

EXECUTIVE REPORT

20 / 12 / 2006

Executive summary

Audit start date
07 / 09 / 2006 19:12

Audit end date
08 / 09 / 2006 09:34

Licenses contracted: 300
Computers audited: 161
items scanned: 703499
Computers not completed: 19

The following technologies have been used during the audit:

Signature-based detection, Genetic Kinship Clustering, Genetic Heuristic, Deep Code Inspection, Rootkit Heuristic

All results have been analyzed by PandaLabs with the following result:

Malicious code discovered on your computers

- Active malicious code with a high danger level has been detected on your computers.
- 13.4% of your computers have active malicious code.

Protection level of your IT resources

- 100% of your computers have inadequate protection.

Malicious code detected

Active malicious code

Danger level	Malicious code	Infected computers
Very High	0	0
High	3	3
Moderate	13	9
Low	4	11

Latent malicious code

Danger level	Malicious code	Infected computers
Very High	0	0
High	7	7
Moderate	52	35
Low	10	21

Security failures

Security protection

Protection	Computers	Malicious code	
		Active	Latent
Deficient	142(100%)	20	70
Medium	0(0%)	0	0
Optimum	0(0%)	0	0

Vulnerabilities

Total	Computers	Malicious code	
		Active	Latent
59	134(94.4%)	14	62

Active malicious code details

Highly dangerous malicious code

No highly dangerous active malicious code has been found

Rest of active malicious code

Infected computers	Code detected	Items detected
19	20	301

Classification by type

Type	Mal. Code.	Type	Mal. Code.
Virus	0	Adware	15
Worm	0	Security Risk	0
Trojan	1	Hacking Tool	0
Spyware	0	Dialer	0
PUP	3	Backdoor Trojan	1

Dangerous malicious code

Name	Type	Danger level	Computers
Bck/Afcore.AS	Backdoor	High	1
Adware/Maxifiles	Adware	High	1
Adware/PurityScan	Adware	Moderate	2
Adware/Qoologic	Adware	Moderate	1
Adware/Zenosearch	Adware	Moderate	1



Latent malicious code details

Highly dangerous malicious code

No highly dangerous latent malicious code has been found

Rest of latent malicious code

Infected computers	Code detected	Items detected
48	69	599

Classification by type

Type	Mal. Code.	Type	Mal. Code.
Virus	0	Adware	50
Worm	0	Security Risk	0
Trojan	0	Hacking Tool	2
Spyware	5	Dialer	3
PUP	9	Backdoor Trojan	0

Dangerous latent malicious code

Name	Type	Danger level	Computers
Spyware/Whazit	Spyware	High	2
Adware/Secure32	Adware	High	1
Adware/DollarRevenue	Adware	High	1
Spyware/ClientMan	Spyware	High	1
Spyware/New.net	Spyware	High	1

Cookies and jokes detected

Computers with cookies	Cookies detected	Items detected
2	24	30

No jokes have been detected on the computer.

Statistics

Malicious code most frequently detected on computers

Name	Type	Computers	Danger level
Application/FunWeb	PUP	15	Low
Adware/Gator	Adware	15	Moderate
Application/MyWebSearch	PUP	14	Low
Adware/Gator.PTime	Adware	8	Moderate
Exploit/iFrame	Hacking Tool	5	Moderate

Computers with most malicious code

Computer	Danger level			
	Very High	High	Moderate	Low
PC 5	0	3	13	2
PC 4	0	1	9	0
PC 3	0	0	6	6
PC 2	0	0	3	0
PC 1	0	0	1	3

Details of the protection

Security protection

Protection	Computers	Mal. code detected
Deficient	142	79
Medium	0	0
Optimum	0	0

Computers with deficient protection

Reason	Computers
Deficiencies in the antivirus	47
Deficiencies in the antispysware	142
Deficiencies in the firewall	140
Deficiencies in the HIPS	142

Details of the vulnerabilities

Vulnerabilities that could allow access to malicious code

	Computers	Percentage	Mal. code detected
Without vulnerabilities	8	5.6%	19
With vulnerabilities	134	94.4%	68

