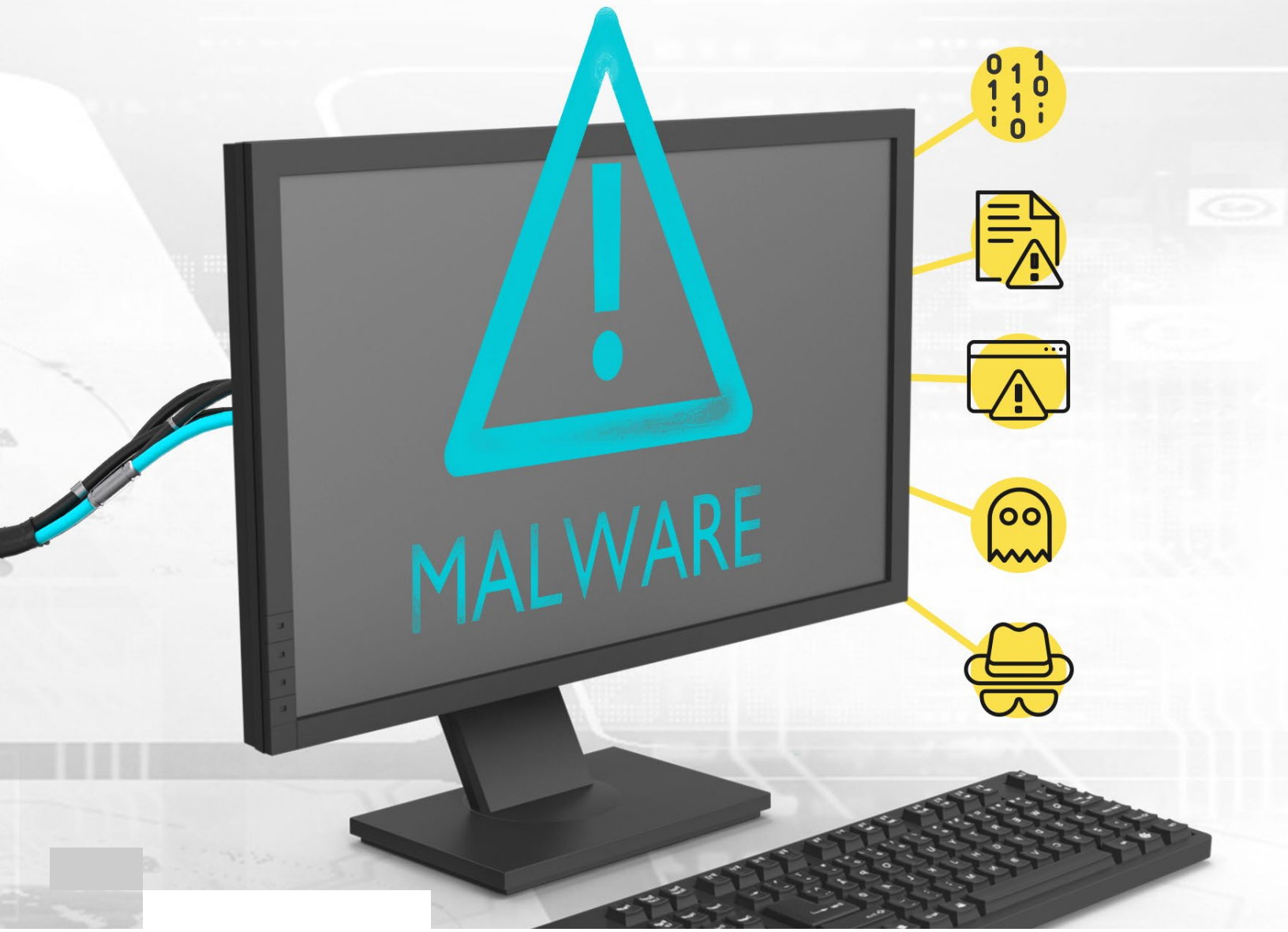
solarwinds msp



eBOOK

Five Cyberthreats that Slip Past Traditional Antivirus

Table of Contents

Five Cyberthreats that Slip Past Traditional Antivirus

The first documented computer virus was Creeper, developed in 1971. Created in an academic setting, the virus was built to demonstrate the ability of a file to transfer across a network. It took six months before computer programmers wrote a successful antivirus program, called Reaper[1]. This was the first time lag between threat and defense.

Ever since, security professionals and computer programmers have been playing catch up. As an industry, we detect threats, update our defenses, then repeat as necessary.

