针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 什么是恶意软件
- 谁？为什么？
- 保护你自己

什么是恶意软件

概览

当人们谈论网络安全的时候，你也许听到这样一些术语，比如病毒、蠕虫、木马或者rootkit。这些术语用来描述网络罪犯用来感染或者控制计算机和移动设备的程序的种类。今天我们把这些不同类别的程序统称为恶意软件。本期我们将解释什么是恶意软件，谁开发它们，为什么开发它们，以及你所能采取的保护自己的措施。

客座编辑

Lenny Zeltser就职于NCR Corp.，专注于保护客户的IT操作安全，并且在SANS Institute教授恶意软件对抗课程。他活跃在Twitter（@lennyzeltser）上，并且有一个安全博客（blog.zeltser.com）。

什么是恶意软件

简单来说，恶意软件是一种用作实施不良行径的电脑程序。事实上，恶意软件（malware）一词就是由“恶意”（malicious）和“软件”（software）两个词来的。大多数网络罪犯的终极目标就是在你的电脑或者移动设备上安装恶意软件。一旦安装成功，这些攻击者就有可能获得对其的全面控制。许多人有这样的误解，那就是恶意软件只针对Windows系统的电脑。当然，Windows使用广泛，因此自然成为了一个巨大的目标，但其实恶意软件能感染任何计算机设备，包括智能手机和平板电脑。事实上，针对移动设备的恶意软件的流行程度正稳步增长。另外，切记，每个人都是一个目标，包括你。网络罪犯感染的电脑和移动设备越多，他们从中牟取的利益就越大。这些罪犯通常不关心他们感染谁，只要感染的人越多就越好。

谁？为什么？

以前恶意软件或许还只是一些爱好者或新手黑客写的，现在不一样了，它们往往由思维缜密的网络罪犯制作以实现特定的目标。这些目标可能包括窃取机密数据，获取登录账密，发送垃圾邮件，发动拒绝

什么是恶意软件

服务攻击，勒索或者窃取身份。比如，一款名为Cryptolocker的恶意软件就是用来感染并且加密你电脑上的所有文件的；一旦感染、加密成功，这些网络罪犯就索要一笔赎金，用以交换解密机会。创造、安装恶意软件并从中获利的，既有独立行动的个人，也有组织有序的犯罪团伙或者政府组织。除此以外，当今那些复杂恶意软件的作者往往都专注于这一目的，他们的全职工作就是开发恶意软件。事实上，他们一做好恶意软件，就经常把它们卖给个人或组织，并且提供日常更新和“客户”服务。其他罪犯购买了这些恶意软件后，就通过在数以百万毫无戒心的受害者的系统上安装它们，创建一个由被感染系统组成的僵尸网络，以此牟利。这个僵尸网络成为了一个远程操控的军队，网络罪犯之后可以将它作为己用，或是将被感染电脑卖给其他违法者。

保护自己免受恶意软件侵扰的最佳方法就是保证设备持续更新，可能的话装有反病毒软件，并且要时刻警惕攻击。

保护你自己

保护电脑和移动设便免受恶意软件侵扰的常见方法是从受信任的厂商安装反病毒软件。反病毒软件——有时叫做反恶意软件软件，是一种设计来检测并组织恶意软件的安全软件。然而，反病毒软件并不能阻挡或清除所有恶意软件。网络攻击者在不停地创新、开发新的更为复杂的能绕过病毒查杀的攻击手段；反过来，反病毒软件厂商也在不停更新它们的产品，往其中加入检测新恶意软件的新功能。在很多方面，这成为了一场军备竞赛，两方都想超越对方。不幸的是，网络罪犯几乎总占上风。因此，记住，尽管反病毒软件能检测出并且阻挡许多恶意软件，攻击者总能创造出新的被反病毒软件忽略的版本。这样一来，你就无法仅仅依赖反病毒软件，你还要采取额外的措施来保护自己。首先，保证你的操作系统和程序启用了自动安装安全更新的功能。你的操作系统越新，网络罪犯就越难感染你的电脑或移动设备。

什么是恶意软件

其次，记住，你是对抗恶意软件的最佳防卫之一。恶意软件在感染过程中经常涉及社会工程学，也就是攻击者欺骗、愚弄你以达到为他们安装恶意软件的目的。一个常见的例子就是钓鱼式攻击，即通过一些看起来合法但其实虚假的电子邮件来骗你感染你的电脑。比如，一个网络罪犯可能给你发送一封电子邮件，这封邮件装作是来自你的银行，要你点一个链接。如果你点击这个链接，你就会被带到一个自动尝试入侵、感染你电脑的网站那儿去。又或许他们给你发一个通知，说你的包裹无法配送，要你大概附件里的跟踪文档，你一打开就会遭遇感染。

社会工程学攻击也在其它技术领域发生，比如电话。举个例子，黑客可能会装作微软技术支持给你打电话，告诉你你的电脑被感染了。他们讲的其实是假话，你的电脑最有可能是安然无恙的。他们的目标是愚弄你，让你相信你被感染了，然后骗你给他们提供你的系统的远程访问权，或者让你买他们的安全软件——其实是恶意软件。有点常识，过过大脑。如果一个电话或者短信有点奇怪、可疑或者好得不可能是真的，那么它们最有可能就是这样。

最后，保护自己免受恶意软件侵扰的最佳方法就是保持软件最新，从知名厂商安装反病毒软件，并且对那些企图愚弄你进而感染你电脑的人保持警惕。

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

OUCH钓鱼攻击:
www.securingthehuman.org/resources/newsletters/ouch/2013#february2013
OUCH保护你的电脑:
www.securingthehuman.org/resources/newsletters/ouch/2012#december2012
海报“你就是目标”:
http://www.securingthehuman.org/resources/posters

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