Anti-exploit tools:
The next wave of enterprise security

Intro

From malware and ransomware to increasingly common state-sponsored attacks, organizations across industries are struggling to stay ahead of the next onslaught of security threats. These types of malicious activities can be especially threatening to highly regulated industries—where sensitive information is plentiful—such as finance, government, defense, healthcare, and manufacturing. Such was the case in May 2014, when the New York Times reported that a number of US military contractors, members of Congress, diplomats, lobbyists and Washington-based journalists found themselves the victims of an elaborate, three-year cyber espionage campaign led by hackers in Iran.[1]

Large organizations of any type are especially vulnerable to the reputational damage that results from often highly publicized failures, such as the 2013 Target breach—which the company itself says could have affected up to 70 million consumers.[2]

In a world where millions of businesses are infected every day with trojans designed to siphon money from bank accounts and wire it to money mules in distant geographies—whether or not they have the latest anti-malware security software installed—no organization is immune to compromise. The culprit in many cases? Software and browser vulnerabilities. The good news is that new technologies are emerging that can help organizations better protect themselves from security exploits.

This white paper examines the current threat landscape, the capabilities—and shortcomings—of traditional approaches to detection and prevention, and the emergence of anti-exploit technology, which is proving to be an effective complement to the traditional security suite in blocking known and unknown zero-day exploit attacks.

---

1 "Cyberespionage Attacks Tied to Hackers in Iran," nytimes.com, May 2014. http://bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/

2 "Payment Card Issue FAQ," target.com. https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888

Malwarebytes

Contents

The current threat landscape

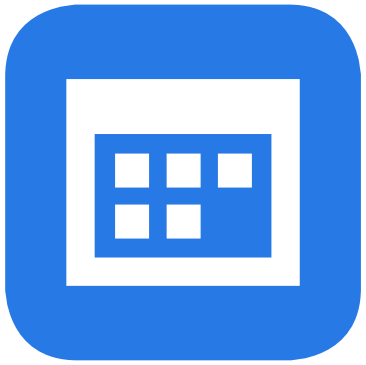
While the variety of attacks launched is almost as endless as those doing the attacking, here we examine three of the most common and most lethal tactics being used today.

Cyber espionage

Among the most feared types of attacks, cyber espionage aims to penetrate the computers of a select group of individuals within an organization in order to steal sensitive or confidential information and intellectual property. Hackers use specially designed emails or documents to obtain remote access, and once inside the network, they move laterally—and with lightning speed—from one computer or server to the next. Once they have installed Remote Access Trojans (RATs), they are free to gain future access as needed.

Advanced targeted attacks

Advanced targeted attacks are also aimed at specific groups of individuals—often those with access to highly sensitive information. Because individuals tend to be easier targets than systems, adversaries use social engineering and social networks to target those with knowledge of, use of, or access to targeted data. The goal of these types of attacks is to persist inside the breached network even after detection and removal. How? By using the targeted individuals' credentials. This type of exploit was specifically designed to penetrate the type of computers typically used by large enterprises and government agencies.



Financial malware and ransomware attacks

Intended to target vulnerabilities in browsers, Java, and Acrobat Reader, as well as other less common applications, financial malware and ransomware is often rooted in organized cybercrime in far-reaching geographic areas, such as Eastern Europe. Special exploitation kits infect users via downloads of financial malware such as Zeus or Zbot, which enables the hackers to access to online banking credentials. They can also infect databases with ransomware, such as Cryptolocker, to both encrypt files in the user's hard drive and demand a ransom to unlock the files.

With new threats emerging every week, exploit remediation for these sophisticated attacks has become increasingly formidable.

Why traditional, reactive approaches are ineffective

The most dangerous phase of a vulnerability exploit is when the malware is actually being executed. Yet traditional antivirus and security suites in use today require that the malicious payload—whether it's a trojan, rootkit, rogue antivirus, virus, bot, or other threat—be both known and detected in order to prevent execution. What's more, they focus on detection only on a per-attack or per-vulnerability basis.

Herein lies the problem. Once the threat is discovered, IT teams rush to develop signature updates for an outdated security model, yet the threat landscape continues to change, morphing into an entirely different set of attacks or vulnerabilities. By the time the security fix is executed, the damage has been done.

This reactive approach renders existing security solutions largely ineffective, simply because they are too slow to respond and require patching, either by receiving up-to-date malware or network attack signatures, before they can provide an effective defense. While the reactive signature approach provides adequate identification of existing attacks, it is virtually useless in protecting against new and unknown attacks.

