

Where Conventional Defenses Break Down

When we look at modern malware and its dimensions of stealth, its targeting of unknown vulnerabilities, and the scoping of its victim to a narrow set of targets, you can begin to see why traditional solutions relying on signatures or heuristics are failing to catch today's new class of blended threats, the advanced stealth Malware and Botnets:

IPS/IDS (Intrusion Prevention/Detection Systems) – Tipping Point, Cisco MARS, McAfee, Blue Coat

- Complex interface/steep learning curve for the solution to know what to alert for
 - Requires regular signature updates and administrative attention and can't stay ahead of many threats
 - Most offer NO web exploit (malicious javascript) detection, however the few that do, rely on signatures.
 - Cannot detect most callback channels (including by content or C&C identity)
 - Can experience high rate of false positive/ false negative if you don't spend a lot of time tweaking detection policy manually
 - No protection against targeted malware (spear phishing) or zero-day attacks.
 - If you're targeting an unknown vulnerability and the exploit is morphing constantly (using obfuscation and polymorphic techniques), IPS and AV are easily bypassed.
-

URL and Reputation Based Filters: Websense, Iron Port, Blue Coat, etc.

- IP-based reputation lists are inherently inaccurate with a high rate of false positives.
 - Hard-coded IPs embedded within the malware defeats DNS based reputation lists.
 - URL filters are based on control lists (blacklists) which are all re-active and require consistently being updated. These are easily bypassed because of the dynamic nature of modern malware (hit and run, drive-by, etc.). They do not persist long in the web landscape.
 - Reputation based filters also require updates from global intelligence networks and do not have the ability to react fast enough to keep up with the dynamic nature of attacks as most are short lived 2-4 days or use fast flux DNS exists for 30 seconds or less.
 - URL and Rep can also be bypassed by having framed or deeply embedded content within the web site.
 - *For example, auction sites or social networking profiles, where users submit their own content. It's difficult to assign reputation on a subset of those sites*
 - Cannot detect most callback channels (including by content or C&C identity)
 - Can experience high rate of false positive/false negative if you don't invest time tweaking detection policies manually
 - No protection against targeted malware (spear phishing) or zero-day attacks.
-

Where Conventional Defenses Break Down

Gateway/Desktop Anti-Virus Solutions: Symantec, McAfee, Trend Micro,

- Requires regular signature updates and administrative attention and can't stay ahead of many threats
 - Cannot detect most callback channels (including by content or C&C identity)
 - No protection against targeted malware (spear phishing) or zero-day attacks.
 - If you're targeting an unknown vulnerability and the exploit is morphing constantly (using obfuscation and polymorphic techniques), IPS and AV are easily bypassed.
-

Unified threat management (UTM) Systems - Firewalls with all the bells & whistles (Firewall, IPS/IDS, Anti-Spam, AV, URL filtering, VPN, & SSL) – Fortinet, Juniper, Palo Alto Networks, & etc.

- No compelling/key differentiators.
 - Most are running traditional commodity security technologies listed above, but on a single platform.
 - See explanations of the above technologies to understand the reasons why UTMs will not detect today's dynamic, polymorphic, targeted, or zero-day threats.
-

Heuristics, Correlation, & Basic Emulation (x86)

- These techniques assume that the attack will be broadly visible and therefore will have heuristic alerts coming from a broad base of sensors (that can then be correlated). This is not the case in a targeted attack.
 - Basic x86 emulation will not uncover an attack that is unknown
 - It runs on a very stripped down model of emulation
 - It cannot model the vulnerability surface of the target. Consider that malware writers are targeting applications like Adobe PDF Reader. Emulation does not check for exploits using this vector.
-



Conclusion:

The FireEye difference is being able to find and track hidden sources of malware, and to eliminate the ability of malware to get into the network environment, versus what is happening with traditional signature-based systems where malware can easily side-step these detection systems.

The new reality of dynamic “adaptive persistent threats”, polymorphic and rapid-changing malicious code, targeted attacks, and zero-day vulnerability exploits, requires a new approach to malware detection and prevention. FireEye's methods are proven effective in exposing and blocking these hidden attack vectors.

For more information, or to start an evaluation of FireEye solutions, contact NLE:

sales@nle.com | **Phone:** 801.377.0074 | **Fax:** 801.377.0078 | **Web:** www.nle.com