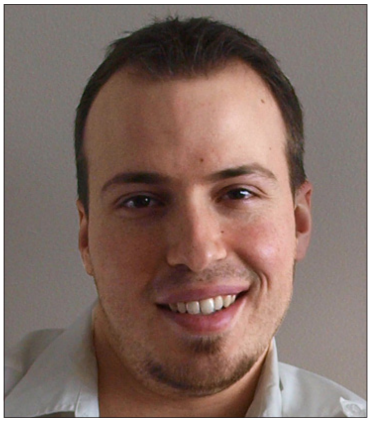
Technology



Ted Kritsonis

> **From a technology standpoint, traditional protections still rely too heavily on signatures and known patterns of misbehavior to identify and block threats**
>
> Ashar Aziz

Breaking the Online Bank

As technology and online behaviors change, so too do methods to compromise a person's – or organization's – most vital assets: their financial details. Ted Kritsonis examines how cyber thieves are adapting, and what the banks are doing to stop them

The way businesses and consumers do their banking online has changed rapidly in a very short period of time, as the cat-and-mouse game between financial institutions and cyber-attackers reaches a new, and somewhat unpredictable, phase.

Back in 2005, the Federal Financial Institutions Examination Council (FFIEC) issued a report of guiding principles meant to be a risk management framework for financial institutions that were offering internet-based products and services to their customers. The basics outlined advisory expectations for effectively authenticating controls applicable to "high-risk online transactions involving access to customer information or the movement of funds to other parties".

Six years later, in a follow-up supplement released in June, the message hasn't really changed, but the context has shifted to a wider scope. In it, the council focuses a great deal on how financial institutions need to consider new and evolving threats, particularly as they relate to assessing risks to online accounts, adjusting customer authentication, layered security and establishing minimum control expectations for online banking activities that need more of them.

Traditional Defenses

"The next generation of threats have changed radically from just a few years ago", says Ashar Aziz, founder, CEO and CTO at FireEye. "Most of today's attacks are targeted with the goal of obtaining something valuable – sensitive personal information, intellectual property, authentication credentials, insider information – and each attack is often a multi-staged endeavor to penetrate the network, spread slowly to key systems, and exfiltrate the sensitive data found on those systems."

Aziz says these types of attacks occur every day, and the ones that grab headlines are just "the tip of a vast iceberg". The stealthy nature of these attacks tends to incorporate web and email-based infection tactics with technology that helps them stay under the radar once they're planted in the network.

The problem can compound quickly because traditional security technologies, like next-generation firewalls, intrusion prevention systems, anti-virus and web gateways, aren't effective enough to deal with these threats, which can be modified to lure unsuspecting end-users into the same trap.

"From a technology standpoint, traditional protections still rely too heavily on signatures and known patterns of misbehavior to identify and block threats", Aziz says. "These defenses are good at detecting the known, but are blind to the polymorphic, dynamic, 'unknown' malware attacks that essentially look 'new', or zero-day, every time they're used to penetrate networks. In addition, these disparate technologies do not coordinate defenses across attack vectors, with email and web as the predominant mechanisms."

Ori Eisen, CTO of 41st Parameter, sees it the same way. The number of websites infected in relation to the number of users who came in touch with that infection point can only be estimated, he says, and these are usually only discovered after information

Phishing for banking info: the death of Michael Jackson made headlines – and bundles of cash for cybercriminals via drive-by infections (Photo credit: Gerry Boughan/ Shutterstock.com)