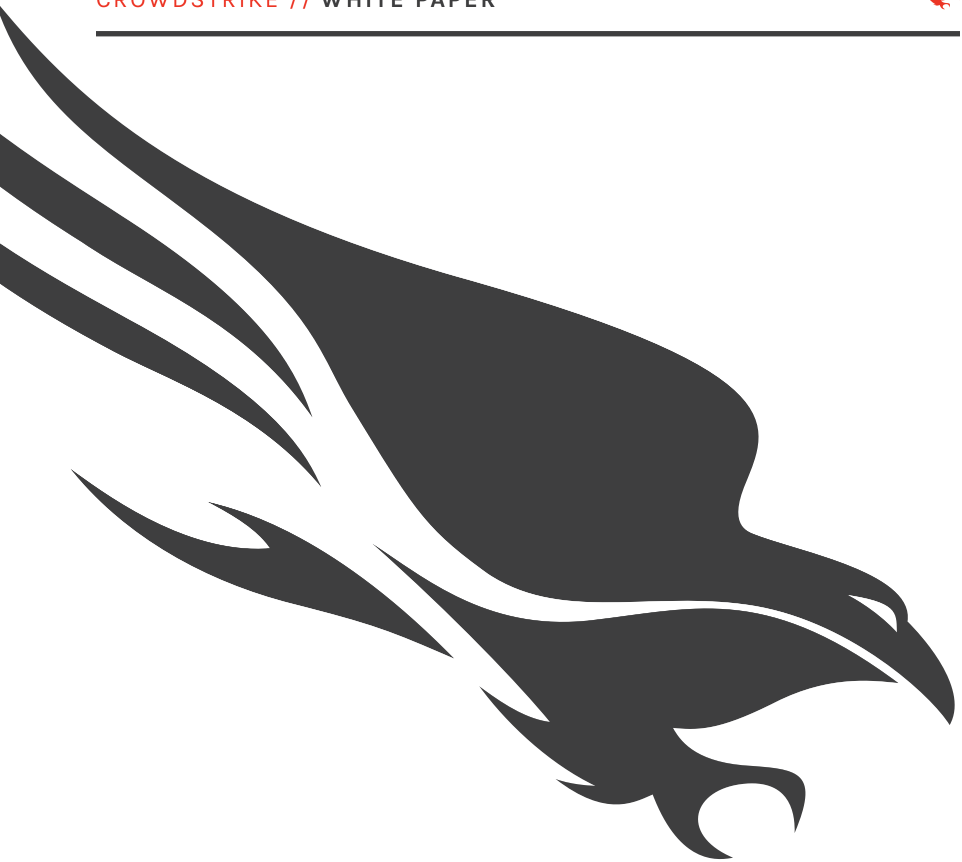
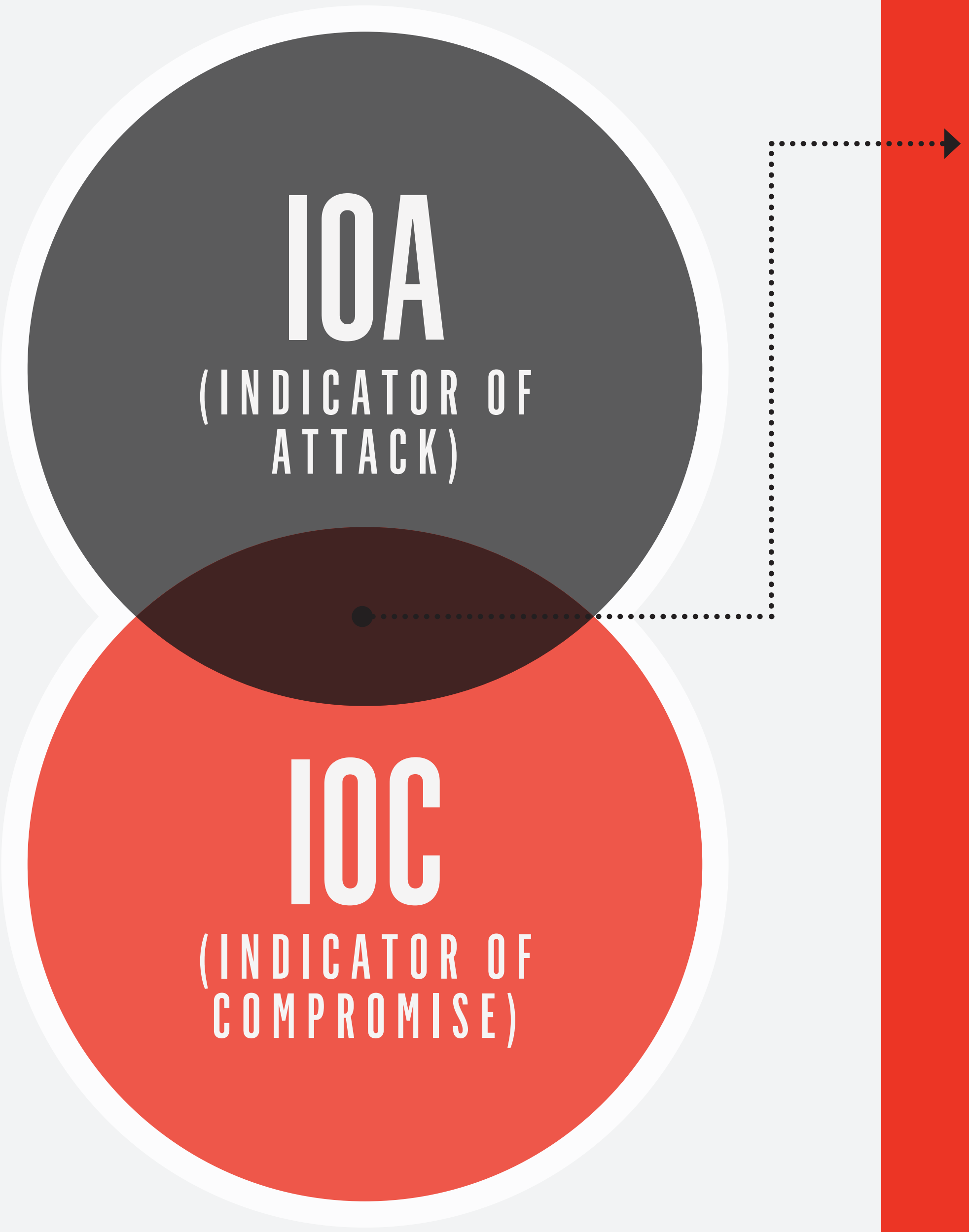
CROWDSTRIKE // WHITE PAPER



