

## 72% of organizations are infected with active malware that remains hidden to traditional security solutions and can cause financial and productivity losses

Analysis by **Panda Research** shows that **72%** of medium and large organizations are **infected** with active malware that remains **hidden** to installed protection and can cause economic and productivity **losses**.

Hackers are professionals spurred on by financial return whose activity is linked to that of **organized criminals** that earn income in a wide variety of ways. Obviously, when **making money illegally**, it is better to be **silent and discreet**.

Malware 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 (**targeted attacks**).

**"By the end of 2007, 75% of enterprises will be infected with undetected, financially motivated, targeted malware that evaded their traditional perimeter and host defenses"**

Gartner Highlights Key Predictions for Organizations in 2007 and Beyond.

### The solution: Malware Radar

**Malware Radar** is an automated audit which **locates infection points** that traditional security solutions **fail to detect**.

Based on our **Collective Intelligence** approach, it **complements** and helps **maximize** your protection against **hidden threats** without additional installation or infrastructure requirements. Malware Radar is the only solution that **transparently** locates and removes hidden threats in your network.

**Collective Intelligence** is Panda's innovative security platform that provides Malware Radar with a **highly superior detection rate** compared to traditional security solutions.

The **Collective Intelligence** platform offers **proactive and real time protection** to users. It leverages the collective knowledge and automates the analysis, correlation, classification and signature generation processes increasing **exponentially** the malware that it can detect every day. This way, the users benefit in real time from global detections. This allows the detection of infections at initial stages or **targeted attacks** that only affect a few users.

**Malware Radar** provides **automated audits** of your network and **detailed reports** with results and recommendations offering the option to automate the **disinfection** routines of all malware detected.

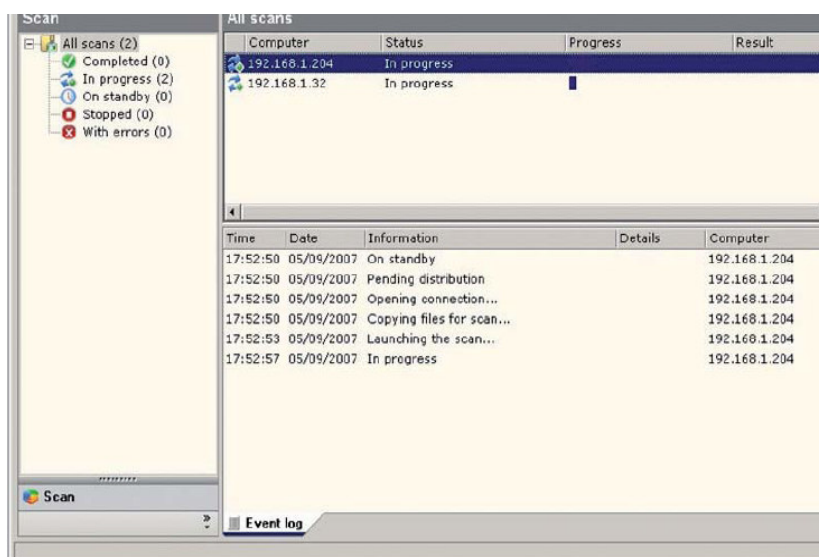


Fig. 1 Malware Radar Distribution Tool

## Panda Malware Radar

Discovering hidden threats

**"Companies looking for a second opinion on the security state of their workstations can use Panda's Malware Radar assessment tool. Malware Radar performs a network-based scan for client infections."**

Gartner Magic Quadrant for Endpoint Protection Platforms. (December 2007)

### Main benefits

- **Prevents identity theft** by detecting hidden malware and targeted attacks that can remove sensitive information from your organization.
- **Reduces productivity loss** by discovering undetected infections that can harm your information resources availability, increase your network resource consumption and distract employees
- **Ensures business continuity** by minimizing disaster recovery time and cost involved when dealing with malware infections.
- **Improves your operational risk management.** Executive and detailed technical information about the security status of your network.
- **Helps enforce compliance** with SOX, PCI, HIPAA, and other regulations by providing regular security audits of your network.
- **Protects existing investment** in security products as it is compatible with installed protections

### Key features

- **Maximized malware detection rate** compared to traditional security software.
- **Compatible with your installed protection** and designed to complement it.
- **Requires no installation and no dedicated infrastructure.**
- **Provides detailed audit reports:** executive and technical reports for each network device.
- **Transparent process** for your employees optimizing available system resources.
- **Optional automated disinfection** of all malware detected.
- **Always updated** and using latest version and technologies (hosted service).
- **Standardized distribution capability** (Tivoli, SMS, LanDesk, etc).
- **System vulnerabilities scanner features** identifying uninstalled patches malware can exploit.
- **Validates existing security software status** by analyzing if it is installed, enabled and up to date.

