Anti-Phishing Test

July 2016

Language: English
July 2016
Last revision: 22nd July 2016

www.av-comparatives.org

Introduction

What is Phishing?

Taken from Wikipedia[1]:

"Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. This is similar to Fishing, where the fisherman puts a bait at the hook, thus, pretending to be a genuine food for fish. But the hook inside it takes the complete fish out of the lake. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies."

For more information about how not to get hooked by a phishing scam, please have a look at e.g. https://www.consumer.ftc.gov/articles/0003-phishing

Test procedure

In our test scenario, we simulate the common situation where users rely on the anti-phishing protection provided by their security products while browsing the web (and/or checking their webmail accounts; anti-spam features are not considered, as they are not within the scope of this test). The test was done using Windows 7 Professional 64-Bit and Internet Explorer 11 (without its built-in phishing blocker, in order to get browser-independent results). All security products were tested with default settings and in parallel, at the same time and on the same URLs.

Test set

The test took place between the 7th and 14th July 2016. Phishing URLs were tested as soon as we discovered them. All phishing URLs had to be active/online at time of testing and attempt to get personal information. After removing all invalid, offline and duplicate (sites hosted on same server/IP) test-cases, **531** valid phishing URLs remained. The phishing campaigns targeted various types of personal data, including login credentials etc. for PayPal, online banking & credit cards, e-mail accounts, Dropbox, eBay, social networks, online games and other online services. The set of legitimate online banking websites consisted of **500** clean URLs.

[1] http://en.wikipedia.org/wiki/Phishing

Tested products

The tested product versions are the ones that were available at the time of testing. The test was performed with default settings. Vendors who took part in the test and whose products scored over 90% are listed below:

- Bitdefender Internet Security 2016
- ESET Smart Security 9.0
- Kaspersky Internet Security 2017 TR

Anti-phishing false alarm test

For the anti-phishing false-alarm test we selected 500 popular banking sites (all of them using HTTPS and showing a login form) from all over the world, and checked if any of the various security products blocked these legitimate online banking sites. Wrongly blocking such sites is a serious mistake. Of the three products listed above, there were **no false alarms** with the tested 500 legitimate online banking sites.

AV-Comparatives Approved Anti-Phishing Product Award

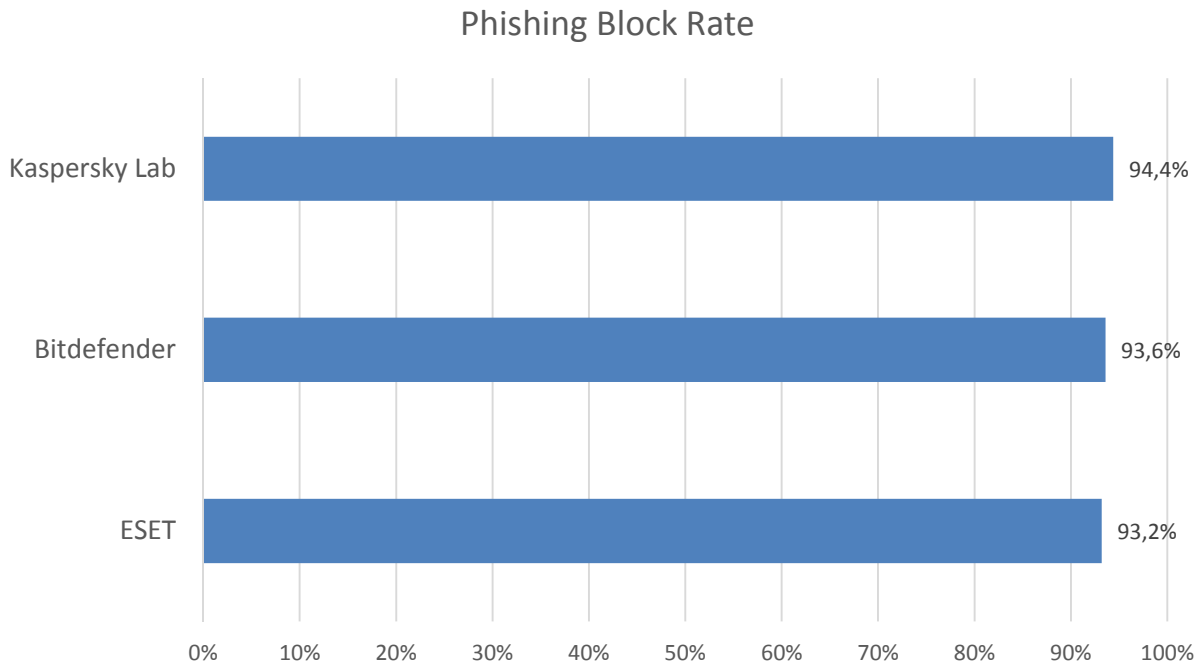
In order to be approved by AV-Comparatives for Anti-Phishing Protection, at least 90% of the phishing URLs used must be detected and blocked, without causing any false alarms with legitimate online banking sites.

