



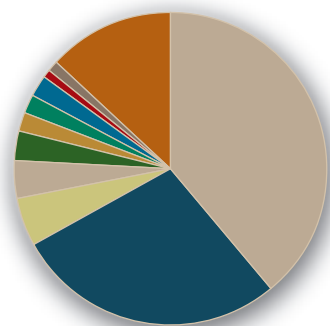
Changing Internet threats

By Todd Bransford

Over the last two years, the number of online attacks targeting the members or customers of financial institutions has more than tripled. Fraud schemes have become so pervasive that most credit unions have to assume their member data will soon be targeted by criminals through various online attack vectors. With the recognition that attacks are imminent, one of the most important steps a credit union can take is to make sure its incident response plans are up-to-date.

The rapidly changing nature of online attacks can quickly render obsolete those response plans put in place just a year ago. One of the most significant changes is the increasing number of Internet threats that target credit unions from far regions of the world. Attacks emanating from Eastern Europe and Asia typically require more time, different relationships and often new language skills in order to eliminate fraudulent sites and other online activity.

For example, the number of blended online attacks that leverage financial brands to distribute malware has more than doubled from the beginning of 2007. And of these malware attacks, more than 70 percent of the malicious downloads are delivered by Web sites hosted by ISPs outside the United States. It's vital that security professionals have response plans in place to deal with attacks originating in these foreign nations.



Country	Q2	Q3
China	34%	39%
United States	25%	28%
Russian Federation	10%	5%
Korea, Republic of	3%	4%
Germany	2%	3%
Malaysia	2%	2%
Hong Kong	<1%	2%
United Kingdom	2%	2%
France	2%	1%
Brazil	1%	1%
All Others	14%	13%

Source: Cyveillance

As phishing attacks have recently evolved, so too have the requirements for taking down phishing sites. During 2007, phishing attacks became far more sophisticated—mostly due to the efforts of a largely unknown hacker group called Rock Phish. This group is widely believed to be responsible for more than 50 percent of recent phishing attacks. Perhaps more importantly, Rock Phish appears to be one of the pioneers of “Fast Flux”—a new technique used in phishing attacks. Fast Flux is an approach that assigns multiple IP addresses to a single domain name associated with a phishing site. This allows

phishers to quickly switch from one IP address to another, making it very difficult to shut down the phishing site.

The increasing use of Fast Flux means incident response plans need updating. For attacks using the Fast Flux technique, getting a phishing site taken down is no longer as straightforward as contacting the hosting ISP. Instead, security professionals must contact the domain name registrar, which means a different set of contacts and a process that can take longer to complete.

While online attacks are changing rapidly, the public and private sectors are doing a better job of exchanging information and collaborating to combat fraud. As you update or create your online incident response plan, make sure to consider the following in your efforts:

- If you haven't done so already, provide an easy way for your members to report potential online fraud to you. The earlier you detect an issue, the faster it can be resolved.
- Know how you will respond to new attacks once discovered. Who is responsible in your organization? What internal or external resources are there to support the response team?
- How will you communicate new problems with members? Should the media contact you about an attack, how will you respond?
- Broaden your relationships to include law enforcement, the Secret Service and other agencies.
- Know how you'll work with registrars in the event you are faced with a Fast Flux-based attack.
- Consider using an outsourced service provider for threat detection and take down.

It is important to keep in mind that even the savviest users of well-known brands can be deceived into sharing valuable personal information through these more complex and sophisticated phishing schemes. To address these threats, you need an intelligence-led approach to security—one that can identify risks early for effective prevention and mitigation. Make sure your security team, whether internal or outsourced, has the necessary intelligence to quickly identify, shut down and recover from online scams that mislead your members through fraudulent use of your corporate identity. 🌐

Todd Bransford is vice president of marketing at Cyveillance Inc. (www.cyveillance.com), a preferred partner of NAFCU Services. Cyveillance provides intelligence-led security solutions to proactively identify online risks, enabling its customers to preserve their reputation, revenues and member trust.