# Credit Unions Are Now in the Crosshairs of Cyber Criminals

*But there is one way to eliminate the #1 threat vector for cyber attacks – the AirGap browser isolation system from Spikes Security.*

## Introduction

As cyber criminals continue to develop more advanced and targeted attack strategies, it is important to understand the risk that their activities pose to credit unions everywhere. There is clearly a growing cyber-terrorism threat facing credit unions, and NCUA Chairman Debbie Matz spoke about this at the recent CUNA Governmental Affairs Conference.

> *"Attacks, intended to create disruption, can crash networks but can also serve as a diversion for more damaging assaults," Matz told a packed session. "Imagine cyber-terrorists stealing passwords from your credit union and using (it) as an entry point to gain access to every payment system and every vendor with which you have a digital relationship." That scenario is more than just a what-if. Matz said hackers already breached a mid-sized credit union and used the credit union's passwords to access one of the larger credit bureaus.*
>
> Credit Union Times, March 2014

## 5 Questions to Consider About Potential Cyber Attacks on Your Credit Union

1) *Why Are Cyber Criminals Targeting Credit Unions?*
   - Unlike large banks and other financial institutions, most credit unions tend to be smaller organizations with IT teams that are challenged to do more with less. That includes investments in security technologies intended to protect them from potential cyber attacks. While larger banks often have the budget and staff resources to build and manage a multi-layer, defense-in-depth security architecture, credit unions typically do not have that luxury. Cyber criminals recognize that limitation. They also recognize that, like banks, the sensitive data stolen from credit unions offer a significant financial reward on the black market. For all of these reasons, credit unions are becoming a primary target for advanced, targeted attacks.

2) *What is Their Strategy for Targeting Our Organization?*
    - It is now a well-known fact that the #1 strategic target for cyber attacks are traditional web browsers – the same ones that are installed on desktops of employees in your organization. This fact has been confirmed through various industry research, including a report published in 2013 by Palo Alto Networks which indicated that 90% of all unknown (undetectable) malware was entering the network via the web browser. This is actually a very logical attack vector for cyber criminals because firewalls must keep ports 80 and 443 open so that users can leverage the web as a productivity tool for business. Consequently, when employees click on a link or visit a website (even a trusted site) it enables cyber criminals to establish a direct, virtually unrestricted path for delivery of malware to the browser, and ultimately gain access to your internal network.

3) *Aren't Vendors Making Their Browsers More Secure?*
    - Yes, all the major browser vendors – including Google, Microsoft, Apple, and Mozilla – continue to invest efforts to improve browser security. But keep in mind that the browser was never designed to be a security tool. Its primary function is as a productivity tool for all of us to leverage the power of the Internet. As web and cloud applications have become more powerful, so have web browsers. As a result, all major browsers now consist of millions of lines of code cobbled together by multiple developers over many years, which means browsers are loaded with vulnerabilities that can be easily exploited by cyber criminals. This was confirmed at the recent Pwn2Own event in March 2014, where hackers successfully easily exploited all major browsers in exchange for significant cash prizes. So relying on these traditional browsers for protection against cyber attacks is a non-starter.

4) *Why Can't My Current Security Defense Stop Browser-Borne Malware?*
    - Nearly all current generation security products rely on some form of detection technology (signatures, behaviors, etc.) to identify traffic as being good or bad. These products do a nice job when dealing with malware that has been previously identified and can be easily detected and blocked. But cyber criminals don't play by those rules. Instead, they have created a black market to build, buy and sell complex zero-day exploits that are completely undetectable, which means they can easily bypass any traditional detection-based security technology you may have in place. Even worse, according to research from Symantec, these unknown, zero-day attacks can fly under the radar inside your network for an average of 312 days (nearly a year)

before being discovered. By then, the damage will have been done. So the real danger is that you "don't know what you don't know" and relying on any detection-based technology can give you a false sense of security.

5) *How does AirGap stop all browser malware from infecting my network?*

- The only way to ensure 100% protection against all browser-borne malware is to remove all browsers from desktops and isolate all web content outside your corporate network. That's the idea behind AirGap. It consists of an appliance running a specialized browser deployed outside your firewall, instead of on your desktop. Employees inside your network use a lightweight AirGap browser client, which communicates with the external appliance to access all web content. All original web content stays outside the firewall, while the AirGap appliance delivers to each client a fully rendered, clean version of the requested content. From the employee's perspective, it is a high performance browsing experience – but there is absolutely no possibility of malware entering the corporate network and disrupting the business. It's a simple but powerful solution that effectively eliminates the #1 threat vector for cyber attacks on your organization.

If your organization is seeking a truly effective solution for stopping all browser-borne malware and empowering employees to safely access the web, we invite you to learn more about the patented AirGap solution from Spikes Security. Visit us at www.spikes.com or call 855.287.7453.