

Red Condor Warns of IRS Underreported Income Notice Spam

Blended email threat attempts to steal personal information while embedding computers with malware

Rohnert Park, Calif. – March 24, 2010 – Email security experts at [Red Condor](#) have issued a warning for a new blended email threat that once again spoofs the Internal Revenue Service. The text-based email, which has a variety of subject lines, such as “the CP2000 notice (Underreported Income Notice),” is asking recipients to “review your tax statement on Internal Revenue Service (IRS) website.” When someone clicks on the link, they are taken to a landing page that includes the IRS header, as well as a link to the IRS Privacy Policy. On the landing page, visitors are asked to “Please review (download and execute) your tax statement.” The link on the page actually installs a version of the Zbot Trojan, which hides itself on compromised computers and allows remote attackers to steal bank-related information, log-in details and other personal data. This campaign is being sent from a botnet, has a moderate to high volume, and more than 2,000 unique sending IP addresses. A similar campaign was blocked in the fall of 2009.

“Given its familiarity with so many people, the IRS is a common target, especially during this time of the year as consumers and businesses are getting ready for tax season,” said Dr. Tom Steding, president and CEO of Red Condor. “In addition, many people fear the IRS, and an email with the subject line containing under reported income does catch people’s attention. Unfortunately, because the email appears to come from the federal government, they may be more likely to follow the instructions in the email. And it doesn’t take very many people clicking on the links for the spammers to profit from the campaign.”

As with past IRS spam warnings, the IRS has made it very clear that it does not communicate with individual taxpayers via email, so any email with the IRS’ brand on it is likely going to be a scam and should be forwarded to the IRS at phishing@irs.gov and then deleted.

This campaign was detected by Red Condor’s [Spam Trigger](#) filter, which quickly identifies spam and phishing campaigns before they penetrate users’ networks. 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.

###