esentire®

INCIDENT REPORT

In the Nick of Time

In March 2017, a new client employed esENDPOINT™ powered by Carbon Black. Within the first three days, our Security Operations Center (SOC) was alerted of an endpoint breach.

Here's the full report.

2:21 PM - 2:22 PM: The client's network started to experience unknown malicious activities. Java.exe process had been executed and spawned a child process to execute malicious java class. Minutes later, the same code spawned another child process to execute malicious Visual Basic Script, sparking an investigation within the SOC.

3:02 PM - 5:18 PM: An analyst started to dig into the activity and sent a malware alert to the client. When there was no immediate response, the analyst sent an email escalation. Meanwhile, the java.exe process continued to spawn another child process to execute more malicious code. The analyst recruited the help of the Threat Intelligence (TI) team and other SOC analysts. The client eventually responded to say that their antivirus was indicating that the malicious file had been removed from the network. However, after a reboot, the machine was still attempting to run the file.

5:40 PM - 6:10 PM: Armed with the exact file name, the analyst located another machine with the same infection and immediately isolated both machines from the network. The TI team dug further into the file and learned that the malicious code was a Java Backdoor called Adwind. At 5:55 PM, the analyst updated the client and the SOC began a meta data search to determine what network activities occurred between the endpoint and the infected server.

6:49 PM - 7:44 PM: The analyst provided the SOC with connection times and related IPs to perform an analysis. The SOC confirmed that only the SYN packets were sent, and there was no response from the infected server, which could indicate that the server was down at time of connection and no data was exfiltrated. The malicious file was provided to the Threat Intelligence team to analyze further.

2:21 PM - 2:22 PM: Throughout the search, the SOC determined the rough infection date to be February 2, and discovered that only three hosts at the firm were infected. The TI team informed the client that credentials and other sensitive information could have been stolen during the breach and advised them to perform a more in-depth incident response investigation and reset all credentials on the infected server as a precaution.

Is your firm at risk?

Contact us to learn more about how eSentire Managed Detection and Response™ can help.

Quickly uncovering threats is critical to preventing further damage in a compromised network.

At eSentire, our team of elite security analysts lives inside our technology – detecting, hunting and responding to threats around the clock.