SentinelOne

The Wicked Truths About Malware & Exploits

IN TODAY'S CYBER THREAT LANDSCAPE, NOT ALL ATTACKS ARE CREATED EQUAL

Whether you're a security practitioner focused on safeguarding your organization's sensitive data, or an individual consumer seeking to better protect the contents of your personal computer, it's increasingly difficult to keep track of the different types of threats aimed at compromising endpoint devices. Today's cyber threat landscape is driven by a dizzying array of attack techniques that grow constantly in both diversity and sophistication. Furthermore, data breaches have become a staple of modern news headlines; given that these stories all seem to share the same unfortunate ending, it can be easy to confuse one type of attack with another.

To the average person, the often bizarre and cryptic names given to most attacks offer little about the attack's nature. However, it's a fair assumption that not all cyber attacks are created equal; there are several different techniques and vectors to consider, for starters. Regardless whether or not you are technically versed when it comes to cybersecurity, there is much to be gained from a deeper understanding of what differentiates one attack technique from another; namely a more robust security posture for your organization, or for yourself.

This paper aims to describe and deconstruct two distinctly different yet often confused types of attacks: Exploits and Malware. Though the differences between these vectors of attack are significant, there are many scenarios where malware and exploits pair together like peanut butter and jelly. In addition to dissecting these types of attacks, the paper will also offer up a perspective on how organizations can more effectively protect against them.

MALWARE

In Latin, 'mal' is a prefix which denotes 'bad', 'evil', and 'wrong'. Therefore, it should come as no surprise that the name 'malware' was coined to represent an ever-expanding collection of intrusive software and executable code purposely engineered to (you guessed it) do bad things.

The earliest form of malware was the computer virus, which is reported to have first appeared in the wild sometime in the early 1980s. Many early viruses were written for pranks (with arguably little to no criminal intent), but the evolution of malware surged during the dawn of the internet age, with many new types of infections designed to bombard users with intrusive advertising. That picture has changed drastically over the last decade and a half. Malware has steadily evolved to become the weapon of choice for cybercriminals across the globe, leveraged for attacks that are deliberate, rampant, and in many cases—highly targeted. Today's malware is made up of worms, trojans, rootkits and ransomware, virtually all of which are actively used for financial gain (theft of sensitive data, industrial espionage, extortion or ransoming of files) and for destabilizing or destroying infrastructure and organizations. Table 1 below summarizes the main types of malware that threaten organizations and individuals today.

The level of targeting of malware attacks varies significantly. For example, ransomware attacks—whose objective is profit—tend to be very widespread, with the goal of extorting as much money as possibly from its victims. On the other hand, malware designed to exfiltrate sensitive information from an organization would target only a few individual users or small numbers of servers of a specific type.

The endpoint has long been malware's primary penetration target; after all, this is where where sensitive data lives. Today's endpoint devices are numerous, span several different computing platforms, and are more mobile and dynamic than ever before in today's hyper-connected world. As such, they are much more vulnerable against increasingly sophisticated and stealthy malware attacks.

TABLE 1: Popular Types of Malware

MALWARE TYPE	DESCRIPTION
VIRUS	One of the earliest forms of malware, viruses self-replicate when executed, infecting other programs or systems for sabotage or profit. The vast majority of viruses target Microsoft Windows-based computers.
TROJAN	A piece of malware designed to appear as something entirely different to the user, masking its true intent. Trojans are typically spread via social engineering techniques (seemingly benign e-mail attachments) or by drive-by downloads.
WORM	Malware designed to replicate itself in order to spread to other systems through a computer network. Unlike viruses, worms do not need to attach themselves to other programs in order to spread. Worms have been instrumental in the creation of botnets through installing back doors on infected computers.
ADWARE	A form of malware that launches unwanted advertisements (usually pop-up windows) on infected computers. Most adware doesn't present a substantial threat, but it has been routinely classified as a cyber threat, nonetheless.
SPYWARE	A form of malware designed to capture sensitive user data (files or user actions on the target system). Spyware can stealthily infect a system via a Trojan or web browser vulnerability.
RANSOMWARE	A form of malware engineered to extort money from users and institutions. Ransomware attacks will either encrypting a target device's files, or by locking the user out the device completely until a ransom is paid within a short time period.
FILE-LESS / MEMORY-ONLY MALWARE	A malicious program typically injected into some running process, and executes only in RAM. This vector of attack is difficult to detect, but does not persist if the system is rebooted because memory is volatile.

