

## The new malware dynamic: financially motivated cyber-crime.

Until recently, the main motivating factor for the creators of malware was their **quest for notoriety**. As a consequence, rapid and **widespread epidemics** were widely reported by the media the world over.

However, **the underlying driving force for hackers is now changing: they are now spurred on by financial return**. They are becoming professionals, their activity is now linked to that of organized criminals that earn income in a wide variety of ways.

**The nature of malware has therefore shifted:** it is now designed specifically to go unnoticed (e.g. using **rootkits**), it is much more complex and varied, and in many cases, is tailored to achieve a specific objective. In short, **it has become more difficult to detect and combat**.

What's more, the amount of **malware in circulation has increased exponentially**, and anti-malware laboratories cannot cope. In 2006, PandaLabs identified more malware samples than in the last fifteen years combined.

Faced with this situation, traditional IT security solutions are no longer enough. **A new security model is needed.**

## The solution: Malware Radar

According to **Gartner**, the best solution is to **install** a PIPS (Personal Intrusion Prevention System) on every network computer, integrating antivirus protection, anti-spyware protection, a personal firewall and HIPS (preventive technologies that detect malware using behavioral analysis).

Panda goes one step further, complementing PIPS solutions with **Malware Radar**, an **automated audit service** that identifies the malware on your network that is going undetected by your current security solution.

To maximize the detection capacity, Malware Radar is built on a **"collective intelligence"** approach developed by Panda Research and housed in a network of datacenters (initially made up of around 100 servers).

Malware Radar uses innovative technologies to determine the **quantity of malware on computers and where it is hidden**. It also detects critical **vulnerabilities** typically used by exploits and **checks the status and update level of the protection**.

Malware Radar generates **thorough, extensive reports** with results and recommendations, offering you the **option to clean the malware detected**. It also lets you **prioritize and orient your security strategy** based on these results.

*Malicious code detected:*

Type	Detections		PCs affected
	Active	Latent	
Viruses, worms and trojans	1	0	1
Spyware	0	6	6
Adware	15	50	33
Others	4	14	29
<b>Total</b>	<b>20</b>	<b>70</b>	<b>50</b>

*Security problems:*

	Computers	Detections	
		Active	Latent
Deficient	(100%) 1	10	15
Medium	(0%) 0	0	0
Optimum	(0%) 0	0	0

*Critical vulnerabilities:*

Total	Computers	Detections	
		Active	Latent
<b>52</b>	<b>(95%)134</b>	<b>14</b>	<b>62</b>

### Main Benefits

- **Identify and clean even the malware that your current security solution doesn't detect.** Malware Radar seeks out the threats that go undetected by the protection across your network.
- **Know exactly what malware is present, how much there is and where it is located** as well as any malware-related vulnerabilities on your network.
- **Keep one step ahead of new security threats** by redirecting security strategies based on the report results. Malware Radar also lets you monitor the effectiveness of security software installed in your network.
- **Less time and work on your part to control network threats.** Malware Radar offers a quick and straightforward analysis of malware on the network with centralized administration, no need for installation.

### Key Features

- **It detects more malware than traditional security solutions**
- **It does not require installation** and can operate side-by-side with your current protection.
- **Full, detailed reports:** an **executive audit report** with the main results, statistics and recommendations and the **technical report** with full details on each computer scanned.
- **Quick scan** of all your workstations and file servers.
- **Quick and easy evaluation and report** your network status - without wasting your time or resources.
- **Detection of critical vulnerabilities** typically exploited by malware.
- **Advanced detection of all types of malware** -known and unknown- which is undetected by your network protection.
- **No resident.** When the scan is complete, it removes itself without leaving any components installed.
- **Detection of critical malware** and even targeted malware, which is extremely dangerous to your company
- **Automatic cleaning of the malware detected** (optional), with a detailed results report.
- **Analysis of the security software.** Report on the status and update level of the antivirus protection, anti-spyware protection, the personal firewall and HIPS.

## Detects more than traditional solutions

**Malware Radar even detects the malware that goes undetected by traditional security solutions** because it uses the most advanced technologies and the most sensitive heuristics.

