(IN)SECURE

Issue 47 - September 2015

REDEFINING SECURITY VISUALIZATION WITH HOLLYWOOD UI DESIGN

TOKENIZATION / THREAT INTELLIGENCE
VULNERABILITY DISCLOSURE / DDOS
INTERNET OF THINGS / HUMAN ERROR

black hat®

BEST PRACTICES FOR ENSURING COMPLIANCE
IN THE AGE OF CLOUD COMPUTING

Automated threat management: No signature required

by Oliver Tavakoli

The industry approach to detecting threats is inherently reactive, ceding the first-mover advantage to the cyber criminals. Defenses – based on signatures, reputation lists and blacklists – are only designed to recognize threats that have been previously seen. This means someone needs to be the first victim, and everyone hopes it's not them.

We keep doing the same thing over and over, expecting different results. The security industry has put a massive effort into delivering signatures faster and faster, trying to close the gap between when a new threat is detected to when the corresponding new signature is delivered.

But moving faster hasn't made us demonstrably safer. Instead, it has led to more nimble attackers, who easily create and hide their exploits in an infinite number of ways.

The key to understanding the value of signatures is to understand their weaknesses. Signatures are valuable for detecting large-scale commodity threats, such as the command-and-control communications of botnets, automated crawlers and vulnerability scanners that scour the Internet.

But the signature model falls flat with attackers who value stealth over the number of systems they control. And unfortunately, these more sophisticated attackers are more apt to think strategically and can pose a significant risk to organizations.

Attackers can always change malware – requiring a new signature – but they can't change what they need to do to achieve their goal – spy, spread and steal from the victim's network. And those behaviors can be observed, giving organizations real-time visibility

Custom-made malware

Most malware is unique to the organization that received it, which means it won't be caught by signature-based solutions. According to Verizon's 2015 Data Breach Investigations Report, 70 to 90 percent of malware samples have characteristics that are exclusive to the targeted organization.

Attackers aren't handcrafting malware – they use the same malware and alter it just enough to throw off signature-based defenses.

Malware signatures work by creating hashes of a known bad file.

Attackers simply add a few bits to a malware file to change the hash so it's not recognizable as the same malware to signature-based security solutions. These changes occur automatically, with no human interaction required. 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.

A behavior-based approach can detect the behaviors in the network, regardless of the attacker's attempt to evade signatures.

Zero-day vulnerabilities are virtually impossible to detect via signatures, making them some of the most valuable pieces of information to the world's most sophisticated attackers.

Every day is a zero-day

Attackers also exploit vulnerabilities in software and operating systems. And, like the Heartbleed vulnerability in OpenSSL, these mistakes can lurk silently for years until they are exploited. And unfortunately, prevention systems only protect against known vulnerabilities.

Zero-day vulnerabilities are virtually impossible to detect via signatures, making them some of the most valuable pieces of information to the world's most sophisticated attackers.

Even if a vulnerability and its exploit are unknown, the attack behavior that follows exploitation of the vulnerability generally remains the same.

The Duqu 2.0 malware, identified in June 2015, illustrates the power of using behavior-based systems to detect advanced attacks rather than relying on signatures or reputation lists. Duqu 2.0 is a new version of Duqu, which is related to the Stuxnet worm.

While Stuxnet was used to damage uranium centrifuges, the original Duqu was more intent on surveillance and collecting information in a compromised network. Like its predecessor, Duqu 2.0 uses zero-day vulnerabilities to compromise its victims.

Duque 2.0 performs reconnaissance to map the internal network, uses a Kerberos pass-the-hash attack technique to spread laterally, elevates privileges to a domain administrator account, and uses those privileges to infect other hosts.

The core behavior of the Duqu attack creates an indelible marker, even if the bits delivering the malware change. By focusing on the actions that an attacker needs to perform to infiltrate a network and steal data, even the most advanced attacks can be detected using a behavior-based approach.

Watch your behavior

Think of a sentence as an analogy. Signatures try to give every subject a proper name, while a behavior-based approach focuses on the verb. While the names may change, the malicious action remains the same.

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

A behavior-based approach can be used to detect activities like internal reconnaissance scans and port scans, Kerberos client activity and the spread of malware inside a network. Data science also can be effective at neutralizing attackers' use of domain-generation algorithms to create an endless supply of URLs for their threats.

Attackers always look for new ways to hide their traffic, and one of the most effective – and fastest-growing – ways is to tunnel their traffic 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. Data science also can be used to reveal these hidden tunnels by learning and analyzing the timing, volume and sequencing of traffic.

It's time to jump off the signature hamster wheel and get ahead of attackers with advanced threat intelligence that actively watches and analyzes the behaviors and actions that conceal an attack, and neutralize the threat to your business as it happens.

Oliver Tavakoli is the CTO at Vectra Networks (www.vectranetworks.com).