

Controllo automatico del malware



Le nuove dinamiche del malware: cybercrimine con motivazioni finanziarie

Fino a poco tempo fa, la motivazione principale dei creatori di malware era la **ricerca della notorietà** e questo spiega le improvvise e devastanti "epidemie" che si diffondevano nei PC di tutto il mondo.

Oggi però **le motivazioni sono cambiate e gli hacker mirano sempre più al ritorno finanziario**. Sono così nati dei veri e propri professionisti della cyber truffa, con attività spesso legate a quelle di bande criminali che agiscono in un'ampia varietà di modi.

La natura del malware è quindi diversa: oggi è concepito per passare del tutto inosservato (per esempio utilizzando i *rootkits*), è molto più complesso e variegato e in molti casi viene progettato per uno scopo ben preciso. In breve, **è diventato molto più difficile da scoprire e combattere**.

Per giunta, la quantità di malware in circolazione **è cresciuta in modo esponenziale** e i laboratori antimalware non riescono più a tenere il passo. Nel solo 2006, PandaLabs ha identificato più campioni di malware di quanti ne abbia identificati nei 15 anni precedenti.

Per affrontare questa situazione non bastano più le tradizionali soluzioni di sicurezza IT. **C'è bisogno di un nuovo modello di sicurezza.**

La soluzione: Malware Radar

Secondo **Gartner**, la migliore soluzione è **installare** un PIPS (Personal Intrusion Prevention System) su ogni computer di una rete, integrando la protezione anti-virus e antispyware, personal firewall e tecnologie HIPS (tecniche preventive d'identificazione del malware che utilizzano l'analisi comportamentale).

Panda si spinge ancora oltre, aggiungendo alle soluzioni PIPS **Malware Radar**, un **servizio di scansione automatica** in grado d'identificare i malware presenti nella vostra rete aziendale che le attuali soluzioni di sicurezza non riescono a scoprire.

Per massimizzare la capacità di rilevamento, Malware Radar si basa sull'approccio della **Collective Intelligence** sviluppato da Panda Research e ospitato in un DataCenter (composto da più di 200 server).

Malware Radar utilizza tecnologie innovative per determinare **il numero di codici maligni nei computer e dove si nascondono**. Rileva inoltre le vulnerabilità critiche sfruttate dal malware e **controlla lo stato e l'aggiornamento della protezione**.

Malware Radar elabora **rapporti approfonditi** con risultati e raccomandazioni e offre all'utente la **possibilità di eliminare i malware rilevati**. Permette inoltre di **creare delle priorità e di orientare la vostra strategia di sicurezza** in base ai risultati della scansione.

Malicious code detected:

Type	Detections		PCs affected
	Active	Latent	
Viruses, worms and trojans	1	0	1
Spyware	0	6	6
Adware	12	20	33
Others	4	14	20
Total	20	20	50

Security problems:

Deficient	Computers		Detections	
	Active	Latent	Active	Latent
Optimum	0	0	0	0
Deficient	100%	0	0	0
Optimum	0%	0	0	0

Critical vulnerabilities:

Total	Computers	Detections	
		Active	Latent
52	(95%)134	18	32

Vantaggi Chiave

- **Identifica ed elimina il malware non rilevato dalle soluzioni di sicurezza attualmente implementate.** Malware Radar non dà scampo alle minacce che sfruttano le vulnerabilità dei sistemi di sicurezza per infiltrarsi nella vostra rete.
- **Sa esattamente che malware è presente, quanti sono i codici maligni e dove si nascondono**, e identifica le vulnerabilità legate ai malware del vostro network.
- **Vi mantiene un passo avanti rispetto alle nuove minacce** grazie alla rielaborazione delle strategie di sicurezza in base ai risultati dei rapporti. Malware Radar vi permette inoltre di monitorare l'efficacia dei software di sicurezza installati nel vostro network.
- **Riduce il lavoro e il tempo necessario per controllare le minacce nel network.** Malware Radar analizza in modo rapido e diretto il malware presente nel vostro network. Offre un'amministrazione centralizzata e non dev'essere installato.

Caratteristiche principali

- **Rileva più malware delle tradizionali soluzioni di sicurezza**
- **Non richiede installazione** e lavora fianco a fianco con la protezione attualmente installata.
- **Elabora rapporti dettagliati e completi**: un **rapporto della scansione per gli executive** con i risultati, le statistiche e le raccomandazioni più importanti, e un **rapporto tecnico** con tutti i dettagli dei computer controllati.
- **Analizza rapidamente** ogni workstation e server della rete aziendale.
- **Valutazione facile e immediata con rapporto sullo stato della rete** per risparmiare tempo e risorse.
- **Scopre le vulnerabilità critiche** sfruttate in genere dai malware.
- **Rilevamento avanzato di tutti i tipi di malware**, noti e sconosciuti, in grado di superare le barriere dei sistemi di difesa.
- **Programma non residente**: una volta completata la scansione, Malware Radar si disinstalla senza lasciare alcun componente nel sistema.
- **Rileva il malware critico** e persino mirato che rappresenta un grave rischio per la vostra azienda.
- **Elimina automaticamente il malware rilevato** (opzionale), con un dettagliato report sui risultati.
- **Analizza i software di sicurezza**, con un rapporto sullo stato e il livello di aggiornamento delle protezioni anti-virus e anti-malware, firewall e HIPS.

PANDA
SECURITY

One step ahead.