INDICATORS OF ATTACK VERSUS INDICATORS OF COMPROMISE

WWW.CROWDSTRIKE.COM



IOA

(INDICATOR OF ATTACK)

IOC

(INDICATOR OF COMPROMISE)

WHAT'S THE **DIFFERENCE?**

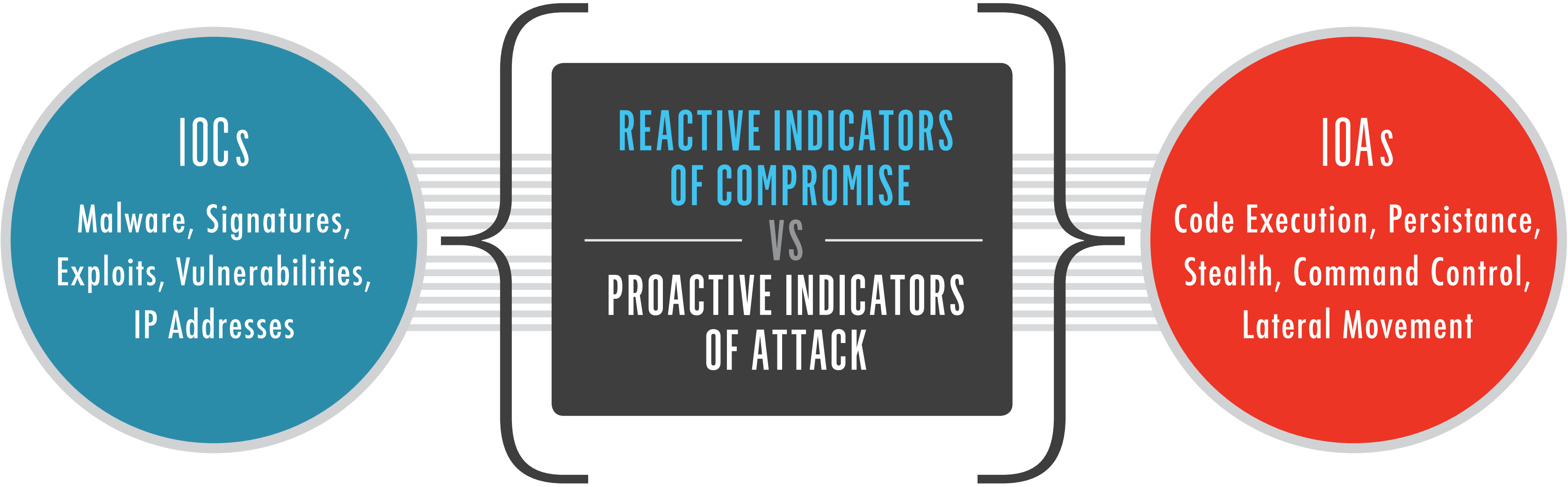
The threat level has never been higher for organizations charged with protecting valuable data. In fact, as recent headlines will attest, no company or agency is completely immune to targeted attacks by persistent, skilled adversaries.

