Security concerns, response, continue to ramp up

Entropay, a European concern that runs a virtual credit card website that allows anyone to open and fund a virtual prepaid Visa card, was repeatedly attacked recently by highly sophisticated online hackers.

The site allows consumers a flexible, and instantaneous way of making and receiving online payments. As such, it also is a prime target of hackers who, even though they never had a chance of actually stealing any money, did it simply because it looked vulnerable.

Over a short period of time the hackers subjected the site to SYN Flood, ICMP Flood, and UDP Flood attacks-basically barrages of digital inputs at various levels of the site's administration. With data coming in at 700 megabytes per second, the site, which is geared to handle up to 100 mbps, was repeatedly taken down.

Fortunately, they called in help from Prolexic, which specializes in such attacks. Prolexic employed its proprietary 500 gigabyte per second mitigation infrastructure and quickly restored Entropay to normal operation.

A number of things can be taken from this report. First, while this happened to occur in Europe, attacks on financial services sites could occur anywhere-Prolexic is based in the United States. Second, the motivation behind such attacks extends beyond monetary gain to the simple reality that, if something can be done, someone will do it. And third, the sophistication of such attacks has ramped up far beyond concerns about user IDs, passwords, firewalls, and virus scans.

The very vocabulary of cybercrime has entered the graduate school level. What, for example, are SYN Floods, ICMP Floods, or UDP Floods? Well, they are types of Level 4 distributed denial of service attacks. What's a Level 4 DDoS? Well, it relies on extremely high volumes (floods) of data to slow down web server performance, consume bandwidth, and eventually degrade access for legitimate users.

Okay, that begins to make sense. Prolexic provides a valuable and free glossary defining all these terms, located at the link listed below.

The larger issue concerns how the bad guys continue to outsmart the good guys, without the good guys even knowing they are being left behind. That's the conclusion of a recent survey by PriceWaterhouseCoopers, called The Global State of Information Security.

It found that 42% of the global executives it surveyed consider themselves "front runners" in information security strategy and execution. However, when examined against a set of criteria, the survey found that only 8% of these actually qualify for the description.

Criteria include: Having a chief information security officer or equivalent who reports to the top executives; having an overall information security strategy in place; measuring and reviewing the effectiveness of their security in the last year; and an understanding of exactly what types of security events have occurred.

"Clearly, many executives have unfounded confidence in their security capabilities. In order to strengthen security practices, organizations must embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the organization. Security strategies and security spending must be well-aligned with business goals," says Bob Bragdon, publisher of CSO Magazine, which collaborated with PwC on the survey.

Digging deeper, the survey found a waning resolve to keep up with threats. Among the protection areas taking a hit are malicious code detection tools for spyware and adware, down to 71% after topping out at 84% in 2008, and intrusion detection tools, once in use by nearly two thirds of survey respondents and now used by just over half.

"Intruders are exploiting business ecosystems, leaving reputational, financial, and competitive damage in their wake. Today's information security leaders must acknowledge that playing the game at a higher level is required to achieve effective security," says Mark Lobel, a principal in PwC's Advisory practice.

Of course, this particular survey paints a broad brush over multiple industries in multiple countries. However, it seems like every month, if not most weeks, other parties come up with similar conclusions and responses.

Case in point: LexisNexis's latest survey on retail fraud found that for every $1 a merchant loses in outright fraud, it costs that company $2.70 in mitigation expenses. These include charge backs for merchandise and the fees and interest to financial institutions and payment processors to replace and redistribute lost or stolen merchandise. That's up from $2.30 a year ago.

Of particular interest to financial institutions, this study finds that retailers that offer mobile, e-commerce, and international solutions are becoming new targets for fraud.

"With the size and pattern of fraud significantly impacted by global economic conditions and the move to mobile

payments, this turbulent time requires merchants to be more vigilant than ever," says Jim Rice, director, market planning, at LexisNexis Risk Solutions.

(As an aside, such a report lends itself to the ongoing move toward EMV adoption in the United States and the subsequent liability transfer to merchants. The Smart Card Alliance's consolidated EMV roadmap should be required reading.)

On the vendor side, some big hitters are teaming up with other big hitters, and are intensifying their various solutions in response to the sophisticated onslaught.

For example, RSA, the security division of EMC, and Booz Allen Hamilton Inc., entered into a consulting and services partnership designed to provide enhanced offerings. These include joint information security services, simplified client engagements for security preparedness and incident response, and assessing the commercialization of advanced security technologies.

"Government agencies and a full range of commercial enterprises today must be able to defend themselves from a growing list of online adversaries, all of whom will be armed with increasingly sophisticated malware and tactics," says Mike McConnell, vice chairman of Booz Allen Hamilton and former director of the National Security Agency.

Adds Mike Brown, vice president and general manager at RSA, "Whether their motives are cybercrime, cyber espionage, or cyber terrorism, the adversaries that organizations face online are highly effective at collaboration, information sharing, and technology sharing."

In a related series of announcements, RSA also introduced its Advanced Cyber Defense Services to help clients deal with sophisticated online threats, and bought Montreal-based Silicium Security, which developed an endpoint monitoring tool that detects malware.

The list of new and improved security services, up and down the financial services food chain, continues to grow. Some recent examples:

· Attachmate introduced Luminet 4.4, an enterprise management tool designed to detect and deter insider fraud and misuse.

· Carbonite unveiled a mobile app that extends its signature data protection capabilities to mobile devices.

There's no doubt that a stream of such products will continue to enter the market. There's no doubt that the market will only grow with increasing demand.

As PwC's Lobel says: "Security models of the past decade are no longer effective. Today's rapidly evolving threat landscape represents a danger that shows no signs of diminishing, and businesses can no longer afford to play a game of chance. Companies that want to be information security leaders should prepare to play a new game-one that requires advanced skills and strategy to win against emerging threats."

Sources used in this report include:

Prolexic Protects EntroPay | DoS and DDoS Attack Mitigation Case Study

DoS and DDoS Glossary of Terms

Despite optimism, companies must improve security strategies as incidents continue to rise, according to PwC, CIO and CSO's The Global State of Information Security Survey 2013

Retail Fraud Taking a Greater Financial Toll According to LexisNexis® 4th Annual True Cost of Fraud Study

Attachmate's Luminet 4.4 Upgrade Helps Stop Fraud and Misuse

Carbonite Mobile App Launches to Help Safeguard Mobile Content and Devices

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 ba 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@sbpub.com