Study From FireEye and Mandiant Reveals Legacy Cybersecurity Products Failed to Protect 97% of Organizations Using Them

Analysis of Real-World Deployments Uncovers Critical Flaws in Most Cyber Defense Architectures Not Using FireEye Solutions

Milpitas, CA - May 20, 2014 – FireEye, Inc. (NASDAQ: FEYE), the leader in stopping today's advanced cyber attacks, today released the report “Cybersecurity’s Maginot Line: A Real-world Assessment of the Defense-in-Depth Model.” A first-of-its-kind study, the report examines attack data captured by FireEye security appliances from 1,217 organizations around the world. These organizations were testing, but were not yet protected by, the FireEye platform from October 2013 to March 2014. Offering a unique glimpse into how well existing security products perform in real-world environments, the study concludes that signature-based firewalls, intrusion prevention systems (IPS), Web gateways, sandboxes, and anti-virus (AV) solutions – and various combinations of those tools – fail to fully block attacks in 97 percent of organizations that deploy them.

“The harsh reality of today’s advanced threats and the threat actors behind them is that their attacks are increasingly unique in nature and morph quickly, meaning they can only be identified and stopped as they appear in the wild,” said David DeWalt, chairman of the board and CEO, FireEye. “Our results with businesses trialing our products around the world show there is a clear need for solutions purpose-built to detect and protect against advanced attacks. And, as attackers find more ways to hide in the real world, our ability to see the multiple threat vectors they use will help keep our customers one step ahead.”

Key findings from “Maginot Line” include:

- Nearly all (97 percent) organizations had been breached, meaning at least one attacker had bypassed all layers of their security architecture.
- More than a fourth (27 percent) of all organizations experienced events known to be consistent with tools and tactics used by advanced persistent threat (APT) actors.
- Three-fourths of organizations had active command-and-control communications, indicating that attackers had control of the breached systems and were possibly already receiving data from them.
- Even after an organization was breached, attackers continued to attempt to compromise the typical organization more than once per week (1.6 times) on average.
- On average, attackers’ software exploits and malware downloads bypassed other security layers 1.51 and 122 times, respectively.

The report details the scale of advanced targeted attacks and how effective they are against entrenched cyber defenses. 348 trial participants also took part in a survey, offering a comprehensive picture of their security architecture and a vendor-to-vendor comparison of each layer of the typical cybersecurity architecture.

In addition, “Maginot Line” offers in-depth analysis from FireEye Labs, explaining why attackers are so easily outmaneuvering traditional security solutions, how their processes work, and what they are after. It provides further advice from FireEye analysts on aligning cybersecurity budgets with today’s real-world threats.

A full version of the report can be found here: “**Cybersecurity’s Maginot Line: A Real-world Assessment of the Defense-in-Depth Model**."

About FireEye, Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The **FireEye Threat Prevention Platform** provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 2,200 customers across more than 60 countries, including over 130 of the Fortune 500.

Media contact:
Vitor De Souza
FireEye, Inc.
415-699-9838
vitor.desouza@fireeye.com