

Red Condor Warns of Aggressive Highly Personalized Spear Phishing Campaign Spoofing Microsoft® Office Outlook® Web Access

Blended threat email attacking large number of domains; includes phishing tactics and an executable containing a Zbot Trojan virus

Rohnert Park, Calif. – January 7, 2010 – Email security experts at [Red Condor](#) today issued a warning for an aggressive spear phishing email campaign inviting recipients to “apply a new set of settings” to their mailboxes because of a recent “security upgrade” of their mailing service. An embedded link in the email connects users to a web site that appears to be a Microsoft® Office Outlook® Web Access page, including official Microsoft® and Microsoft Office logos. On the page, users are directed to “download and launch a file with a new set of settings for your e-mail account.” The executable is actually a Zbot Trojan virus similar to Trojans distributed in recent H1N1 and Facebook phishing attacks. Initially identified and blocked by Red Condor’s Zero Minute Defense System early the morning of Thursday, January 7, the campaign has still only been detected by a few virus scanners.

“This spear phishing campaign is unusual in that it is highly personalized and is targeting a very large number of domains with a customized message for each domain,” said Dr. Tom Steding, president and CEO of Red Condor. “Spear phishing campaigns usually target a single organization or domain, but this attack broke the mold as the volume and targets are very high. Once again, this is a perfect example of scammers modifying their tactics to thwart traditional security systems and demonstrates the importance of having an advanced, real-time email security solution. For Red Condor customers, the messages were blocked immediately, and a new filtering rule was in place within a few minutes of detecting the campaign.”

A spear phishing campaign is a highly targeted form of phishing that typically targets a single organization. Emails appear as if they come from a trusted source, such as an employer who would normally send an email to the entire company or a well-known organization. This campaign was detected by Red Condor’s Zero Minute Defenses, specifically its Fast Flux and [Spam Trigger](#) (formerly Spam Trip Wire) filters. Once identified, the campaigns are quarantined and reviewed as rules are written and automatically distributed to Red Condor’s [antispam appliance](#) and [Hosted Service](#) customers.

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.

###