USE CASE

Incident Report: Malware Report Showcase

The eSentire Security Operations Centre (SOC) reviews thousands of alerts daily. What sets the eSentire SOC apart from other services isn't the amount of alerts they review in a day, but the velocity in which an analyst can detect a potential threat. Our analysts take a mere 35 seconds to look at an event and determine if it needs to be escalated for further review. In some cases, like the one outlined below, the key to resolution is our ability to utilize multiple SOC resources, forensically identify new threat intelligence, and rapidly deploy that intelligence to our global network of sensors.

10:09 AM - 12:00 PM

The SOC is alerted to multiple anomalous events detected on a client's sensor. Based on the sequence and nature of the alerts, analysts realized malicious activity was occurring, and immediately, they launched a full investigation.

12:00 PM - 12:44 PM

The SOC quickly assembled a team to better understand the situation: what activity was occurring and what action the team would need to take to protect the client. An analyst started to pull information from the client's sensor and compared critical information against Cymon.io™, our proprietary threat intelligence platform. Two additional analysts began forensically investigating all signature-based signaling data from eSentire sensors, as well as reviewing all web-based Internet traffic for that location.

1:00 PM - 1:05 PM

The SOC opened a ticket with the client to escalate and establish formal lines of communication for this on-going investigation. The analyst called the client immediately and sent a detailed summary of the initial investigative findings. The customer indicated to the analyst that someone at their firm fell victim to a phishing email.

1:07 PM - 1:28 PM

As the investigation continued, the SOC pulled together a list of infected hosts, based on current intelligence. The more the analyst team continued to dig into this threat the more they were learning about the malware variant at the root of the attack. The team continued to update the client with additional intelligence as the investigation progressed.

1:42 PM - 1:45 PM

Within 14 minutes of receiving the originating phishing email, analysts were able to complete a full spectrum analysis of the threat. They identified all command-and-control traffic associated with the malware. Additionally, the team identified all of the file hashes of the payload(s). They were able to compare these findings against third-party threat intelligence platforms.

Within 3 minutes of the full analysis, our team immediately began to push new threat intelligence to eSentire's network of global sensors.

The SOC and the client were able to pin-point patient zero and determine how the threat was able to infiltrate the customer's environment. The final analysis: 39 hosts were determined to be infected with this variant of malware.

Uncovering threats quickly is critical to preventing further damage in a compromised network. Unfortunately, recent studies indicate that cyber attackers are outpacing the discovery and resolution capabilities available to many organizations. At eSentire, our 24x7 team of elite security analysts live inside our technology – detecting, hunting, and responding to threats around the clock. Is your firm at risk? Contact us to learn more about how eSentire Managed Detection and Response™ can help protect you.