


[Free Subscription](#) | [White Papers](#) | [Webcasts](#) | [Events](#) | [Contact Us](#)
[Malware & Threats](#) | [Cybercrime](#) | [Mobile & Wireless](#) | [Risk & Compliance](#) | [Security Infrastructure](#) | [Management & Strategy](#)
[Vulnerabilities](#) | [Email Security](#) | [Virus & Malware](#) | [White Papers](#) | [Desktop Security](#)
[Home](#) > [Virus & Threats](#)


FireEye Unveils Solution to Thwart Spear Phishing Attacks

 By [Mike Lennon](#) on Feb 17, 2011

[Like](#) [Confirm](#) [Buzz](#) [Tweet](#) 15 [0](#) [Digg](#) [Share](#) [RSS](#)

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 significant 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.

 Google™ Custom Search

SUBSCRIBE TO SECURITYWEEK

SUBSCRIBE



MIS TRAINING INSTITUTE'S

INFOSEC WORLD

CONFERENCE & EXPO 2011

 April 19 - 21, 2011 • Orlando
Disney's Contemporary Resort

Most Read | Most Recent

- » [Hacker Uses XSS and Google Street View Data to Determine Physical Location](#)
- » [The Rise of the Small Botnet](#)
- » [An Inside Look at Hacker Business Models](#)
- » [Defense Department's Cyberwar Credibility Gap](#)
- » [ATM Hacking Video - Barnaby Jack Demonstrates ATM Hacking at Black Hat USA 2010](#)
- » [Are Nigerian Scams From Nigeria?](#)
- » [The Top Five Worst DNS Security Incidents](#)
- » [The Three Providers Who Decide Whether You Will Be Hacked](#)
- » [The Root is Signed with DNSSEC - Now What?](#)
- » [China's Cyber Threat Growing](#)

M86 Security Sponsored Content
[How to Protect Your Organization Against Advanced Persistent Threats](#)



This paper will outline the evolution of APTs, explain the motivation behind them, and determine best practices for defending

"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.

Like
 Confirm
 Buzz
 Tweet
 15
 Digg
 Share
 RSS



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](#)

- sponsored links**
- » [Can You Safeguard Companies from IT Threats?](#)
 - » [2010 Device Integrity Report: U.S. Unprepared for Internet Device Flood](#)
 - » [Security Focus on Consumer Electronics w/ BONUS Free Software Trial](#)
 - » [Introduction to Security for Smart Object Networks Devices w/ BONUS Free Software Trial](#)
 - » [Mobile & Smart Device Security Survey 2010 - Concern Grows as Vulnerable Devices Proliferate](#)
 - » [Mitigation of Security Vulnerabilities on Android & Other Open Handset Platforms](#)
 - » [Building Firewalls for Embedded Systems w/ BONUS Free Software Trial](#)

Tags: NEWS & INDUSTRY Virus & Threats Phishing Malware

Like
 DISQUS

Showing 0 comments

Sort by Best rating **Subscribe by email** **Subscribe by RSS**

Add New Comment

Post as ...

against these threats.

[Learn More..](#)

Red Hat Sponsored Content
Webinar: Red Hat Clouds Today



Gordon Haff - Senior Cloud Product Manager, Red Hat You can build a private cloud today in an evolutionary way that makes use of and integrates with technologies that you already own. Proceed at ...

[Learn More..](#)

Google Sponsored Content
Shiny New Year with Chrome, Chrome OS and Google Apps for Business



Google's Chrome is successfully bringing productivity and security benefits to today's businesses. But how? Hear how Chrome and Chrome OS are innovating for Apps for Business, along with a review...

[Learn More..](#)

Visit the Smart Device Security Resource Center

>>

Sponsored By

Trackback URL

Popular Topics

- » Information Security News
- » IT Security News
- » Risk Management
- » Cybercrime
- » Cloud Security
- » Application Security
- » Smart Device Security

Security Community

- » IT Security Newsletters
- » Events
- » Comments
- » Most Read

Stay Intouch

- » Twitter
- » Facebook
- » LinkedIn Group
- » Stuxnet Group on LinkedIn
- » RSS Feed
- » Submit Tip

About SecurityWeek

- » Team
- » Advertising
- » Events
- » Writing Opportunities
- » Feedback
- » Contact Us

Wired Business Media

Copyright © 2011 Wired Business Media. All Rights Reserved. [Privacy Policy](#) | [Terms of Use](#)