

PROTECTING IDENTITY, DATA AND COLLABORATION ON THE INTERNET

While malicious software (malware) and targeted attacks gain attention through the press, worms are still the most prevalent and fast spreading form of malware today. Attention is often focused on the most vulnerable systems—the roaming PCs that are occasionally connected to corporate networks. These PCs are connecting in new, more social ways and are doing so from multiple locations over different networks. This flexibility can result in attacks from this fast propagating malware that is not detected by standard antivirus software when it occurs before definitions, signatures or patches are available to prevent the attack.

Primary Response MemoryShield Client provides buffer overflow protection for individual PCs, preventing worm attacks at the heart of the system. While anti-virus software can protect against some known attacks, these worms often attack new vulnerabilities in software, particularly the Windows operating system. Software patches are typically made available for newly discovered vulnerabilities, but the time to deployment leaves a critical gap where systems are unprotected. Primary Response MemoryShield Client stops that gap by protecting core services from fast-moving worms. Once installed, Primary Response MemoryShield Client requires no configuration, no updates and no signatures. Users gain the benefit of:

- Protecting personal identity and data
- Assuring overall system health
- Detecting threats when they occur
- Eliminating the need for definition updates and system scans

Primary Response MemoryShield Client is priced right for a quick buy decision. Installation is straightforward and takes a minimal amount of time. The software does not require configuration; it provides “always on” protection right out-of-the-box. No complex tutorials to understand how to implement and use. With Primary Response MemoryShield Client, Windows core services are protected on an ongoing basis.

For organizational deployment, Primary Response MemoryShield Client can be managed through industry standard systems management applications, since it uses standard interfaces to log events to the Event Viewer, and runs as a service. The impact to system resources is virtually undetectable, as the software is streamlined for its particular type of protection. No IT personnel intervention is required.

Worms are dangerous because:

- No user action is required for propagation. Once they are on a network, they can spread undetected.
- They take advantage of vulnerabilities in Microsoft Windows, the most popular operating system. They do not rely on specific e-mail tools, for instance.
- They can masquerade as core Windows services, and thus gain a high level of system authority.

What is a code injection threat?

A code injection threat is an attack that takes advantage of buffer overflow (or similar) vulnerabilities to inject code into memory or the file system and execute its own commands. When a program writes to memory, its allocated space is a buffer. A buffer overflow sends more data to that space, overflowing the buffer and writing to another area of memory. This allows malicious code to be injected and executed from read/write memory. Worms target vulnerabilities in Windows core services because these programs are broadly used and provide high levels of access, allowing the worm to do the most damage and to spread to the other machines.

Doesn't antivirus software protect my system from worms?

No. Because antivirus programs generally detect existing worms based on known signatures residing in file systems, antivirus protection from worms is inherently limited and reactionary. Until a worm is known and a signature created and updated, the antivirus program cannot provide protection against the malware. Even when the worm is known, if it executes itself from memory without installing in the file system, most antivirus programs are not capable of protecting a system against it.

How does Primary Response MemoryShield Client work?

Sana Security's Primary Response MemoryShield Client monitors the normal behavior of Windows core services at the system call level. As a result, any abnormal behavior, including a code injection from a known or unknown worm, is identified and prevented.

Antivirus software can provide some protection for systems. Updates are typically deployed over the Internet after they have been developed and tested. While this ensures ongoing protection, it also widens the gap of unprotected time from a new worm attack to detection through signatures. Primary Response MemoryShield Client provides instant protection during that gap, allowing a more methodical application of updates rather than an emergency procedure.

Primary Response MemoryShield Client provides real-time security by protecting your system at the core of the problem: in memory where programs are executing. With this low-cost, low-touch solution, your system can have instant protection from the most common threats today: worms. You gain an extra level of protection for your personal identity, personal data and the transactions you perform over the Internet every day.

ABOUT SANA SECURITY

Sana Security creates award-winning, autonomous threat protection software that is aware of environment change, adaptive to new threats and active in preventing attacks before they do harm across mission-critical computer systems.

For more information, contact Sana Security's sales team by calling [1-866-900-SANA](tel:1-866-900-SANA) or email sales@sanasecurity.com