White paper

VECTRA®

Automated threat management: No signature required

VECTRA

TABLE OF CONTENTS

Gaining speed but always behind

Signatures, reputation lists and blacklists are an inherently reactive approach to detecting threats. By design they only recognize threats that have been seen previously, and this means someone always needs to be the first victim.

It's an open secret that cyber-threats are growing faster than organizations can detect them. According to the most recent Verizon Data Breach Investigation Report, in 60 percent of cases, attackers are able to compromise an organization in minutes.

Over the past several years, the information security industry has made a concerted effort to deliver signatures and rules faster and faster. The idea is to reduce the window of time from when a new threat is detected to when corresponding new signatures are delivered. This has spawned an entire market focused on aggregated security intelligence feeds.

The problem with signatures

While these security intelligence efforts can be beneficial and reduce the time of exposure, it is insufficient on its own. The signature model inherently ensures that attackers are always ahead of defenders – the only question is, how far?

The core problem is that faster signatures have led to faster attackers. There's a near-infinite supply of IP addresses and URLs, so it's easy for attackers to pick up and move to a clean new residence. They can easily create new malware and hide their exploits in a limitless number of ways.

The key is to understand the value of signatures while being aware of their weaknesses. Signatures are valuable for controlling large-scale commodity threats, such as:

- Large common botnets with command-and-control methods that are easy to detect
- Automated crawlers and vulnerability scanners scour the Internet looking for known vulnerabilities

However, the signature model falls flat with attackers who make the effort to avoid detection. These are often the more strategically focused attackers and they pose the greatest risk to an organization. They always enjoy a first-mover advantage over signature-based defenses, which is why it's important to complement those defenses with behavior-based threat detection models.

While attackers can always change signatures, they can't change what they need to do – spy, spread and steal from the victim network. These behaviors are always observable.

By focusing on these actions, security professionals can jump off the signature hamster wheel, where they are perpetually behind and exhausted, and set up a strategic position to monitor where an attacker will eventually arrive.

> *Attackers can't change what they need to do – spy, spread and steal from the network. These behaviors are always observable.*

Isn't that special?

Most malware is unique to the organization that receives it and won't be caught by signature-based solutions. The Verizon data breach report found that 70-90 percent of malware samples are unique to a single organization.

This may seem outlandish because how much custom malware can there really be? The reality is that the malware isn't actually custom. It's the same malware, altered just enough to throw off signatures.

Malware signatures work by creating hashes of a known bad file. If an attacker adds a few bits to the malware file, the hash changes and security solutions won't recognize it as bad. This is done easily and automatically without a human attacker being involved.

For example, to avoid signature-based detection, a Web server with malware can make small changes automatically each time a malicious file is served. The technical name for this behavior is *server-side polymorphism* and it is a key way that vast volumes of seemingly custom malware are generated each day.

The key takeaway is that the malware is not actually different. It still behaves the same way and does the same things. The changes are superficial and only serve to avoid signatures. A behavior-based approach continues to detect these behaviors in the network, regardless of the attacker's attempt to evade signatures.

> *The key takeaway is that malware is not that different. It behaves the same way and does the same things.*

Every day is a zero-day

Even before malware is delivered, attackers often want to exploit a target device. These exploits are designed to take advantage of a vulnerability in software or an operating system.

These little mistakes in code can reside silently within software for years. The infamous Heartbleed vulnerability existed in Open SSL years before it was discovered. With the vast amount of software, operating systems and updates that are written on a daily basis, the opportunity to make mistakes is massive.

Just as signatures only detect threats that are already known, this is also true of vulnerability detections. Intrusion prevention system (IPS) signatures only apply to vulnerabilities that are already known. Zero-day vulnerabilities refer to vulnerabilities that exist but are not known to the general security community.

These 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.

Nation-states closely guard knowledge of zero-day vulnerabilities and use them for their most sophisticated attacks. But even though the vulnerability and its corresponding exploit are unknown, the attack behavior that follows remains the same.

> *Zero-day vulnerabilities are virtually impossible to detect via signatures.*

For example, the Duqu 2.0 malware, which was identified in June 2015, is a new version of the Duqu threat actor, which is related to the infamous Stuxnet worm.

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

A deeper analysis of Duqu 2.0 shows the importance of using of behavior-based systems to detect advanced attacks, rather than relying on signatures or third-party reputation lists.

Duqu 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 deliver MSI packages to infect other hosts.

