CASE STUDY

A large financial services company resolves an evolving APT with behavior-based detection

BACKGROUND

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. Every forensics investigation revealed that each endpoint connected to different IP address and to a unique domain name.

CHALLENGE

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 Indicators of Compromise (IOCs) and find the source of the compromise. Typical IOCs include virus signatures, IP addresses, MD5 hashes of malware files and URLs or domain names of botnet command-and-control servers.

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, IOCs were harvested in an effort to spot other compromised machines, but the IOCs were only present on the infiltrated machines and later vanished.

APPROACH

The organization worked with Cybereason's incident response team and deployed the Cybereason platform across its endpoint environment. Rolling out the Cybereason sensors on 5,000 of the bank's PCs and servers only took a few hours and didn't interfere with business operations.

The Cybereason Hunting Engine is designed to detect an attack's Tactics, Techniques, and Procedures (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, Domain Generator Algorithms (DGA) for command-and-control communication and DLL injection.

BENEFITS

Because the organization deployed the Cybereason platform, adopting a detection strategy based on TTPs, the security team was able to shift the balance of power back to the good guys. Looking for TTPs turns an attacker's most important assets into weak spots that can expose an entire hacking operation if they are discovered.

- **Cybereason showed how TTP-based detection leads to faster threat remediation compared to approaches that use IOCs**
- **Cybereason provided immediate value by quickly detecting an advanced attack**
- **Fast endpoint sensor deployment without disrupting business operations**

cybereason

cybereason.com
200 Clarendon St, Boston, MA 02116