

Cyveillance SEPA aims to shield humans from the growing threat of social engineering

Analysts: Josh Corman, Lauren Eckenroth

Cyveillance (acquired by **QinetiQ** in May 2009) has announced the latest addition to its arsenal of threat-intelligence products. Its Social Engineering Protection Appliance (SEPA) helps combat targeted social engineering, spear phishing and whaling attacks by performing a range of checks from email-intent analysis for baseline customers up to high-value-target protection for specific customer-defined employees. Sharks patrol these waters. Many organizations are finding themselves saying, 'We're gonna need a bigger boat.'

The 451 take

The most memorable chapter of *The New School of Information Security* was 'Amateurs Study Cryptography; Professionals Study Economics.' As a twist, we offer 'Amateur Attackers Study Reverse Engineering; Professionals Study Social Engineering.' With no disrespect to other important security, there is no doubt that attackers have been climbing the stack to exploit the less-defended content, application and human layers. While SEPA may, at a glance, look like just another mail-security appliance, it aims to pick up where traditional mail security leaves off. There may be no patch for human stupidity, but SEPA may be a filter. We see SEPA less as an appliance and more as a delivery mechanism for some pretty solid intelligence from Cyveillance. In the trinity of people, process and technology, security vendors tend to forget the people, or design around them. We see SEPA as an enlightened recognition that attacks are launched by intelligent adaptive adversaries that do study their human prey as they prepare for attack. In kind, SEPA can leverage gathered intelligence from the public footprint of a specific executive to raise the bar for attackers and thwart otherwise successful attempts. If thwarted via the email vector, we recognize there are other means to levy social engineering campaigns, but introducing such a hurdle is directionally correct, and a thwarted attempt can put teams on higher alert. We also believe the executive profiling process alone will be highly educational (and behavior-modifying) to employees – once they see just how easy they've made it for attackers to harvest their social networks for actionable intelligence.

Cyveillance's SEPA provides customers with a scaled level of social-engineering protection. Baseline customers begin with real-time in-line email behavior-and-intent analysis, wherein SEPA will analyze the content and context of an email for suspicious behavior, such as links or requests for specific information. Embedded Web links are opened and analyzed for URL redirects, file page behavior, infected content or suspicious context (such as the reputation of the hosting provider, etc.). Cyveillance takes pains to note the majority of its analysis is on the URL itself and not the malware that it may be linked to.

The product catches mass phishing attacks by nature, but the company claims it is best used to protect against targeted social-engineering attacks. The company does, however, use its threat-intelligence feeds and lookups to its Global Threat Intelligence to inform its analysis of suspicious behavior and intent. As we've covered before, Cyveillance does a good deal of intelligence work and sells multiple feeds. These various intelligence feeds enable SEPA to spot more elusive threats, such as poisoned Web links, zero days and, with some cases, highly targeted spear phishing.

For more focused deployments, SEPA can protect high-value executive targets, as defined by the customer. Targets can (and probably should) include any employee with access to sensitive data, including system administrators, human resources employees, executives and executive assistants. The first step in offering this protection is to create a profile by considering the target's public footprint on the Web. From there, if the target receives an email attempting to leverage information available on a social networking website to establish assumed familiarity and request information or a favor, that email will be filtered through a rule-based workflow and classed as a social engineering attempt. Profiles are created once as an initial baseline and updated on an interval. Such a baselining can be a real wake-up call and make many gasp when they see what they've freely volunteered to attackers about themselves, their loved ones and their peers. While your CFO may take great pride in being the **Foursquare** 'Mayor' of his local private cigar lounge, it may not feel so good when that and other information empowers an adversary to compromise his system and run off with sensitive financials.

SEPA was developed in response to (and in coordination with) target-rich customers facing very real social-engineering enabled attacks. Although the compliance checkbox majority will not understand the need for such an investment, the intelligence community, defense contractors, **Fiserv** and pharma industries are likely to take notice. The ever-growing list of 2011 breach victims will also take notice – after the fact. Whether targeted by nation states or chaotic actors like Anonymous or LulzSec, social engineering is a weapon of choice. Any defensive advantage against this may get a healthy look.

Competition

While many mail security products can help with spam, obviously bad URLs, phishing and the like, SEPA goes much further – and, therefore, stands somewhat alone as a complement to traditional mail security. **Cisco's** IronPort does attempt to leverage its very large SenderBase Network to help with some targeted phishing, but doesn't offer any SEPA-comparable employee-specific intelligence filtering.

Since noncomparable 'anti-APT' approaches often compete for the same limited budget, organizations interested in something like SEPA may give a look at **FireEye**, which specializes in spotting unknown malicious code, but not social engineering. In the same vein, **Fidelis Security Systems** comes up with these buyers – either to help spot/stop exfiltration of sensitive data, suspicious conversations or even some malicious payloads. Network forensics and analysis products like **EMC/RSA**-acquired **NetWitness** and **Solera Networks** also make short lists for target-rich environments. These are often post-infection though – as would be botnet command-and-control identification from **Damballa**. Finally,

post-incident, offerings like **MANDIANT's** Intelligent Response and supporting products and services are finding their way into these shops. Again, none of these are really direct competitors to SEPA, but they are often used in concert. In fact, we've recently covered one end user's idea of 'better security' and his list of a complementary slate of offerings to fight off adaptive persistent adversaries.

Reproduced by permission of The 451 Group; copyright 2010-11. This report was originally published within The 451 Group's Market Insight Service.

For additional information on The 451 Group or to apply for trial access, go to:
www.the451group.com