针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 概览
- 反病毒软件工作原理
- 反病毒小贴士

什么是反病毒软件?

概览

客座编辑

Jake Williams是Rendition Infosec（www.renditioninfosec.com）的创始人，并且是一名认证的SANS讲师和课程作者。他活跃在Twitter（@MalwareJake）上，并且有一个博客（malwarejake.blogspot.com）。

反病毒软件是一种安装在电脑或移动设备上的用来避免恶意软件感染的程序。“恶意软件”这个术语是对病毒、蠕虫、木马和间谍软件等恶意软件的统称。事实上，这个术语（malware）源于“恶意（malicious）”和“软件（software）”两个词。如果你的电脑被恶意软件感染，那么攻击者就能捕捉你的击键记录，窃取你的文档，并且用你的电脑去攻击他人。和一些人以为的相反，任何操作系统——包括Mac OS X和Linux——都能被感染。

你可以购买单独的反病毒软件，抑或是购买包含反病毒软件的安全套装。问题是反病毒软件赶不上攻击者的变化，攻击者时刻都在开发、发布新的恶意软件。每天都有种类繁多的新恶意软件被发布，没有反病毒软件能检测并且完全阻止它们。这也就是为什么你一定要了解，反病毒软件可以保护你的电脑，但它不能阻止一切种类的恶意软件。为了更好地理解为什么，让我们来看看这些反病毒软件是如何工作的。

反病毒软件工作原理

大体上反病毒软件有两种识别恶意软件的方法，一种是签名检测，另一种是行为检测。签名检测就像是人的免疫系统，它扫描电脑并通过查询已知恶意软件的字典，寻找已知的恶意程序的特征或者签名，如果找到就将之清除。如同人的免疫系统，恶意软件字典需要更新来防范新的恶意软件，这就好比注射流感疫苗一样。反病毒软件只能防范那些它们认识的恶意软件。问题在于，攻击者以极快的速度研发新型恶意软件，以至于反病毒软件厂商难以跟上。结果是，即使你的反病毒软件刚刚

什么是反病毒软件?

才更新，总会有能绕过你的反病毒软件的新的恶意软件变种。

尽管反病毒软件是安全构成的一个重要要素，但它并不能检测并且阻止一切攻击。归根结底，你——而非技术，才是最强的防线。

通过行为检测，反病毒软件并不是要尝试识别已知的恶意软件，而是要监控电脑上安装的软件。当某个程序行为可疑——如尝试访问受保护的文件或修改另一个程序——时，基于行为的反病毒软件就能发现可以举动并且向你报警。这一方法能让你免遭已知恶意软件字典之外的新型恶意软件的侵扰。这种方法的问题在于，它可能会误判。你，作为电脑的使用者，也许经常并不确定到底该允许还是不允许一些操作，于是久而久之你就对这些警告麻木了。你也许想在每次警告出现时都点“允许”，而这回让你的电脑处于被攻击和被感染的风险之下。除此以外，在行为被检测到之前，恶意软件已经在电脑上运行了，你也许不知道在反病毒软件识别它之前，它都做了些什么。

反病毒软件是保护你电脑的一项重要举措。我们建议你只要可能，就安装并且积极地使用它。然而，关键要记住，无论你的反病毒软件如何工作，它都不能帮你抵御所有种类的恶意软件。归根结底，你——而非技术，才是最强的防线。

反病毒小贴士

1. 只从已知的受信任的来源和厂商获取反病毒软件。攻击者的一个常用伎俩就是打着反病毒软件的旗号传播恶意软件。
2. 确保你安装了最新的反病毒软件，你的年订阅付了款且处于活跃状态，并且你的反病毒软件配置为自动更新。如果你的电脑离线或者关机了一段时间，那么你的反病毒软件就需要在你开机或重连互联网后更新自己。不要推迟这些更新。

什么是反病毒软件?

3. 确保你的杀毒软件自动扫描便携介质，如U盘，并且确保实时保护处于开启状态。
4. 注意屏幕上由反病毒软件生成的警告或报警。大多数报警包含获取更多信息或下一步建议的选项。如果你在公司配备的电脑上看到报警，务必马上和咨询台或你的上司取得联系。
5. 不要因为你觉得反病毒软件在拖慢你的电脑速度、阻止一个网站或不让你安装一个app或程序就禁用或者卸载它。禁用你的反病毒软件将让你暴露在不必要的风险之下，并且可能造成严重的安全问题。如果工作电脑上问题持续，就联系你的咨询台；如果个人电脑上问题持续，就联系反病毒软件厂商，访问他们的网站获取更多信息或者替换你的反病毒软件。
6. 不要在电脑上安装多个反病毒软件。这样做很有可能会让它们之间互相冲突，从而导致电脑安全性不升反降。
7. 学习辨认反病毒软件生成的警告。攻击者能建立恶意网站，制造假的反病毒软件警告，说是要帮你“修复”你的电脑。点击网站上的这些链接或按钮实际上会损害你的电脑。

了解更多

订阅OUCH！安全意识月刊，访问OUCH！过往存档，了解更多关于SANS安全意识解决方案的信息，请访问：http://www.securingthehuman.org

相关资源

反病毒软件比较: http://www.av-test.org/en/

《社会工程学》: http://www.securingthehuman.org/ouch/2014#november2014

《钓鱼邮件》: http://www.securingthehuman.org/ouch/2013#february2013

《我被入侵了，怎么办？》: http://www.securingthehuman.org/ouch/2014#may2014

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻译：成自豪