ActZero

THREAT INSIGHT

Signature-Based Antivirus Bypass Threats

Antivirus (AV) software has generally been regarded by businesses as the best and simplest defense to keeping data and systems secure. That somehow, it is nearly unconquerable. In reality, while AV products are certainly a must-have in your security solutions suite, they do not provide 100% protection against threats.

Traditional signature-based antivirus software is fairly simple. It generally uses a database of virus signatures composed of previously identified viruses found in attacks. If signatures are detected within a user's systems, they are blocked or quarantined, depending on the established rules. These lists are maintained by the security community, and whenever a new virus is discovered, the antivirus provider is informed, and a digital signature or hash of the virus is created and added to the database.

Antivirus vulnerabilities

Time Lag: For signature-based AV, there may be a gap between when a new signature is first detected and when AV tool is updated and in production.

Threat Sophistication: With the adoption of the internet and cloud, the threat landscape and its attack surface has grown immensely. Threats have become increasingly sophisticated and complex.

76% of respondents who had been compromised say the attack was a new or unknown zero-day attack

- Ponemon Institute 2018 State of Endpoint Security Risk study

Hackers have evolved ways to get past antivirus programs. No matter how quickly AV evolves protection, hackers will always be able to test their payload against the latest AV, just by purchasing a single license.

Fileless Attacks: AV often works with other types of malware because it detects the traditional "footprints" of a signature. In contrast, fileless malware leaves no footprints for antivirus products to detect. Fileless malware is effective because it's already hiding in your system, and doesn't need malicious software or files to enter.

Why legacy antivirus software alone isn't enough

There are numerous ways that viruses and malware can get by antivirus solutions. Some of the more popular evasive tactics include:

Signature Swaps/Code Changes: Polymorphic malware works when the virus changes some of its code while it is propagating, resulting in a signature change (sometimes an encryption algorithm change) without affecting the way the virus works, evading antivirus software.

Obfuscation: Distorting the malware while keeping its form, using obfuscation, like randomizing the case of the characters in a PowerShell script aids some attackers. A well known scenario is an attacker changing all references in the memory tampering tool Mimikatz to Mimidogz, along with changing a few other common strings.

Encoding Payloads: Another technique for evading antivirus scanners is to encode payloads, by deploying a small header program bolted on to the front of the encoded virus. This disguises the threat as data. Shellter, for example, is capable of re-encoding any native 32-bit standalone Windows application. It avoids using anything that looks suspicious to AV software, such as packed applications that have more than one section containing executable code.

Sandbox Aware: Some malware is 'sandbox aware', meaning it attempts to identify whether or not it is being executed in a virtual machine 'quarantine' environment and acts differently. The veil framework includes payloads with various checks such as host name, detecting debuggers and checking for known VM files.

User Behavior: No antivirus tool can protect you from yourself 100% of the time. Users who open an email attachments that they don't recognize and run it, often install a virus before the antivirus software has a chance to catch and quarantine it. Security Awareness Training and application is essential to good security hygiene.

While most AV solutions now use machine learning and more advanced detections, some legacy antivirus solutions still rely on signature-based detection alone for known types of malware to detect and prevent further attacks of similar types. Sophisticated attackers have found ways around these older AV defenses, and even those using heuristic models. Per a recent Ponemon Institute study, legacy antivirus solutions using signature and heuristics alone only detected 57 percent of all potentially dangerous attacks. And once a threat has passed through the antivirus gates, businesses are in reactive mode.

The role of NGAV and MDR in modern security

Adding **Next Generation Antivirus (NGAV)** to your cybersecurity stack helps protect against unknown threats as well as known threats, which is increasingly important as the use of fileless attacks rises among attackers. Our cloud-native and on-device NGAV solution, part of our Managed Detection and Response platform, is designed to employ a lightweight agent that is unobtrusive and has a minimal endpoint impact.

By adding in our machine learning (ML), behavioral detection, and artificial intelligence, ActZero's NGAV eliminates reliance on signatures to detect malicious activity, enabling threats to be exposed faster and more accurately, and br blocked in near real time. Our integrated threat intelligence enables the immediate assessment of the origins, impact, and severity of threats in the environment, rapidly adjusting to changing tactics, techniques, and procedures (TTPs) used by adversaries in attacks. And, our MDR service provides detailed guidance for response and remediation.

ActZero's NGAV solution provides a number of prevention capabilities including for known and unknown malware, and malware-free attacks including:

Signature-less malware protection, using ML algorithms to increase the likelihood that a file is malicious. Reducing time-to-value on new threat to zero.

Indicators of Attack (IOAs) detections that correlate endpoint events to find indications of stealthy malicious activity. The online algorithms that use ML do not require entire data sets to perform useful analysis, and therefore much faster.

Behaviour-based event detections such as ransomware, rate of file operations, suspicious process chains, persistence, etc.

Exploit Detections, helping catch and stop attacks such as drive-by downloads

Lateral movement and credential access protections, designed to mitigate movement of attackers across customer environments

Learn more about the product capabilities that safeguard organization against breaches, and why our NGAV solution is an industry-recognized AV replacement.

CONTACT US NOW

Email: info@actzero.ai
Phone: +1.855.917.4981