eSENTIRE

INCIDENT REPORT:

# You're Only as Strong as Your Weakest Link

*A cautionary tale about third–party risk*

## Attack Types:

Cobalt Strike

## Industry:

Legal

## The Threat:

Legal entities and court systems store sensitive and confidential information. Due to the nature of the data they keep on file, maintaining data security to ensure client confidentiality is critical to protecting brand reputation and continued business operations.
No matter how mature an organization's security posture is, they are only as safe as their weakest link.

This was the case for one eSentire customer in the legal industry who experienced a Cobalt Strike attack via a 3rd party partner. Fortunately, eSentire's Security Operation Center (SOC) leveraging MDR for Endpoint's proprietary machine learning capabilities detected the threat actor presence and mitigated the threat before exfiltration could occur.

## Who is Patient Zero?

In this cautionary tale of third-party risk, it is unknown who patient zero was, as the attack originated with the customer's business partner who had access to their network. This did not affect eSentire's ability to stop the attack but it put a wrinkle in the investigation, as there was not access to complete data to see where and how the attack originated.

## The Initial Alert

eSentire's proprietary machine learning module, BlueSteel, alerted the Security Operation Center (SOC) to malicious PowerShell activity on one of the customer's machines. Via the MDR for Endpoint service, the security analysts went to the dashboard to view the alert and spotted the malicious activity. There was a connection to an external IP address, which indicates a Command and Control channel. The SOC alerted the customer and began their investigation.

## The Investigation

eSentire's security analysts began their investigation by looking for lateral movement. They discovered fourteen other machines communicating with the malicious IP address, so they alerted the customer to lateral movement and flagged the security event in the eSentire SOC.

Further investigation uncovered that the PowerShell command was being used to inject malicious code into the memory of each machine. That code was the Cobalt Strike Server Message Block (SMB) beacon, which opens a backdoor that allows the attacker to remotely control the machine.

## What is Cobalt Strike?

*Cobalt Strike is a commercial penetration testing tool designed to simulate targeted attacks and emulate the post-exploitation actions of advanced threat actors. Cobalt Strike contains numerous features used to avoid detection and has flexibility in deploying many types of malicious payloads while providing the tools to manage compromised assets, which has made it a tool of choice for cybercriminals who use it to gain access to networks and move laterally, looking for valuable data. If high-value data is found, ransomware is often deployed.*

The eSentire Security Analysts observed two movement techniques deployed by the attacker. The first was a file copy (the SMB beacon) to the admin share folder on the machines that was accessible from the network. This technique was not working for the attacker, however, as it was most-likely being blocked by the customer's antivirus. Due to that failed attempt, the attacker deployed a second technique using Windows Remote Management (WinRM).

eSentire Analysts observed the WinRM activity and saw correlation to successful WinRM sessions on each lateral machine movement, all originating from one machine that did not have eSentire's MDR for Endpoint protection installed on it. We were, however, able to see that it was that one machine that was sending out the SMB beacon.

## Introducing a "Special Guest"

With no endpoint visibility on the originating machine, eSentire was unable to go any further with the investigation. That created a "hop" in the investigation of the lateral movement. The customer did some digging and informed us that the machine shared a Network Segment (Subnet) with some third-party providers. They informed us that the infection actually originated with a partner organization, and we had to work with the customer and coordinate with the partner organization to clean up the incident. eSentire worked with our customer to isolate their infected machines, and shared investigation information with the partner. Having no visibility into the partner organization, eSentire could only share the information we had with the partner and hope that they then cleaned up the attack in order to avoid reinfection.

## Threat Eliminated

Even though the attacker was able to take over several machines on the customer's network, no visible damage or exfiltration had occurred. eSentire had isolated the machines and stopped the intrusion before the attacker's intent was made clear, or their plan fully-executed. The customer disabled the infected account in order to avoid reinfection.

**If you're experiencing a security incident or breach contact us 1-866-579-2200**

eSENTIRE