HOW MALWARE WORKS

Though there are many different types of malware today, such attacks follow roughly the same framework in terms of how they unfold.

PHASE 1: Attack Targeting and Inception

Every malware-based attack begins with some sort of targeting strategy. Based on the end goal, cybercriminals will determine the method of launching their attack. If profit is the primary objective—such as with ransomware attacks—then attackers will target as many users as possible, and opt for an install route with the highest likelihood of success. In these cases, attackers use spear-phishing e-mail blasts in which recipients are incited to open up the message's attachment, which then launches the malicious malware program. Other widespread targeting methods involve the use of websites, where attacks are initiated through hidden redirects and drive-by-downloads. Attackers will typically focus their attention on public websites running vulnerable web or application servers that they can leverage. Attacks targeting specific systems or individuals might also leverage exploits and different types of social engineering techniques to entice an insider to unknowingly install the malware from within the organization's firewall. If the goal is to compromise a specific type of endpoint system, the malware could be engineered to remain hidden or dormant until it finds itself on that system.

PHASE 2: Exploit Discovery

Many attackers favor packaging malware into exploit kits that they covertly place on legitimate websites, or host the malware on a fake website designed to look like a legitimate site. When a potential victim's browser connects with a website hosting an exploit kit, the kit probes the visitor's system and extracts information like OS version, browser type, and installed applications, in order to find vulnerabilities to exploit.

Exploits and malware go hand in hand. All types of enterprise and consumer applications have vulnerabilities that can potentially be exploited, paving the way for malicious programs to find their targets.

PHASE 3: Payload Delivery

In the payload delivery stage, the malicious program will download and install a "payload" to the target endpoint device. This payload could be the piece of malware itself, or it could be a hidden downloader which then creates a backdoor through which multiple types of malware can be downloaded, allowing different attacks to be executed.

PHASE 4: Execution of Attack

At this point, the malicious program has reached its target and begins to run on the system, carrying out the attacker's intent. In the case of ransomware, the program will begin to encrypt the user's files or block critical system operations, thus locking the user out. More sophisticated attack code can be designed to trigger off of specific system events, or stealthily steal data over an extended period of time.

PHASE 5: Malware Propagation

If a malware attack goes undetected or unmitigated, it will likely spread laterally, infecting other endpoints or even launching further targeted attacks via the network. As the malware persists, it communicates back to the attacker's back end, or to other command & control servers. Lateral spread is often the goal of attacks leveraging RATs (Remote Access Trojans). RATs are malware programs designed to establish administrative control over the host computer through back doors. Once such control is gained by an attacker, they can distribute RATs to other vulnerable computers on the network, establishing a botnet.

PROTECTING AGAINST MALWARE ATTACKS

Much of malware's sophistication is attributed to its ability to evade detection by security solutions. A considerable portion of malware out there today is well known and has been classified by threat intelligence services used by traditional antivirus (AV) solutions to identify and preemptively block malicious programs from running. With static prevention, the currency of threat intelligence is signatures. Every piece of known malware has a distinct signature; typically a static hash consisting of a calculated numerical value of a segment of code unique to that particular malware variant.

However, static prevention methods are completely ineffective at catching new, never-before-seen malware. Simply put: no signature equals no detection. It's interesting to note that new malware isn't necessarily new; an existing piece of malicious code can be quickly transformed into a brand new binary with only a slight modification of its source code, or by packing that code into an entirely different program in order to obfuscate it. By today's cybersecurity standards, getting past AV is no remarkable feat.

