USE CASE

Incident Report: Financial Services Ransomware Attempt

An investment management firm, managing roughly $12 billion in assets under management, recently encountered a known malware downloader. eSentire analysts successfully blocked the attack with eSentire Managed Detection and Response™ services.

Sound the Alarm

The eSentire Security Operations Center (SOC) sent a malware alert to the client, highlighting traffic consistent with a known malware downloader. At the time the alert came through, there was no post-infection traffic present.

In response to the alert, the client isolated the machine from the network and notified the SOC that they were experiencing, what appeared to be, ransomware. The client was assured that there would be further investigation with details of the event in question.

Initiate Human Investigation

Inside a sandbox environment, our SOC reviewed a sample of the malicious Microsoft Word document that the end user had opened. This environment allows analysts to better understand the type and behaviour of the malware used. Analysts discovered domains that would have been contacted by the macro to retrieve additional payloads but found that the command-and-control had already been blocked. They also discovered and provided the name of two files that were dropped into their system and recommended that the user change all corporate credentials as a precaution.

A Detailed Review

The client followed up with SOC analysts after resolution to gain insight and a better understanding of the situation. Analysts went into detail and walked them through every piece of information that would explain how the malware operated once the machine was infected. The client's goal was to learn as much as possible about the event to understand how it happened and how it could be managed in the future. Their response: *"BTW - eSentire ROCKS!"*

Uncovering threats quickly is critical to preventing further damage in your network. Unfortunately, recent studies clearly indicate that cyber attackers are outpacing discovery and resolution capabilities for financial services firms. Our 24x7 team of elite security analysts live inside our technology – detecting, hunting, and responding to threats around the clock. Are you at risk of a ransomware attack? Contact us to learn more about how Managed Detection and Response can help protect you.