FireEye Unveils Solution to Thwart Spear Phishing Attacks

By Mike Lennon on Feb 17, 2011

Email Security Appliance Provides with Real-Time Analysis of Embedded URLs and Attachments To Protect Against Targeted, Socially Engineered Attacks

It can happen to anyone. Even Intel's CEO, Paul Otellini has been a victim of a spear phishing attack. At a Forrester security event in Boston this past fall, Intel's CISO Malcolm Harkins shared a story of how its top executive fell victim to a targeted attack. In this case, the attacker decided to use public information from a lawsuit that Intel was involved in at the time. The attacker crafted clever emails, appearing to be from Intel's attorney, and sent along some malicious attachments which Otellini decided to click on. It was from a trusted source, right? Wrong. In the end no sigificant harm was done, but the attacker was successful in penetrating one of the largest tech companies in the world and getting its top executive to do his part in helping the attack be a success.

FireEye, a provider of anti-malware solutions, at the **RSA Conference** in San Francisco, today announced a solution designed to specifically protect against these types of spear phishing attacks. The new "**FireEye Email Malware Protection System**" helps stops targeted email attacks to prevent malware-induced network breaches and data theft.

These types of targeted attacks, often referred to as **Advanced Persistent Threats**, until recently, were quite rare. Not anymore. "Consider the Operation Aurora attacks, which employed some of the tactics we touched on above. The Operation Aurora attacks targeted many companies, in addition to Google, such as Adobe Systems, Juniper Networks, Rackspace, Yahoo, Symantec, Northrop Gruman and Dow Chemical," **said** Terry Cutler of Digital Locksmiths and a *SecurityWeek* columnist.

With the launch of the FireEye Email MPS, enterprises and government agencies can protect data and networks from recurring Modern Malware infections and advanced, persistent threats (APTs) that attack using malicious email content and attachments. "The Email MPS represents a new generation of messaging security protecting against email attacks using malicious URLs and attachments exploiting zero-day vulnerabilities," said Ashar Aziz, CEO, CTO and Founder of FireEye. "FireEye's integrated MPS solutions protect organizations across the Web and Email attack vectors."

The solution features a Real-time Attachment and URL Analysis engine that evaluates emails for zero-hour malware using virtual machines running a cross-matrix of operating systems and applications, such as various web browsers and plug-ins. This dynamic analysis enables FireEye to detect and stop spear phishing email attacks aimed at known and truly unknown OS and application vulnerabilities. Using data collected from its Cloud Intelligence network, customers get security content about malicious attachments targeting zero-day vulnerabilities, malware callback channels, and URL blacklist updates. With blended attacks using email and the Web on the increase, it is critical to have a zero-hour, signature-less malware protection engine to analyze links in email as well as file attachments, such as PDF documents, Microsoft Office files, multi-media content, and other file formats.

"Using the FireEye Email MPS, we've been able to stop over three dozen separate spear phishing attacks over the course of two weeks," said an IT administrator at a defense contractor, who asked to remain anonymous.

The FireEye Email MPS is an appliance that requires no tuning and deploys as an MTA (Message Transfer Agent), SPAN device, or as a BCC destination. The appliance is deployed behind an existing email control point such as an antispam gateway.

“While you read about how security threats have grown more menacing, it's important to also remember that security defenses also have grown more powerful. The critical thing is to take the necessary steps to protect your infrastructure and your data. That's where most businesses fall short. And it's a mistake that is growing increasingly costly to make,” cutler **adds**.

Available in the second quarter of 2011, pricing begins at $54,950 for the appliance, with per seat licenses starting at $11.68 for a 5,000 seat organization.

Managing Editor, SecurityWeek.

Previous Columns by Mike Lennon:

- Commercial Software Harnesses Amazon Cloud to Crack Passwords Faster
- BreakingPoint Provides War Game Training Using its Network-Crushing Device
- RSA Breach: Reactions Pour in, Many Questions Remain Unanswered Following SecurID Attack
- McAfee Executive Addresses Committee on Homeland Security on Threat Sharing
- Twitter Enables Option for HTTPS by Default

Tags: NEWS & INDUSTRY Virus & Threats Phishing Malware

Trackback URL http://disqus.com/forums/securityweek/fireeye