FireEye
SECURITY REIMAGINED

Global developer avoids major attack hours after FireEye platforms are deployed

CUSTOMER STORY

SECURITY REIMAGINED

CUSTOMER PROFILE

Globally recognized developer of integrated resort and destination properties.

"By rapidly deploying the FireEye Email Threat Prevention Platform inline with their newly rebuilt Office 365 cloud email solution, the company prevented a second attack attempt to destroy their e-mail system."

BUSINESS CHALLENGE

As a multinational firm with many high-profile properties, the company was concerned about security. Hundreds of thousands of guests shop, dine, sleep, and enjoy entertainment at their facilities daily, which means the company processes an extensive amount of sensitive customer information. A data breach would be extremely costly for this company. It could potentially damage the company's reputation and put customers' personally identifiable information at risk. To protect against this, the company's leadership took a proactive approach to security and sought technology solutions that had proven to be effective against advanced attackers.

SOLUTION

The security team's first step towards improving their security posture was to protect against one of the most common entry points for advanced attackers: Malicious URLs. After evaluating several alternatives and consulting with industry peers, it selected FireEye® Network Threat Prevention Platform and FireEye® Email Threat Prevention Platform (the NX and EX series). The platforms confirm and block inbound web and email application exploits and prevent outbound callbacks from malicious code. By detecting attempts to compromise their network and email system, the security team would be protecting the two primary attack vectors of advanced threat actors.

On the day FireEye Professional Services arrived at the company's headquarters, before they could begin the installation, the company discovered it was the victim of a vicious email phishing attack. An employee had clicked on a link included in an unobtrusive email. As a result, the malicious site downloaded code onto the employee's machine, which was connected to the corporate network. This malware was armed to induce maximum damage to internal systems. Within minutes, the

With no hardware or software to install, the company was able to procure and operationalize the cloud-based FireEye Email Threat Prevention Platform in one business day.

company's Microsoft Exchange and Active Directory servers were destroyed and over a terabyte of data lost.

One day later, the company was rebuilding its email capability, and chose the cloud-based Office 365 email solution instead of Exchange. Although the company had not initially opted to purchase the FireEye Email Threat Prevention Platform, given the origin of this insidious attack and the company's rapid move to a cloud-based email service, the platform was deployed inline between the Message Lab anti-spam product and Office 365.

With no hardware or software to install, the company was able to procure and operationalize the cloud-based FireEye Email Threat Prevention Platform in one business day. Less than 24 hours later, the platform detected and blocked a repeat attack by utilizing FireEye's Dynamic Threat Intelligence (DTI), which applied global intelligence to detect a malicious URL. Because the Email Threat Prevention Platform was deployed inline, the email, with its malicious payload, was isolated, preventing a second round of damage.

Today, with FireEye's Email Threat Prevention Platform deployed inline and Network Security appliances installed, the company's emails are routed through FireEye's patented Multi-Vector Virtual Execution Engine (MVX), which analyzes email content and attachments. The solution is further enhanced through global intelligence and context provided by FireEye's cloud-based Dynamic Threat Intelligence solution. When a threat is detected, the email is quarantined to prevent an attack and other targeted recipients of the email are identified. Benefits of the solution:

Enhanced email controls: Dynamic analysis of malware and email attachments significantly enhances the static, signature-based detection provided by anti-spam and anti-virus gateways.

- **Integration with the FireEye Network Threat Prevention Platform and attacker context:** By blocking malicious URLs delivered via phishing emails the company can prevent data theft over multiple protocols, such as HTTP or IRC while receiving context about the attackers that are targeting them.

- **Rapid deployment:** The Email Threat Prevention solution is a cloud-based service, which can be operational in less than a day and deployed in active protection mode or monitor-only via a BCC rule.

Quarantine of email attacks: In active protection mode, advanced attacks using malicious images, PDFs, Flash, or compressed archives (ZIP, RAR, TNEF) are quarantined.

By blocking malicious URLs delivered via phishing emails, the company can prevent data theft over multiple protocols, while receiving context about the attackers that are targeting them.

BUSINESS BENEFITS

By deploying the FireEye Network Threat Prevention Platform and the Email Threat Prevention Platform together, the company is able to implement a broader defense that protects against the two most common attacker entry points. With the addition of the inline Email Threat Prevention Platform the company is able to detect attacks earlier in the lifecycle, when attackers are attempting to deliver malicious code via spear-phishing campaigns.

Some of the specific benefits the company has already realized with the combined FireEye email and network threat prevention solutions include:

- **Rapid Detection:** By rapidly deploying the Email Threat Prevention Platform inline with their newly rebuilt Office 365 cloud email solution, the company prevented a second attack attempt to destroy their e-mail system.
- **Reduced Business Disruption and Remediation Costs:** By identifying and stopping a follow-up attack the company avoided the business disruption that would occur if emails were destroyed and the e-mail system were rendered inoperable, as well as the time and money involved in rebuilding the e-mail system a second time.
- **Low Cost of Ownership:** As a cloud solution the Email Threat Prevention Platform requires minimal ongoing maintenance and can be rolled out to new offices in less than a day.
- **Intelligence Sharing:** Dynamically generated threat intelligence from around the globe, such as callback coordinates and communication characteristics are validated and shared with the company in a continuous feedback loop through FireEye's Dynamic Threat Intelligence (DTI) cloud.

VISION

The company is expanding its deployment of FireEye technologies in offices throughout the United States and Asia, with the CISO insisting that the FireEye Email Threat Prevention Platform remain inline to monitor every single email before delivery.

To learn more about FireEye, visit:
www.fireeye.com

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**