INCIDENT REPORT:

Zero Day Attack

The Challenge:

On the morning of February 25, 2016, a Registered Investment Advisor (RIA), who employs eSentire Managed Detection and Response (MDR), was infected with ransomware. Over the next 40 minutes, eSentire analysts learned what happened, how the ransomware was deployed, and how we helped the firm resolve the situation.

Are you at risk of a ransomware attack?

Contact us to learn how eSentire Managed Detection and Response can help protect your network.

7:43 AM Patient Zero

Employees at the RIA started to receive emails from a hacker, who claimed the firm had outstanding invoices from a frequently used car service. One employee in their New York City office opened the email and downloaded the fake invoice. Within a matter of seconds, JavaScript software tried to download 87 .exe, a version of ransomware called TeslaCrypt. As a known threat, this was blocked by the blacklist through eSentire Asset Manager Protect, a feature provided by esNETWORK™. However, a second download, from an unknown IP address not yet on the blacklist, was successful. This new variant of TeslaCrypt began to install on the user's computer, as it was unrecognized as malware by the firm's firewall.

7:44 AM Initiate Human Investigation

Twenty seconds after install, the malware sent a message back to the originating IP address giving the hacker a green light to start encrypting. At the same time, it also sent an alert to the Security Operations Center (SOC) for an analyst to investigate. As it looked for files to encrypt, catching the threat quickly was critical given the quick encryption process and an ultimatum: pay a ransom or lose the data.

7:54 AM Mitigate and Escalate

SOC analysts evaluated the alert and immediately called the client directly to notify them of the ransomware in their network. In parallel, the analyst put a block in place to ensure the hacker could not infiltrate the network further, while the firm remotely deactivated the victim's connection.

8:30 AM All Clear

The client notified eSentire that the physical machine had been located, wiped clean, and separated from the network. Human monitoring, hunting, and intervention was key to discovering, isolating, and killing this unknown threat quickly. eSentire analysts had eyes on this event 60 seconds after initial infection. By contrast, another financial firm infected with a similar threat did not have the same outcome. Without human discovery, more than 700GB of data was encrypted within 5 hours. Even when they thought they had removed the threat, the incident recurred a week later.