The unprecedented success of these attacks against large and well-equipped organizations around the world has led many security executives to question the efficacy of traditional layered defenses as their primary protection against targeted attacks. At the same time, many organizations have begun reviewing and revising their security best practices in advance of suffering a debilitating cyber attack.

Based on extensive use of CrowdStrike's next-generation endpoint protection platform to detect and prevent sophisticated attacks against large organizations, CrowdStrike's in-house team of security experts, adversary hunters, intelligence analysts and incident responders have pooled their knowledge to produce this valuable guidebook and checklist for proactively enhancing your corporate information security procedures while avoiding common mistakes and pitfalls.

FUNDAMENTAL DIFFERENCE BETWEEN IOCs AND IOAs

As the chart below illustrates, IOCs constitute a reactive posture. The presence of malware, signatures, exploits, vulnerabilities and IP addresses are typical of the evidence left behind when a breach has occurred. IOAs, on the other hand, represent a proactive stance, in which defenders are looking for early warning signs that an attack may be underway, such as code execution, persistence, stealth, command control and lateral movement within a network. It is the difference between arriving at a crime scene after the crime has taken place and trying to recreate the crime based on evidence left behind, versus being vigilant for the more subtle indicators that an attack is imminent or already in progress.



IOCs

Malware, Signatures, Exploits, Vulnerabilities, IP Addresses

REACTIVE INDICATORS OF COMPROMISE

VS

PROACTIVE INDICATORS OF ATTACK

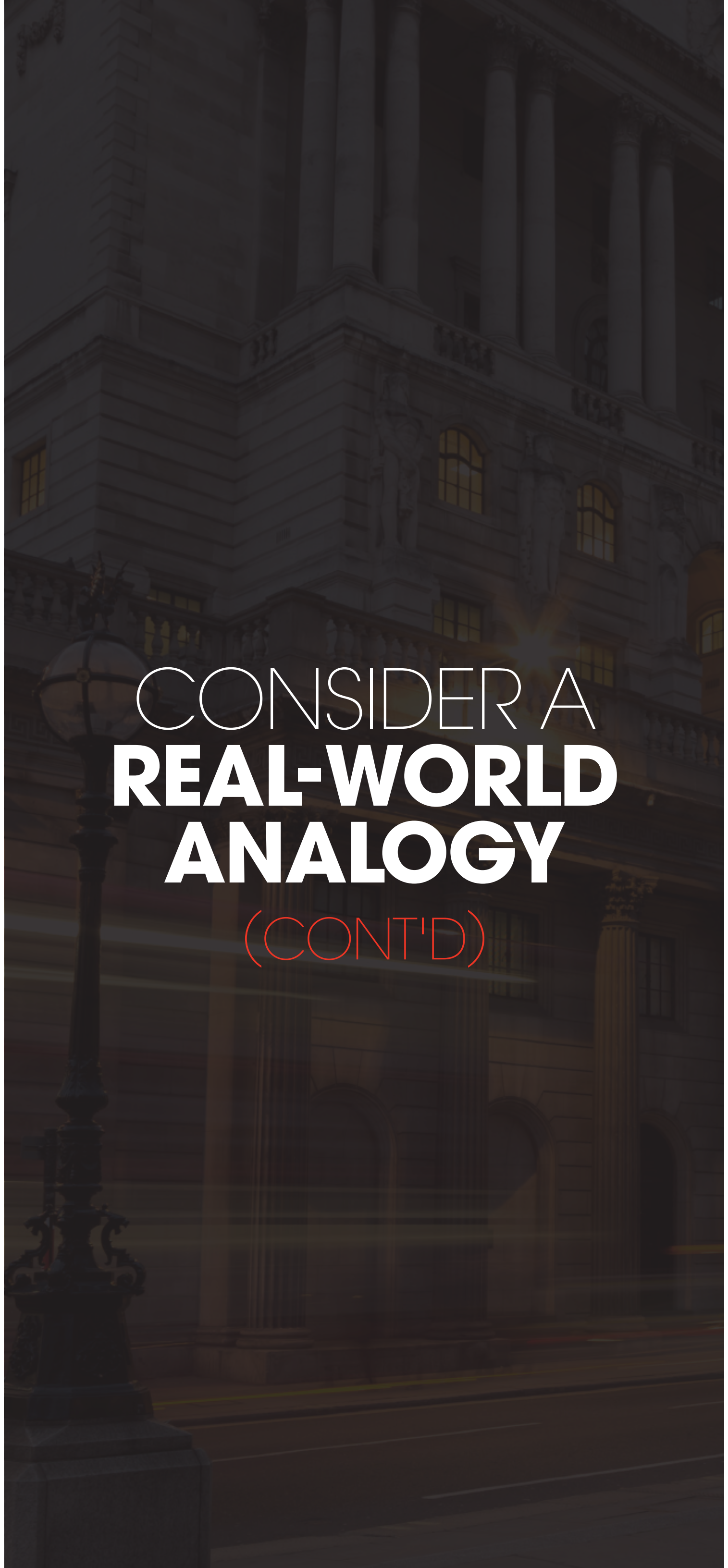
IOAs

Code Execution, Persistance, Stealth, Command Control, Lateral Movement

CONSIDER A REAL-WORLD ANALOGY

