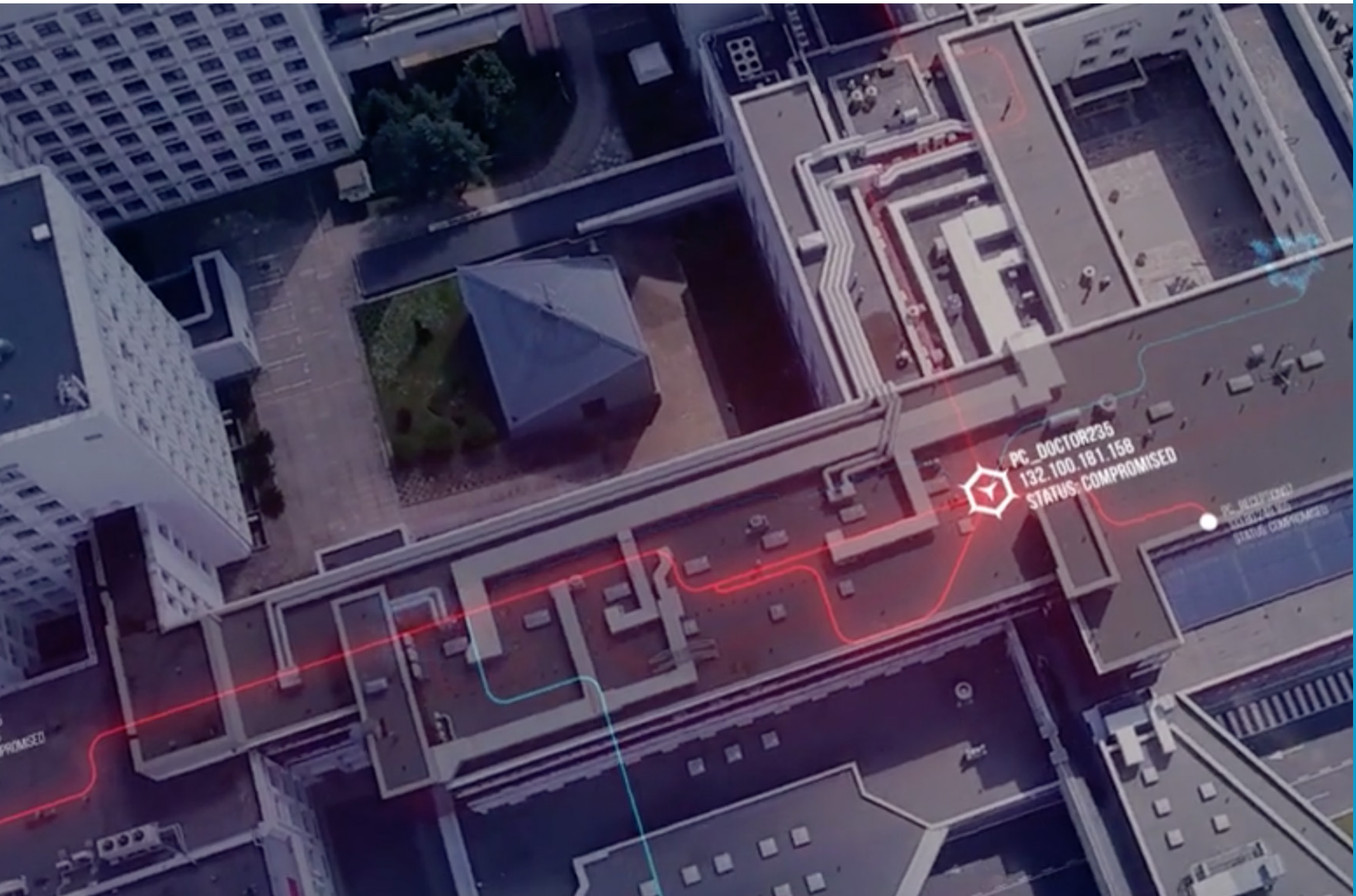
cybereason

The End Game: Exploiting Attacker Weak Spots with TTP-based Detection

Indicators of compromise (IOCs) are a losing battle for security teams as they are easily changed by the attackers. Adopting a detection strategy based on Tactics, Techniques, and Procedures (TTPs) returns power to the defender.



Chasing IOCs: A static approach

First we should supply a definition of Indicators of Compromise (IOCs). IOCs are artifacts observed on a network or in an operating system that, when discovered, indicate an intrusion with a high degree of confidence. Typical IOCs include virus signatures, IP addresses, MD5 hashes of malware files and URLs or domain names of botnet command-and-control servers.

