Anti-Virus Comparative

真实世界中文版XP

漏洞防御测试

语言：中文

2014年11月

最后编译：2014年12月8日

本测试由腾讯委托

www.av-comparatives.org

1 简介

现在，上网已经成为家庭和企业用户日常活动不可分割的组成部分。人们日常的沟通、生活、游戏、商务、购物、教育等等，几乎都离不开网络。但人们在家里和工作单位常常使用过时的软件上网，殊不知，这些过时的应用程序包含着已知的漏洞。微软已宣布从2014年4月8日开始，停止为Windows XP提供更新服务。然而，很多人仍然在自己的家庭或工作电脑中使用Windows XP。这些程序漏洞为攻击者在受害者的电脑上运行恶意代码提供了机会，而受害者一方却得不到任何警告。受害者的电脑被感染后，攻击者可以使用这些恶意代码，来窃取用户的网上银行、信用卡、个人隐私、企业的商业秘密等信息，甚至通过锁定用户的电脑来逼迫受害者支付赎金。

在企业环境中，最大的威胁和考虑是对偷渡式下载的利用，因为这种攻击不需要用户互动就可以启动受害者电脑上的恶意软件。甚至企业常用的传统的、合法的站点也会受到恶意软件的感染。高级持续性威胁（APT）攻击也常常利用漏洞和偷渡式下载攻击。

家庭用户和中小型企业往往对于漏洞、漏洞预防、定向攻击及软件更新的重要性缺乏了解和认识。大型企业要面对管理复杂IT系统的挑战，因此，他们往往会成为漏洞和恶意软件攻击的目标。

对于系统的保护，终端保护产品经历了一个从传统的基于特征码的保护，到使用现代的方法来实施保护的漫长的演变过程。目前，高级启发式扫描技术、沙盒技术、入侵防御系统、URL过滤、基于云的网页信誉服务系统、Java脚本分析、内存损坏保护等，都被用于抵御现代的恶意软件的威胁。为了测试终端保护系统，首先需要测试由该系统所部署的所有保护模块，还需准确地模拟标准用户的操作行为进行测试。当今绝大部分的威胁是通过网页进行传播的，所以，我们将测试的重点集中在基于网页的漏洞方面进行测试，但测试还涉及其他的感染场景。当终端保护系统无法保护用户避免恶意软件入侵时，损害则可能是灾难性的。有可能产生灾难性破坏的威胁的例子不胜枚举：比如，有可以窃取机密信息的恶意软件，或者可以删除重要文件或整个工作站的恶意软件。这些攻击可能对企业的知识产权造成巨大的经济损失，甚或几个星期内无法正常执行业务流程。我们的测试包含范围广泛的、不同的恶意软件类型，从而尽可能地模拟现实世界的使用情况。

本次评测由腾讯委托，我们对适用于Windows客户端的腾讯电脑管家进行了评估。

本报告是对腾讯电脑管家的功能性，以及当安装到客户端后，腾讯电脑管家对偷渡式攻击漏洞防御的评估。为了客观地进行评估，本次测试另外还选用了六个竞品一同测试。每款产品都安装在终端上，使用39个in-the-field和Metasploit 的漏洞进行了测试。

简要的漏洞防御测试结果，如下图所示：

（每个测试案例的详细结果说明请参考第3章节）

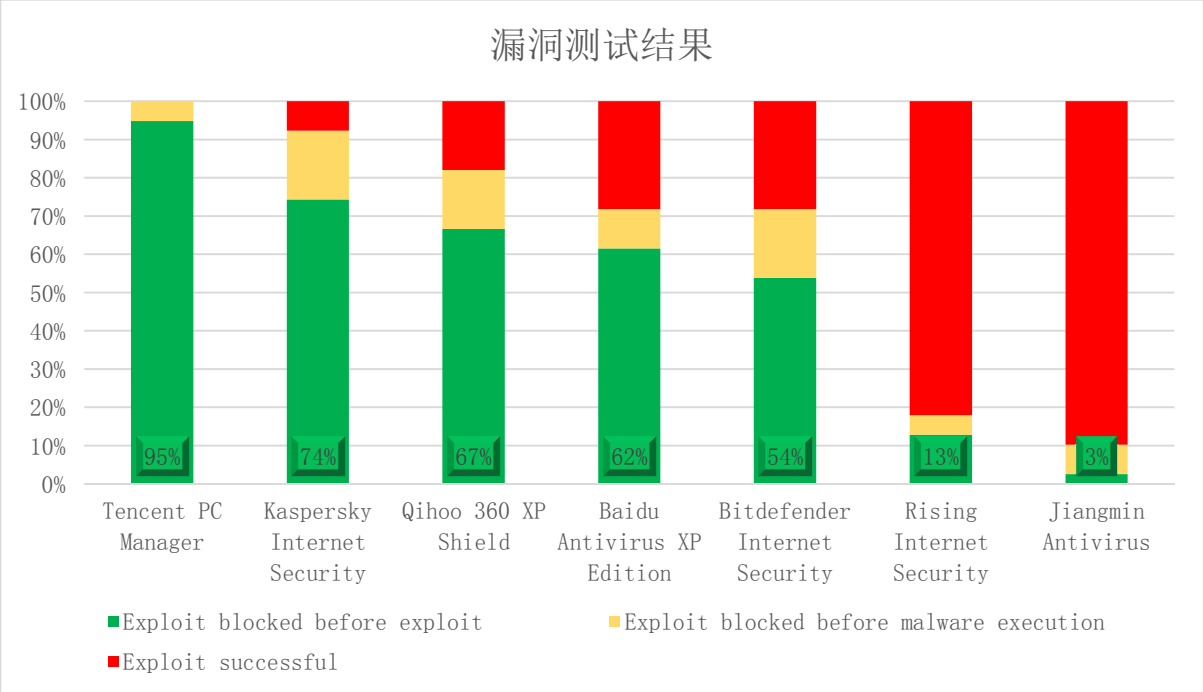

图 1 - 漏洞检测分布图

从结果中我们可以得出结论：有一款保护程序与其他保护程序相比凭借其卓越的保护功能而胜出。

- 腾讯电脑管家

1.1 测试方法

测试按下列方法执行：

1. 1.创建了一个默认安装Windows XP（简体中文）SP3的终端虚拟机(Virtualbox).（中文Windows XP仍然是流行的操作系统)。配置了一个桥接和NAT接口。将默认HTTP/HTTPS的代理服务器配置指向在主机操作系统中使用桥接接口运行的代理服务器。代理服务器上的SSL/TLS数据未被拦截，因为没必要增加测试的复杂性，毕竟凭借有效的SSL证书却能被漏洞挟持的站点是非常少见的。
2. 2.操作系统的安全性通过下列操作被减弱:
    a. IE浏览器的SmartScreen被禁用
3. 安装了下列易受攻击的软件：
    a. Adobe Reader 9.1.0
    b. Internet Explorer 8.0.6001.18702
    c. Microsoft Office 2003

    这些版本号码要求必须具备下列两个条件：
    1. 能够利用这个指定版本的in-the-field漏洞的数量是最高的，从而提高测试的覆盖率。
    2. 这个版本目前必须是用户普遍使用的。
4. Windows更新被禁用。
5. 从现在开始，从虚拟机上创建了8个不同的快照（Snapshot），每个快照都有不同的终端保护产品，其中一个没有。此过程可确保各测试系统之间的基本系统是完全相同的。下列终端安全产品使用如下配置参与了本次测试：
    a. 没有额外保护，此快照已被用于感染操作系统，并验证漏洞的重现（详细信息请参考2.5).
    b. 百度杀毒 XP 专版 3.0.0.4605
    c. Bitdefender Internet Security 18.19.0.1345
    d. 腾讯电脑管家10.0.15127.901
    e. 江民速智版杀毒软件16.0.0.100
    f. Kaspersky Internet Security 15.0.1.415 (a)
    g. 奇虎 360 XP 盾甲 9.7.0.1004
    h. 瑞星杀毒软件V16+ 24.00.21.37

    安装了使用默认配置的终端保护程序，开启了清除可能不受欢迎的软件的功能，如果安装过程中，选择云/社区参与的话，该选项就会启用。
6. 使用未受到保护的操作系统，抓取恶意URL或利用Metasploit漏洞，以及测试人员等待新进程（恶意软件）启动，或如果启动Metasploit时，都将会打开一个新的会话。除了传统的偷渡式下载漏洞以外（启动恶意程序时无需用户干预，只需访问受感染的URL），我们模仿那些打开 Office 文件（例如.xls、.doc、.pdf文件）的用户和那些在同一局域网内攻击Windows服务的攻击者。如果是偷

渡式漏洞，整个漏洞的数据会被代理服务器记录下来。除了其他的“真实世界保护测试”，未直接启动二进制可执行文件下载（例如.exe文件）。基于Downloader的ActiveX，VBscript和Office 宏文档不在测试范围。

7. 当一个in-the-field漏洞成功执行后，虚拟机被恢复到干净状态，数据会被代理服务器重现。重现意味着浏览器像以前一样运行，但是由代理服务器取代原始的网络服务器，在所记录的数据的基础上来答复请求。在重现过程中，不允许其它的通讯。这意味着不匹配的请求（先前没有记录的）一律使用 HTTP404代码答复。当“重现的漏洞”能够感染操作系统的时候，漏洞数据被标记为一个测试来源。这一方法可以保证，即使原始的漏洞利用元件在测试期间出故障的情况下，完全相同的数据也将会被终端保护程序检测到。如果是Metasploit漏洞，且漏洞对操作系统/浏览器的攻击已进行了测试，要是漏洞失效，我们就调整漏洞来支持测试配置。虽然这或许是公理，但重点需要注意的是，本测试步骤之后，没有漏洞数据案例被删除，每个测试都包含在最后的结果中。对于HTTPS通讯数据的测试，是连接原始站点，而不进行重现。
8. 当新的漏洞数据或Metasploit漏洞被成功利用后，终端保护程序按照随机的顺序进行测试。在测试漏洞站点之前，验证终端保护程序已经更新到具有最新病毒库的最新版本，并且每个云连接都有效。如果需要重启系统，则会重新启动。为了保证有效的云连接，设置代理服务器时，允许不匹配的请求通过，也未加密SSL/TLS。本阶段的测试也未使用VPN。当需要用户参与时（例如访问不建议的网站等），则会选择阻止/拒绝操作。除了Sysinternals 的Process Monitor外，系统中未运行其他进程。
9. 导航到漏洞站点后，打开被感染的文档，或攻击系统，为了检查新的进程，该系统受到监控，或为了将要被打开的会话窗口而检查Metasploit服务器。分析的结果请参阅 1.5.
10. 当一个终端保护套装测试完毕后，随机挑选新的终端保护程序进行测试，直到所有终端保护产品全部测试完毕。
11. 进程再重新回到第7步，直到所有39个漏洞测试案例一一完成。

虚拟机专门使用了下列硬件：

- 内存1GB
- 1核Core-i7 1.7 GHZ处理器
- 15G 硬盘空间
- 1NAT 和1个桥接接口

1.2 In-the-field漏洞来源

本次测试的漏洞来源仅包括那些进入系统后立即启动恶意软件的漏洞。通过进程管理器（Process Monitor）验证，寻找Operation = Process Create，要么引导恶意软件执行，要么通过regsrv32，cmd.exe，wscript.exe等进行。或者如果在内存恶意软件中，检测到其他人为感染，如恶意软件C&C回调函数。

对不同的终端保护程序，都是在6小时内执行随机测试。

所使用漏洞的差异，请参阅第2.5节。

合作的厂商都是在测试完成后，才得到详细的样本，包括URL和代码。

1.3 Metasploit漏洞

对于 Metasploit 漏洞，我们使用了下列Metasploit漏洞设置：

- 未做修改的内置漏洞
- 为了支持中文XP系统，已修改的漏洞
- 内存恶意软件
- 已入侵的定制的恶意软件
- Javascript 脚本混淆
- 加密的载荷传输

1.4 误报测试

由于没有相关的误报测试能够真正衡量在此种复杂情况下的误报率，所以未执行误报测试。对网站拦截功能组件执行误报测试,不能被视为有效的误报测试，因为这只是衡量终端保护程序的一个功能组件。

1.5 漏洞测试结果

本次测试时间从2013年11月13日持续到2014年11月25日。

对于in-the-field漏洞，终端保护程序需要在以下几个阶段阻止漏洞：

1. 通过URL数据库（本地或云数据库）阻止URL(受感染的URL、Exploit Kit URL、重定向URL)，或通过分析然后阻止包含恶意Javascript的页面（重定向、iframe、进行模糊处理的Javascript等）。通常受到终端保护的浏览器，可以显示一个通知消息 “网站已被阻止”。
2. 在漏洞Payload被执行前（如“下载恶意软件并执行shellcode”）阻止漏洞。比如，如果是IE漏洞，该漏洞页面被传输给浏览器，浏览器对页面进行判断，但在代理通讯过程中，它可以得到验证，恶意软件的加载请求尚未启动。
3. 在启动之前，通过分析恶意软件，阻止下载有效载荷（进程创建）。如在代理通讯过程中，可以看到恶意软件的载荷数据下载（Cleartext数据或加密文件），但不启动恶意软件进程。
4. 已由入侵的恶意软件完成进程创建，或者恶意软件已通过其他机制完成加载。

为了简化结果，第一和第二个漏洞防御阶段已被合并。在这一阶段，在被执行攻击的电脑上没有运行恶意指令。这是对终端保护系统能够预料到的保护行为；攻击者没有机会对被执行测试的电脑执行任何不受信任的代码。

第三阶段是终端保护系统阻止恶意软件的最后机会。值得一提的是，本拦截阶段非常重要，因为恶意代码（漏洞代码的payload-又名shellcode）需要能够在受攻击的电脑中先运行。虽然这通常是某种恶意软件偷偷植入被攻击电脑的“下载并执行”的一种代码，但攻击者很容易在不被终端防御系统察觉的情况下，更改这个有效载荷。

如果是Metasploit漏洞，当漏洞被利用后，Metasploit控制台打开一个会话时，则被算作是一次系统保护失败。当杀毒/互联网安全套装发出了攻击预警，阻止了会话窗口，但Shellcode却能够运行，这种情况被当作是警告。如果Metasploit控制台没有会话被打开且Shellcode不能运行，则杀毒/互联网安全套装保护成功。

如果终端保护系统没能阻止漏洞，而是让Payload继续下载恶意软件并运行，那么该被测试的产品对系统的保护彻底失败。大多数情况下，被测试的终端保护系统都能够检测到某些或全部的恶意软件，但由于以下原因,无法进行记录/计数：

- 测试的范围是漏洞防御，而不是对在系统中运行的恶意软件的检测。
- 无法确定恶意软件所执行的命令或恶意软件已泄露的信息。数据泄露无法撤消或修复。
- 由于终端保护系统已阻止了恶意软件，所以无法确定已停止运行的恶意软件，或恶意软件发现了监控进程（procmon.exe）、虚拟机，或未发现其目标环境而停止运行。

- 检查恶意软件的修复极其耗时，且修复成分很难界定。例如，测试过程中我们收到过几种警告，说终端保护系统拦截了URL/页面/漏洞/恶意软件，但恶意软件始终能够在系统中执行且运行。还有几次，终端保护系统已将恶意软件代码从磁盘中删除了，但恶意软件进程仍在运行，或恶意软件的一部分已被检测到并被处理，但是其它部分却未被检测到。
- 有时产品阻止了运行中的恶意软件的某些部分或全部，但却未能向用户或管理员通知/警报该事件。

通过使用简单的度量标准，我们相信零容忍理由可以帮助消费者选择最好的产品。手动验证恶意软件的成功修复，在一定程度上需要人力和财力的付出。我们认为，必须在恶意软件运行之前将其拦截。如果用户收到电脑中的恶意软件已被拦截的警报，强烈建议在专业人士的帮助下，花点儿时间更深入地查验此警报。

