Machines by State of Anti-Malware Protections	8
4.2.2 Machines by Operating Systems	9
4.2.3 Machines by Country	10
4.3 Malware Infections in Protected Machines	11
4.3.1 Malware Infections by Type of Malware	12
4.3.2 Malware Infections by Anti-Malware Solution	13
5 Corporate Study	14
5.1 Statistical Sample Information	14
5.1.1 Companies by Country	14
5.1.2 Workstations by Operating Systems	15
5.1.3 Workstations by State of Anti-Malware Protection	16
5.2 Malware Infections in Protected Networks	17
5.2.1 Malware Infections per Networks Tested	17
5.2.2 Malware Infections by Type of Malware	18
5.2.3 Malware Infections by Anti-Malware Solution	19
6 Conclusions	20
7 Appendix – July Detections & Prevalence	22
8 References	24

1. Abstract

If there is more malware than ever and antivirus laboratories cannot keep up with the pace of creating signatures fast enough to protect users, it stands to reason that **a significant portion of users are infected, even if they have an up-to-date security solution with the latest virus signature database.**

We have conducted a research project with the objective of uncovering the real malware situation at real computers with updated protection installed. The ongoing study was conducted between May and July 2007 on both consumer PCs and corporate networks worldwide. Of the consumer PCs tested, which had a variety of different security solutions installed and up-to-date signature database, **over 23% of PCs were infected with malware loaded into memory.** Out of all the companies tested which executed the audit on over 100 workstations that had active and updated anti-malware protection, **72% of the companies tested had malware infections.**

As a conclusion of this research project we have found that users who are active and paying subscribers to anti-malware or security solutions are suffering from unsuspecting malware infections. It seems that in some cases security software provides a false sense of security. This notion is already known by part of the anti-malware industry. It's even supported by the industry as a whole, in some cases providing users with "product certifications" which users perceive as a quality certification but which in reality only prove that the solution is able to detect a fraction of a percentage of the malware which is really in the wild.

New cooperation among the industry players as well as new technological approaches to anti-malware protection are needed to provide protection against today's malware landscape. This research study is released in the hopes that the barriers for innovation can be analyzed, such as antivirus testing standards, quality standards and product certification standards, which keep this situation hidden under the rug.

2. Introduction to the Research Study

This ongoing research study is focused on providing statistics of active malware infections in systems protected by anti-malware or security solutions and with the latest signature database installed. The final objective of this study is to provide a timeline of infection ratios over time to be able to analyze the progression of the effectiveness of different protection technologies.

Even though there are user-based surveys that try to show similar research¹ we could not find one that showed scientifically verifiable conclusions based on:

- Automatically gathered data which can be segmented based on users with and without anti-malware protection.
- Malware infections in systems protected with the latest updates and anti-malware engines.
- A large population sample that reflects the situation in different geographical locations.
- Statistics which show the infection rates specifically and separately for consumer and corporate markets.

Our project is aimed at automatically gathering data from hundreds of thousands of computers worldwide, therefore giving a much more realistic view of the actual security situation. During the course of the investigation we have also been able to gather other significant statistics which shed quite a bit of light into the real situation at users' PCs.

3. Methodology

The research study was conducted by physically scanning consumer and corporate computers from over 80 different countries. Tested machines included protection from over 40 different security vendors. Testing was performed using different online systems and auditing tools with millions of malware and goodware signatures and scanning-from-the-cloud capabilities:

Consumer Study:

- Consumers scanned their PCs using a special online scanner.
- Consumer users who scanned their PCs multiple times are accounted for only once.
- Only the result of the first scan is taken into consideration.

Corporate Study:

- Audits were physically performed on corporate networks worldwide using a malware auditing tool specifically build for the purpose of uncovering non-detected malware.
- Companies that performed multiple audits are only accounted for once.
- Only the result of the first audit of each PC is taken into consideration.

Infection Criteria:

- A PC **is considered infected** when we find malware (trojan, adware, virus, worms, etc.) actively running in memory. .
- A PC is **NOT considered infected** if it only has latent malware (malware in email databases, saved on the hard drive or otherwise) which is not actively running, executed in memory, registered as a BHO or otherwise active.
- A PC is **NOT considered infected** if it only has tracking cookies, jokes or other non-malicious applications.

Protected System Criteria:

- We consider a PC as protected if it has an anti-malware or security solution installed and updated with the latest available virus signature database.
- The statistics about the anti-malware or security solution status (resident driver active or inactive) and its signature database information (updated or outdated) is queried directly from the Microsoft Windows Security Center under Windows XP SP2 and Windows Vista. Certain security vendors do not appear in our statistics as they do not register or share information with the Microsoft Windows Security Center.

In order to be able to determine if a PC is infected or not we have built a system capable of positively detecting all known (and a large portion of unknown) samples of malware, regardless of whether we have signature detection for it in our regular products.

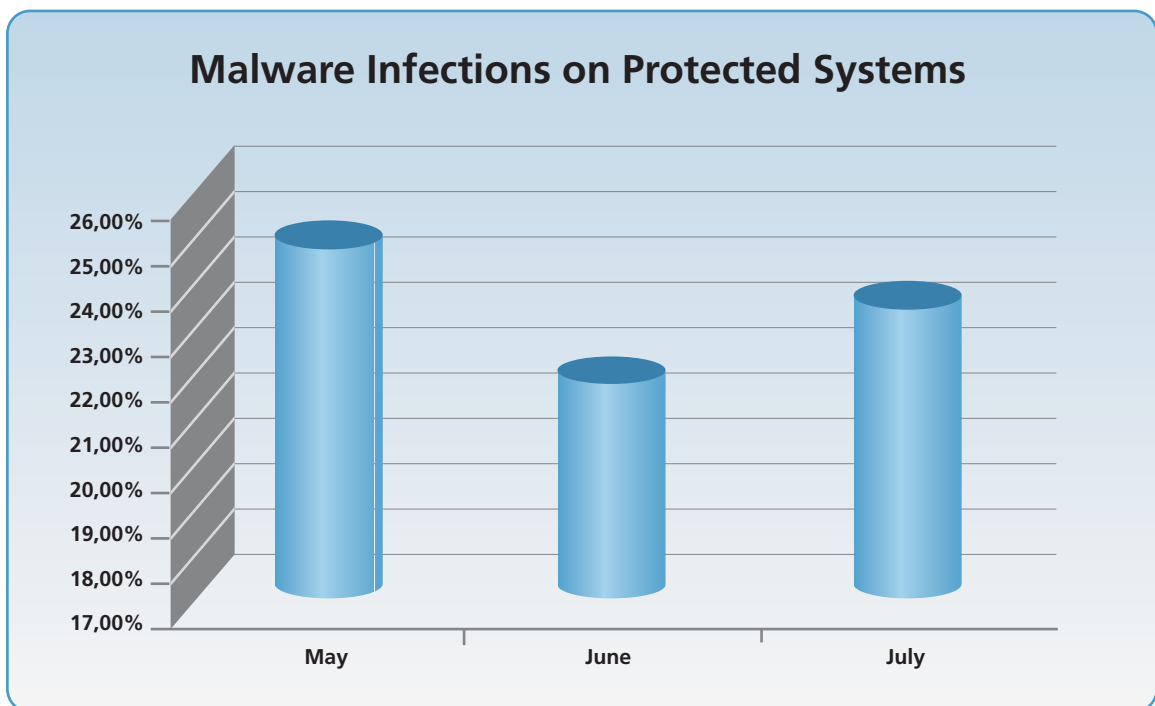
We achieved this with a platform we call Collective Intelligence, which is an online system hosted at several Network Operating Centers that automates the processes of malware collection, malware classification and malware detection and which correlates the results from the scans from all the users. Users execute a small 600kb online scanner which checks their security protection, processes, objects loaded into memory and various other heuristic checks. There are other added benefits such as being able to use much more advanced technologies which are not limited by the resources of a PC's RAM and CPU.