When a bank is robbed, authorities arrive after the crime has taken place and begin collecting evidence. For example, security cameras might reveal that the bank robber drove a purple van, wore a Baltimore Ravens cap, and used liquid nitrogen to break into the vault. These points of evidence are all indicators that the bank has been compromised. The money is gone, but the evidence trail could eventually lead to the perpetrator – unless the criminal changes his modus operandi (MO). What happens when the same individual instead drives a red car to his next crime, wears a cowboy hat and uses a crowbar to access the vault? The result is another successful robbery, because the surveillance team relied on Indicators of Compromise (IOCs) that reflected an outdated profile.

However, if investigators were using an approach built around Indicators of Attack (IOA's), the outcome could be very different. For example, a smart thief would begin by "casing" the bank, performing reconnaissance and understanding any defensive vulnerabilities. Once he determines the best time and tactics to strike, he proceeds to enter the bank. The robber disables the security system, moves toward the vault, and attempts to crack the combination. If the team protecting the bank could detect those behaviors that typically precede a successful robbery – in other words, had they been capable of identifying Indicators of Attack (IOAs) – they might have foiled the attempt before a single dime was removed from the bank's premises.



CONSIDER A REAL-WORLD ANALOGY (CONT'D)

In the case of an information breach, IOCs might include a variety of electronic evidence left behind, such as an MD5 hash, a C2 domain or hardcoded IP address, a registry key, filename, etc. These IOCs are constantly changing, however, making a proactive approach to securing the enterprise impossible. Because IOCs represent a reactive method of tracking the bad guys, by the time you find an IOC, there is a high probability that you have already been compromised.

