

Fight fraud the new-fashioned way

Let's face it: The bad guys are smart. Way back when, most relied on bogus phishing expeditions, sending hundreds of millions of emails baited with links to introduce malware into unsuspecting victims' computers.

Some still do this, but potential victims have become more suspecting, and the efficacy of such a strategy has waned. The result: The bad guys changed tactics. For example, simple phishing has evolved into spear-phishing, in which high-value individuals are targeted. More on this later.

Banks must be able to adjust their defenses quickly, in as near to real-time as possible, to effectively thwart attacks on them or their customers. That means yesterday's defenses—firewalls, encryption, authentication—may not be enough any more.

In its latest cyber-threat report, Websense Security Labs discusses the trifecta that's driving what it calls "epidemic" levels of data theft: extremely effective social media lures; evasive and hard-to-detect infiltration of malware; and sophisticated exfiltration of confidential data.

"Traditional defenses just aren't working any more. Organizations need real-time defenses with multiple detection points that deeply analyze both the inbound content of each website and email as well as the outbound transmission of sensitive data," says Charles Renert, vice-president of research and development for Websense. "Nearly all data-stealing attacks today involve the web and/or email. And many increasingly use social engineering to take advantage of the human element as the weakest link. Since the current generation of attackers use multiple data points and threat vectors to target their victims, only a solution that understands the entire threat lifecycle and combines data from each phase can protect against them."

Enter the web, cloud, managed service—whatever you want to call it. In this case, it means relying on outsourced vendors that remotely provide fraud protection. Individual vendors may approach the problem differently and through proprietary ways, but essentially they're stand-off guardians. They protect against the bad guys, so banks can focus on serving legitimate customers.

According to Forrester Research, such managed security-service (MSS) providers are the wave of the future.

"Information security is changing as a discipline. Security is no longer that critical function that must remain in house. Just a year and a half ago, Forrester reported that only one in four security organizations outsourced their email filtering. Today, more than half of security organizations outsource email filtering. An increasing number of [chief information security officers (CISO)] now view security outsourcing as a viable method for reducing costs and improving their security capabilities," Forrester says in a March report.

It estimates that MSS adoption will grow 30%-40% in the coming year, and gives these reasons:

- MSS providers offer better resources, scalability, and talent—for a cheaper price.

- CISOs want trusted, strategic partners.

- Advanced technologies, such as threat intelligence and correlation, drive future demand.

“Cost management is certainly one factor contributing to the fast adoption of MSS, but more important, security organizations need the bandwidth and talent that top MSS providers can offer,” Forrester says.

In the same report, the research company evaluates nine specific MSS providers, including Trustwave, the company endorsed for information security, compliance management, and data loss prevention by ABA’s Corporation for American Banking. Trustwave was noted for leveraging its payment card industry expertise and strong monitoring capabilities. Says Forrester: “Those looking for a strong technical team and customizable services should be sure to consider Trustwave.”

Forrester has similarly good things to say about IBM, Dell SecureWorks, Symantec, Verizon, CSC, and AT&T. Check the full report at the link below.

And here are more suppliers (in no particular order):

- Entrust demonstrated software authentication platform IdentityGuard at the recent FS-ISAC annual summit in Miami. Of note, says Entrust President and CEO Bill Conner, “After enduring the management headaches of stove-piped security solutions, financial institutions are now migrating to flexible platforms to not only support broad ranges of authenticators—including mobile and physical logical controls across diverse user groups—but also demanding the ability to provision and deprovision authentication and fraud policies within hours or even minutes.”

- Visa introduced Strategy Manager to help financial institutions create and implement strategies for identifying and stopping fraudulent transactions in real time at check out. “Financial institutions have to process thousands or millions of transactions each day. This means that a vast amount of data must be analyzed for fraud risk,” says Mark Nelsen, head of global risk and authentication product development at Visa.

- Unisys is offering its Stealth Solution suite of cyber-security software through a new channel program. Resellers

will target specific industries, including financial services. The suite uses techniques designed to cloak data communication endpoints—to make transactions invisible on the network and therefore removed as targets for hackers.

All this circles back to how smart the bad guys are, and what the good guys need to do to protect themselves. It is worth repeating that basic online defense relies on the awareness of the online user. To that end, KnowBe4, an internet security-awareness training firm, says these are the top five spear-phishing scams to watch out for now:

- **Better Business Bureau complaint.** Executives receive a spoofed BBB email that includes a link purporting to go to a specific claim against them.

- **Smartphone security app.** A spoofed email from a company's CEO goes to the CFO asking to click a provided link. While installing a keystroke logger on the CFO's computer, it also urges the officer to install a bogus security app, which gives the bad guy the CFO's login credentials, plus a way to thwart two-factor authentication.

- **Layoff notice.** A spoofed email tells an employee that he or she has been laid off, and asks the employee to click on a link to view severance benefits.

- **Free dinner in return for feedback.** A spoofed email mentions a particular restaurant the recipient is known to frequent, then asks that a malware-loaded PDF questionnaire be downloaded.

- **New lawsuit.** A spoofed email apparently from the organization's legal department to its executives contains an infected PDF with details of a nonexistent lawsuit.

Here's the best advice: "I would encourage all email users to get in the habit of thinking before they click, because cyber criminals' spear-phishing emails are becoming increasingly indistinguishable from legitimate messages by known senders," says Stu Sjouwerman, CEO of KnowBe4.

Sources for this article include:

Award-winning Websense Security Labs outlines top recommendations and insights for protecting from and containing sophisticated malware and targeted attacks

Entrust Demonstrates Enterprise-Wide Security Framework at 2012 FS-ISAC & BITS Annual Summit

KnowBe4 Alerts Businesses to the Top 5 Spear-Phishing Scams Targeting Executives

Unisys Makes Its Stealth Cybersecurity Offerings Available Through New Software Channel Initiative

Visa Strategy Manager Boosts Issuer Fraud Detection

Helps issuers better pinpoint and stop fraud before it happens

The Forrester Wave: Managed Security Services: North America, Q1 2012

About the Author

John Ginovsky is contributing editor of ABA Banking Journal and editor of the publication's TechTopics e-newsletter. For more than two decades he has written about the commercial banking industry. In particular, he's specialized in the technological side of banking and how it relates to the actual business of banking. He previously was senior editor for Community Banker magazine (which merged with ABA Banking Journal) and was a staff writer for ABA's Bankers News. You can email him at jginovsky@sbspub.com