Common security tools

With traditional approaches to defense, applications can still easily be exploited via present or future zero-day vulnerabilities. Let's examine the tools and techniques most organizations are using today:

Antivirus—
While antivirus is effective in detecting millions of varieties of malicious code, it must have knowledge of the type of threat being executed in order to protect against it, whether that is the physical binary needed to create a signature; multiple similar binaries needed to create a generic signature; a heuristic algorithm; or previous knowledge of the attacker's infrastructure.

Intrusion detection and prevention systems, firewalls, and email and web filters—
These tools are essential to an organization's security arsenal, but they are also reactive in nature and contain inherent weaknesses. First, they are fragmented, designed to monitor only a portion of communication traffic. Second, while each is designed to work by creating reactive signatures for known vulnerabilities and filters at the web layer, hackers often employ known bypasses that use special encoding mechanisms during communication, leaving the perimeter unprotected—and zero-day threats undetected.

Built-in Microsoft OS protections—
The addition of Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) have improved the resiliency against attacks, but they are no match for the myriad third-party software applications that users install on their own, often without the knowledge of IT. Attackers use these applications to target non-ASLR-compliant libraries and disable DEP with Return-Oriented Programming (ROP) to execute the vulnerability exploit shellcode and payloads.

Common security techniques

While blacklisting bans threatening malware, it simply can't stay ahead of new malware quickly enough to prevent infections. And with the constantly changing barrage of new threats, these negative lists have become unmanageably large, and are only effective against known threats.

Whitelisting
in which only software that has been designated as safe is allowed to run, also only guards against known threats. Again, these lists are difficult to maintain.

Sandboxing
while somewhat effective in guarding against unknown threats, only addresses the segregation of running programs for either untested code or untrusted applications, users, or websites. While such segregation is necessary, running such programs still leaves the organization exposed to attack and consumes considerable system resources.

Best practice:
Detect and block exploitation as it occurs

Organizations need a way to detect shielded applications that are being exploited maliciously without relying on blacklisting, whitelisting, or sandboxing, or relying solely on traditional tools—methods that are ineffective in preventing both new and unknown zero-day threats. Anti-exploit tools, or exploit mitigation tools, provide a relatively new approach that focuses not on what threat is being delivered to a computer or server, but how it is getting there. Designed to shield vulnerable applications, such as browsers, PDF readers, Microsoft Office applications, and media players, anti-exploit tools offer an effective, proactive way to stop attacks before they occur by detecting malicious activity, such as Adobe Acrobat Reader attempting to download and run an .exe file from the Internet—a clear indication of infection.

While traditional tools such as antivirus and web filtering products can provide effective protection in some cases, and organizations should continue to use them, adding anti-exploit tools provides additional layers of protection that traditional products simply cannot match.

Guard against known and unknown threats

To provide adequate protection against today's sophisticated attacks, organizations should focus on building a multi-faceted, layered approach to defense in which protective technologies can work in tandem to block exploit attempts. They need a proactive rather than reactive way to determine if a shielded application is being exploited maliciously, without relying exclusively on blacklisting, whitelisting, sandboxing, or traditional security weaponry—and without requiring knowledge of the type of malware being executed.

Designed to protect organizations from attacks targeting software and browser vulnerabilities, Malwarebytes Anti-Exploit for Business incorporates multiple protection layers and techniques that work cohesively to provide exploit remediation at different stages. Vulnerability-agnostic, Malwarebytes Anti-Exploit employs generic techniques that do not rely on blacklisting signature updates, whitelisting, or sandboxing, making it extremely reliable and resilient to known and unknown zero-day vulnerability exploit attacks against browsers and applications. An extremely effective complement to the traditional security suite, Malwarebytes Anti-Exploit can block hundreds of zero-day attacks without any previous knowledge of the vulnerability or the exploit.

This simple-to-use endpoint security solution provides three layers of protection against malware attacks, including:

- Protection against operating system security bypasses, using multiple advanced memory protection techniques to detect attempts to bypass existing operating system protections
- Memory caller protection, to prevent exploit code from executing from memory
- Application behavior protection against exploits designed to circumvent all memory protections or to use sandbox escape techniques—such as those typically used in Acrobat Reader and Java exploits

In short, Malwarebytes Anti-Exploit detects what traditional anti-malware and anti-virus products normally miss, making it an ideal addition to organizations' traditional vulnerability detection and intrusion detection and prevention tools.