Anti-Phishing Test

July 2012

Language: English
July 2012
Last revision: 14th August 2012

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. the Consumer Alert of the FTC: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm

Test procedure

In our common test scenario, we simulate a user that relies on the Anti-Phishing protection provided by its security product while browsing the web (and/or checking his webmail e-mail account, i.e. anti-spam features are not considered, as they are not the scope of this test). The test was done on real machines, using Windows XP SP3 and Internet Explorer 7 (without the build-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 on the same URLs.

Test Set

Phishing URLs were mainly taken out from phishing mails during 6th to 27th July 2012. All phishing URLs had to be active/online and attempt to get personal information. After removing all invalid, offline and duplicate (sites hosted on same server/IP) test-cases, only 574 different and valid Phishing URLs remained. The phishing campaigns targeted various types of personal data. Among those were (in the following order) phishing attempts to gather e.g. login credentials etc. for: PayPal, Online Banking & Credit cards, E-mail accounts, eBay, Social networks, Online Games, and other online services.

The lifespan of phishing URLs is getting shorter, and more and more phishing sites are targeted/small campaigns to remain under the radar, which makes it increasingly difficult for Anti-Phishing/URL-Blocker countermeasures to be efficient in time.

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

Tested products

The tested product versions are the ones that were available at time of testing (July 2012). The following products were included in the Anti-Phishing test:

- **Avast** Free Antivirus 7.0
- **AVG** Internet Security 2012
- **Avira** Internet Security 2012
- **BitDefender** Internet Security 2012
- **BullGuard** Internet Security 12.0
- **eScan** Internet Security 11.0
- **ESET** Smart Security 5.0
- **Fortinet** FortiClient Lite 4.3.3
- **F-Secure** Internet Security 2012
- **G DATA** Internet Security 2013
- **GFI Vipre** Internet Security 2012
- **Kaspersky** Internet Security 2012
- **McAfee** Internet Security 2012
- **PC Tools** Internet Security 2012
- **Qihoo** 360 Internet Security 3.0
- **Sophos** Endpoint Security 10.0
- **Trend Micro** Titanium Internet Security 2012
- **Webroot** SecureAnywhere Complete 2012

Notes:
Panda Cloud Free Antivirus was also tested, but unfortunately, Panda had technical issues during the period of the test. There was a downtime of the server pushing out URL filtering signatures in July. Therefore, the measured results would not reflect the usual phishing protection of the product. Due to that, we decided to do not publish the results of PCAV.
ESET v5 does not have a dedicated module for anti-phishing protection yet. However, phishing sites are currently blocked along with other potentially harmful sites (like in most other products), employing various technologies such as webfilter, parental control and detection of suspicious content aimed at the phishing landing pages themselves. The new version (v6.0) of ESET includes dramatically improved anti-phishing protection. We evaluated the new version in parallel: it would have blocked 93,9% of the phishing sites.
Kaspersky is also going to release a new version (2013) soon, which includes improved phishing protection too. The new version would have blocked 97,4%.
Qihoo is mainly targeted to block Chinese phishing sites.

Anti-Phishing "False Alarm" Test

For the Anti-Phishing False Alarm Test we selected 300 very 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 those legitimate online banking sites. Wrongly blocking such sites is a serious mistake. From the tested products, only GFI Vipre had one false alarm on the tested 300 legitimate online banking sites:

GFI Vipre (one false alarm):