相对于我们之前所做的测试而言，本次测试包括In-the-field的Fileless攻击，该恶意程序并未被写入硬盘，而只是在内存中。

1.6 用于测试的漏洞工具分析

除了Metasploit漏洞外，本次测试还使用了下列漏洞工具：

- Nuclear Pack
- Fiesta
- Astrum
- Sweet Orange
- Angler EK

在测试IE Metasploit 漏洞时，为了支持中文版XP系统，不得不对7个漏洞进行修改。通常，IE漏洞取决于DLL版本，而对于XP而言，还取决于操作系统使用的语言。如果DLL版本或操作系统使用的语言不同，漏洞通常会失效。另一方面，除了版本和语言的差异外，有些漏洞需要进行适当调整。

1.7 对测试所使用的漏洞的简要说明

下图表显示的是所使用的漏洞的分布数量，我们使用了多个杀毒引擎来对漏洞进行分类。

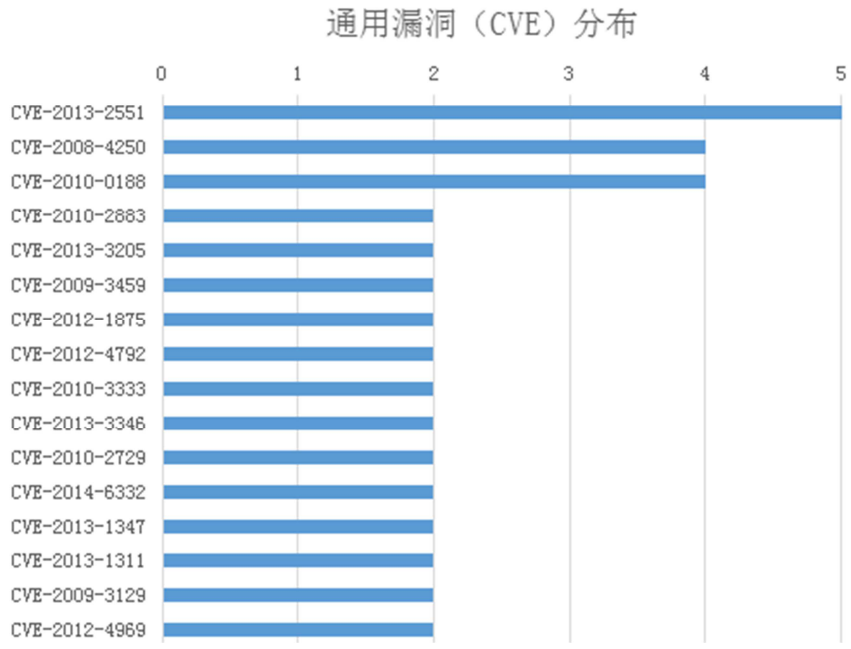

图 2 - 通用漏洞（CVE）分布数量

下图显示的是漏洞利用的软件的分布数量。MSF代表Metasploit漏洞数量，代表in-the-field漏洞数量。

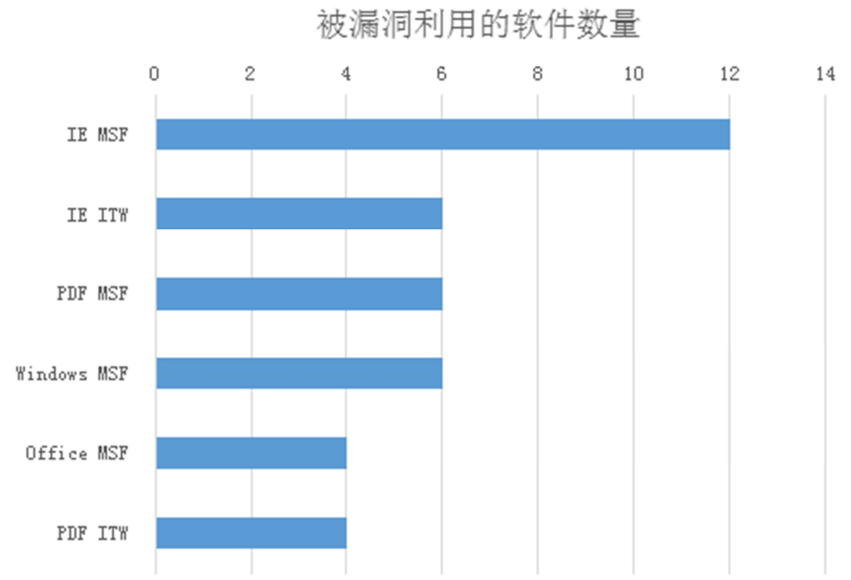

图 3 - 漏洞利用的软件的分布数量

