GLOBAL MANAGEMENT FIRM EVALUATES SECURITY EFFECTIVENESS USING CYBER THREAT DIAGNOSTICS

OVERVIEW

A global asset management firm engaged the Mandiant team to perform a Cyber Threat Diagnostic — a point-in-time evaluation of present and emerging threats targeting the organization, its industry and critical systems. The customer's primary concern was focused on cyber espionage activity within the environment. They were looking for evidence of threat activity not previously identified within their environment. Additionally, they were particularly interested in evaluating the effectiveness of security program improvements made since a previous engagement. Mandiant consultants worked with the customer to scope an engagement, focusing on 90 days of network logs — specifically web proxy logs, email logs, antivirus and intrusion detection logs from early 2016.

Mandiant in action

Mandiant received over 2 TB of data, extracted key observables from the logs including IP addresses, URLs, email sender and email attachment information and correlated these observables to over four million indicators of compromise within FireEye iSIGHT's intelligence holdings. Subsequent analysis of the logs identified suspected cyber espionage activity attributed to a group with a nexus to China that has been known to target financial entities in the Asia-Pacific region. This suggested there may be a pattern of suspected cyber espionage affecting the organization's base of operations in that region, as similar activity was observed in a previous Cyber Threat Diagnostic conducted for this organization. Additionally, consultants were able to uncover and advise on significant cyber-crime trends occurring that were evident in the logs — including surges in macro downloaders, credential theft and ransomware activity.

Tactically, given the regional nature of the espionage targeting, the customer was able to leverage the findings to develop a defensive strategy to protect against similar espionage activity in the future. The customer also leveraged the findings to determine where in the attack lifecycle their deployed countermeasures were breaking down, specifically focusing in on the initial compromise stage. For example — phishing emails and the initial execution of

MANDIANT®
A FireEye® Company

Cyber Threat Diagnostic services identify advanced threat activity often missed within critical systems as well as new threats evolving in the global digital underground.

FireEye®

By revisiting themes from previous engagements, Mandiant provided insight into the effectiveness of customer action taken, showing positive results from actions taken to limit infection to detection time.

the included attachments was a significant weak point. Using this, user-education programs were revisited, internal response procedures were modified and plans for evaluating new technology deployments were being considered. Finally, procedures were implemented to proactively mitigate phishing attempts and minimize end user exposure.

Mandiant consultants provided a comparative analysis of findings between the previous and current engagements that suggested measures taken to improve time to detection were effective. During the first Cyber Threat Diagnostic, a sophisticated malware known as Vawtrak was identified in the customer's environment across numerous hosts with infections lasting up to several days. The second Cyber Threat Diagnostic identified much less Vawtrak activity in the environment and evident activity was effectively remediated within an hour. The customer corroborated this comparison with details about improvements made to more rapidly remediate infected machines.

Mandiant worked with this customer to re-baseline its threat profile uncovering key signs of activity previously unidentified by exposing a broader set of indicators. This allowed the customer to make operational decisions based on the capabilities of the actors perpetrating the evident activity. Additionally, by revisiting themes from previous engagements, Mandiant was able to provide insight into the effectiveness of customer action taken — with evidence suggesting positive results from actions taken to limit infection to detection time.

For more information on FireEye, visit:
www.FireEye.com

About FireEye, Inc.

FireEye is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye