反钓鱼测试

2011 年 8 月

语言：中文

2011 年 8 月

修订:2011 年 10 月 15 日

www.av-comparatives.org

简介

本测试报告仅是对德国“个人电脑杂志[1]”委托的，且最近已在该杂志上发表的一项反钓鱼测试的简要总结。由于所有的测试结果已印刷成杂志的形式，结果是几个月前的，本测试始于 2011 年 8 月。委托方在其杂志上公布了自己的报告后，我们也被允许发表这个简短的报告。

目前，在我们每年的主要测试系列中，反钓鱼测试还不是固定的测试，但是可以将此次作为反钓鱼测试的首次尝试。因此，本次测试（至少此次）没有设立任何评测结果。

什么是网络钓鱼？

Wikipedia [2]的解释是：

“网络钓鱼攻击是一种通过以电子通讯的方式，伪装成一个可信任的实体来尝试获取机密信息例如用户名、密码和信用卡资料的方法。它类似于钓鱼，钓鱼的人将诱饵放到鱼钩上，为鱼提供假象，鱼以为是真正的鱼食。但里面藏有钩子，这样钓鱼的人几乎能钓到整湖的鱼。这些电子通讯声称自己来自流行的社交网站、拍卖网站、在线支付网站或 IT 管理员，常用来引诱不知情的公众。钓鱼攻击通常通过欺骗性电子邮件或即时通讯软件达到目的，它往往引导用户将详细的信息，输入到一个无论外观还是感觉，都同合法网站基本相似的假冒网站。”

更多关于如何避免网络钓鱼诈骗的信息，请登录反钓鱼工作组消费者咨询网站：

http://www.antiphishing.org/consumer_recs.html

测试步骤

我们仅在本次测试中，模拟普通的用户凭借已安装的安全产品提供的反钓鱼保护功能，而正常浏览网址的情形（和/或进入邮箱检查电子邮件，反垃圾邮件功能不被考虑，由于它不属于本次测试的范围）。测试在 VMware 下，使用了 Windows XP SP3 和 IE7（为获取第三方的浏览结果，未使用内置钓鱼拦截器）。对所有安全产品使用默认设置进行了测试。对所有产品的测试，使用相同的网址在同一时间同时进行。

[1] PC Magazin 11/2011:http://www.pc-magazin.de

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

测试的产品

被测试的产品由委托本次测试的杂志选择。测试产品的版本在测试的时候（2011 年 8 月），都已投入使用。以下 19 个产品被列入本次反钓鱼测试：

- **AVG** Internet Security 2011
- **Avira** Premium Security Suite 10.1
- **Bitdefender** Internet Security 2012
- **Bullguard** Internet Security 10.0
- **eScan** Internet Security 11.0
- **ESET** Smart Security 4.2
- **F-Secure** Internet Security 2011
- **G DATA** Internet Security 2012
- **K7** Total Security 11.1
- **Kaspersky** Internet Security 2012
- **McAfee** Total Protection 2011
- **Panda** Internet Security 2012
- **PC Tools** Internet Security 2011
- **Qihoo** 360 Internet Security 2.0
- **Quick Heal** Internet Security 2011
- **Symantec** Norton Internet Security 2011
- **Trend Micro** Titanium Internet Security 2012
- **Trustport** Internet Security 2012
- **Webroot** Internet Security Complete 7.0

我们也被要求测试 **Avast**、**MSE** 和 **Sophos**。但 AVAST 和 Sophos 这两款产品，除了可以使用垃圾邮件过滤器功能阻止钓鱼邮件外，不具有任何反钓鱼功能。微软能用其浏览器（Microsoft Internet Explorer）和垃圾邮件过滤器（例如 Microsoft Outlook）拦截钓鱼站点；但这并不是它的设计初衷。

注：

ESET 还没有一个专用的反钓鱼保护模块。然而，它部署的各种技术，如针对钓鱼登陆页面本身可疑内容的网页过滤、家长控制和检测，目前钓鱼网站已连同其他可能有害的网站一同被阻止（如同其他大多数产品一样）。