Panda's Collective Intelligence is a new concept on malware protection that benefits in real-time of the information provided by the community of its users and the automation of the sample gathering, processing and remediation to increase its detection capacity².

4. Consumer Study

The data for this part of the statistical study were collected from 1.48 million users who scanned their PCs with one of our Collective Intelligence online scanners since May 2007. Out of the 1.48 million we are only interested in those that (a) had active and up-to-date anti-malware or security system installed and (b) had active malware infections. The PCs that match these two criteria are, in average, 23% of all tested PCs, as shown below.

4.1 Evolution of Malware Infections



Study period	Users scanned	Infection rate of unprotected systems	Infection rate of protected systems
May 2007	730.237	34.85%	24.17%
June 2007	443.214	31.25%	21.78%
July 2007	306,836	33.74%	22.97%
TOTAL	1,480,287	33.28%	23.21%

It is important to stress that the infection rates we are interested in are the “infection rates of protected systems”, which are systems with installed and up-to-date anti-malware or security solution. The actual infection rate of unprotected machines is obviously greater as shown above.

In the following sections we will analyze the data from the last period of the research study in depth, which corresponds to July 2007.

4.2 Statistical Sample Information

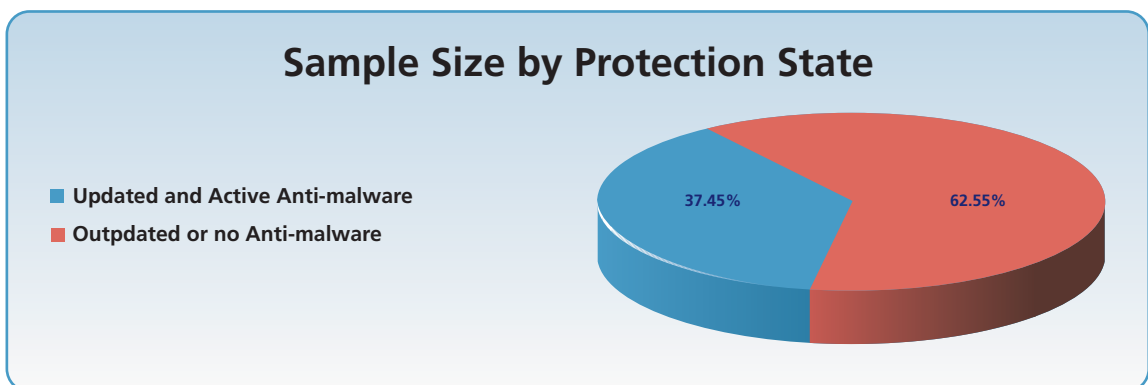
As this is an ongoing study which is being published regularly we are tracking both the evolution of the infection rates on systems with anti-malware protection (section 4.1 above) and an analysis of the data of the last period of the study, which corresponds to this current section 4.2.

The study for July 2007 involves a total number of 306,836 unique PCs scanned. Data was gathered from July 1st to July 20th 2007.

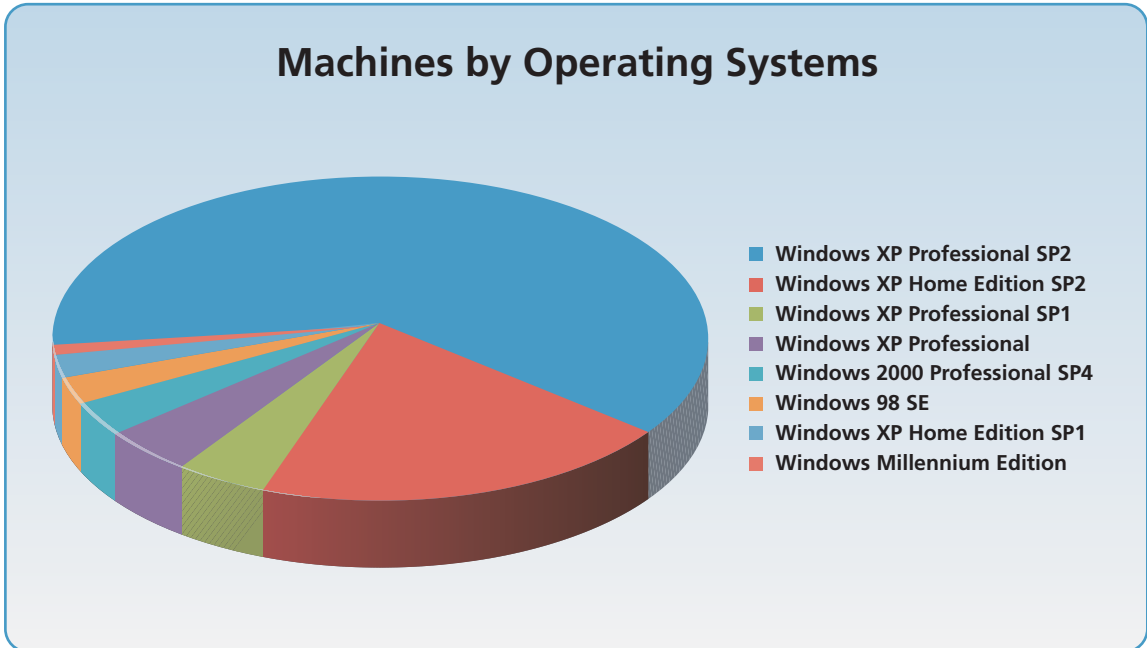
In the following subsections we can see how this data is broken down and correlated by Operating System, countries, status of the protection, infection rates on protected systems, type of malware infections and infections by vendors.

4.2.1 Machines by State of Anti-Malware Protections

As mentioned previously, this study is focused on determining the rate of malware infections in systems actively protected by up-to-date anti-malware solutions. In the case of the current study, only 37.45% of the systems tested had updated and active anti-malware protection. The remaining 62.55% either had outdated signatures and inactive resident drive, outdated signatures and active resident driver, or no anti-malware installed at all.



