REPORT

On a Direct Comparison Between the MessageLabs® and Postini® Hosted E-Mail Security Services

"The MessageLabs service offers significantly superior performance both to the commercial products and to the competitor service, resulting in a measurably reduced risk in terms of the expected cost of major security incidents."

- Professor R A Walton
  Information Security Group
  Royal Holloway, University of London

University of London has validated the design of the experiments, the models and assumptions underlying the analysis, the analysis of the results, and the conclusions.

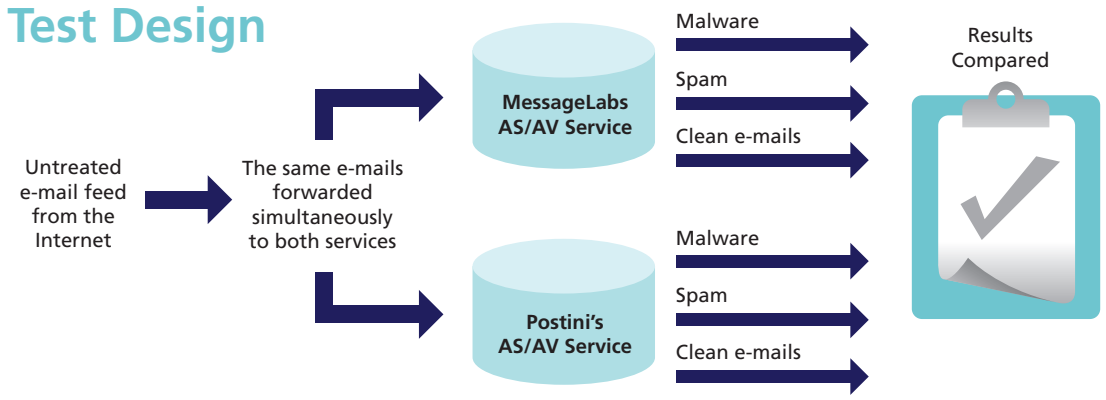
JOHN LEACH
INFORMATION
SECURITY
LIMITED

MessageLabs services have been scientifically proven to be better at stopping harmful malware than Postini

In a side-by-side test conducted in the second quarter of 2009, MessageLabs has been proven to be many times more effective than Postini at protecting its customers from harmful malware. The test results indicate that, whereas a Postini customer with 3000 staff can expect to get hit by major e-mail-originated malware incidents on average once every 18 months, an equivalent MessageLabs customer can expect to stay incident free for a very much longer period.

A direct comparison of the Anti-Virus (AV) effectiveness of the Postini and MessageLabs hosted e-mail services has been conducted as a scientific experiment by Dr. John Leach, an independent security expert.

A feed of several million live e-mails was passed simultaneously through both the MessageLabs and Postini hosted e-mail services, and the output from the two services compared.



The test examined how each service handled those e-mails: which e-mails were found to contain malware, which were flagged as spam, and which passed through as clean. The test then focussed on how many of the e-mails passed as clean by each service still contained malware, and in particular how many of those contained malware which could cause the receiving customer real harm beyond simply the cost of cleaning the malware up.

The results showed that both MessageLabs and Postini successfully identified most of the harmful malware present in the live e-mail feed. And both were clearly very much better at identifying malware than commercially available market-leading AV products.

However, when looking at the harmful malware each service missed, the results clearly set the two services apart. The full results are shown in the table that follows on the next page. They show that Postini correctly detected 58% of the harmful malware in the live e-mail feed. Fortunately, a large part of the harmful malware Postini failed to detect did not get sent on to the customer because Postini flagged the e-mails carrying the malware as spam.

In aggregate, one way or another, Postini stopped approximately 97.9% of the harmful malware present. However, that still left 2.1% which evaded all Postini's protection mechanisms and was sent on by Postini to the e-mail recipient in the mistaken belief that it was clean.

This missed malware comprised a variety of malware strains. In this particular test, there was a higher incidence of password grabber malware than other malware. If the test were to be run again at a different time, the missed malware would probably cover a different set of strains altogether.

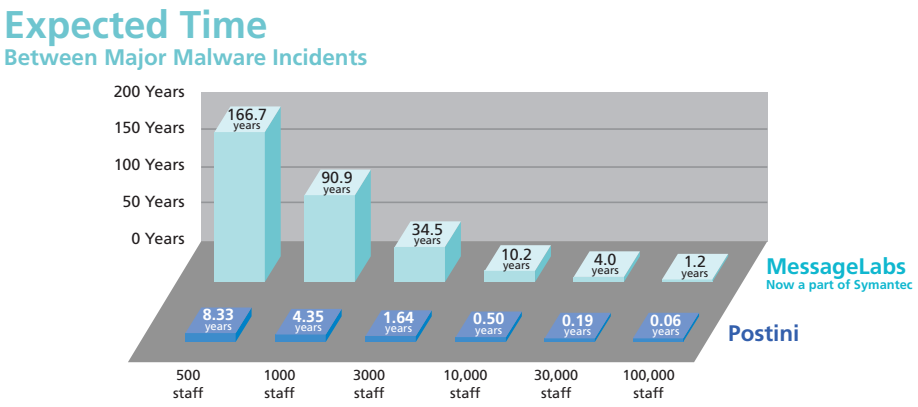
	MessageLabs	Postini
The number of e-mails in the live feed	Over 24 Million	
The number of those e-mails carrying harmful malware	20,587	
The number detected correctly as carrying harmful malware	20,587 (100%)	12,010 (58.3%)
The number in which the harmful malware was missed	0 (0.0%)	8577 (41.7%)
Of those, the number subsequently stopped as spam	0 (0.0%)	8154 (39.6%)
The number of e-mails carrying harmful malware passed to the customer as clean	0 (0.0%)	423 (2.1%)

The results for MessageLabs show that MessageLabs correctly detected 100% of the harmful malware in the incoming source feed, leaving none to be sent on erroneously to the recipient.