Bypassing advanced security measures requires significantly more effort and ingenuity on the part of attackers and malware engineers. Sandboxing solutions are a substantial step up from traditional antivirus, which many organizations deploy for their ability to dynamically detect new or more advanced malware. Sandboxing attempts to detect malware attacks by running suspicious programs in a virtualized environment designed to emulate the target device. Signatures are dynamically created by the sandbox for programs it deems malicious, and can be shared with firewall solutions for enhanced localized prevention. This approach has proven to be successful in alerting of 'patient zero'. However, more advanced forms of malware can detect sandbox environments, and the malicious program can be designed to lie dormant until it finds itself on a 'real' endpoint device of a specific configuration.

Figure 1 below summarizes various types of types of countermeasures employed by attackers.

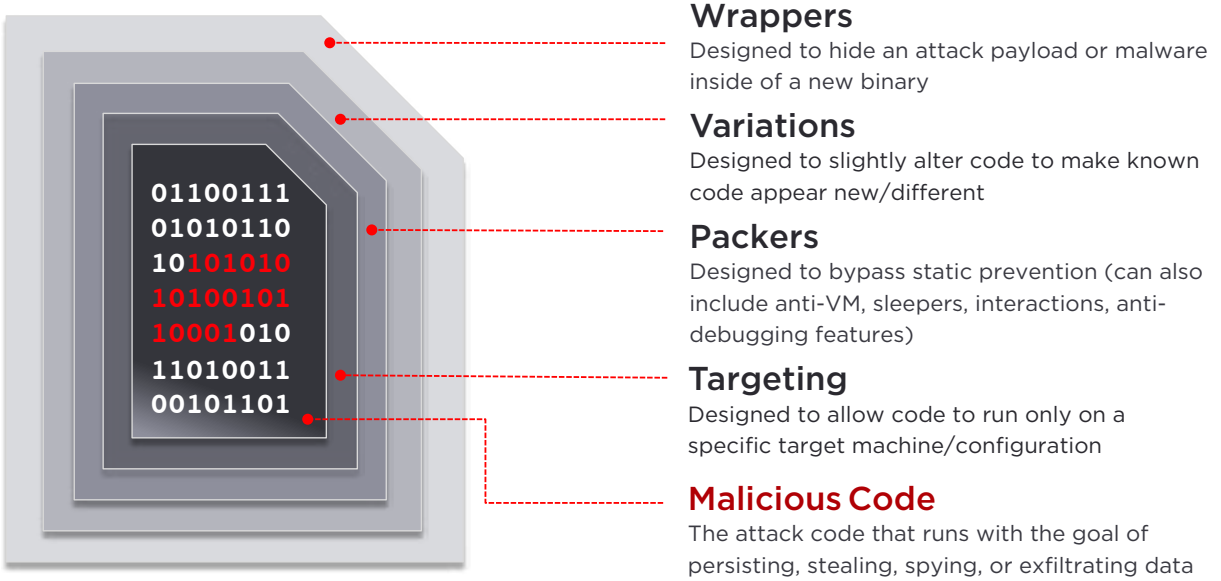

Figure 1: *Anatomy of an Advanced Malware Program*

Basic malware can be made to appear new or benign to antivirus protection with just a few simple code alterations, and more sophisticated pieces of malware can be engineered to evade detection by more advanced security solutions, like sandboxes. In order to effectively protect against all types of malware attacks—simple or sophisticated—a Next-Generation Endpoint Protection (NGEP) solution is required. NGEP detection is based on how a malicious program behaves, and not just on what the program actually is. Though there are many different types of malware, and millions of variants in existence, malware in general tends to follow specific behavioral patterns. Behavior-based detection is proven to be highly effective in detecting malware attacks.