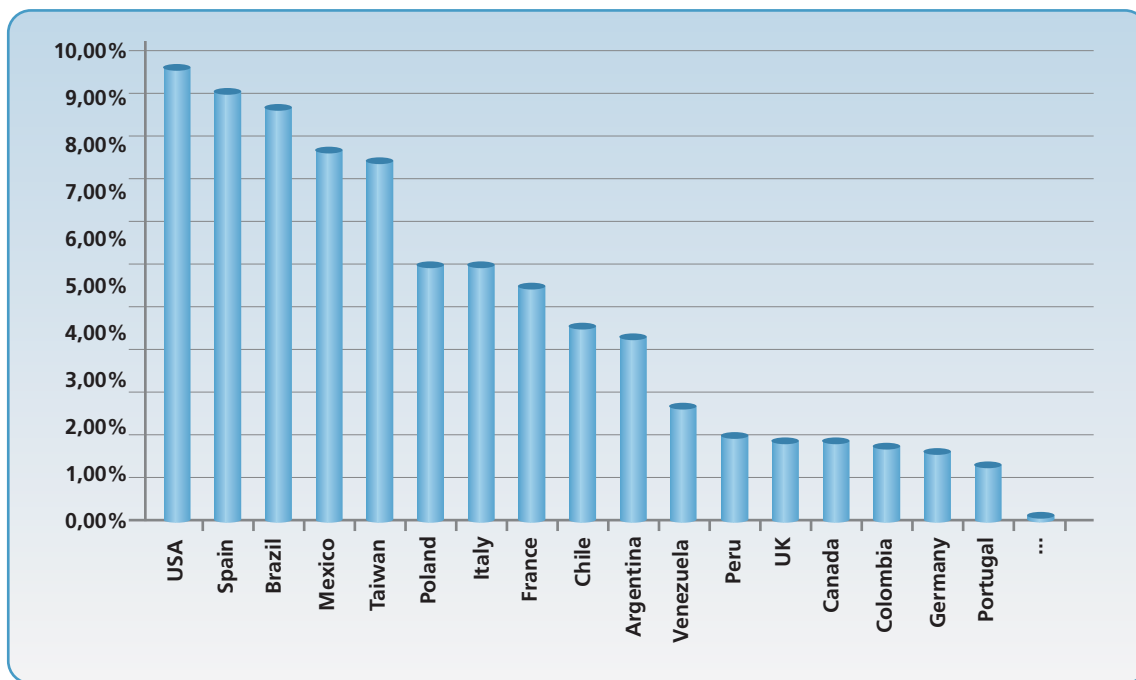
4.2.2 Machines by Operating Systems



Operating System Scanned	Sample Market Share
Windows XP Professional SP2	59.16 %
Windows XP Home Edition SP2	20.74 %
Windows XP Professional SP1	4.01 %
Windows XP Professional	3.66 %
Windows 2000 Professional SP4	3.55 %
Windows 98 SE	2.74 %
Windows XP Home Edition SP1	1.45 %
Windows Millennium Edition	1.03 %

* Data shown over total number of PCs scanned.

4.2.3 Machines by country



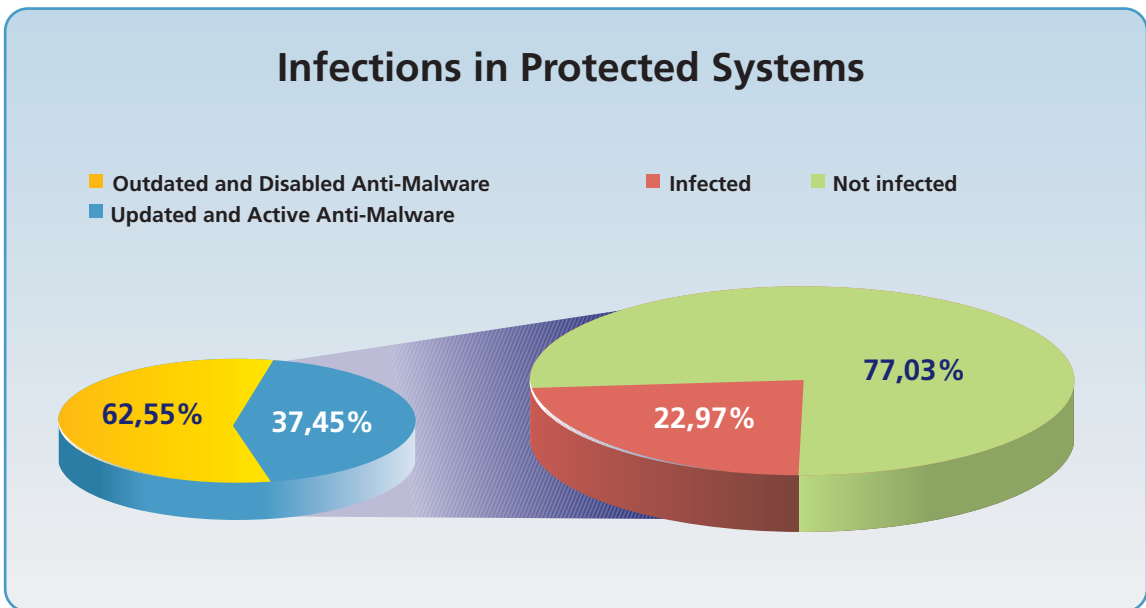
Distribution by country	Sample Market Share
United States	9.60 %
Spain	9.12 %
Brazil	8.70 %
Mexico	7.83 %
Taiwan	7.55 %
Poland	5.14 %
Italy	5.08 %
France	4.61 %
Chile	3.80 %
Argentina	3.67 %
Venezuela	2.68 %
Peru	2.11 %
United Kingdom	1.96 %
Canada	1.93 %
Colombia	1.88 %
Germany	1.75 %
Portugal	1.39 %
...	...

* Data shown over total number of PCs scanned. Only top reporting countries are shown.