IOCs supply the good guys with a reactive method for spotting the bad guys. When you find an IOC, you've most likely already been compromised. IOCs are detected during post-breach forensics work that identifies the artifacts left in the network and on endpoints. After the IOCs have been detected at a few organizations, they are shared with the greater security community and can then be used by intrusion detection systems and antivirus software for early detection of future attack attempts.

While security professionals can easily build detection rules and mechanisms based on IOCs discovered in previous cyber attacks, these artifacts are just as easy for attackers to modify, making securing the enterprise impossible.

Attackers use a variety of mechanisms to generate multiple random artifacts that will not be spotted by IOC-based detection tools, making this approach unuseful for detecting both sophisticated and more common attacks.

Changing hash values and signatures is only a matter of either rebuilding or obfuscating malicious code, which is done automatically in some commodity programs like the Angler exploit kit. Maintaining a supply of IP addresses is simple to accomplish by using botnets, hacked servers, anonymous hosting or a domain generation algorithm (DGA) mechanism, ensuring there's a constant supply of domain names that can host malware and are never reused. As for host artifacts, their URLs can be randomized and payloads can be fully randomized, which is a feature commonly found in malware.

Falling for the attacker's deception plan

Attackers use IOCs as a deception tool: they implant tools with known IOCs to distract security teams from the main operation, in which they use new, never-before-seen tools, or tools that have the ability to periodically generate new artifacts. An incident response approach that only uses static IOCs leads security teams to falsely believe they have detected and remediated an entire attack. In reality, security teams usually only find the part the hackers wanted them to discover.

While in the past only nation-state attackers were able to offset IOC-based detection tools and build new-to-the-world, targeted malware tools, or ones that can mutate to change the artifacts left in the attacked environment, cyber criminals are increasingly adopting these techniques. They're purchasing tools from the dark Web or visiting certain websites to learn tactics. With information on how to hack like the Russians or Chinese easily accessible online, the ability to conduct a nation-state attack has become a commodity. Now anyone can become a nation-state attacker.

TTPs: The attack's static components

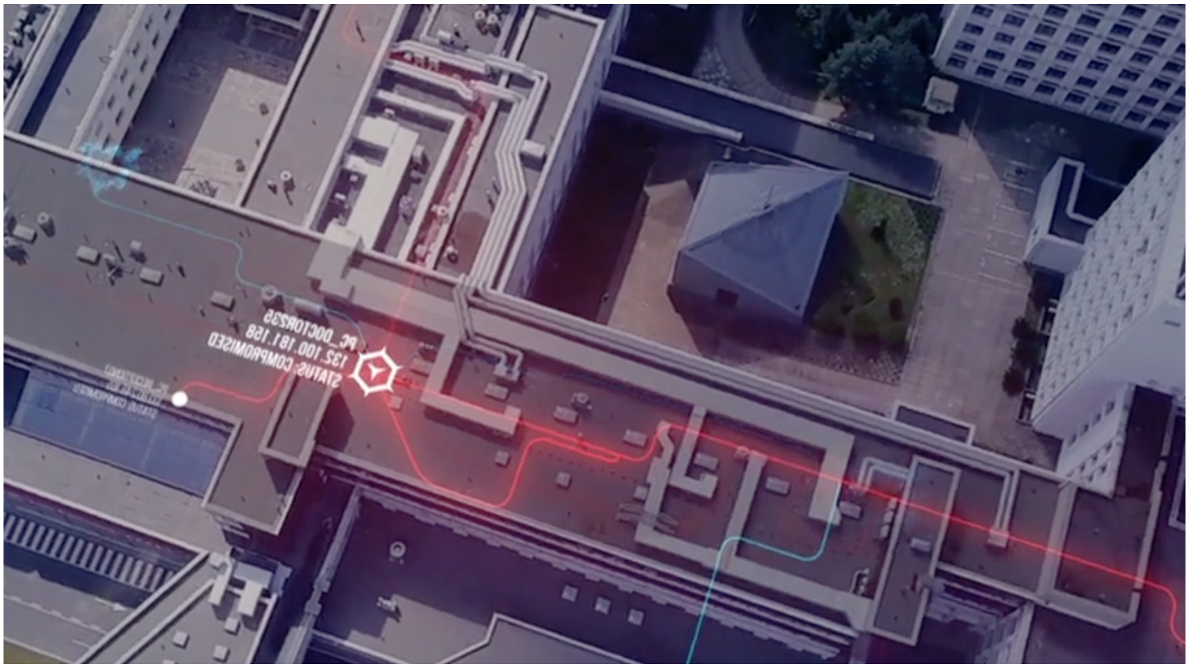
When planning an attack, hacking teams choose a set of tactics, techniques and procedures (TTPs) to use in the hacking operation and stick with them. There's a finite number of techniques available to hackers; developing an entirely new technique would take a great deal of time and knowledge of the target's systems.

