EXCERPT FROM VIRUS BULLETIN ANTI-SPAM COMPARATIVE REVIEW, JUNE 2017

INTRODUCTION

In an era where one dramatic statement after another is made about the state of security, it's a good idea sometimes to take stock and look at how far we have come.

When the ILOVEYOU virus wreaked havoc 17 years ago, all it took for a victim to become infected was to open the email attachment. To make matters worse, spam filters were still in their infancy and many email accounts weren't protected at all.

In 2017, it would be rare to find an email account that wasn't somehow protected by a spam filter. Moreover, while malware that executes upon opening an attachment does exist, such attacks are a lot less common these days, and when they do happen they almost always depend on the user running a vulnerable version of the affected software.

Email remains an important attack vector though, and five malicious emails that caused problems for some of the products in this month's test provide a good illustration of how users' machines get infected via emails. The emails in question appeared to reference an invoice, about which the attachment – which was a PDF file – promised to contain more details.

Upon opening the attachment, however, the recipient was asked to open a second file. For many users, alarm bells would go off here, and rightly so, but for many others they wouldn't, which isn't too surprising, given that *Adobe*'s PDF reader also asks for permission to print a document. If the second file was indeed opened, another prompt would be given, asking the user to enable macros. Once enabled, these macros would download the actual payload.

At each step in the infection process (receipt of email, opening of attachment, opening of second document, enabling of macros), the likely number of successful infections decreases – and anti-virus running on the endpoint reduces this probability even further. But nothing reduces it as much as a spam filter which, as data in this test demonstrates, could block 99% or more of the emails with malicious attachments.

VBSPAM TEST SET-UP

The test ran for 19 days, from 12am on 13 May to 12am on 1 June 2017.

The test corpus consisted of 218,231 emails. 209,468 of these were spam, 134,768 of which were provided by *Project Honey Pot*, with the remaining 74,706 spam emails provided by *spamfeed.me*, a product from *Abusix*. There were 8,418 legitimate emails ('ham') and 345 newsletters.

Moreover, 1,958 emails from the spam corpus were found to contain a malicious attachment; though we report separate performance metrics on this corpus, it should be noted that these emails were also counted as part of the spam corpus. (Note: the 'malware SC rate' refers to products blocking the emails as spam and not necessarily detecting the attachments as malicious.)

Although we stress that different customers have different needs and priorities, and thus different preferences when it comes to the ideal ratio of false positives to false negatives, we created a one-dimensional 'final score' to compare products. This is defined as the spam catch (SC) rate minus five times the weighted false positive (WFP) rate. The WFP rate is defined as the false positive rate of the ham and newsletter corpora taken together, with emails from the latter corpus having a weight of 0.2:

WFP rate = (#false positives + 0.2 * min(#newsletter false positives , 0.2 * #newsletters)) / (#ham + 0.2 * #newsletters)

Final score = SC - (5 x WFP)

Fortinet FortiMail

SC rate: 99.997%
FP rate: 0.00%
Final score: 99.997
Project Honey Pot SC rate: 99.996%
Abusix SC rate: 99.997%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet's *FortiMail* appliance has been taking part in *Virus Bulletin*'s VBSpam tests since 2009, and in the nine years since, has not failed a single test. While that in itself is impressive enough, the product has consistently been among the top performers in the test. In the most recent test, *Fortinet* missed only seven out of more than 200,000 spam emails, blocked all of the 1,958 malware samples hidden within the emails, and avoided false positives altogether, giving the product the highest final score among participating products.

Fortinet, Inc. 899 Kifer Rd Sunnyvale, CA 94086, USA
Web: http://www.fortinet.com/products/fortimail

Date of test	FPs	Final score	VBSpam
June 2017	0.00%	99.997	SPAM + Verified
March 2017	0.00%	99.98	SPAM + Verified
December 2016	0.00%	99.94	SPAM + Verified
September 2016	0.00%	99.94	SPAM + Verified
July 2016	0.00%	99.97	SPAM + Verified
May 2016	0.00%	99.997	SPAM + Verified
March 2016	0.00%	99.95	SPAM + Verified
January 2016	0.00%	99.97	SPAM + Verified