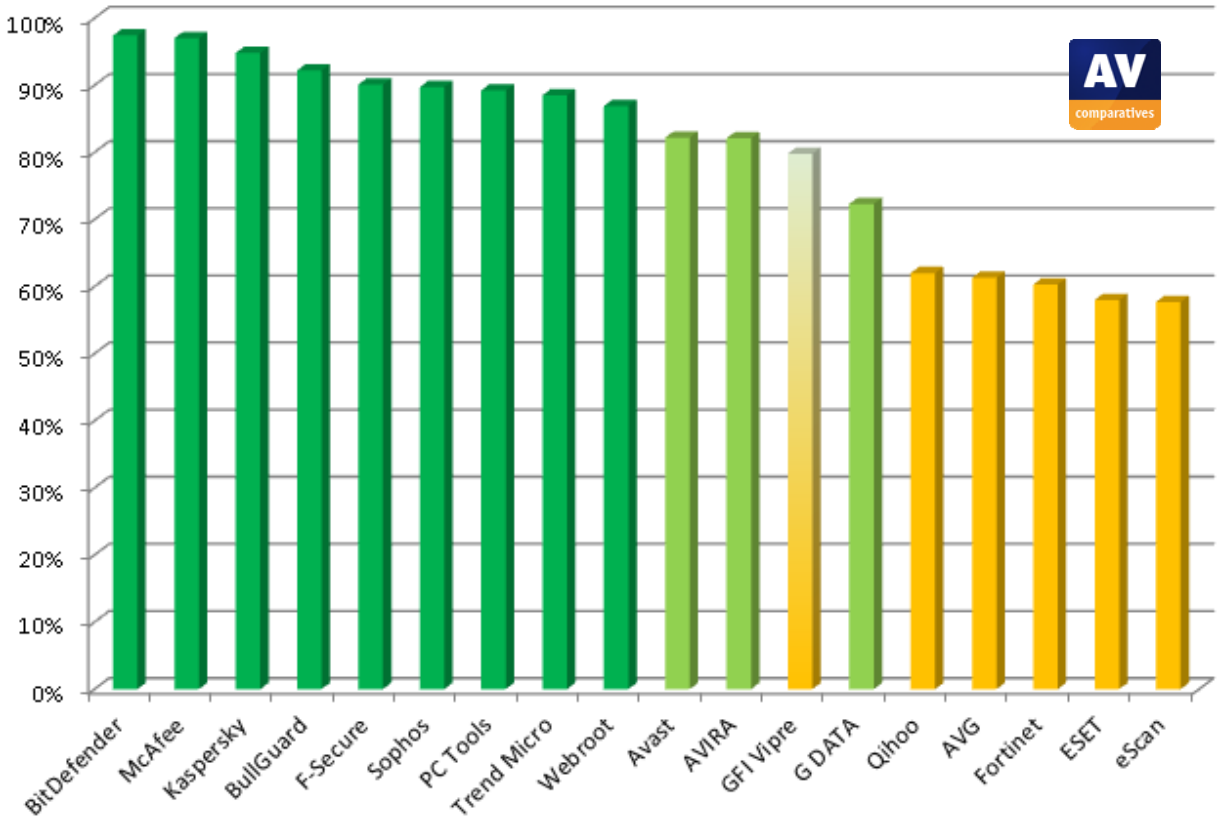
- Bank24 from Russia

The discovered false alarm has been reported to the respective vendor and is now no longer blocked.

Test Results

Below you see the percentages of blocked phishing websites (size of test set: 574 phishing URLs). Please take into consideration the false alarm rates when looking at the below results (products with false alarms are marked with an asterisk).

1.	BitDefender	97,4%
2.	McAfee	97,0%
3.	Kaspersky	94,8%
4.	BullGuard	92,2%
5.	F-Secure	90,1%
6.	Sophos	89,7%
7.	PC Tools	89,2%
8.	Trend Micro	88,5%
9.	Webroot	86,9%
10.	Avast	82,2%
11.	AVIRA	82,1%
12.	GFI Vipre*	79,8%
13.	G DATA	72,3%
14.	Qihoo	62,0%
15.	AVG	61,3%
16.	Fortinet	60,3%
17.	ESET	58,0%
18.	eScan	57,7%



Award levels reached in this test

The awards are decided and given by the testers based on the observed test results (after consulting statistical models). The ranking system for this Anti-Phishing test was:

Ranking system	**Anti-Phishing Protection under 50%**	**Anti-Phishing Protection Cluster 3**	**Anti-Phishing Protection Cluster 2**	**Anti-Phishing Protection Cluster 1**
zero FPs	Tested	Standard	Advanced	Advanced+
1 to 3 FPs	Tested	Tested	Standard	Advanced
4 to 6 FPs	Tested	Tested	Tested	Standard
More than 6 FPs	Tested	Tested	Tested	Tested

The following awards are for the results reached in this Anti-Phishing Test:

AWARD LEVELS	PRODUCTS
	BitDefender McAfee Kaspersky BullGuard F-Secure Sophos PC Tools Trend Micro Webroot
	Avast AVIRA G DATA
	GFI Vipre* Qihoo AVG Fortinet ESET eScan
	-

** downgraded by one rank due to a wrongly blocked banking site (FP).*

Copyright and Disclaimer

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

AV-Comparatives e.V. (August 2012)