Qihoo 主要针对中国的钓鱼站点。

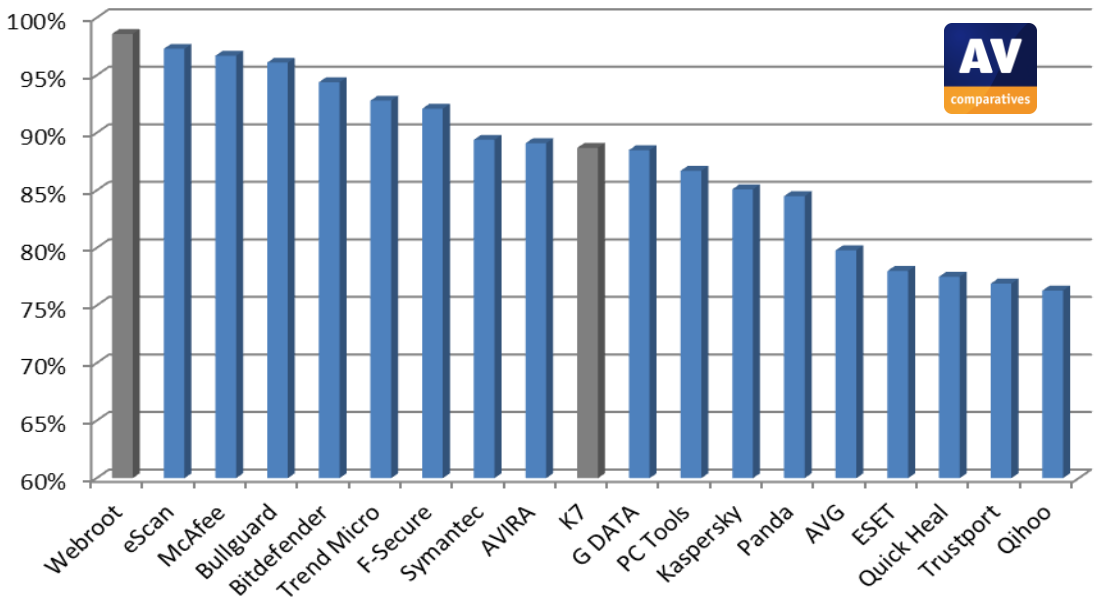
测试集

有的钓鱼网站是从发送的流行钓鱼邮件中提出，有的是由我们的抓网程序和研究人员收集的。所有钓鱼网站须曾经活跃或在线，且试图获得个人信息。重复的钓鱼网站，以及钓鱼活动在同一台主机或 IP 地址的也被移除。测试后，所有的测试情况又被手动重新核实。最终，仅保留了 697 个不同和有效的钓鱼网站。钓鱼行动将各类个人资料作为索取目标。在这些目标中（安照下列顺序），钓鱼攻击试图收集例如登录验证信息等，用于：PayPal、eBay、网上银行和信用卡、社交网络、网络游戏、电子邮件账户和其他通过网络提供的服务。

测试结果

下面您看到的是拦截的钓鱼网站的百分比（测试集的大小：697 个钓鱼网址）。看下面的结果时（有误报的产品拦截率后标有星号），也请将误报率考虑进来（在下页）。

1. Webroot 98.6%*
2. eScan 97.3%
3. McAfee 96.7%
4. Bullguard 96.1%
5. Bitdefender 94.4%
6. Trend Micro 92.8%
7. F-Secure 92.1%
8. Symantec 89.4%
9. AVIRA 89.1%
10. K7 88.7%*
11. G DATA 88.5%
12. PC Tools 86.7%
13. Kaspersky 85.1%
14. Panda 84.5%
15. AVG 79.8%
16. ESET 78.0%
17. Quick Heal 77.5%
18. Trustport 76.9%
19. Qihoo 76.3%



反钓鱼“误报”测试

对反钓鱼误报测试，我们选择了全球 1000 个合法的银行站点（全部使用 HTTPS），来检查这些安全产品是否会对这些合法的在线银行站点进行拦截。误报拦截此类站点属于严重的错误。在测试的 19 个产品中，只有两款产品（K7 和 Webroot）对这 1000 个测试用的合法的网上银行网站做出了误报：

K7（1 个误报）：

- 马来西亚的伊斯兰银行（ Bank Islam）

Webroot (12 个误报):

- 俄罗斯的 AB Finance Bank
- 肯尼亚的肯尼亚银行（Bank of Kenya）
- 黎巴嫩的 BLC 银行
- 日本的大和银行
- 印度的 Dhanlaxmi 银行
- 阿联酋的 Habib Bank Zuricj
- 荷兰的 ING 银行
- 塞浦路斯的 Marfin Laiki Bank
- 以色列的 Refah Bank
- 瑞典的 Saxo eBank
- 墨西哥的 ScotiaBank
- 印度的 UCO Bank

误报结果已分别呈报给厂商，目前已不再被拦截。

产品分别支持哪些浏览器？

多数浏览器已包含自己的反钓鱼技术。然而，由于社交网络诈骗和钓鱼攻击的复杂性以及数量之众，还是建议用户使用专业安全产品提供的反钓鱼功能。几乎所有的安全产品，都支持主流浏览器（如 Internet Explorer 和 Firefox），而只有少数产品也支持其他浏览器。因此，使用受安全产品支持的浏览器来执行网上银行操作可能更安全。

	Microsoft Internet Explorer	Mozilla Firefox	Google Chrome	Opera	Apple Safari
AVG Internet Security	支持	支持	支持	不支持	不支持
AVIRA Premium Security Suite	支持	支持	不支持	不支持	不支持
Bitdefender Internet Security	支持	支持	支持	支持	支持
Bullguard Internet Security	支持	支持	不支持	不支持	不支持
eScan Internet Security	支持	支持	不支持	不支持	不支持
ESET Smart Security	支持	支持	支持	支持	支持
F-Secure Internet Security	支持	支持	不支持	不支持	不支持
G DATA Internet Security	支持	支持	支持	支持	支持
K7 Total Security	支持	支持	不支持	不支持	不支持
Kaspersky Internet Security	支持	支持	支持	支持	支持
McAfee Total Protection	支持	支持	不支持	不支持	不支持
Panda Internet Security	支持	支持	支持	支持	支持
PC Tools Internet Security	支持	支持	支持	不支持	不支持
Qihoo 360 Internet Security	支持	不支持	不支持	不支持	不支持
Quick Heal Internet Security	支持	支持	不支持	不支持	不支持
Symantec Norton Internet Security	支持	支持	支持	不支持	不支持
Trend Micro Titanium Internet Security	支持	支持	支持	支持	支持
Trustport Internet Security	支持	支持	不支持	不支持	不支持
Webroot Internet Security	支持	支持	不支持	不支持	不支持

版权及免责声明

AV - Comparatives 是在奥地利注册的非盈利性组织。

更多关于 AV - Comparatives 及测试方法，请访问我们的网站。

AV-Comparatives e.V. (2011 年 10 月)