4.3 Malware Infections in Protected Machines

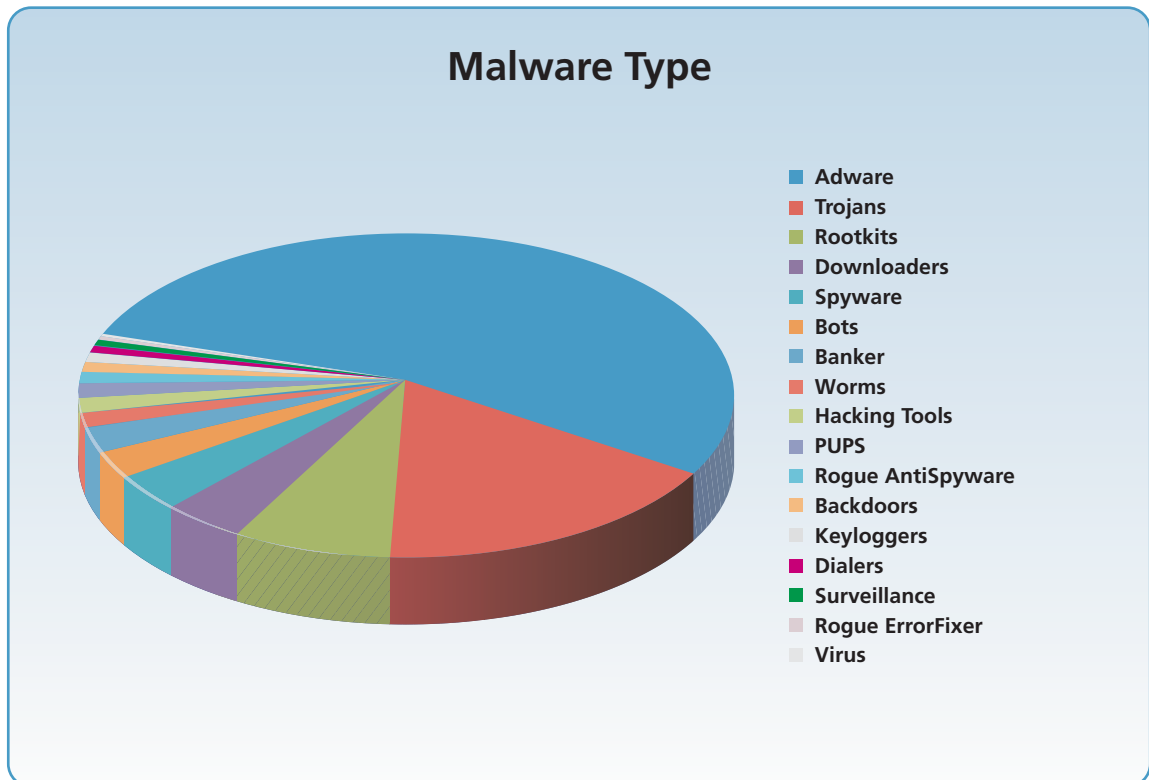
We discovered that out of the 37.45% of tested systems, even though they were protected with current up-to-date and active anti-malware protection, 22.97% of them were actually infected by malicious code.

Protection status	Sample share	Not infected	Infection rate of active malware
Outdated and Disabled Anti-Malware	55.32 %	66.46 %	33.54 %
Outdated and Active Anti-Malware	7.23 %	64.75 %	35.25 %
Updated and Active Anti-Malware	37.45 %	77.03 %	22.97 %



4.3.1 Malware Infections by Type of Malware

The following table shows the percentage of protected PCs actively infected by malware type. One PC can have multiple types of malware.



Malware Type	Found in x % de PCs*
Adware	54.50 %
Trojans	15.46 %
Rootkits	7.21 %
Downloaders	5.20 %
Spyware	4.80 %
Bots	2.65 %
Banker Trojans	2.22 %
Worms	2.21 %
Hacking Tools	1.06 %

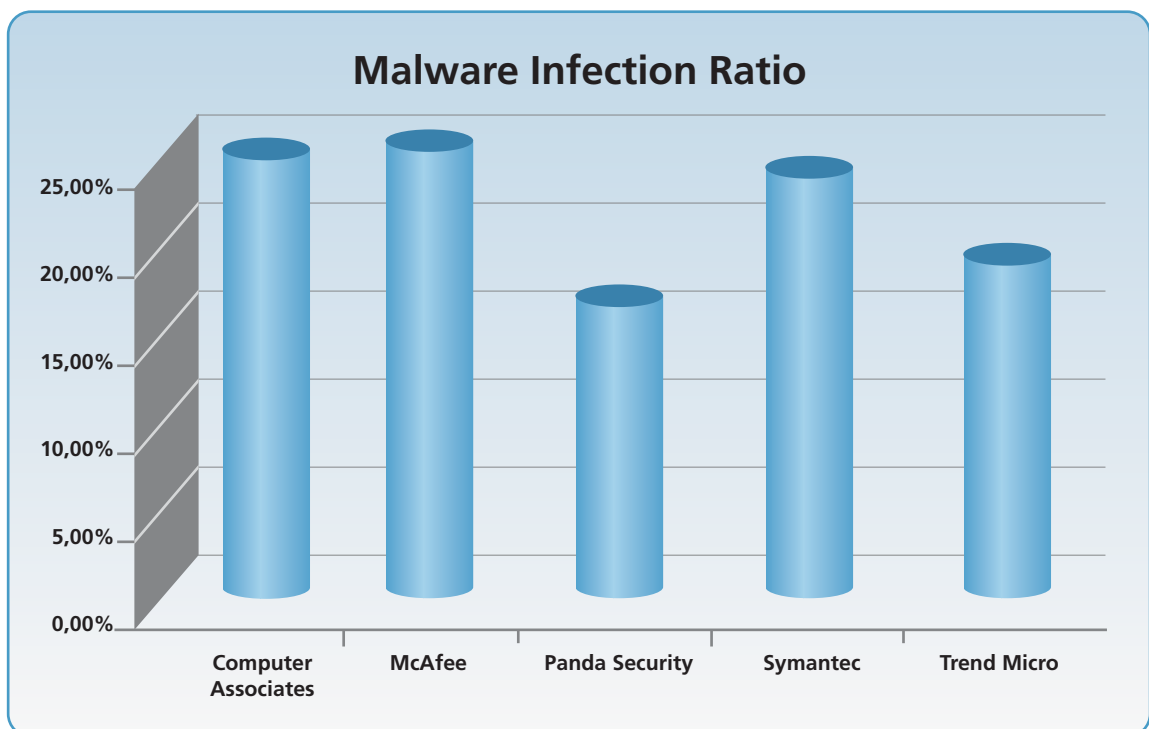
Malware Type	Found in x % de PCs*
Potentailly unwanted programs	1.03 %
Rogue AntiSpyware	0.96 %
Backdoors	0.86 %
Keyloggers	0.56 %
Dialers	0.45 %
Surveillance	0.40 %
Rogue ErrorFixer	0.26 %
Virus	0.18 %

* Data shown is based on total number of protected PCs.

4.3.2 Malware Infections by Anti-Malware Solution

Every time a system is scanned we query the Windows Security Center for its installed anti-malware solution, installed firewall, system state and state of updates. This information is stored and correlated against the infection state.