Recommendations

1. Now disinfect in the same way the computers that have running malicious code. (PC6, PC 2, PC 7, PC 8, PC 9, PC 10, PC 4, PC 11, PC 12, PC 13, PC 1, PC 14, PC 15, PC 16 PC 17, PC 18, PC 5, PC 19, PC 3).
2. Eliminate the latent malicious code (including cookies) in the following order of priority: Firstly, viruses, worms, trojans and spywares. Secondly, adwares, hacking tools, PUPs, dialers, jokes and cookies. Similarly, it is advisable to prioritize computers with more malicious code (PC 5, PC 4, PC 3, PC 2, PC 1, PC 20, PC 9, PC 21, PC 14, PC 11, PC 15, PC 22, PC 12, PC 6, PC 23, PC 17, PC 18, PC 24, PC 16, PC 25, PC 26, PC 27, PC 28, PC 29, PC 30, PC 31, PC 32, PC 33, PC 10, PC 34, PC 35, PC 8, PC 19, PC 36, PC 7, PC 37, PC 38, PC 39, PC 40, PC 41, PC 42, PC 43, PC 44, PC 45, PC 46, PC 47, PC 48, PC 49, PC 50, PC 13).
3. To carry out detailed disinfection, one of the following two options is recommended: Use the disinfection function integrated in the Malware Radar solution or carry out an on-demand scan with the corporate security software and when the malicious code detected is eliminated (To ensure disinfection it should at least include elimination of viruses, worms, trojans, spywares, adwares, jokes, cookies, PUPs, hacking tools and dialers). If the corporate security software cannot eliminate the malicious code discovered it is advisable to distribute other security software that can eliminated it and then the perform an on-demand scan.
4. A large amount of malicious code has been detected in Internet temporary files. This could indicate some kind of deficiency in the perimeter protection of the organization or in the protection in each of the computers. (If any of them functions correctly, this malicious code could have been eliminated). It is advisable to check that the perimeter protection is properly installed and updated and if not, make the necessary modifications.
5. It is advisable to install antivirus protection, antispysware, firewall and HIPS in all computers which have been identified as having insufficient protection (Computers with medium or deficient protection).It is advisable to carefully check those computers with active malicious code (PC 6, PC 2, PC 7, PC 8, PC 51, PC 10, PC 4, PC 11, PC 12, PC 13, PC 1, PC 14, PC 15, PC 16, PC 17, PC 18, PC 5,PC 19, PC 3). Similarly, it is advisable to prioritize adequate installation of antivirus and antispysware in those computers with deficient protection and then install a firewall and HIPS.
6. It is advisable to fix vulnerabilities identified by installing the corresponding patches.



Annex I. Listed

Computers in which very highly dangerous malicious code has been detected

No very highly dangerous malicious code has been detected

Computers in which active malicious code has been detected

PC 6	PC 2	PC 7
PC 8	PC 9	PC 10
PC 4	PC 11	PC 12
PC 13	PC 1	PC14
PC 15	PC 16	PC 17
PC 18	PC 5	PC 19
PC 3		

Computers in which latent malicious code has been detected

PC 42	PC 47	PC 48
PC 44	PC 5	PC 43
PC 22	PC 29	PC 12
PC 4	PC 6	PC 21
PC 26	PC 23	PC 2
PC 38	PC 7	PC 41
PC 15	PC 8	PC 46
PC 20	PC 34	PC 40
PC 3	PC 24	PC 51
PC 30	PC 31	PC 25
PC 27	PC 1	PC 36
PC 14	PC 37	PC 35
PC 28	PC 16	PC 17
PC 18	PC 32	PC 33
PC 10	PC 39	PC 50
PC 45	PC 11	PC 49

Computers in which malicious code has been detected

PC 1	PC 6	PC 9
PC 21	PC 24	PC 35
PC 42	PC 36	PC 23
PC 43	PC 2	PC 38
PC 25	PC 14	PC 7
PC 37	PC 22	PC 7
PC 39	PC 40	PC 35
PC 27	PC 41	PC 28
PC 29	PC 47	PC 12
PC 48	PC 15	PC 16
PC 3	PC 8	PC 34
PC 17	PC 44	PC 50
PC 10	PC 18	PC 30
PC 45	PC 46	PC 31
PC 5	PC 4	PC 33
PC 20	PC 49	PC 32
PC 9	PC 13	

