PhishPatrol: A Purpose-built Anti-Phishing Email Filter

wombat™ security technologies

helping organizations combat phishing

http://wombatsecurity.com/phishpatrol

April 2012

PhishPatrol – A Purpose-built Filter to Catch Those Crafty Spear Phishing Emails That Make It Past Other Email Security

Learn why:

- Enterprises need to supplement their existing anti-virus/anti-spam email filters with a purpose-built anti-phishing email filter
- When it comes to phishing, anti-spam vendors are comparing apples with oranges
- Those phishing emails that make it past your existing filters are precisely the ones your employees are most likely to fall for
- PhishPatrol®, Wombat Security's purpose-built anti-phishing email filter, catches many of the phishing emails that make it past your existing email security

Find out what PhishPatrol customers say about our product.

SPEAR PHISHING ATTACKS: A NEW PLAGUE

Over 500 million phishing emails are sent each day.

Over 500 million phishing emails appear in inboxes every day. While this number pales in comparison to spam, which accounts for almost 70% of all email traffic, spam is mainly a nuisance whereas phishing can lead to dramatic security breaches. Just in the US, phishing attacks on customers have been reported to result in direct financial losses in excess of 1 billion dollars per year[1]. But for corporations and government organizations this is just the tip of the iceberg, as more targeted "spear phishing" attacks can lead to potentially devastating security breaches, loss of sensitive data and significant financial losses.

ANTI-SPAM VENDORS COMPARING APPLES WITH ORANGES

Anti-Spam filters primarily rely on manually maintained black lists that are typically several hours behind …yet most employees read their email within a few hours…

While most anti-spam/anti-virus vendors have repurposed their filters to also catch phishing emails, their solutions rely primarily on manually maintained "black lists". These typically come in the form of lists of fraudulent URLs that are manually vetted by people - to minimize the risk of flagging legitimate sites. By their very nature, these black lists are always one step behind, lagging by at least several critical hours and sometimes days. During that time, many phishing emails will go undetected by spam filters and many of the malicious websites to which phishing victims are directed will not be flagged by their browsers - since browsers heavily rely on black lists too. Yet studies have shown that, during regular work hours, 50 percent of users who fall for phishing attacks read their email within 2 hours from the time it reaches their inbox. This percentage reaches 90 percent within 8 hours[2]. In other words, a lag of just a few short hours in updating backlists used by anti-spam filters can have devastating consequences.

"Reply-to" phishing emails with no attachments and no links are another example of phishing emails that will often go undetected by anti-spam/anti-virus filters. This is in part because most anti-spam filters use simple "bag of words" techniques. These are techniques that look for emails containing collections of words indicative of spam. These techniques are good to catch spam but unable to differentiate between phishing emails and legitimate emails, since many phishing emails are crafted to look just like legitimate emails.

Spam vendors are comparing apples with oranges

This sad state of affairs is not entirely obvious if one looks at the statistics advertised by many vendors to promote their anti-virus/anti-spam filters. Many continue to boast about their ability to catch "up to 99%" of malicious email, a confusing statement that clumps together spam, viruses and phish. Because almost 70% of all email traffic is spam, while phishing attacks amount to only

---

[1] Gartner Group, "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks", December 2007. http://www.gartner.com/it/page.jsp?id=565125

[2] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., and Pham, T. 2009. School of phish: a real-world evaluation of anti-phishing training. In Proceedings of the 5th Symposium on Usable Privacy and Security (Mountain View, California, July 15 - 17, 2009). SOUPS '09. ACM, New York, NY, 1-12. http://cups.cs.cmu.edu/soups/2009/proceedings/a3-kumaraguru.pdf

about 0.5%, “catching up to 99% of malicious email” is an ambiguous statement. The consequences of finding an unfiltered spam email in your inbox cannot be equated to those of receiving a phishing email. To put it plainly, spam vendors are often comparing apples with oranges. In addition, they fail to tell us about the number of false positives they may end up flagging to reach the 99% performance they often boast about. False positives are those legitimate emails they sometimes classify as spam and move to your junk box, forcing you to regularly go and check whether an important email did not find its way there by mistake. In truth, to reach 99% effectiveness, many spam filters require settings that also lead to more false positives, effectively reducing the value of the filter, as users have to regularly check the content of their junk box.