In the graph and table below we can see the infection rates of systems per installed and updated anti-malware solution. Even though we have collected and correlated information from over 40 different anti-malware and security vendors, the ones shown below correspond to the main vendors by worldwide market share according to Gartner. This information should not be taken as a comparative analysis as the objective of this data is to show that there is a problem, common to the entire industry, with the current state of anti-malware solutions. In fact there are other vendors from the complete list of over 40 that have higher and lower infection rates than the ones shown.³



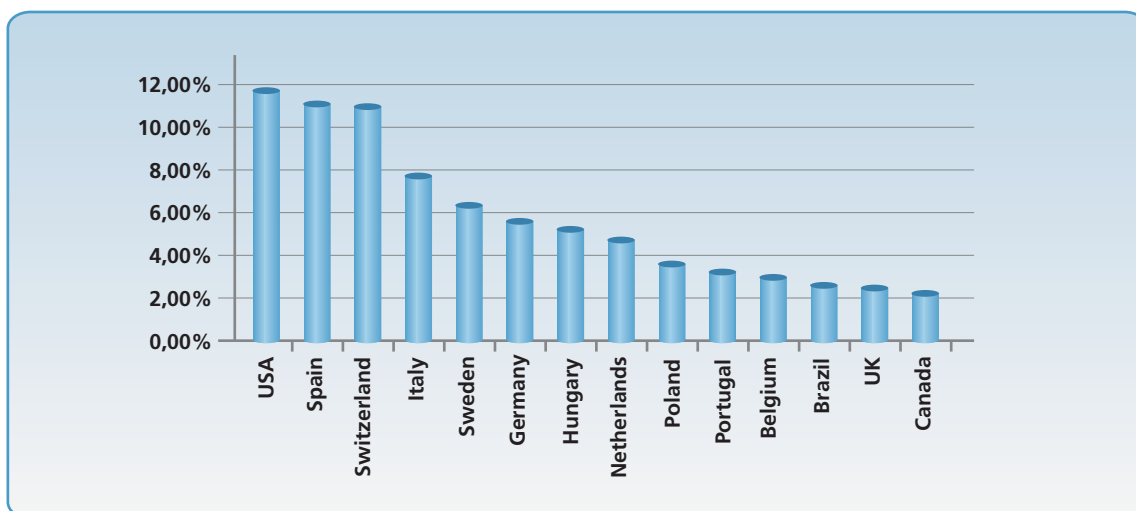
Vendor	Active Malware Infection Ratio
Computer Associates	23.32 %
McAfee	24.18 %
Panda Security	15.54 %
Symantec	22.20 %
Trend Micro	17.08 %

5. Corporate Study

5.1 Statistical Sample Information

Data gathered from April to July 2007 of 1,206 companies involved in the study. A total of 17,809 PC scanned.

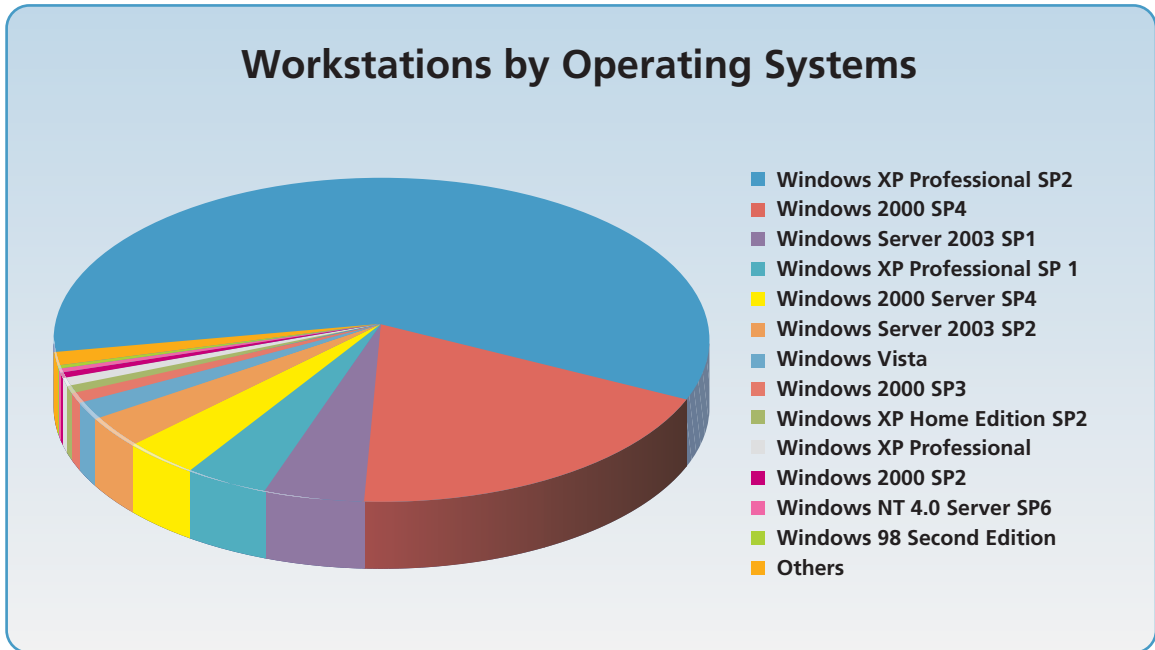
5.1.1 Companies by Country



Country	Sample Market Share
USA	11.77%
Spain	11.19%
Switzerland	11.03%
Italy	7.96%
Sweden	6.05%
Germany	5.47%
Hungary	4.81%

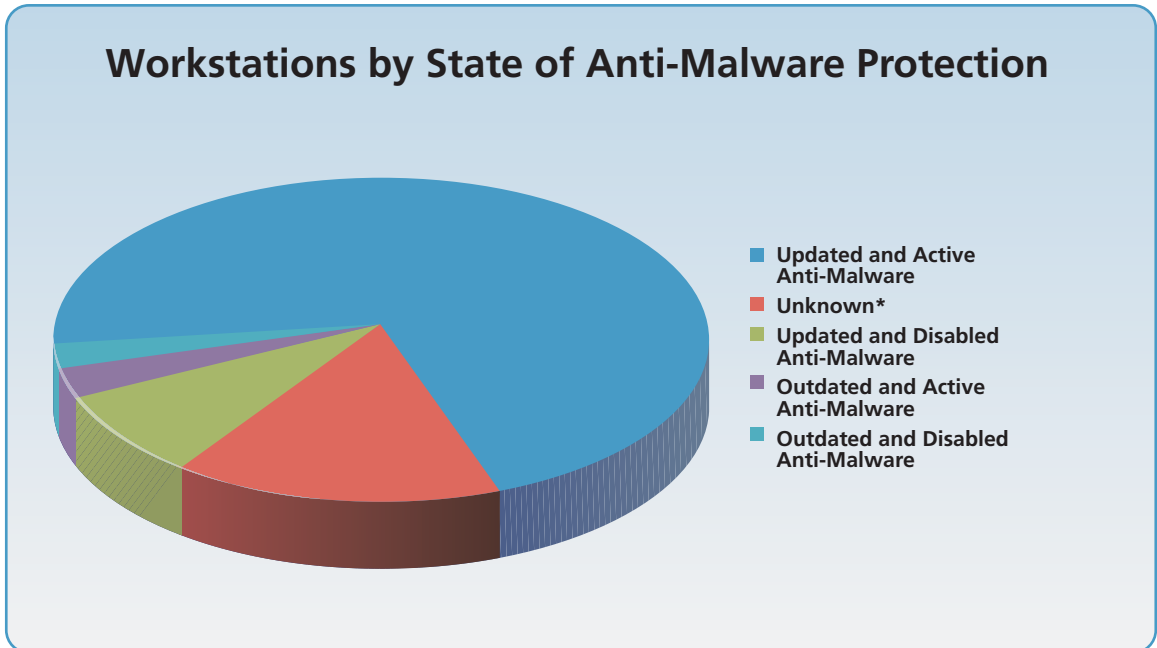
Country	Sample Market Share
Netherlands	4.56%
Poland	3.57%
Portugal	3.23%
Belgium	3.07%
Brazil	2.40%
UK	2.24%
Canada	2.07%
...	...

