

## Phishing Attack Blacklists College - Red Condor to the Rescue!

In the spring of 2009, Dominican University was hit by serious phishing attacks. The emails warned users that their university web mail accounts were going to be cancelled unless they replied to the emails with their usernames and passwords. Unfortunately, some users fell victim to the scam, and it wasn't long before some of their email accounts were being used to send spam messages around the world. In reaction to the spam messages, Dominican University was blacklisted by some of the major email providers, including MSN, Yahoo and Hotmail.

"While we were in the process of contacting all the email providers to get our domain removed from their blacklists, we experienced another attack," said Don Ralis, associate director of information technology for Dominican University. "While some of the hackers used phished email accounts immediately, others waited and used the accounts later. We had to constantly monitor our email queues to determine whose accounts were being spoofed, and the multiple, scattered attacks really hurt our efforts to clean our domain."

### Playing "Whack-A-Mole" with Spam

In addition to the phishing and spoofing attacks, Ralis noted that the university was "just getting by with its inbound spam filtering." No matter how much "tweaking" Ralis and his IT group did to the university's email filtering solution, the spam did not stop.

"We felt like we were playing 'whack-a-mole' with spam," commented Ralis. "Just when we thought we had the right filtering rules in place, more spam would make it past the filter. We were annoyed that we could not do anything to improve the spam block rate or put controls on our outbound activity. We had already spent hours trying to get off the email blacklists and were constantly monitoring our Exchange queues to identify additional hijacked accounts."

### Moving to Red Condor's Fully Managed Appliance

After evaluating systems by Red Condor, Barracuda, and other providers, Ralis was impressed with Red Condor's established filtering rules and 24x7 monitoring. Red Condor's fully managed appliances stop all varieties of email threats. The company's Zero Minute Defense Network gathers knowledge in real-time from a worldwide sensor network to create new detection and protection rules, which are then sent out to customers as updates on a continuous basis. The fact that Red Condor is a fully managed solution and does not rely on publicly available blacklists, were important to helping Ralis decide that Red Condor's MAG3000 appliance was the right solution for Dominican University.

"From our initial evaluation, Red Condor seemed like it was a superior product," commented Ralis. We talked to other local colleges and universities that loved Red Condor, and then read



***"We felt like we were playing 'whack-a-mole' with spam...We had already spent hours trying to get off email blacklists and were constantly managing our Exchange queues to identify hijacked accounts."***

***- Don Ralis,  
Associate Director of IT  
Dominican University***

### About Dominican University

Dominican University is a private Catholic institution located 10 miles west of downtown Chicago. It is home to nearly 4,000 students and more than 400 faculty members and ranks in the top tier of Midwest regional universities, according to *U.S. News & World Report*.



some third-party reviews that helped sway us, particularly from an InfoWorld analyst, who was really impressed with Red Condor's solution."

**Migration to Red Condor's appliance is a simple process.**

The actual time to get Dominican set-up took a matter of hours. Once Ralis and his team completed the Administrator dashboard training, Red Condor demonstrated the process of exporting mailbox addresses, whitelists and blacklists and domain configurations. After changing the IP addresses, updating the company's firewall to permit filter updates, LDAP access and Red Condor's failsafe redundancy Vx Technology, and configuring the university's DNS resources, they system was ready to go.

Ralis added, "Once we got the device in place, we basically changed DNS addresses, flipped a switch, and it started to work. Whenever you change something with your network infrastructure, there are always concerns, but we were pleasantly surprised with how easy it was to change to Red Condor."

Critical for Dominican was also Red Condor's outbound filtering capabilities, which monitors outbound traffic to identify computers that have been surreptitiously converted to a "zombie" or "bot net" clients. Red Condor's MAG appliances can block outbound spam and malicious emails sent from these accounts and then notify Dominican's network administrators so that any zombie computers can be identified and cleaned.

**Red Condor: A Constant, Watchful Eye**

Since deploying the Red Condor device, Ralis has been impressed with the solution's outbound controls, which have prevented additional phishing and spoofing attacks.

He stated, "Red Condor is much better at catching phishing attacks, and even if they do get through, we have the extra security to stop the types of attacks that resulted in our domain being blacklisted. Red Condor had made our jobs easier, as we no longer have to pay constant attention to our email filtering, since we know it works. The real proof that we know Red Condor is working is that we are not getting the volumes of help desk calls that we used to receive. Rather than the constant complaints, people are telling us, 'I am not getting spam anymore.' That's nice to hear."

With Red Condor Ralis now has the capability to produce reports that help his team identify email trends, and the university better understand its email traffic. Of the more than 718,000 emails addressed to Dominican University accounts in the first half of September, roughly 315,000 were delivered. The rest were blocked or quarantined for end-users to review through their personal Spam Digest reports.

Ralis concluded, "The entire turnover process to Red Condor has been great, and we have no complaints. Red Condor is always available to help us. In fact, we have received calls from Red Condor's support team at 3 a.m. because they could not see our server. It turned out that our ISP had a scheduled shut-down of our network, but it was nice to know that someone is out there watching over us."

## About Red Condor

Red Condor is revolutionizing spam fighting technology. Red Condor's highly accurate Email DNA™ 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 business, as well as ISPs with millions of email inboxes, Red Condor has a cost effective, time saving 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%. This next generation technology is backed by a 24x7 customer care center staffed by email security experts at Red Condor's headquarters.



*Red Condor's Security Operations Center*

### RedCondor

1300 Valley House Drive, Suite 115  
Rohnert Park, CA 94928

**www.RedCondor.com**

Toll Free: 888-9NO SPAM

Sales: sales@redcondor.com

Resellers: resellers@redcondor.com

Support: help@redcondor.com

Information: info@redcondor.com