

THREE THINGS ANTIVIRUS COMPANIES DON'T WANT YOU TO KNOW

:60 THE ALADDIN MINUTE

VOL. 3

BY SHIMON GRUPER, CISSP

executive vice president - internet technology

The world of malware has changed, and conventional AV vendors are struggling to keep pace.

Here's why:

- 1: Their response time is far too slow to stop new viruses.** It can take up to two full days for a new virus to be placed on a signature list, while viruses can circle the globe in just a couple of hours. The password-protected variant of the Bagle virus spread for weeks, unhindered by major antivirus vendors.
- 2: They don't inspect HTML web pages for known vulnerabilities.** Conventional Web page scanning slows browser performance, so it's offered as an option that most users don't activate—opening up networks to dangerous automatic downloads such as spyware.
- 3: They leave you wide open to a targeted attack.** The entire technology model of conventional antivirus companies is built around mass-propagated viruses—that's how they get samples for analysis. But virus writers now are writing code for money, not for fame. A malicious program targeting only your company will wreak havoc before your typical vendor even hears of it.

What is required is a technology model founded on rapid product innovation and an understanding of new attack vectors, built into comprehensive content security. For example:

- Beyond blocking identified threats, plug the security holes exploited by viruses so that similar new threats also are blocked.
- Emulate suspicious programs within a safe, isolated environment to see exactly what it is trying to accomplish, allowing for a much more rigorous screening than the typical "heuristics."
- Provide security and IT managers with the tools to enforce security rules at the gateway, including the ability to inspect and filter all Web traffic with no latency—something proxy-based solutions simply can't do.

What do you think? Is this just crazy talk or do you agree? Send your reactions and questions to AladdinMinute@Aladdin.com. For more information on the approach Aladdin takes to content security, call 800-562-2543 or visit Aladdin.com/eSafe.

for more information
visit www.aladdin.com/esafe


SECURING THE GLOBAL VILLAGE