

Red Condor Warns of “Adobe Security Update” Malware Campaign

Email campaign uses sophisticated social engineering in attempt to fool recipients

Rohnert Park, Calif. – May 5, 2010 – [Red Condor](#) today issued a warning of a new malware threat crafted to appear as an email thread discussing vulnerabilities in Adobe software. The campaign targets Adobe customers and consists of a fake thread of forwarded emails that begins with a security update message from an employee in “Adobe Risk Management.” The campaign warns recipients of a “Denial of Service Vulnerability” in the Adobe software and “strongly advises” that companies running the software update their systems with the “latest security patch.”

But the most convincing and potentially damaging aspect of the campaign is the structure of the forwarded thread, which is spoofed and customized per message and recipient. The thread contains what appear to be the full names and email addresses of people in higher positions in the recipient’s organization, possibly a technique to make the message and call to action seem legitimate. Embedded in the body of the email are links to a PDF file that contains the update instructions for the security patch, and an executable, which has been identified as a Trojan virus. Red Condor is the first to detect the malware campaign; the vast majority of AV engines failed to recognize the malicious download.

“This sophisticated campaign demonstrates the length scammers will go to get their emails past security so they can deploy malware on unsuspecting users’ systems,” said Dr. Tom Steding, president and CEO of Red Condor.

“The email itself contains convincing language and appears to have already made it through chains of command at the victim’s company. Overall, it’s a convincing campaign that could be a significant threat if the message volume increases.”

Red Condor advises recipients of the fake Adobe Security Update email to delete it immediately and not to click on the embedded PDF or web site links. The campaign was detected by Red Condor’s Spam Trigger filter. As with all threats captured by Red Condor, once identified, this campaign has been quarantined and reviewed and rules have been written for automatic distribution to Red Condor’s [anti-spam 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.

###