

Red Condor Warns of Aggressive Malware Attack Disguised as Flash Player Upgrade

Latest threat asks email users to change the security settings of their email box, download bogus Macromedia Flash Player executable

Rohnert Park, Calif. – November 24, 2009 – Email security experts at [Red Condor](#) issued a warning about the latest spam campaign that contains a phishing ploy and a malware threat. The email requests that recipients click on a link in the body of the email to update the “security mode” of their email box. Users that click on the link are taken to a web site that recommends that they update to the latest version of the Macromedia Flash Player by downloading “flashinstaller.exe.” The executable is actually a banking Trojan that is known to disable firewalls, steal sensitive financial data and provide hackers with remote access capabilities. The malware is more commonly known as Win32:Zbot-MGA (Avast), W32/Bifrost.C.gen!Eldorado (F-Prot), PWS-Zbot.gen.v (McAfee) or PWS:Win32/Zbot.gen!R (Micosoft). The spam campaign was detected late on November 20, 2009, and within the first six hours, Red Condor had blocked more than 500,000 emails. To date, Red Condor has stopped more than 3.5 million messages belonging to this campaign.

“Protecting in-boxes is seen as business critical, so it is no surprise that spammers and cybercriminals are playing off of email users’ growing security concerns with security-focused junk mail,” said Dr. Tom Steding, president and CEO of Red Condor. “Within moments of detecting the spam, Red Condor had established and pushed out a [filtering rule](#) to all of our [email firewall](#) and [Hosted Service](#) customers. Unfortunately, several hours after the campaign was detected, only about 50 percent of the anti-virus engines on the market had recognized it.”

Steding added, “Spam that suggests users update their Flash Player is a common type of scam during the holidays, but it is often associated with viewing a fake e-card or a viral video. We encourage email users, particularly those returning to full inboxes after the Thanksgiving holiday, to immediately delete these messages and notify their IT administrators.”

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.

###