E-book

VECTRA®

How cyber attackers evade threat signatures

At risk in the cybersecurity gap

There's an alarming cybersecurity gap between the time an attacker evades prevention security at the network perimeter and the clean-up phase when an organization discovers that key assets have been stolen or destroyed.

Attackers have a big advantage in the cybersecurity gap. It's easy for them to circumvent signatures, reputation lists and other prevention security defenses by using complex and intelligently constructed attack methods.

The traditional, widely embraced approach to detecting threats is inherently reactive, ceding the first-mover advantage to cybercriminals.

Signatures, reputation lists and blacklists only recognize threats that have been previously seen. This means someone needs to be the first victim, and everyone hopes it's not them.

Detecting threats usually depends on key security applications installed at endpoints and gateways. New threats are caught in virtual sandboxes and new signatures are generated on-the-fly. The process takes time, and malware can gain a foothold as endpoints and networks are left vulnerable.

Creating new signatures is a tried and tested solution. It's the bedrock of everything from antivirus software to next-generation firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS). However, they are always several steps behind attackers and can create a false sense of security.

Although signatures can stop known threats – Trojans, rootkits and other malicious code – the most dangerous ones are those that have yet to be captured and mapped. We don't know if they exist, we don't have visibility into what they do, and there's no way signatures can catch them.

The inherent limitations

Signatures have had a good run, especially at detecting large-scale commodity threats like command-and-control communications of botnets, automated crawlers and vulnerability scanners that scour the Internet.

But the signature model is limited and leaves multiple blind spots for a barrage of perilous attacks.

Attackers who value stealth over the number of systems they control are finding ways around signatures. And unfortunately, these sophisticated attackers tend to think more strategically and pose a significant risk to organizations.

Understanding the blind spots caused by signatures requires understanding the weaknesses.

For example, signatures have no response to insider threats. They won't help you identify and stop a malicious insider with legitimate access and legitimate tools. Attack behaviors and deviations from normal activity can't be detected with signatures.

Custom malware also makes its way around signatures. Most malware is unique to the organization under attack, which means it won't be caught by signatures. According to the 2015 Verizon Data Breach Investigation Report, 70-90 percent of malware samples have traits that are exclusive to the targeted organization.

Attackers don't handcraft malware; they modify existing malware just enough to throw off signature-based defenses. Malware signatures work by creating hashes of known bad files, so the smallest modification prevents a match.

Attackers simply add a few bits to a malware file so the hash won't recognize it as malware. These changes occur automatically with no human interaction. Vast volumes of seemingly custom malware are generated daily in this way.

The key is that while the malware's bit pattern may differ, its behavior is the same. The changes, which are designed to avoid signature-based detection, are superficial.

Signatures also miss zero-day attacks that target vulnerabilities in software or operating systems, such as Heartbleed or Duqu 2.0. These vulnerabilities are virtually impossible to detect via signatures because they only stop known threats.

Watch your behavior

Attackers can change malware, search for unknown vulnerabilities and steal data from systems they have permission to access. But they can't change their attack behaviors as they spy, spread and steal from a victim's network.

These behaviors can be observed, giving organizations real-time visibility into active threats inside their networks. Today, the savviest organizations complement their signature-based defenses with automated threat management.

Combining data science, machine learning and behavioral analysis, automated threat management detects malicious behaviors inside the network, regardless of the attacker's attempt to evade signatures and whether it's an insider or outsider threat.

By focusing on attack behaviors and actions, automated threat management can identify every phase of an active attack – command and control, botnet monetization, internal reconnaissance, lateral movement and data exfiltration – without signatures or reputation lists.

Behavior-based threat detections also identify internal reconnaissance scans and port scans, Kerberos client activity, and the spread of malware inside a network. Data science models are effective at neutralizing an attacker's use of domain-generation algorithms to create an endless supply of URLs for their threats.

Cybercriminals always look for new ways to conceal their attack communications, and one of the most effective – and fastest-growing – ways to do this is by hiding within another allowed protocol.

For example, an attacker can use benign HTTP communication but embed coded messages in text fields, headers or other parameters in the session. By riding shotgun on an allowed protocol, the attacker can communicate without detection.

However, the detection models inherent in automated threat management can reveal these hidden tunnels by learning and analyzing the timing, volume and sequencing of traffic.

Staying ahead of network threats

Nimble attackers can easily create and hide their exploits in an infinite number of ways. Consequently, the limitations of signatures should be complemented with automated threat management models that continuously learn new attack behaviors and adapt to network changes.

It's time to jump off the signature hamster wheel and get ahead of attackers by automatically detecting and analyzing the behaviors and actions that belie an attack and mitigate the threat before damage is done.

For a deep-dive into how signatures work and why they fall short when it comes to detecting modern threats, download the white paper.

VECTRA