Annex II. Glossary

1. Computer protection status: The protection level of a computer could be:
 - Optimum protection: The computer has a PIPS (Personal intrusion prevention system) enabled and up-to-date.
 - Medium protection: The computer has no Firewall or HIPS (Host Intrusion Prevention System), or at least they are not enabled or up-to-date, but it does have antivirus and antispyware and both are enabled and up-to-date.
 - Deficient protection: There is some problem with the antivirus or the antispyware. Either because they are not installed or because they are not enabled or up-to-date.
2. Active malicious code: Malware that is running and carrying out the actions for which it has been programmed.
3. Latent malicious code: Malware which is on the system but not running.
4. The organization's risk factor:

There are four possible risk levels for the organization, considering the malware detected (quantity and seriousness) the vulnerabilities found, and the protection status:

 - Severe risk: Jeopardize the continuity of the organization.
 - Damage its competitive position.
 - Seriously damage the image/reputation of the organization.
 - Seriously affect the availability of resources (preventing employees from working, affecting customer services, etc. These resources include the information itself and the other elements that use it).

This level does not take into account protection status or vulnerabilities given that the seriousness of the malware, its status and distribution (the more serious the malware the less widely it would have to be distributed to merit categorization at this level) are the causes of this status, regardless of other factors. This level of risk demands immediate action. Example: An organization in which at

least one computer has been identified with targeted viral malware or an organization in which some computers have high danger level active malware.

- High risk:

The risk of an organization will be high if the seriousness of the malware, its status, distribution and location as well as the status of the protection and vulnerabilities could for example:

- Generate temporary or limited damage to the availability of resources (for example, temporary saturation of networks).
- Considerably reduce the organization's productivity.

This level requires rapid action, although not necessarily immediate. Example: An organization with a considerable amount of computers in which protection is deficient and with active or latent malware classified as serious or very serious.

- Moderate risk:

The risk of an organization is moderate if the seriousness of the malware discovered, its status, distribution and location as well as the protection status and vulnerabilities could:

- Cause minor or moderate inconvenience for the organization
- Slightly reduce the level of productivity

This level requires short term action, although not necessarily rapid or immediate. Example: An organization with a considerable amount of computers with active adware or latent viral malware to a lesser degree, and with deficient or medium protection status in some computers.

- Normal risk:

The risk of an organization is normal if the seriousness of the malware discovered, its status, distribution and location as well as the protection level and vulnerabilities, even if they are not optimum are considered acceptable and the damage that could be caused to the organization is practically insignificant.



It could be advisable for the organization to take some measures but there is no need for urgent or immediate action. Example: An organization whose computers have optimum protection are free from malware or have inactive cookies, jokes or adware.

5. Vulnerability: A vulnerability is a flaw in the programming of an application that can be exploited to carry out an intrusion on a computer with the program installed. It could be an entry channel for viruses or other threats. For this reason, it is highly advisable to apply the most recent security patches released by the application vendor.
6. Danger level: We distinguish between four malware danger levels:
- Low danger level: Non-destructive malware which does not have the capacity to spread or install itself nor hide on the system. For example: jokes, hoaxes, cookies, etc.
 - Moderate danger level: General threats, non-destructive but capable of causing limited damage to the organization (viruses that slow down systems, programs that spy on Internet movements, etc.)
 - High danger level: General threats that could inflict serious damage on an organization (viruses that can infect documents, Trojans opening communication ports for attacks). They inflict serious damage, either because of their severity or the number.
 - Very high danger level: Specific threats, either destructive or aimed at stealing information, able to use advanced stealth, infection or propagation techniques (rootkits, targeted malware,...). Malware that can inflict critical damage, either because of their severity or the number.
7. Computers audited: Computers in the organization to which the scan client has been deployed in order to carry out the audit process on them.
8. Computers not completed: Computers in which the audit has begun but has not been completed. (These could be because the audit has been closed before all computers have been completed).
9. Items: Items are understood as both files (stored or in memory), and mail (including attachments). In the case of compressed files both the compressed file and its

contents are counted. In the case of emails with attachments, both the email and its attachments are counted.