PHISHING EMAILS THAT MAKE IT PAST YOUR EXISTING FILTERS ARE ALSO THOSE YOUR USERS ARE MOST LIKELY TO FALL FOR

Targeted spear phishing emails are by far the most dangerous ones. Yet they are also the least likely to be detected by anti-spam/anti-virus filters.

Even when it comes to phishing, not all emails are created equal. Studies have shown that high-volume phishing campaigns involving emails claiming to come from well-established organizations such as large banks, ISPs, or the IRS, are those that people are least likely to fall for. In contrast, targeted phishing emails, or “spear phishing emails” as they are called, directed at small groups of people such as employees of a particular department, or even single individuals tend to trick a significantly higher percentage of recipients. These spear phishing emails have been used to initiate many of the high profile security breaches reported over the past couple of years, as well as many lower profile attacks on smaller organizations and many unreported attacks. Statistics that simply look at percentages of phishing emails caught, including many of the easy-to-detect, high-volume phishing emails for which people are least likely to fall, fail to recognize this reality and produce seemingly reassuring numbers that are skewed towards the least dangerous types of phishing emails.

Smartphone users three times more likely to fall for phishing emails.

Studies have also shown that when reading email from smartphones, people are three times as likely to fall for phishing attacks than when they access email from a laptop or desktop computer[3]**.** With an increasing percentage of the workforce relying on smartphones to keep up with email, the urgency of deploying better anti-phishing solutions is further intensifying.

PHISHPATROL: A PURPOSE-BUILT ANTI-PHISHING EMAIL FILTER DESIGNED TO BEEF UP YOUR EXISTING INSTALLATION

PhishPatrol’s superior performance relies on predictive technology that analyzes attributes and features of emails to identify phishing attacks.

Wombat’s PhishPatrol is a purpose-built anti-phishing email filter that optimizes an organization’s email security by catching significantly more phishing emails than leading anti-spam/anti-virus software. PhishPatrol’s superior performance relies on predictive technology that analyzes attributes and features of emails to identify phishing attacks.

[3] Source: Lookout Mobile Security. July 2011.

PhishPatrol typically catches the majority of phishing emails that go undetected by other leading email security solutions.

The predictive technology within PhishPatrol utilizes a multi-layered architecture where each layer analyzes emails based upon a number of contextual attributes that in combination are indicative of phishing attacks. Contextual attributes include but are not limited to linguistic features and reputation metrics associated with elements of an email.

Analysis results are vetted by proprietary layers whose sole purpose is to minimize the chance of filtering legitimate emails. This approach has enabled PhishPatrol to maintain an effective zero false positive rate, while catching many of the phishing emails missed by other filters. Extensive evaluation of PhishPatrol shows that it catches the majority of phishing emails that go undetected by other leading email security solutions. This includes many of the highly targeted spear phishing emails that employees are most likely to fall for and that also go undetected by other filters.

While no filter will ever be able to catch all phishing emails, PhishPatrol's customers have reported significant performance improvements.

"PhishPatrol was able to improve our filtering of phishing emails with zero false positives, minimal configuration and no noticeable load increase."

Lou Anschuetz, Network Manager

"PhishPatrol was able to improve our filtering of phishing emails with zero false positives, minimal configuration and no noticeable load increase", Lou Anschuetz, Network Manager at major research & education organization.

PHISHPATROL: EASY TO INSTALL ALONGSIDE OTHER FILTERS

PhishPatrol was designed to be easy to deploy alongside a wide range of anti-spam/anti-virus installations. It comes available in multiple configurations, including:

- Virtual appliance
- Spam filter plug-in

This flexibility allows organizations to choose the deployment option that is right for them. Wombat has an option that will work for you and can have you up and running in no time.

ABOUT WOMBAT SECURITY TECHNOLOGIES

Wombat Security Technologies is a global leader in the fight against phishing attacks through innovative training solutions and breakthrough filtering technology. In their first line of defense, Wombat's anti-phishing email filter, PhishPatrol has been shown to catch significantly more phishing emails than other leading filters. As a second line of defense, Wombat offers engaging and highly effective software-driven anti-phishing assessment and software-based training solutions for end users.

Wombat's customers include Fortune 500 companies, government agencies and small to medium businesses across numerous market segments.

For more information about Wombat Security Technologies, visit www.wombatsecurity.com.