电脑用户安全意识月刊

OUCH!

本期摘要

- 什么是恶意软件
- 是谁开发的恶意软件?
- 自我保护

恶意软件

概述

当你跟别人讨论网络安全的时候，或许已经听说过诸如病毒、木马、勒索软件或者rootkit之类的名词。这些都是网络罪犯用以入侵电脑和其他设备的程序，统称为恶意软件。我们将在本期简刊中解释什么是恶意软件，谁在开发恶意软件，为什么会有人开发恶意软件，以及最重要的是你该如何进行防范。

客座主编

Lenny Seltzer任职NCR Corp，负责公司客户的系统安全，并在SANS机构教授恶意软件防范。关注Lenny的推特账号@lennyzeltser以及安全知识博客zeltser.com。

什么是恶意软件?

简单来说，恶意软件是用于进行恶意行为的软件，即计算机程序。实际上，恶意软件(malware)这个术语就是由两个单词恶意的(malicious)以及软件(software)组合而成。网络罪犯在你的电脑或者设备上安装恶意软件从而对其进行操控或者获得所存储资源的访问权限。一旦恶意软件安装成功，攻击者能够使用恶意软件来监控你的网上活动，盗取你的密码或文件，或者利用你的系统来攻击他人。恶意软件甚至可以剥夺你对自己文件的访问权限，从而向你勒索钱财。

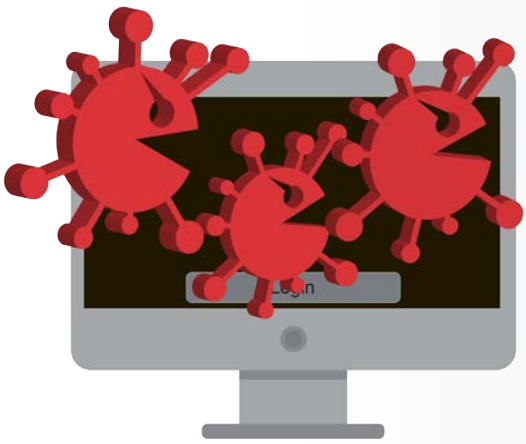
很多人认为恶意软件只针对于运行Windows系统的电脑，这是不对的。Windows作为最为广泛使用的操作系统天然地成为一大攻击目标，但是恶意软件可以入侵苹果电脑、手机或者平板电脑等。网络罪犯入侵的电脑和设备越多，他们赚的钱就越多。所以，每个人都是他们的目标，当然，你也不例外。

谁在开发恶意软件

恶意软件的开发者不再是热衷于计算机技术的业余黑客或者电脑技术爱好者，而是专业的网络罪犯。他们的目标就是利用你受感染的电脑或其他设备赚钱，比如售卖所盗取的数据，发送垃圾邮件，开展拒

恶意软件

绝服务攻击或者进行敲诈。这些软件很多不是小团体或者个人秘密地编写和散播，反而有很多知名企业甚至政府部门涉嫌此类软件。如今的开发者普遍将此作为全职工作，致力于恶意软件的开发。另外，一旦他们开发出了恶意软件，往往会卖给其他的个人或者组织，甚至向其提供定期的软件更新和技术支持。



防范恶意软件，请警惕可疑信息，更新设备并安装杀毒软件。

自我防范

一个普遍的方法是安装可信任的杀毒软件。这类工具，有时也被称为反病毒软件，是用来检测并停止恶意软件。然而，杀毒软件并不能够阻拦或者移除所有的恶意程序。网络罪犯不断地创新，开发新型的、复杂度更高的恶意软件以规避杀毒软件的检测。另一方面，杀毒软件的提供商也在不断地更新他们的产品，从而能够检测到更多的恶意软件。从很多方面来看，这已然是一场军备竞赛，双方不断地试图智取另一方。不幸的是，道高一尺，魔高一丈。既然不能够完全依赖杀毒软件，以下是几点自我保护的其他措施：

- 网络罪犯通常利用软件的漏洞来入侵电脑或其他电子设备。所以，你的设备上运行的软件版本越新，漏洞就越少，被攻击的难度就越高。所以，确保你的操作系统、应用软件和设备已开启自动更新。
- 一种常用的感染移动设备的方法就是开发一个假的移动应用，发布到网络上然后骗取人们下载安装。因此，只从可信任的网络商店下载应用。另外，只安装发布时间比较长、下载人数众多并且好评较高的移动应用。
- 在电脑上使用有权限限制的使用者账户，而不是像管理员、超级用户等特权账户。这样能够阻止很多类型的恶意软件进行自我安装。
- 网络罪犯通常诱骗人们自行安装恶意软件。比如说，他们可能给你发送一封看似合理的有附件或者链接的邮件。或者这个邮件看起来是来自你的银行或者朋友。然而，一旦你打开了附件或者点击了链接，你将激活恶意程序从而在你的系统上安装恶意软件。如果一个信息试图营造一

种很紧张的气氛，或者很让人困惑，又或者是像天上掉馅饼，那这很有可能是一次攻击行为。保持警惕性，你的生活常识是最佳防御手段。

- 定期在云端或者移动硬盘上备份你的系统和文件，从而保护你的备份免受恶意软件的加密或者移除。系统备份很重要，一旦被恶意软件入侵，这有可能是你恢复系统的唯一途径。

最后，防御恶意软件入侵的最佳方法就是使用最新版本的软件，安装来自知名厂商的杀毒软件以及时刻保持警惕，以防有人企图诱骗你感染自己的系统。

了解更多

订阅OUCH! 安全意识月刊，查看OUCH!往期内容，以及了解有关SANS安全意识方案的其他内容，尽在http://www.securingthehuman.org.

Dyn is a cloud-based Internet Performance company. Dyn helps companies monitor, control, and optimize online infrastructure for an exceptional end-user experience. Through a world-class network and unrivaled, objective intelligence into Internet conditions, Dyn ensures traffic gets delivered faster, safer, and more reliably than ever.

相关资源

网络钓鱼:	https://securingthehuman.sans.org/ouch/2015#december2015
保证安全的五个步骤:	https://securingthehuman.sans.org/ouch/2014#november2014
安全使用移动APP:	https://securingthehuman.sans.org/ouch/2015#january2015
平板电脑安全使用手则:	https://securingthehuman.sans.org/ouch/2016#january2016
社交媒体:	https://securingthehuman.sans.org/ouch/2015#august2015

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻译：陈柳希