It is based on a "collective intelligence" approach developed by Panda Research. This system analyzes the data received by PandaLabs from the community of users and automatically returns verdicts (malware or goodware) on the new files seen by the community. This allows Panda to significantly increase its detection capacity compared to traditional anti-malware approaches.

## No installation

**Malware Radar does not need to be installed and does not require maintenance of permanent client/server architecture.** It can operate alongside your current protection, so you do not need to uninstall your security software in order to use **Malware Radar**.

## Thorough, extensive reports

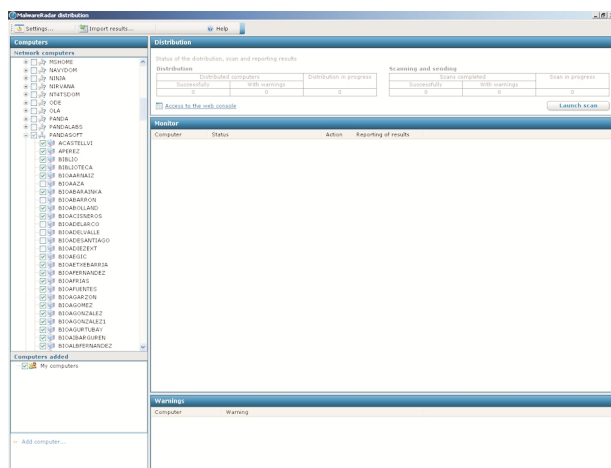
As a result of this scan, **Malware Radar** provides two full reports with information about detections (**type and quantity of malware** detected and its **exact location**), the vulnerabilities detected and the status of the protection:

- An **Executive report** with the main results and recommendations.
- A **Technical report** with full details on each computer scanned

## Quick scan of your network

**Malware Radar** quickly scans all workstations and file servers, regardless of whether they are permanently networked, laptops or even completely unattached to the network.

To scan all computers, you can use your usual distribution method (login scripts, tools like Tivoli or SMS, email, etc.) or, if you prefer, **Malware Radar** includes a **distribution tool** through which you can select the network computers to scan and then it will automatically launch the scan.



## Quick and easy

**The scan and reporting process is automatic, quick and centralized.**

The administrator can easily access the deployment tool through the Internet. When the scan is launched the process is fully automatic and you will have a centralized, online view of the scan in real-time. When it is complete, you will be able to access two detailed reports.

## Detection of critical vulnerabilities

**Malware Radar** detects **critical vulnerabilities** that represent security holes that malware (**exploits**) could use to enter your network. You will be informed about each vulnerability detected and the threats that exploit them.

## Advanced malware detection

**Malware Radar** is able to detect **all types of malware –known or unknown–** that could be active (running) or latent (present, but not running) on your network.

This malware could have gone unnoticed by your security software either because it is not included in the signature file or is designed to remain hidden (for example, using rootkits).

## No resident

**Malware Radar** does not remain in the scanned computers, i.e. **it does not go resident**. When the scan is complete, it removes itself without leaving any components installed.

## Detection of critical malware

**Malware Radar** is capable of detecting **highly critical** or extremely dangerous **malware** which traditional antivirus solutions cannot detect, such as **targeted malware**, a silent and imperceptible type of malware that could steal information and inflict financial damage on your company.

## Automatic cleaning of malware detected

When the scan is complete, the administrator can **launch automatic cleanup** of the malware found. This is done by distributing the cleaning process, using the usual deployment methods or the **Malware Radar** distribution tool.

When the cleanup process is complete, you will receive a **Technical report with the results of the process for each computer**.

## Analysis of the protection status

**Malware Radar** checks the status of the protection (existence and update status of the antivirus, anti-spyware, personal firewall and HIPS - Host Based Intrusion Prevention System) and provides reports including recommendations for your specific situation.

## For workstations:

Windows 95, 98, Me, NT 4 Server/WS SP6, 2000, XP, 2003, Vista 32 bits  
RAM: 64 MB  
Hard disk free space: 30 MB.  
Internet Explorer 5.5.

## For the distribution tool:

Windows 2000 WS/Server, XP, 2003, Vista 32bits  
RAM: 64 MB  
Hard disk free space: 30 MB.  
Internet Explorer 5.5.

## Technical requirements