The large number of e-mails used in this test means that the above results for the numbers of harmful malware detected and missed can be shown to be accurate to better than +/- 0.1%. This means the numbers of malware-carrying e-mails quoted for each service are accurate to better than +/- 20.

Dr. Leach then went on to calculate how often Postini and MessageLabs customers could expect to experience major malware incidents based on these results. As expected, and as shown in the following chart, the average period between incidents falls as the size of customer grows. This is primarily because larger companies receive more e-mails per day than smaller companies and are, as a result, exposed to more malware per day.

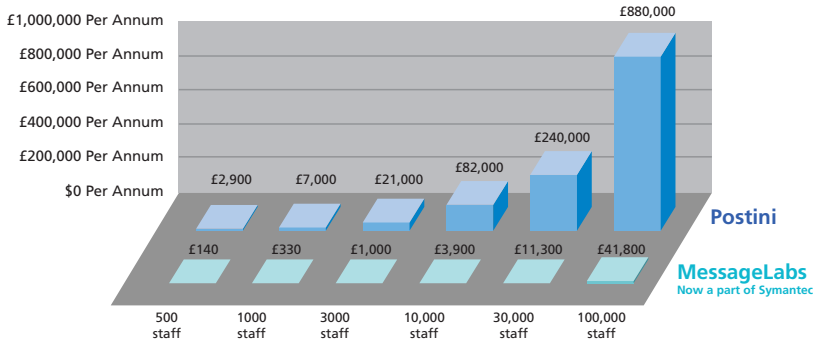
A Postini customer with 3000 staff can expect to suffer a major malware incident about once every 18 months. Even allowing for the small level of uncertainty in the results (+/- 0.1%), a MessageLabs customer of that size can expect to stay incident-free for a very much longer period of time. The average interval between incidents for a 3000-user MessageLabs customer, as indicated by the data, is sufficiently long that, by the time that customer should be coming due for an incident, malware dynamics would no doubt have changed sufficiently that a whole new set of experiments and data would be needed to describe the risk.



Then, using results from a UK government-sponsored security survey[1] , Dr. Leach estimated the financial harm customers could expect to be caused by this level of malware. As the Postini customer would get hit by malware incidents much more frequently than the MessageLabs customer, the average cost per year of malware incidents for them would be much higher than the cost for MessageLabs customers. This equates to a very real savings which the MessageLabs customer would see through having far fewer malware incidents to deal with.

Using the published results from that survey, a typical cost of a major malware incident for an organisation with 3000 staff was estimated at £30,000. This includes the costs of cleaning the malware out of infected systems and the costs of lost productivity and business due to the un-

Annualised Cost
Of the Major Malware Incidents Experienced



planned disruption. For Postini customers with 3000 staff, one major incident every 18 months equates to annualised incident costs of £20,000. For equivalent MessageLabs customers, the annualised incident costs they would see would be negligible. And, the larger the Postini customer, the greater the size of this cost differential.

This experiment was designed and the results were calculated independently of MessageLabs. Dr. John Leach has a background as a research scientist as well as now being a well known security expert. MessageLabs provided the mail servers and systems needed to run the side-by-side test following Dr. Leach's design and gave him open access to the raw data generated by those systems.

The analysis which created these results from that data is entirely free of any interference by MessageLabs. And just to make doubly sure that this test is truly unbiased and the results calculated fairly, both the design and analysis have been checked separately by a renowned security expert from the University of London and given a clean bill of health.

These results are believed to represent a world first. This test is believed to be the first time security professionals have taken a properly scientific approach to measuring security effectiveness. It shows that it is possible for companies to measure the real return they are getting from their security investments and to determine whether their security budgets are indeed being spent efficiently and in the right place. This work will raise the bar for what customers can expect of the claims made by their service providers, not only in the AV realm but across all areas of security.

About Dr. John Leach

John Leach has been an Information Security professional for more than 20 years. He has held senior positions in the security teams of a number of organisations, most notably NatWest Bank, Zergo and Global Integrity (part of SAIC). In December 2002, he formed his own company to enable him to provide consultancy services independently and to pursue research into a special interest of his, analytic techniques for modeling security risk.

John Leach has an academic scientific training and long experience working with Blue Chip national and international organisations in the security field. He brings these together to create innovative solutions to complex problems and to develop a unique range of consultancy services. Many of the services John Leach provides build on his ability to use security data scientifically to describe the dynamics behind security risk and to quantify how the countermeasures people apply reduce the security risks they face.

John Leach has worked for clients across most sectors of industry including Financial Services, Oil and Petrochemicals, Manufacturing, IT and Telecommunications, Civil Government and Defence, and the service sector. He has developed and delivered numerous training courses and workshops for clients, and presented at public conferences on a variety of subjects, most recently on risk modeling, identity assurance and people-centric information assurance.

John Leach has been an active member of the Management Committee for the Information Assurance Advisory Council (www.iaac.org.uk) continuously since May 2002. He is also a member of the International Board of Referees for Computers and Security.

Dr. John Leach
John Leach Information Security Ltd.
Tel.: (+44) (0)1264 332 477
Mobile: (+44) (0)7734 311 567
E-mail: john.leach@jlis.co.uk
www.jlis.co.uk

Comparison test conducted at the request of MessageLabs, now a part of Symantec Corporation.

1 The Information Security Breaches Survey, 2008. That survey's results show that, for a 3000-staff company, the all-in cost of a worst case security incident could be as high as £120,000. The results reported in this paper have taken the typical all-in cost of a major malware incident to be about one quarter of that worst case cost, i.e. about £30,000.