



Red Condor Detects Sophisticated One-Two Punch Malware Campaign

Scammers using spoofed brands, social engineering and phishing tactics to distribute malware on personal computers via drive-by download

Rohnert Park, Calif. – June 9, 2010 – [Red Condor](#) today issued a warning of a new sophisticated email malware threat that spoofs YouTube and uses a redirect on a compromised website to a common Canadian Pharmacy web site to distribute malicious PDFs via drive-by download. The pharmacy page is actually a red herring that has distracted many security researchers from the true motive of these campaigns, a stealth drive-by download. With a single click, users can infect their computers.

The malware, which as of the morning of June 9, 2010 had not been detected by any anti-virus engines, comes in the form of a malicious PDF download. Red Condor has captured 10 versions of the malicious PDF, which likely exploits vulnerabilities in Adobe Acrobat. The campaign appears to be part of a much larger attack first detected by Red Condor several weeks ago (see [Red Condor blog entry April 23, 2010](#)) and has also recently spoofed Facebook and Twitter, among other popular brands. As unsuspecting users wait for what they believe is a YouTube or Twitter friend request, a greeting card, or even a Facebook login page to load, their browsers download and execute the malicious code, and then the Canadian Pharmacy page appears.

“The amount of effort behind these new campaigns is not commensurate with the typical Canadian Pharmacy spam campaigns that we have seen in the past. It’s the primary reason we started to suspect weeks ago that these campaigns have an ulterior motive and are more than just a series of mundane Canadian Pharmacy spam,” said Dr. Thomas Steding, CEO of Red Condor. “After analyzing this threat over the past several weeks, we now believe that this malicious drive-by downloading may be a new trend; a double-purposing spam campaign, or a twist on the blended threat spectrum of attacks we have seen so prevalent in the past year.

Spammers are starting to use social engineering hooks, including those common with phishing attacks, which will generate clicks. If users click on the spam link, there is an opportunity for a sale and to steal their identities while infecting their computers – a sophisticated one-two punch.”

An interesting feature of this malware campaign is the distribution points appear to actively take measures to make researching the exploits difficult. The malware is served only if it thinks it can infect, and even then only upon the first request. Subsequent, identical requests from the same IP address do not result in the malware download. This level of intelligence and effort prevents traditional email security solutions, which rely on only automated detection methods from stopping the threat. Red Condor’s email security experts monitor for and analyze new threats twenty-four hours a day, seven days a week.

Key attributes of this new campaign include:

1. The URL uses a compromised middleman redirect that includes a slight delay before the redirect (http-refresh) occurs. The redirection page includes an iframe injection from a known malware distribution point. When users click on the link in the spam message, a blank page opens up in their browser and five seconds later a Canadian Pharmacy site pops up. While the user was waiting for what they think is a YouTube friend request to appear, a malicious JavaScript is fetched from the remote server referenced in the iframe resource.
2. The malware distribution point mentioned changes behavior depending on the details of the browser request. For example, it appears to be sensitive to User-Agent, as well as Accept HTTP Get request header items, which specify to the HTTP server what kind of device is making the request and what its capabilities are.
3. Only one request is allowed per IP. After the initial request, subsequent requests issue a null response (0 data returned).
4. There is likely a timing component as well that triggers the malware download.

Screen captures and images of campaign available upon request.

About Red Condor

Red Condor is revolutionizing spam fighting with its next-generation technology. Red Condor's highly accurate email filter, [hybrid](#) architecture Vx Technology™, and fully [managed appliances](#) lead to a dramatic reduction in the cost of owning a premium [spam filter](#). With solutions for [small businesses](#), as well as ISPs with millions of email inboxes, Red Condor has a cost-effective, timesaving solution that is rapidly gaining market share. The system's design has built-in zero tolerance for lost email, and a near zero false positive rate while achieving long-term spam block rates greater than 99%. Red Condor *Archive* is a secure [message archiving service](#) with lifetime retention and unlimited storage. The company's next-generation technology is backed by a 24x7 customer care center staffed by email security experts at Red Condor's headquarters. For more information, visit www.redcondor.com.

###