Only products which were submitted for the Anti-Phishing Test, and which passed the test, are listed in this report. Other vendors can reapply for approval in 2017.

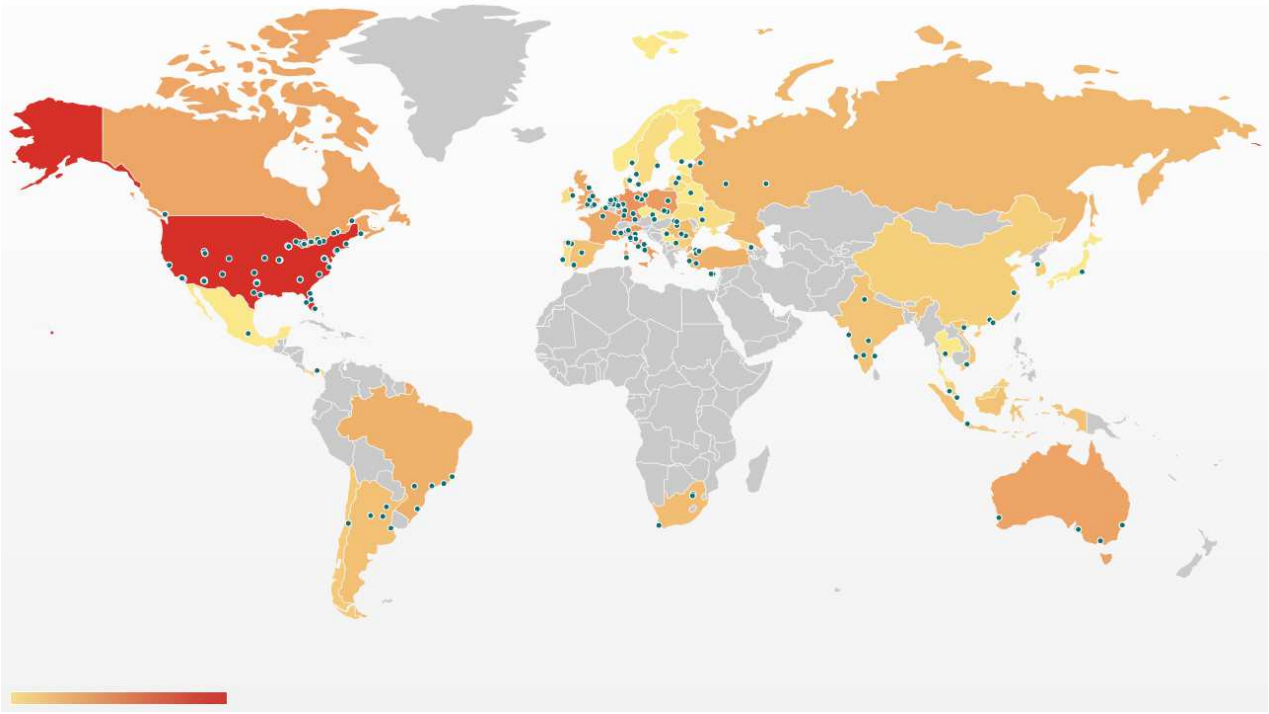
Test results

Below you can see the percentages of blocked phishing websites (size of test set: 531 phishing URLs).

1. Kaspersky Lab 94,4%
2. Bitdefender 93,6%
3. ESET 93,2%



The map below shows where the phishing websites used were hosted, based on their IP addresses.



Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies please visit our website.

AV-Comparatives (July 2016)