## Maximized detection rate compared to traditional security software

Panda's unique **Collective Intelligence Technologies** and the **most advanced heuristics** enable Malware Radar to detect infections that traditional security software fails to find.

## Compatible with traditional security solutions

Malware Radar is **compatible** with traditional security solutions as it is designed to complement them. It can operate alongside your current protection, so you do not need to uninstall your security software in order to run Malware Radar's audits.

## Requires no installation and no dedicated infrastructure

**Malware Radar** does not require installation in those workstations and file servers you want to analyze. No dedicated hardware is needed to manage the audits.

## Transparent process for your employees

**Malware Radar** can be configured to use CPU resources in dead CPU cycles, **optimizing** available system resources when conducting the audits.

## Detailed audit reports

As a result of the scan, Malware Radar provides two full reports with information about malware **detections** (type and quantity of malware detected and its exact location), the **system vulnerabilities** detected and the **status of the protection**: An **executive audit report** with main results, statistics and recommendations, and a **technical report** for each network device in detail.

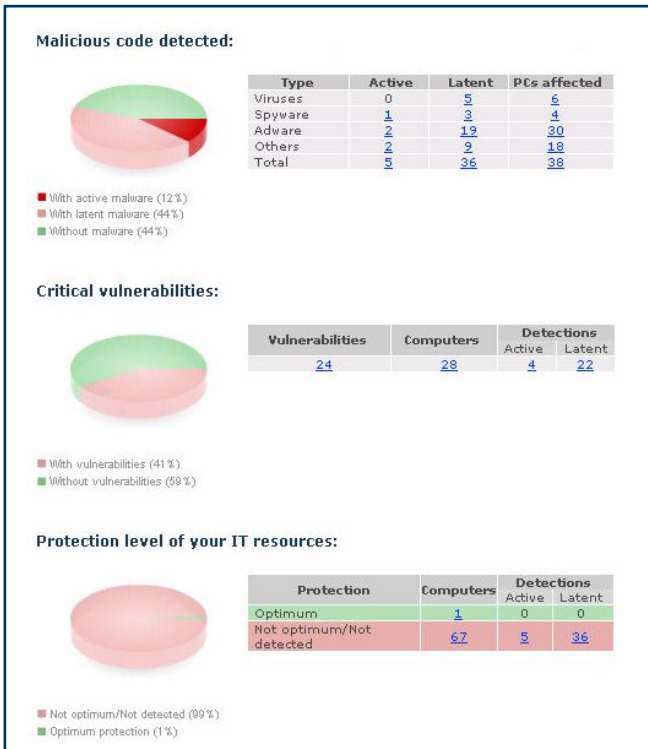


Fig. 2 Malware Radar results overview

## Optional automated disinfection of all malware detected

When the scan is complete, the administrator can configure and launch an **automated disinfection** of all malware found.

When the disinfection process is complete, Malware Radar provides a Technical Disinfection report **with the results for each device**.

## Always updated

Malware Radar is a **hosted service** that is always **up-to-date** and uses the **latest version** and technologies without having to worry about updates or upgrades.

## Standardized distribution capabilities

The scan deployment is compatible with **standard distribution tools** such as Tivoli, SMS, LanDesk, Login Scripts, etc.

Or, if you prefer, **Malware Radar** includes a **distribution tool** (see fig.1) through which you can select the network computers to scan and then it will automatically launch the scan.

## System vulnerabilities scanner features

**Malware Radar** looks for **system vulnerabilities** that malware can **exploit** providing the information about uninstalled **critical patches** and how to resolve them

## Validates existing security software status

**Malware Radar** checks the status of the security software (antivirus, anti-spyware, personal firewall and HIPS - Host Based Intrusion Prevention System) by analyzing if they are **installed, enabled and up-to-date**.

## Technical requirements

### For workstations:

- Windows 95, 98, Me, NT 4 Server/WS SP6, 2000, XP, 2003, Vista 32 and 64-bit
- RAM: 512 MB
- Hard disk free space: 100 MB.
- Internet Explorer 5.5.

### For the distribution tool:

- Windows 2000 WS/Server, XP, 2003, Vista 32 and 64-bit
- RAM: 512 MB
- Hard disk free space: 100 MB.
- Internet Explorer 5.5.

## Panda Security certifications