Many traditional antivirus (AV) programs operate on signatures—as malicious software is discovered, a signature describing the file is generated, added to a database, then the database gets pushed out to the customer base. If the antivirus discovers a file on your machine that matches a signature, that file gets quarantined and/or removed. By December 2018, malware was being discovered at the alarming rate of 350,000 new threats per day[2]. Signature-based AV solutions can have a hard time keeping up with this volume, often leaving devices vulnerable.

Over time, we have seen the rise of new defenses; however, each defense triggers a corresponding change in tactics from the bad guys. These changes include malware designed not just to exploit vulnerabilities, but to outwit an AV's defenses. Here are five types of attacks that slip past traditional antivirus.

1. POLYMORPHIC MALWARE

As mentioned in the introduction, 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 clear 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 protective techniques to avoid detection by AV companies.

1. "All About Creeper, the First Virus in History," Softonic. en.softonic.com/articles/all-about-creeper-the-first-virus-in-history (Accessed April 2019).
2. "Malware," AV-TEST. av-test.org/en/statistics/malware/ (Accessed April 2019).

The key flaw here is there's often knowledge or a time gap in coverage. Polymorphic malware was designed to exploit this flaw. If, for example, the malware gets detected by an antivirus 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[3]. This ensures those using signature-based AV will almost always be catching up.

2. WEAPONIZED DOCUMENTS

Criminals often exploit flaws in different document formats to compromise a system. These documents typically use embedded scripts. The criminals often obfuscate the code or script within these weaponized documents. It looks harmless even to the trained eye, and will slip past AV because the AV only scans the initial document rather than the code or script after it executes. The attack, once launched, 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 complete 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.

3. 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 the antivirus 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. In fact, in October 2017, the city of Issaquah, Washington was hit by a ransomware attack that took services offline for four days[4]. It all began with a drive-by download after an employee opened a malicious PDF on a website.

3. "Malware," AV-TEST. av-test.org/en/statistics/malware/ (Accessed April 2019).
4. "How a Drive-by Download Attack Locked Down Entire City for 4 Days," The Hacker News. thehackernews.com/2017/10/drive-by-download-ransomware.html (Accessed April 2019).

4. 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, rundll32.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[5]. As these attacks increase in prevalence, businesses will need to go beyond file-based detection to better protect their assets and data.

5. OBFUSCATED MALWARE

Earlier, we wrote about how 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 environment. This makes it impossible for the AV to detect with behavioral methods while it's 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.

5. "Fileless Malware Attacks | How They Can Be Detected and Mitigated," SentinelOne. sentinelone.com/blog/fileless-malware-attacks-can-detected-mitigated/ (Accessed April 2019).

HOW SOLARWINDS CAN HELP

To protect against modern threats, managed services providers (MSPs) need to take a layered approach to security. By overlapping multiple security controls, you can mitigate the risk of falling victim. SolarWinds MSP offers two remote monitoring and management platforms—SolarWinds® RMM and SolarWinds N-central®—to help you provide several layers of protection for your clients. If an AV solution can't catch a threat, you can use web protection to blacklist malicious links, email protection to keep out spam and help prevent phishing attempts, and patch management to close vulnerabilities in both the operating system and third-party software. And if an attack does succeed, you can use built-in backup and recovery to restore your files or systems.

Additionally, both platforms offer SolarWinds Endpoint Detection and Response (EDR), powered by SentinelOne®. SolarWinds EDR is designed to prevent, detect, and respond to evolving cyberthreats to customer endpoints. It goes beyond traditional antivirus via a signatureless approach—that means no waiting for recurring scans or updates to signature definitions. And in the event of an attack, EDR can take steps to help contain the threat, reverse the effects, and automatically roll back the endpoint or compromised files to a healthy state.

solarwinds msp

Learn more today at ***solarwindsmsp.com***

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT management software. Our products give organizations worldwide—regardless of type, size, or complexity—the power to monitor and manage their IT services, infrastructures, and applications; whether on-premises, in the cloud, or via hybrid models. We continuously engage with technology professionals—IT service and operations professionals, DevOps professionals, and managed services providers (MSPs)—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures and applications. Targeted for MSPs, the SolarWinds MSP product portfolio delivers broad, scalable IT service management solutions that integrate layered security, collective intelligence, and smart automation. Our products are designed to enable MSPs to provide highly effective outsourced IT services for their SMB end customers and more efficiently manage their own businesses.