5.1.2 Workstations by Operating Systems



Operating System Scanned	Sample Market Share*
Windows XP Professional SP2	65.94 %
Windows 2000 SP4	17.93 %
Windows Server 2003 SP1	4.01 %
Windows XP Professional SP 1	3.91 %
Windows 2000 Server SP4	2.46 %
Windows Server 2003 SP2	2.24 %
Windows Vista	0.92 %
Windows 2000 SP3	0.57 %
Windows XP Home Edition SP2	0.47 %
Windows XP Professional	0.43%
Windows 2000 SP2	0.23%
Windows NT 4.0 Server SP6	0.13%
Windows 98 Second Edition	0.06%
Others	0.70%

5.1.3 Workstations by State of Anti-Malware Protection



Protection Status	Sample Share
Updated and Active Anti-Malware	69.34 %
Unknown*	14.50 %
Updated and Disabled Anti-Malware	9.25 %
Outdated and Active Anti-Malware	4.49 %
Outdated and Disabled Anti-Malware	2.43 %

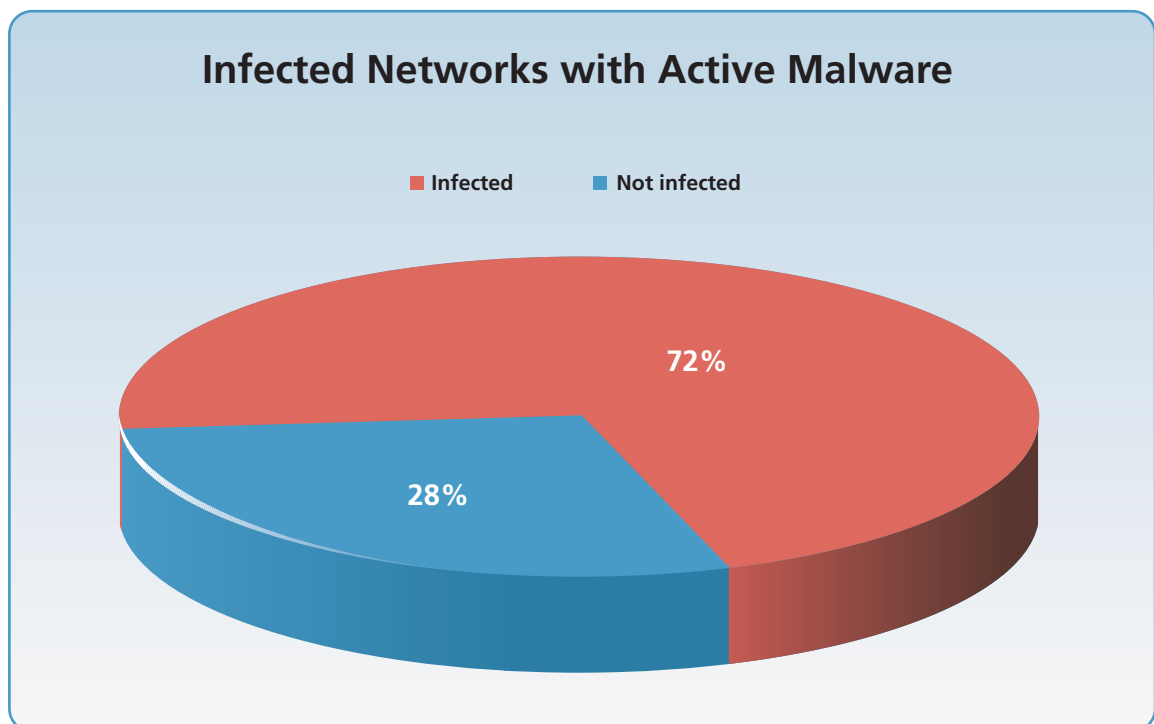
* "Unknown" refers to PCs with OS different than Windows XP SP2 and Windows Vista which do not support Windows Security Center and/or computers with errors during the reporting process.

5.2 Malware Infections in Protected Networks

Even though the study was conducted on over 1,200 different companies worldwide, we will put the focus on the details of the companies that performed the audit on over 100 PCs in order to more accurately reflect the situation on the target segment of the corporate market. Companies that performed audits on less than 100 PCs are considered departmental audits or non-relevant to this study.

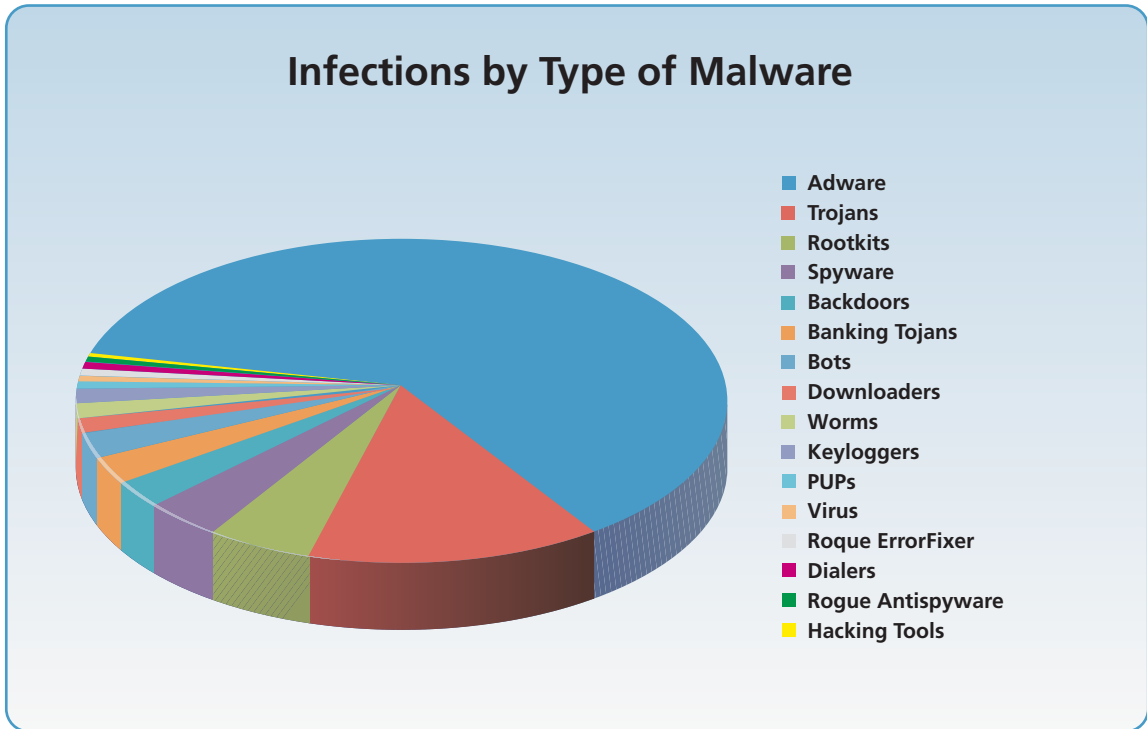
5.2.1 Active Malware Infections per Networks Tested

The following graphs the percentage of total companies where malware infections were found during the audit in at least one workstation within the corporate network.



