

31 October 2008

By: Lucian Constantin, Web News Editor



Phishing campaigns  
target domain account  
login credentials  
Rahul Hacking Articles

## [EstDomains' Accreditation Problem Prompts Domain Accounts Phishing Campaigns](#)

*The customers of the eNom and Network Solutions domain registrars have been targeted*

Analysts from security vendor Sophos [warn](#) of two new online scams that are targeting domain owners. The campaigns are focusing on phishing login information for eNom and Network Solutions accounts and they might be the result of ICANN starting the de-accreditation procedure for EstDomains, a registrar commonly used by cybercriminal groups.

According to Savio Lau, security researcher at Sophos, the two campaigns started simultaneously and are very similar in the techniques used. The only difference is that one targets the customers of the eNom domain registrar, while the other targets the clients of Network Solutions. Both campaigns fake the From: field and claim to be sent by the technical support departments of the two companies.

The eNom scam invokes a system maintenance that will allegedly start on the 1st of November at 1 AM PT. The e-mails claim that as a result, hosting and e-mail services will be down for up to three hours and encourage the customers to immediately log into their accounts and take whatever preventive measures they see fit. The provided login link takes the user at a <http://www.enom.com.otherdomain.tld> address where a fake eNom login page is displayed.

"The fake login site is probably lifted from the real eNom login page in its entirety. Looking at the HTML source of the phish site, one would find that even the Google Analytics link was copied," writes Savio Lau. Even so, the scam is believable enough, as in comparison with other regular spam campaigns, the message is properly spelled and the jargon is accurate.

The Network Solutions campaign claims that domain names belonging to the users expired because they were not renewed. As a result, the e-mail says, a backorder on the domain names was honored and the users, as the previous owners, are entitled to a sum of money resulting from the transaction. This scam, just like the eNom one, features accurate jargon and proper spelling, too.

"Given the two targets so far, it is quite possible that other registrar providers will be targeted next," warns Mr. Lau, while also pointing out that a connection between the campaigns and EstDomains' problems is very likely. As we previously reported, ICANN announced having started the process of [terminating](#) the accreditation agreement with EstDomains, a registrar harboring a large percentage of the domains used in online illegal activities. They later [halted](#) the process in order to analyze newly received documents, but attackers might already plan for the future, just in case they lose their primary source for domains. "If the computer underground feels that EstDomains won't be a safe harbour for its websites any longer, could they be looking to steal domain registration accounts from innocent parties?" rhetorically asks [Graham Cluley](#), Senior Technology Consultant at Sophos.