Rileva molto più delle soluzioni tradizionali

Malware Radar scopre anche i malware che superano l'analisi delle tradizionali soluzioni di sicurezza perché utilizza le tecnologie più avanzate e analisi euristiche estremamente sensibili.

Si basa sull'approccio dell'**Intelligenza Collettiva** sviluppato da Panda Research, un sistema che analizza i file trasmessi ai PandaLabs dalla comunità di utenti e stabilisce se si tratta di *malware* o *goodware*, per poi diffondere automaticamente i risultati. Questo permette a Panda di aumentare in modo significativo le proprie capacità di rilevamento rispetto ai tradizionali approcci anti-malware.

Niente installazione

Malware radar non dev'essere installato e non richiede manutenzione dell'architettura client/server. Lavora fianco a fianco con la protezione attualmente installata e quindi non è necessario disinstallare il vostro software di sicurezza per poterlo usare.

Rapporti dettagliati e completi

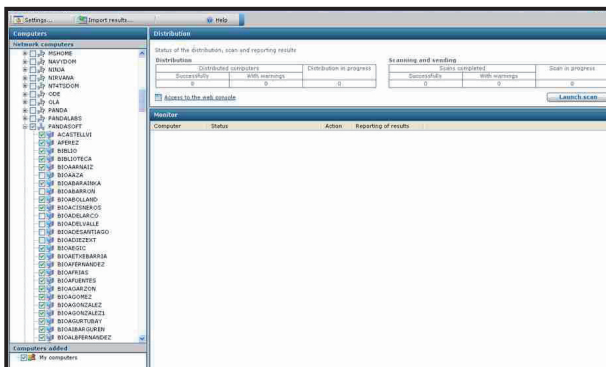
Una volta completata la scansione, **Malware Radar** genera due rapporti con informazioni sull'analisi (**tipo e quantità di malware rilevato** e sua **precisa posizione**), sulle vulnerabilità del sistema e sullo stato della protezione:

- Un **report per gli executive** con i risultati e le raccomandazioni più importanti
- Un **report tecnico** con tutti i dettagli dei computer analizzati

Scansione rapida della vostra rete aziendale

Malware Radar esamina rapidamente server e workstation, anche quelli che non sono connessi in permanenza al network e persino i laptop che ne sono del tutto scollegati.

Per la scansione di tutti i computer si può utilizzare il sistema di distribuzione già presente (script di login, strumenti come Tivoli o SMS, email, eccetera). In alternativa, **Malware Radar** offre uno strumento di distribuzione che permette di selezionare i computer della rete da esaminare, dopodiché l'analisi viene lanciata automaticamente.



Semplice e veloce

La scansione e l'elaborazione dei rapporti avviene in modo automatico, rapido e centralizzato.

L'amministratore può facilmente accedere allo strumento di attivazione tramite Internet. Una volta lanciata la scansione, il processo è completamente automatico e offre una panoramica centralizzata online e in tempo reale delle analisi in corso. Terminata la scansione, il sistema genera due rapporti dettagliati.

Rilevamento di vulnerabilità critiche

Malware Radar scopre le vulnerabilità critiche che i malware sfruttano per insinuarsi nella vostra rete e vi informa sulla presenza di questi "buchi nella sicurezza" e sui malware capaci di approfittarne.

Rilevamento avanzato del malware

Malware Radar è in grado di rilevare **tutti i tipi di malware noti e sconosciuti**, a prescindere che siano attivi o latenti, cioè presenti nel network ma ancora inerti.

Molti malware riescono a superare la barriera creata dai sistemi di sicurezza perché non sono inclusi nei file delle firme virali, oppure perché sono progettati per nascondersi (per esempio utilizzando i *rootkits*).

Malware Radar non rimane nel computer analizzato, cioè **non diventa un programma residente**. Una volta completata la scansione, viene automaticamente rimosso senza lasciare alcun componente installato nel sistema.

Rilevamento di malware critico

Malware Radar è in grado di rilevare codici maligni **estremamente critici e pericolosi** che sfuggono alle tradizionali soluzioni antivirus. I **malware mirati** rappresentano un buon esempio, poiché si tratta di codici maligni silenziosi e assolutamente invisibili creati per sottrarre informazioni alla vostra azienda e/o infliggere una perdita finanziaria.

Cancellazione automatica del malware

Una volta completata la scansione, l'amministratore può lanciare la **pulizia automatica** del malware rilevato utilizzando sia il normale sistema di distribuzione aziendale che lo strumento distributivo offerto da **Malware Radar**.

Una volta completata la cancellazione, il sistema genera un rapporto tecnico con **i risultati del processo per ogni singolo computer**.

Analisi della vostra protezione

Malware Radar verifica lo stato della protezione (esistenza e livello di aggiornamento di antivirus, anti-spyware, firewall e HIPS) e genera rapporti con raccomandazioni specifiche per la vostra situazione.

Requisiti tecnici

Per le workstation:

Windows 95, 98, Me, NT 4 Server/WS SP6, 2000, XP, 2003, Vista 32 bits
RAM: 64 MB
Spazio libero su Hard Disk: 30 MB
Internet Explorer 5.5

Per lo strumento di distribuzione:

Windows 2000 WS/ Server, XP, 2003, Vista 32 bits
RAM: 64 MB
Spazio libero su Hard Disk: 30 MB
Internet Explorer 5.5

Certificazioni Panda Software