Network Size	Rate of infected networks
Less than 50 workstations	36.63 %
51 to 100 workstations	62.26 %
Over 100 workstations	71.79 %

5.2.2 Malware Infections by Type of Malware



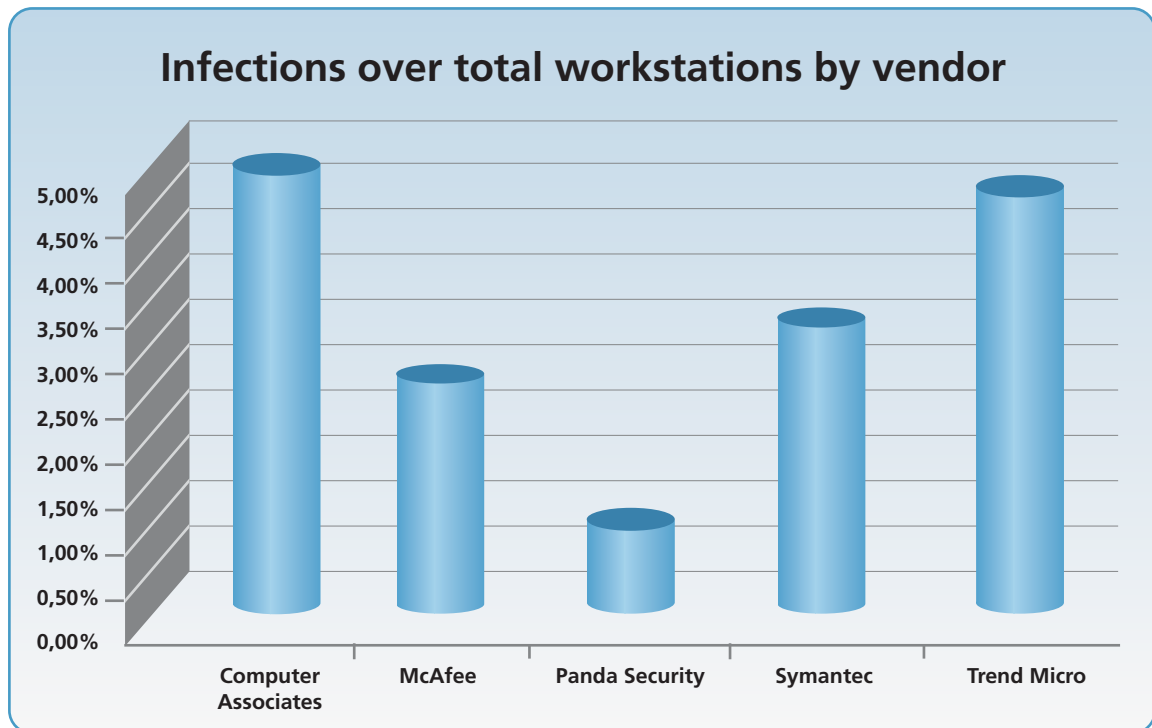
Malware Type	Percentage of detections*
Adware	63.04 %
Trojans	12.57 %
Rootkits	4.50 %
Spyware	3.75 %
Backdoors	2.44 %
Banking Trojans	2.44 %
Bots	2.44 %
Downloaders	1.69 %
Worms	1.69 %
Keyloggers	1.50 %
PUPs	1.13 %
Virus	0.94 %
Rogue ErrorFixer	0.75 %
Dialers	0.75 %
Rogue AntiSpyware	0.19 %
Hacking Tools	0.19 %

* Detections shown over all malware detections.

5.2.3 Malware Infections by Anti-Malware Solution

As a corporate network may have different anti-malware solutions on different machines, the graph and table below shows the infection rates of the total workstations audited per installed and updated anti-malware solution.

Even though we have collected and correlated information from many different corporate anti-malware and security vendors, the ones shown below correspond to the main vendors by worldwide market share according to Gartner. This information should not be taken as a comparative analysis as the objective of this data is to show that there is a problem, common to the entire industry, with the current state of anti-malware solutions. In fact there are other vendors from the complete list of vendors that have higher and lower infection rates than the ones shown.



Vendor	Active Malware Infection Ratio
Computer Associates	4.55 %
McAfee	2.28 %
Panda Security	0.73 %
Symantec	2.80 %
Trend Micro	4.30 %

6. Conclusions

The shift in motivation for creating malware, combined with the use of advanced techniques, has resulted in an exponential growth of criminally professional malware being created and distributed to infect unsuspecting users. According to AusCERT, 80% of new malware defeats antivirus defenses⁴.

Also known as targeted attacks, this new malware dynamic has become the next big plague for users and companies alike. It is estimated that 75% of enterprises will be infected with undetected, financially motivated, targeted malware that evaded their traditional perimeter and host defenses by the end of 2007⁵.

As a result antivirus laboratories are under a constant and increasingly frequent distributed denial of service attack. We are literally being bombarded with thousands of new malware samples every day. Some antivirus vendors have either tried to deal with it by increasing lab resources⁶ or called for involvement⁷ by law enforcement⁸ to help ease the workload by convicting the most active malware creators. Initiatives to get law enforcement more involved are a step in the right direction but unfortunately these seem insufficient. As developers and distributors of security solutions we need to continue assuming our responsibility of protecting users.

On the other hand antivirus and security vendors are making great efforts and investments to develop and provide better security technologies such as HIPS and behavioral blocking and analysis, to better protect users. There is a great deal of effort within the industry to improve the WildList⁹, product certifications and comparative testing methodologies¹⁰.

Still the problem persists and has no easy solution. A significant portion of paying customers are infected with malware even if they are protected with the latest and most advanced security solutions from a variety of vendors. Of course having an anti-malware or security solution installed is much better than not having one at all, but in no way does the security solution guarantee that the user will be "completely protected" from today's Internet threats, cyber-crime, identity theft nor malicious attacks.

The next question we need to ask ourselves is “what is the solution to this problem?” As we know information security is incrementally effective as it incorporates different layers of protection techniques. The current minimum bar of protection is to have an integrated HIPS¹¹ which incorporates at least a signature-based antivirus, advanced heuristics, deep packet inspection firewall, network access control, vulnerability exploitation prevention, behavior blocking and behavior analysis. However as we have proved in this study, an integrated HIPS is still not enough to keep all users protected from infection.

The industry needs to develop and deploy new layers of protection that, in addition to the current state of technology, are able to tackle the problems of exponential malware increments, signature evading techniques and targeted attacks. In our case we are making progress in deploying Panda’s Collective Intelligence¹², a new concept of security radically different than the traditional approach and which is proving very effective in its initial stages of deployment.