2 最终结果

我们将结果划分为两个部分：

第一部分是产品真正拦截漏洞的能力：当威胁出现在恶意URL中、HTML/Javascript 或处于漏洞阶段时，都对威胁进行了拦截。

第二部分是当威胁出现在URL中、 HTML/Javascript中，漏洞或Shellcode执行阶段时，威胁被拦截。

两部分之间的区别是，如果某款产品第二部分的拦截结果高于第一部分，则意味着产品缺乏对特定漏洞的检测，仅仅检测到二进制的有效载荷。这一保护的问题是，它在防御的最后阶段才将恶意软件拦截，而恶意软件可能会通过使用新的变异或通过一个新的或有针对性的恶意软件，轻易地绕开安全产品的拦截。从攻击者的角度，开发新的不被检测到的恶意软件比寻找和利用新的漏洞更容易。另一个问题是，漏洞的Payload已经能够在机器上运行，除了“下载并执行”外（例如创建后门用户，非持久性的后门壳，内存恶意软件等），还有不同的功能。

2.1 漏洞测试结果

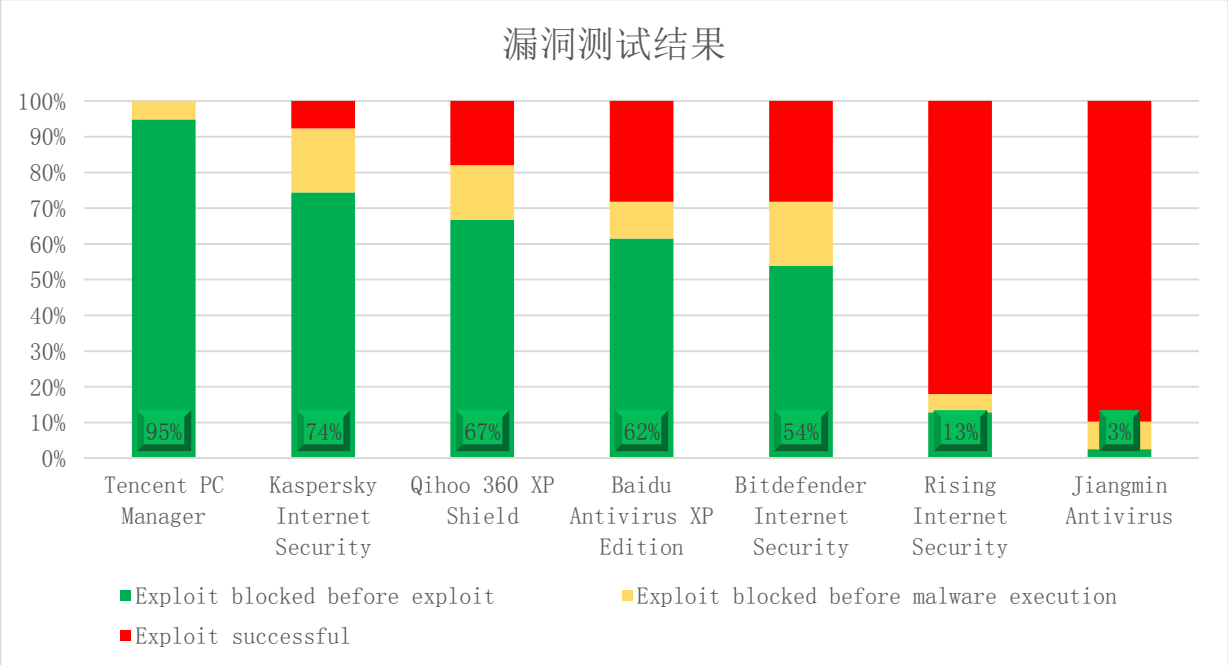

图 4 – 漏洞拦截比例分布

从结果中我们可以得出结论：有一款终端保护程序与其他保护程序相比凭借其卓越的保护功能而胜出。

- 腾讯电脑管家

Copyright and Disclaimer

(December 2014)