CASE STUDY

Mobile Device Maker Adds EDR Technology for Rapid Detection of Attacks

THE CUSTOMER

A mobile device manufacturer with annual revenue in the millions of dollars

THE PROBLEM

The company needed a way to detect threats without flooding its analysts with alerts

Detection of never-before-seen threats

Better use of scarce security resources

Effective incident response

CHALLENGE: THE FAILURE OF IOC-BASED DETECTION

Relying on indicators of compromise to detect network intrusion was a losing proposition for the security team of this large mobile device manufacturer. After chasing alerts triggered by IOC artifacts in various security solutions, the company's security team realized this method wasn't helping them quickly detect and shut down threats. The security analysts realized that attackers could easily change malware hashes, virus signatures, IP addresses and other IOC artifacts to avoid detection. Since the organization's antivirus software and firewall solutions weren't updated with the malware's modified hashes or the new, malicious IP addresses, these threats infiltrated the company's network.

THE ALTERNATIVE: BEHAVIOR-BASED DETECTION

The organization's CISO wanted an endpoint detection and response platform that used behavioral analysis to discover attacks. To him, a combination of endpoint data collection and behavioral analytics would provide a more accurate way to determine what was occurring in the company's environment.

"The IOCs will be out of date pretty much as soon as they're discovered so nobody else can use them. I [want to] find something bad on my network because it shows characteristics of doing bad things, not because [it had an artifact] that triggered an alarm," he said.

SPOTTING AN ATTACK DURING A PROOF OF CONCEPT

Intrigued by Cybereason's ability to use behavior to detect attacks and eliminate data overload by linking suspicious activities together into a complete attack story, the company deployed the platform on 2,500 endpoints during a proof of concept.

The company deployed Cybereason in the cloud and was able to start hunting for attacks a few hours after deployment. **The platform provided value immediately: four days after rollout, Cybereason detected a few computers in a regional headquarters connecting to a server in a location where the organization didn't conduct business.**

Using Cybereason, analysts were able to see that attackers were using domain generation algorithms (DGAs) to connect to command-and-control servers. Cybereason spotted this by looking for behaviors associated with DGAs, such as the ratio of resolved to unresolved queries or the process it was launched from. For example, if domain requests are related to a process launched out of a non-Web browser program and none of the queries are resolved, this is extremely suspicious. Many tools, including the one used by the mobile device maker, do not provide process-level information or information on whether the queries have been resolved. Without this information, DGAs can be easily missed or there could be a high false positive rate of legitimate activity being flagged as DGAs.

STOPPING THE BIG DATA DELUGE

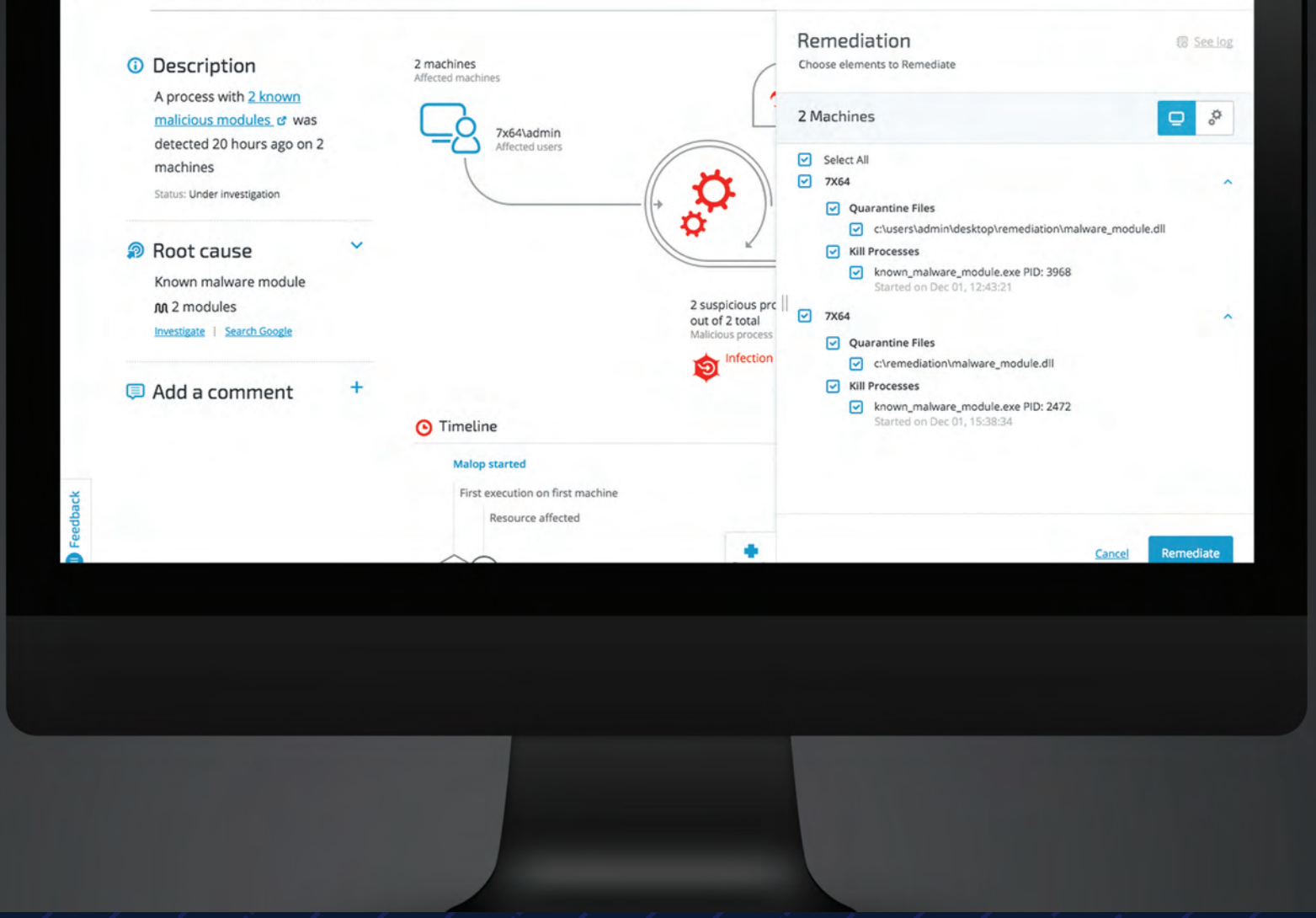
While assessing the Cybereason platform, the company also considered several competing endpoint detection and response platforms that performed behavioral-based detection. None of them presented data in a way that was easy for analysts of all skill levels to understand and use to eradicate threats. Big data is only useful if you're able to find meaning in it, the CISO said.