Once again, it's the core behavior of the attack that creates an indelible marker. If we focus on the actions that an attacker needs to perform to infiltrate a network and steal data, we can detect even the most advanced attacks.

The Vectra difference: A world without signatures

Vectra introduces a new approach to detecting threats that does not depend on signatures or reputation lists.

Instead of attempting to create a unique fingerprint for each individual threat, Vectra seeks out the fundamental actions and behaviors that threats must perform to succeed.

If you think of a sentence as an analogy, signatures try to give every subject a proper name, while Vectra focuses on the verb. While the names may change, the malicious action remains the same.

> *"Vectra is amazingly easy. There are no filters to configure. No signatures or reputation lists to update."*
>
> *Dr. Hernan Londono*
> *Associate CIO*
> *Barry University*

Some of the latest network attacks illustrate this point. In the case of the recent Duqu 2.0 threat, highly sophisticated attackers infiltrated a prominent security firm by exploiting zero-day vulnerabilities. And while these exploits were effectively invisible, the attacker behaviors remained predictable and observable.

The attackers first performed internal reconnaissance to map the internal network. Then they used pass-the-hash techniques to move laterally. Finally, the attackers delivered new malicious payloads to a variety of hosts within the network.

Vectra leverages a combination of data science, machine learning and behavioral analysis to identify all phases of an attack – including command and control, botnet monetization, internal reconnaissance, lateral movement and data exfiltration – without requiring signatures or reputation lists. Here are specific examples:

- **Internal darknet scans and port scans** – These Vectra detections reveal an attacker mapping out the internal network and identifying available services on any newly found hosts.
- **Kerberos client activity** – This detection reveals a number of attacks, such as the use of stolen credentials and pass-the-hash attacks, which enable attackers to move laterally within a network. While there are many variants of pass-the-hash, Vectra can identify the fundamental behavior they have in common.
- **Automated replication** – This detection reveals a particular host propagating similar payloads throughout the network, such as the malicious MSI packages used to infect additional hosts.

> *"With Vectra, I don't need any more signature-based products or reputation lists."*
>
> *Bryan McClenahan*
> *Senior Information Security Analyst*
> *Santa Clara University*

Detecting threats the first time

Attackers and malware use URLs for a variety of malicious behaviors, ranging from delivering malware to sending and receiving command-and-control. For this reason, security solutions continuously write signatures and build reputation lists for malicious URLs.

But with an endless supply of URLs, attackers can simply create new ones as needed. This can be done in a highly automated way using domain-generation algorithms (DGAs), which ensures that attackers will always be several steps ahead of you.

Using data science, Vectra breaks this call-and-response cycle and identifies algorithmically-generated domains the first time they are used. In this case, the attackers depend on the ability to create predictable computer-generated URLs. But data science models proactively recognize the difference between computer-generated URLs and more human-readable URLs seen in legitimate sites.

Revealing threats in SSL without decryption

Attackers always look for new ways to hide their traffic, and one of the most successful methods involves tunneling their traffic within another allowed protocol. With tunneled behavior, the attacker's communication is so customized that it's almost impossible to detect the internal protocol via traditional means.

For example, the attacker may use normal benign HTTP communication as a vehicle but embed coded messages in text fields, headers or any number of parameters within the session. By riding within an allowed protocol, the attacker can communicate back and forth without detection.

Vectra software is uniquely suited to identify this type of evasion. Unlike an IPS or next-generation firewall that may attempt to decode the protocol, Vectra applies data science to the communication pattern itself.

If an HTTP session is carrying a hidden second conversation, there will be discernible patterns in the timing, volume and sequencing of traffic. By learning these patterns, Vectra can identify hidden tunnels within HTTP, HTTPS and DNS.

> *"Rather than relying on signatures to identify threats, Vectra implements machine learning techniques that observe network behavior over time."*
>
> *Tony Palmer*
> *Senior Lab Analyst*
> *Enterprise Strategy Group*

Time to break the rules

As organizations become more threat-aware, billions of dollars are being spent on information security. Unfortunately, the barrage of news about network security breaches indicates that tried-and-true methods are failing and attackers are gaining ground. While signatures can be valuable, it's now clear that they are insufficient on their own, especially when facing sophisticated attackers.

It's time for security professionals to break the rules. With Vectra, organizations can build their defenses around how attackers behave as they attempt to spy, spread throughout the network, and steal valuable information. And that changes the game entirely.

VECTRA®

Email info@vectranetworks.com **Phone** +1 408-326-2020 www.vectranetworks.com