Case Study

BINARY DEFENSE™

Binary Defense threat hunting team finds malware attack in progress at large technology firm

Business

Fortune 500 technology organization and Binary Defense customer

Challenges

International customer base that could be heavily impacted by an interruption in service if a breach occurred

Results

Binary Defense threat hunting team detected suspicious activity on the customer's network that was determined to be malware

Affected computers were taken offline to prevent further spread of the malware

Binary Defense helped customer understand the type of attack and how to remediate it, which shut down the attack

Fortune 500 company with international client base relies on Binary Defense to keep its data secure

A Fortune 500 technology firm relies on Binary Defense to monitor for suspicious activity on its network. With a vast, international client base, a breach at this firm could have wide-reaching effects, including disruption of services, as well as significant financial losses.

The firm uses Binary Defense to manage and monitor its SIEM. Additionally, the Binary Defense team performs threat hunting, a proactive service that attempts to identify new threats that may have evaded traditional security. Many security solutions, such as antivirus, are only programmed to catch known threats–allowing newer threats to pass through networks undetected. While endpoint detection programs will note suspicious activity, it takes a team of skilled analysts to determine whether the threat is real or not.

Suspicious activity detected on employee workstation

While searching for unusual events on the firm's endpoints, Binary Defense analysts found evidence that a JavaScript file had been saved to an employee's workstation as a result of a macro in a Word document that was opened from a zip file. This was suspicious enough to warrant further investigation by a Binary Defense analyst. They discovered that the JavaScript file had communicated with a web server that appeared to be compromised and used to deliver malware. The firm was notified immediately, and the affected computers were taken offline so they could not harm other computers on the network.

Skilled analysts identified threat and helped contain it

The firm needed to know whether the attack had been successful, so Binary Defense analysts followed the digital evidence to retrieve and reverse-engineer the malware payload, taking apart the anti-analysis defenses that the malware author had put in place. They quickly identified the capabilities of the malware, as well as the servers that it communicated with, and used that information to search through logs and determine whether the final stage of the attack had been successful as well as what computers it had affected. The analysis revealed that the attacker had made a mistake in a critical step of delivering the final stage of the malware.

Because the customer was promptly notified of the attack in its early stages, they were able to take quick action to stop a threat before it had a chance to harm the company. Fully understanding the attacker's methods helped the client be prepared to respond quickly in case of a repeat attack.

Learn more about Binary Defense at: BinaryDefense.com/cybersecurity-solutions