Proactively managing your business technology

Five Cyberthreats that Slip Past Traditional Antivirus

Polymorphic malware

Many traditional AV programs rely on signature-based detection. This involves comparing a file against a known entry, otherwise known as a signature, in a database of known threats.

This style of protection has some flaws. First, the AV user must have the most recent list of signatures, requiring frequent updates on their part. If that user hasn't kept their virus definitions current, they'll be defenseless against newer files. Beyond that, this method of protection is purely reactive. The AV company must know about the signature before it can flag it to their user base, and malware often uses evasion techniques to avoid detection by AV companies.

The key flaw here is there's often a knowledge or time gap in coverage. Polymorphic malware was designed to exploit this flaw. If, for example, the malware gets detected by an AV program, it will regenerate itself using new characteristics that do not match known signatures. This makes it hard for signature-based AV to truly put a stop to the infection. Additionally, there are roughly 350,000 new malware variants created each day. This ensures those using signature-based AV will almost always be catching up.

Weaponized documents

Criminals often exploit flaws in different document formats to compromise a system. These documents typically use embedded scripts. The criminals obfuscate the code or script within these weaponized documents. It looks harmless even to the trained eye and will slip past AV because it only scans the initial document rather than the code or script after it executes. Once launched, the attack runs in the background without the user's knowledge.

Criminals can use Adobe® PDF files with embedded JavaScript® to execute operating system commands or download executables to compromise the devices and networks they access. Hackers often use embedded scripts to execute PowerShell® commands, and since PowerShell is built-in to the Windows® operating system, these attacks can damage endpoints and even entire networks. However, PDFs aren't the only vulnerable file types—XML-based documents, HTML, and Office® documents often carry these malicious scripts hidden within them. An AV solution based on comparing executable signatures will miss weaponized documents because it will scan only the initial document, not the malicious code the document launches.

Browser drive-by downloads

Drive-by downloads are files downloaded to the endpoint using vulnerabilities in the browser or a browser add-in. By doing this, the file downloads, and the user and AV program are none the wiser. The download could come from a legitimate website with a compromised script or ad service, or it could be a malicious website specifically set up to initiate the download. These attacks start with email or social phishing, email attachments, or well-disguised pop-up links to lure users to a website. Criminals then leverage exploits in browsers or plugins to download malware and begin the attack. Once this is complete, the criminal can start doing damage— whether that involves installing a cryptominer, a remote access trojan, or ransomware.

Fileless attacks

Most antivirus programs rely on inspecting a file as it's written to the device. However, if there isn't a file to begin with, the AV program typically can't detect the malicious behavior.

Fileless attacks occur without installing an actual payload on a system, making them extremely difficult for antivirus to detect. They're typically executed in the endpoint's memory, and use PowerShell, undll32.exe, or other built-in system resources to infect machines.

Fileless attacks can often start with documents or malicious scripts on a website, but that's certainly not the only way they infect machines. For example, when an endpoint enables remote desktop protocol (RDP), it leaves open a listening port on the machine that would allow someone to connect to the machine and start running malicious processes, including downloading actual file-based malware, changing the registry, or stealing data.

As if that's not scary enough, SentinelOne® found a 91% increase in fileless malware attacks in the first half of 2018. As these attacks increase in prevalence, businesses will need to go beyond file-based detection to better protect their assets and data.

Obfuscated malware

Security professionals and researchers consistently play "catch up" with the cybercriminals. AV companies use several methods for discovering malware. One common discovery method involves executing files in sandbox environments and observing for malicious behavior. Another common discovery method involves scanning the code for common signs of malicious intent.

Cybercriminals have found ways around this. In the same way security professionals put up defenses to protect their data and assets, hackers also have ways of protecting the malicious payload within a piece of malware.

Newer malware will detect a sandbox environment and remain benign in the sandbox environment, only to attack in a live setting. This can make it impossible for the AV to detect behavioral methods while in the sandbox environment.

Another method to circumvent AV involves "packers," which use either encryption or compression to prevent someone from seeing within the file. Additionally, malware creators may wrap the malicious code within benign code within a file to hide the bad code.

Any of these techniques make it hard for security researchers to detect (and understand) these malicious files to begin with. Further, if you use an antivirus program using heuristic scans within a sandbox environment, these techniques help the malware evade detection before it goes live on a machine.