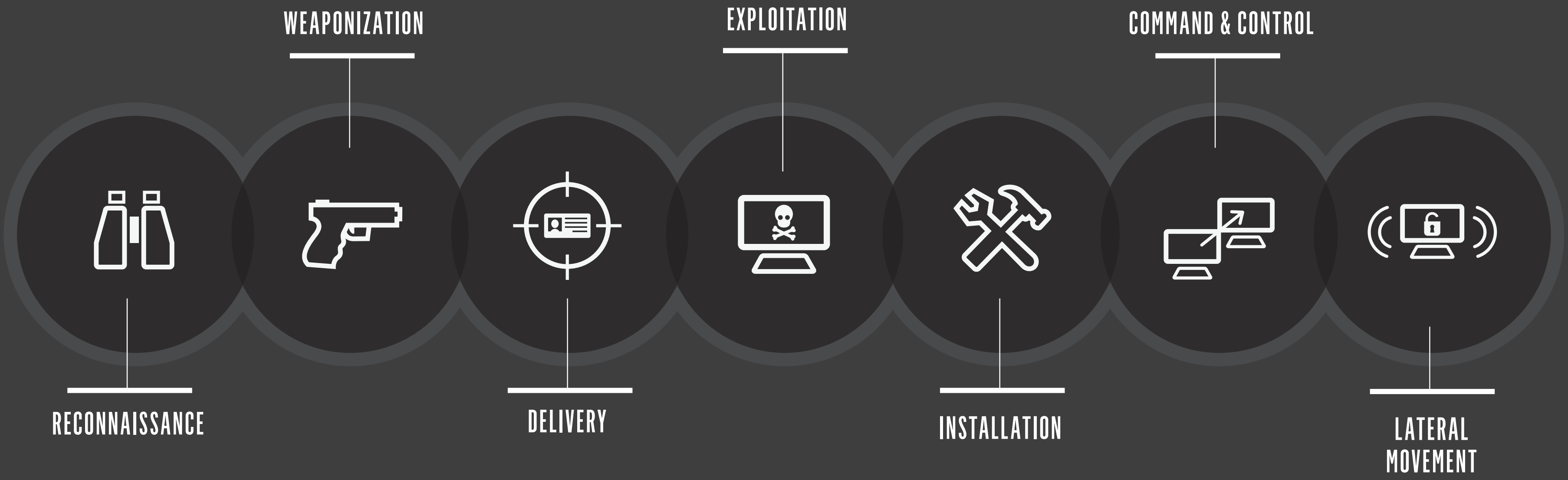
In contrast, an IOA in the cyber world represents a series of actions that an adversary must conduct in order to succeed. If we break down the most common – and still the most successful – tactic of determined adversaries, the spearphishing attack, we can illustrate this point.

A successful phishing email must persuade the target to click on a link or open a document that will infect the machine. Once compromised, the attacker will silently execute another process, hide in memory or on disk and maintain persistence across reboots of the system. The next step is to make contact with a command and control site, informing his handlers that he awaits further instructions.

IOAs are concerned with the execution of these steps, which expose the intent of the adversary and the outcomes they are trying to achieve. IOAs are not focused on the specific tools criminals use to accomplish the objectives, and are thus more adaptable to the ever-changing tactics they employ to accomplish their goals.

By monitoring these execution points, gathering the indicators and analyzing them, we can determine how an actor successfully gains access to the network, and we can infer intent. No advance knowledge of the specific tools or malware (IOCs) is required to stop the attack while it's still in progress. In fact, IOAs can detect attacks where no malware is present.