Detecting TTPs is a more effective approach to discovering attacks. This methodology targets the behavioral elements of an attack, which are much more difficult for an attacker to change.

Consider the effort that goes into developing a tool, for example. The process attackers use to create a hacking tool isn't different from the one used by vendors to build legitimate software. In both situations, a research and development team develops a prototype, tests it and eventually shapes it into a tool, a process that can take months. Once the defender detects the tool, attackers can probably swap it out for another one from their toolset. But there is a limited number of tools attackers can immediately use. Building a new toolset takes time and effort. The same is true for the tactics and techniques used in an attack: once the attacker has chosen a specific attack vector, switching to another one requires substantial time and effort, making it hard for the adversary to change. Given the amount of time development takes, attackers have a limited supply of tools, making TTPs impossible to scale.

And that's a key issue when discussing the problem with IOC detection: it targets the parts of an attack that are easily scalable. In fact, an entire operations team is dedicated to changing the scalable parts of an attack based on how the defender responds. The infrastructure to carry this out is put in place before the attack is launched, allowing changes to be made within days or even hours. They have stockpiled stolen credit cards for purchasing domain names and can use DGAs to generate a stream of IP addresses. By focusing on IOC detection, security teams are fighting a losing battle against the ever-changing aspects of an attack.

Discovering the TTPs and tools an adversary uses gives defenders a much better chance at detecting a complete attack campaign since attackers change them less frequently.



CASE STUDY

How a large financial services company discovered the shortcomings of IOCs

The organization, a large financial services company with 120,000 employees and a sophisticated incident response team, detected data exfiltration to an unknown location. Forensics analysis of the compromised endpoint revealed the domain names and IP addresses used by the command-and-control servers as well as scheduled tasks to maintain persistence.

The incident response team then searched the organization for other endpoints that shared the same IOCs, but only discovered one: the machine that was already compromised. Shortly after these IOCs disappeared from that specific machine.

This pattern repeated itself for the next six months on dozens of computers: data exfiltration to an unknown location was detected on a set of endpoints and IOCs were harvested in an effort to spot other compromised machines. However, the IOCs were only present on the infiltrated machines and later vanished.

Every forensics investigation revealed that each endpoint connected to different IP address and to a unique domain name. The incident response team realized the attacker was using a variety of IP addresses and hashes on each compromised endpoint and frequently changing them to evade detection. But this information wasn't enough to stop the attack since it was impossible for the incident response team to predict the various IOCs and find the source of the compromise.

The organization worked with Cybereason's incident response team and deployed the Cybereason platform across its endpoint environment. The Cybereason Hunting Engine is designed to detect an attack's TTPs and the behaviors used by the hackers.

At the end of a five-day search, Cybereason discovered a total of 3,000 compromised endpoints. From an IOC perspective, each machine had a unique set of IOCs that changed daily. Tens of thousands of IOC combinations were likely used, preventing a remediation approach based on IOC detection from successfully stopping the attack. However, from a TTP perspective, only seven techniques were used, including three specific lateral movement techniques, DGA for command-and-control communication and DLL injection.

TTP detection returns the power to the defenders

Adopting a detection strategy based on TTPs or attacker behavior shifts the balance of power to the defender. Instead of chasing slightly modified attack tools and static IOCs that an attacker can easily change, TTP-based detection goes after an attacker's core methodologies. Every TTP and behavior that's exposed forces an attacker to either exit the environment or completely revamp the campaign within the operation's timeframe, a task that's challenging for even the most sophisticated threat actors. Looking for TTPs turns an attacker's most important assets into weak spots that can expose an entire hacking operation if they are discovered.

About Cybereason

The Cybereason Detection and Response Platform leverages big data, behavioral analytics and machine learning to uncover, in real-time, complex cyber attacks designed to evade traditional defenses. It automates the investigation process, connects isolated malicious events and visually presents a full malicious operation. The platform is available as an on-premise solution or a cloud-based service.

Cybereason Inc. is privately held and headquartered in Boston with offices in Tel Aviv and Tokyo.

GET A DEMO

To see the benefits of switching to a TTP-based detection approach with the Cybereason prevention, detection, and response platform.