EXPLOITS

In the realm of cybersecurity, exploits are malicious programs that take advantage of application software or operating system vulnerabilities. Such vulnerabilities represent critical security gaps for organizations and individual users alike, and software vendors are compelled to regularly issue patches that fix vulnerabilities discovered through their own internal quality testing or by application users themselves.

Exploits typically target productivity applications such as Microsoft Office (Word, Excel, etc.), Adobe applications, web browsers and operating systems, and they continue to pave the way for many malware-based attacks. Though not all exploits involve file-based malware (for example: null/default system password exploits, DDoS attacks), the exploit/malware combination is highly prevalent when it comes to targeting endpoints.

One prominent example of an exploit-facilitated malware attack involves a known vulnerability in Microsoft Office. The exploit is crafted to fool the targeted application into executing malicious code, which is hidden within the document as shellcode. The running malware would then allow the attacker to take control of the affected system. Should the logged-on user have admin privileges, the impact of the attack would be more severe. Though this vulnerability is known and documented, the exploit is still in use by attackers simply because many organizations and users have not gotten around to installing the released patch.

PROTECTING AGAINST EXPLOIT-BASED ATTACKS

Aside from constantly pushing users to exercise basic caution when opening up e-mail attachments from unknown senders and downloading files, minimizing the risk of exploit-based attacks begins with routine patch installations for software applications and operating systems. Most organizations endeavor to routinely patch their critical applications and operating systems in a timely manner for compliance and security purposes. However, the ones who fall behind by not having the latest patches installed expose themselves to substantial risk of attack; usually, with each new patch release, details of the vulnerabilities fixed by the patch are made available to everyone—including attackers. With this information, attackers can develop a corresponding exploit and launch a successful attack against any unprotected endpoint system whose software isn't up-to-date with the latest vulnerability fixes. In fact, 99.9% of exploited vulnerabilities were compromised more than a year after the Common Vulnerabilities and Exposures report was published, according to Verizon's 2015 Data Breach Investigations Report. A glaring example of this is that the number one exploit found still affecting Windows systems in the second half of 2015 is old and long-patched Windows Shell flaw (CVE-2010-2568), according to Microsoft's latest Security Intelligence Report. The exploit was reportedly used in the Stuxnet attacks on Iran's Natanz nuclear plant to sabotage its uranium enrichment program in 2010.

The latest patches will keep endpoint devices safe from attacks involving known exploits, but there is always the possibility of a zero-day exploit being developed; an exploit based on a vulnerability whose existence is completely unknown to everyone in the world but the attacker. Zero-day exploits appear to be on the decline, simply because it is far easier for an attacker to succeed using alternative vectors of attack. However, organizations should deploy security measures that can detect exploits, in addition to having the latest patches installed.

There are a finite number of techniques employed by attackers (buffer overflows, heap spraying, unauthorized code execution, etc.), when crafting an exploit, and the best defense is a dedicated endpoint protection platform capable of detecting these behaviors. A Next-Generation Endpoint Protection approach dramatically reduces the risk of compromise via exploit, and if it is compliance-certified, it allows for flexibility in patching cycles as a compensating control.

CONCLUSION

Given today's complex and ever-expanding threat landscape, both individuals and IT teams have a lot to contend with in protecting their respective endpoint devices from attacks. Understanding the nature of different types of attack vectors and techniques is critical in establishing a robust endpoint protection strategy. Though malware and exploits are used in combination for both widespread and targeted attacks, they present distinctly different threat vectors that must be examined individually. Many organizations take a piecemeal approach to endpoint security, deploying point solutions for protection against individual vectors of attack. However, a Next-Generation Endpoint Protection solution leveraging behavior-based threat detection will offer much more comprehensive protection (with a single endpoint agent and a single management console) against malware, exploits and live/insider attacks.

To request more information, and to schedule an exclusive demo, visit **www.sentinelone.com/contact**.