7. Appendix – July Detections & Prevalence

Malware name	Malware Type	Prevalence in PCs
Application/MyWebSearch	Adware	14773
GenericMalware	Trojan	4536
Adware/VideoActiveXObject	Adware	3073
Trj/Downloader.MDW	Downloader	2283
Spyware/Virtumonde	Spyware	1977
Generic Trojan	Trojan	1799
Adware/SaveNow	Adware	865
Adware/VideoActiveXAccess	Adware	709
Adware/SweetBar	Adware	691
Trj/Lineage.BZE	Rootkit	675
Application/DriveCleaner	Hacking Tool	547
Adware/ActiveSearch	Adware	545
Adware/PurityScan	Adware	536
Adware/DriveCleaner	Adware	500
Trj/Clicker.WM	Rootkit	494
Application/MyWay	Adware	485
W32/MSNWorm.K.worm	Worm	472
Adware/SecurityError	Adware	372
Adware/Spylocked	Adware	354
Adware/OneStep	Adware	347
W32/IrcBot.AYK.worm	Bot	342
Adware/WebSearch	Adware	339
Adware/Zango	Adware	327
Spyware/New.net	Spyware	321
Adware/Comet	Adware	309
Application/FunWeb	Adware	308
Adware/VirusProtectPro	Adware	250
Adware/SpywareNo	Adware	241
Application/Messengerskinner	Adware	236
Trj/Mitglieder.OW	Rootkit	232
Adware/GoodSearchNow	Adware	214
Adware/IST	Adware	203
Adware/BaiduBar	Adware	197
Adware/VideoExtension	Adware	190
Application/Winantivirus2006	Rogue AntiSpyware	187
Adware/Borlander	Adware	184
Adware/NaviPromo	Rootkit	182
Application/MSNContentPlus	Adware	181
Trj/Banker.FWD	Banking Trojan	174

Malware name	Malware Type	Prevalence in PCs
Adware/PopupSearches	Adware	165
Application/ViewPoint	PUP	165
Adware/Lop	Adware	160
Adware/Starware	Adware	160
Adware/Gator	Adware	25
Trj/Multidropper.BPX	Trojan	8
Adware/WUpd	Adware	6
Application/ErrorSafe	Rogue Error Fixer	6
W32/Spamta.QO.worm	Bot	6
Bck/Hupigon.KMV	Backdoor	5
Application/ServUBased.A	Backdoor	4
Generic Adware	Adware	4
Trj/Keylog.LO	Keylogger	4
Trj/VB.OO	Trojan	4
W32/UsbStorm.A.worm	Worm	4
Adware/DeluxeComunications	Adware	3
Adware/Exact.BargainBuddy	Adware	3
Trj/Banker.HDQ	Banking Trojan	3
Trj/Nabload.ACN	Rootkit	3
Trj/Rizalof.ABS	Trojan	3
W32/MadCoffee.C.worm	Worm	3
W32/Irutas.G	Virus	3
Adware/123Mania	Adware	2
Adware/Alexa-Toolbar	Adware	2
Adware/CommanderToolbar	Adware	2
Adware/DelFinMedia	Adware	2
Adware/Maxifiles	Adware	2
Adware/WebBuying	Adware	2
Application/MediaPipe	Adware	2
Dialer.BCI	Dialer	2
W32/SdBot.KGP.worm	Bot	2
...

* Data shown is malware ID and type based on top prevalence on number of unique PCs on both the consumer and corporate study. We are not showing the complete list of detections as it contains quite a long tail with low level of prevalence.

8. References

- ¹ AOL survey finds rampant online threats, clueless users. AOL. October 2004.
<http://www.computerworld.com/securitytopics/security/story/0,10801,96918,00.html>
- Know Your Enemy: Tracking Botnets. German HoneyNet Project. March 2005.
<http://project.honeynet.org/papers/bots/>
- Study says over 1m Windows PCs compromised. Sydney Morning Herald. March 2005.
<http://www.smh.com.au/news/Breaking/Study-says-over-1m-Windows-PCs-compromised/2005/03/18/1111085984429.html>
- Symantec Internet Security Threat Report, Volume XI.
http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_internet_security_threat_report_xi_keyfindings_03_2007.en-us.pdf
- US tops spam relaying and malware leagues of shame. The Register. January 2007.
<http://www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en>
- Microsoft Security Intelligence Report. Microsoft Corporation. October 2006.
<http://www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en>
- ² Technology Paper: From Traditional AV to Collective Intelligence. Panda Research. August 2007.
http://research.pandasoftware.com/blogs/research/archive/2007/08/27/Technology-Paper_3A00_-From-AV-to-Collective-Intelligence.aspx
- ³ Market Share: Security Software Worldwide, 2006. Gartner.
<http://www.gartner.com>
- ⁴ Eighty percent of new malware defeats antivirus. ZDNet Australia. July 2006.
http://www.zdnet.com.au/news/security/soa/Eighty-percent-of-new-malwaredefeats_antivirus/0,130061744,39263949,00.htm
- ⁵ Gartner's 10 Key Predictions for 2007. eWeek. December 2006.
<http://www.eweek.com/article2/0,1895,2072416,00.asp>
- ⁶ The Zero-Day Dilemma. Security IT Hub. January 2007.
http://www.security.ithub.com/article/The+ZeroDay+Dilemma/199418_1.aspx
- ⁷ Welcome to 2007: the year of professional organized malware development. Michael-St. Neitzel at Hispasec. February 2007.
<http://blog.hispasec.com/virustotal/16>
- ⁸ Call the cops: We're not winning against cybercriminals. ComputerWorld. February 2007.
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010041>
- ⁹ The Disconnect Between the WildList and Reality. Panda Position Paper for Anti Virus Product Developer (AVPD) Confidential. January 2007.
- ¹⁰ Security Vendors Challenge Antivirus Tests. IDG News. June 2007.
<http://www.pcworld.com/article/id,133409-page,1/article.html>
- ¹¹ HIPS Update: Why Antivirus and Personal Firewall Technologies Aren't Enough. Gartner. January 2007.
http://www.gartner.com/teleconferences/attributes/attr_165281_115.pdf
- ¹² Technology Paper: From Traditional AV to Collective Intelligence. Panda Research. August 2007.
http://research.pandasoftware.com/blogs/research/archive/2007/08/27/Technology-Paper_3A00_-From-AV-to-Collective-Intelligence.aspx
- ¹³ The Long Tail: malware's business model. Panda Research. January 2007.
http://research.pandasoftware.com/blogs/research/archive/2007/01/08/The-Long-Tail_3A00_-malware_2700_s-business-model.aspx

PANDA SECURITY

Panda SPAIN

Ronda de Poniente, 17
28760. Tres Cantos. Madrid. SPAIN
Phone: +34 91 806 37 00

Panda USA

230 N. Maryland, Suite 303
P.O. Box10578. Glendale, CA 91209 - USA
Phone: +1 (818) 5436 901

www.pandasecurity.com

© Panda 2007. All rights reserved. 0907-WP-PSDRS-I-01