"More information is not always better because it muddies the waters," he said.

In many of the competing products the company considered, the collected endpoint data was placed in a database and required an analyst to extract value from it. But finding meaningful information in such a huge amount of data required multiple complex searches and knowing what to look for, the CISO said. *"That's hard because there are too many different ways for bad guys to disguise themselves,"* he said.

IMMEDIATE THREAT INFORMATION WITHOUT SIFTING THROUGH MASSIVE AMOUNTS OF DATA

By using Cybereason, the company's analysts detected threats more effectively, the CISO said. Instead of forcing them to dig through data stored in an unwieldy database, Cybereason automatically analyzed the data and told the analysts what threats were present.



"Cybereason focuses on what's actually happening. It's like the difference between using a phone book and Google."

- Chief Information Security Officer

With the user interface, analysts checked the entire enterprise to see, for example, if malware had spread to other machines, if any data had been exfiltrated and what users were affected, among other features. This level of visibility is critical since organizations always have multiple infections, the CISO said. *"No other tools are providing that level of data to analysts,"* he added.

All of the company's analysts, regardless of skill level, were able to use Cybereason to detect and stop advanced attacks. Like all companies, this organization struggles to find and retain skilled security workers. Cybereason allowed the company to essentially expand the skill level of its analysts without having to hire additional staff. With Cybereason, level 1 analysts were able to examine malicious operations detected by the platform, eliminate false positives and remediate all known threats.

IMPROVED INCIDENT RESPONSE WITHOUT COMPLEX INVESTIGATIONS

Having access to the right data improved the company's laborious incident response process, said the CISO, who called it a *"bang-my-head-on-the-wall way of doing things."* Previously, the company re-imaged every potentially compromised machine without knowing if this step was necessary. The organization used Cybereason to quickly gather data about what exactly happened on its endpoints and avoid the hassle of re-imaging all machines, he said.

"Before Cybereason, every time you had an alert on an incident, you had to pull out the police tape and dust for fingerprints, and 90 percent of the time you found that nothing happened," the CISO said. *"Investigating incidents under the old process involved the time of four employees and spending large amounts of money on third-party incident response teams for nothing in return."*

ENHANCING EXISTING SECURITY TOOLS

The company also used Cybereason to improve its security toolset. For example, if Cybereason detected a new malicious tool, its hash was added to the company's antivirus program to prevent re-infection. This was especially appealing to the CISO since most security vendors can only provide customers with information on previously known threats. Unfortunately, by the time security vendors know about a threat, hackers are already using new attack methods. *"The new security paradigm is you against the world,"* he said.

Cybereason closed the gap from unknown to known: a never-before-seen threat was detected based on its behavior, and immediately its signatures and hashes were added to the company's static detection tools. This led to a faster response cycle and better protection for the organization.

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.

Founded by members of the Israeli intelligence agency's elite cyber security Unit 8200, Cybereason mirrors the founders' expertise in managing some of the world's most complex hacking operations. Cybereason developed the world's only military-grade, real-time detection and response platform and has a proven track record of protecting global enterprises. The company has received many awards and accolades since its founding. Cybereason is privately held and headquartered in Boston with offices in Tel Aviv, Tokyo, and London.