Netintelligence

OPINION SHEET

Don't let a Phisher leave your reeling

Just a couple of years ago, the mention of Fishing in the office conversation may have conjured up idyllic images of being thigh high in the waters of the Laune, delicately casting out a fly in the hope of attracting a spring salmon, but that may now not be the case.

The phonetically similar term 'phishing' is now becoming far more prevalent in everyday use. Unlike the traditional angler, this new breed of 'phisherman' does not have to brave the elements to catch their prey, they simply sit at a computer, send out electronic bait, and then wait for the the fallibilities of human nature to kick in and land rewards that have a far greater poundage value than the average Atlantic specimen.

The phishers of today create fake websites that sucker people into giving up highly confidential account numbers and other sensitive online information. To get visitors to their sites they use the lure of an email. The email looks as though it has come from a legitimate source, such as a bank or an online retailer, but it has not. About 18 months ago, phishing emails were pretty clumsy and threatening, but today's versions are pretty slick and professional. They now often consist of cut and paste copies of legitimate organisation's customer emails. The victim of the phisher uses an embedded link within the text to direct him/her to the fictitious web site. Once they have arrived at the web site, they will then usually provide account and credit card details in the mistaken belief that they are transacting or validating an existing account held with a respected organisation. Recent phishing spam emails have 'targeted' possible account holders of Lloyds TSB, Citibank, Westpac, Barclays, NatWest, Halifax, Nationwide, MBNA, Allied Irish, AOL and eBay. The phisher then uses these details as real internet currency. Thieves don't have to physically own or hold the credit card to use it. On the web, phishers can order goods and services, make deposits with organisations such as PayPal within a few minutes of receiving the account details. By the time, the victim has realised they have been duped; the phisher has received the goods or cash and has long gone (most fake websites are available for only 5 days). But the danger doesn't stop with illicit charges being applied to that account. Credit card numbers can be used to apply for new cards and loans - actions which can seriously affect the victim's credit rating.

And don't think be fooled into thinking that this latest scam is simply aimed at the humble consumer. With more and more businesses trading and interacting on line, for example booking travel and purchasing supplies, companies now represent lucrative targets for the criminals. In fact, to a degree they are softer targets than individuals as many companies usually operate monthly credit card expense/reimbursement/ consolidation policies - thus providing a longer period of time before the theft comes to light. Perhaps more worrying than losing money, is that the more sophisticated phishers can furtively install spying software, key loggers and remote access software on your computer. So they could be taking all of your confidential information as well. This is now becoming big business and is set to stay.

The Anti-Phishing Working Group counted 9,019 new and unique phishing e-mail messages in December 2004, four times the number recorded in August of last year. The Group also reported it had actively tracked no fewer than 1,707 phishing web sites in December. Gartner have estimated that phishers stole goods and services worth $1.2 billion globally last year. Figures released at the end of last year suggested that the UK and Ireland suffered around £18M in losses.

So what can be done by businesses to protect themselves against this new cyber threat?

As with most things in life, prevention is better than cure, and the most obvious form of protection from phishing emails is to have them removed before they reach your inbox. Therefore the easiest and most cost effective remedy is to deploy a commercial Mail Filter.

Phil Worms, Marketing Director for NetIntelligence, stated *'We are now finding that 1% of the total Spam email we are blocking for our clients displays phishing characteristics."*

"The pickings are potentially very lucrative for phishers, particularly given that it is estimated that 5% of recipients will respond to a phishing email. And it would appear that the phishers will stop at nothing to attract new revenue streams as demonstrated by a recent Tsunami Relief email which invited organisations to donate to a fictitious 'Red Cross' website".

The NetIntelligence MailFilter works by examining every email, comparing its properties against known criteria and then taking the appropriate actions. Characteristics that are examined include: header information, composition, message body content, attachment name and true file type, attachment contents, message size, images and determine the likelihood of spoofing. Once examined, the message is then compared in real time: against a database of over 30 million digitally fingerprinted threats, signatures, various white and black lists, directories, key words, threat categories, urls etc. This proprietary database process ensures that NetIntelligence MailFilter delivers Zero False Positives. The databases are updated 24 hours per day x 7 days per week and on average over 100 000 new files are added to the databases each week. Once the examination analysis is completed, the Mail Filter will take the appropriate action, as instructed through a policy decision determined by the customer e.g. to Block, quarantine, remove, log, report, cleanse, pass through to end user. The databases currently reduce spam by 94%, identify/ remove inappropriate/harmful content by 100% and viruses by 100%. These statistics compare more than favourably with other vendors due to the nature and content of the databases.

Phil added *'If you do not deploy a MailFilter then would strongly advise anyone receiving an e-mail claiming to be from a bank or other legitimate financial institution to completely ignore it and then report the email to the appropriate organisation's customer service department. Under no circumstances should any information be divulged over the web."*

For further details:
Netintelligence. www.netintelligence.com
or email:info@netintelligence.com.
Tel: 44 (0) 870 050 0121