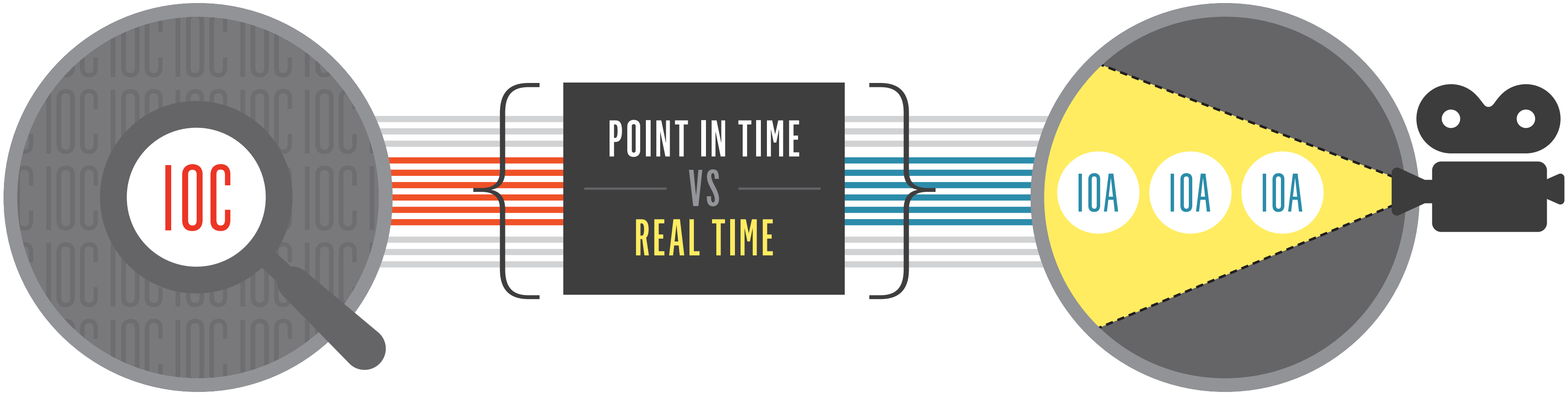
INDICATORS OF ATTACK



IOAs PROVIDE REAL-TIME RECORDING & VISIBILITY

A by-product of the IOA approach is the ability to collect and analyze exactly what is happening on the network in real-time. The very nature of observing the behaviors as they execute is equivalent to observing a video camera and accessing a flight data recorder within your environment.

By recording every action as it takes place, IOAs show you exactly how an adversary slipped into your environment, accessed files, dumped passwords, moved laterally in your network, and perhaps eventually exfiltrated your data.



EXPLORING REAL-WORLD ACTIVITY THAT ELUDES **EXISTING DEFENSES**

CrowdStrike's Intelligence Team documented the following example activity attributed to a Chinese actor. The following example highlights how one particular adversary's activity eluded existing defenses.

THIS ADVERSARY USES THE FOLLOWING TRADECRAFT:

{1} In memory malware – never writes to disk
{2} A known and acceptable IT tool – Windows PowerShell with command line code
{3} Cleans up logs after themselves leaving no trace

Let's explore the challenges that other endpoint solutions have with this tradecraft:

Anti-Virus – since the malware is never written to disk, most AV solutions set for an on-demand scan will not be alerted. On-demand scanning is only triggered on a file write or access. In addition, most proactive organizations perform a full scan only once a week because of the performance impact on the end user. If defenders were performing this full scan, and if the AV vendor was able to scan memory with an updated signature, they may provide an alert of this activity.

AV 2.0 Solutions – these are solutions that use machine learning and other techniques to determine if a file is good or bad. PowerShell is a legitimate Windows system administration tool that isn't (and shouldn't be) identified as malicious. Thus, these solutions will not alert clients to this behavior.

EXPLORING REAL-WORLD ACTIVITY THAT ELUDES **EXISTING DEFENSES** (CONT'D)

Whitelisting – Powershell.exe is a known IT tool and would be allowed to execute in most environments, evading whitelisting solutions that may be in place.

IOC Scanning Solutions – since this adversary never writes to disk and cleans up after completing their work, what would we search for? IOC's are known artifacts and in this case, there are no longer artifacts to discover. Moreover, most forensic-driven solutions require periodic "sweeps" of the targeted systems, and if an adversary can conduct his business between sweeps, he will remain undetected.

MOVING TO NEXT-GENERATION PROTECTION

At CrowdStrike, we know that our clients face much more than just a malware problem. In fact, studies indicate that 60 percent of data breach incidents don't even involve the use of malware. True next-generation endpoint protection addresses the full range of attacks -- known and unknown, with or without malware -- by combining conventional IOC-based endpoint protection with IOA analysis. When delivered in real time via cloud architecture, IOA technology adds contextual and behavioral analysis to detect and prevent attacks that conventional defense-in-depth technologies cannot even see.

This innovative approach allows enterprise security professionals to quickly discern the tactics, techniques and procedures used by sophisticated attackers. In this way, we can determine who the adversary is, what they are trying to access, and why.

ABOUT CROWDSTRIKE

CrowdStrike™ is a leading provider of next-generation endpoint protection, threat intelligence, and pre- and post incident response services. CrowdStrike Falcon is the first true Software as a Service (SaaS) based platform for next-generation endpoint protection that detects, prevents, and responds to attacks, at any stage - even malware-free intrusions. Falcon's patented lightweight endpoint sensor can be deployed to over 100,000 endpoints in hours providing visibility into billions of events in real-time.

CrowdStrike operates on a highly scalable subscription-based business model that allows customers the flexibility to use CrowdStrike-as-a-Service to multiply their security team's effectiveness and expertise with 24/7 endpoint visibility, monitoring, and response.

Request a demo of CrowdStrike Falcon
and learn how to detect, prevent, and respond to attacks, at any stage - even malware-free intrusions.
http://www.crowdstrike.com/request-a-demo

CROWDSTRIKE | WWW.CROWDSTRIKE.COM | @CROWSTRIKE