SANS SECURITY AWARENESS

OUCH!

給大家的安全意识通讯月刊

停止此恶意软件

概述

当人们提到网络安全时, 您可能已经听说过诸如病毒、特洛伊木马、勒索或 Rootkit 之类的术语。 这些是不同类型的恶意程序, 称为恶意软件, 亦是网络罪犯用来感染计算机和设备上的。 一旦安装了, 他们便可任意做他们想要做的。 要了解恶意软件是什么, 它会构成什么样的危险, 最重要的是你能做些什么来保护自己免受它的伤害。

什么是恶意软件

简单而言, 恶意软件是指软体: 一个计算机程式: 用于执行恶意操作。 这一用语是恶意和软件的组合 网络犯罪分子会在您的计算机或设备上安装恶意软件, 以获取它们的控制权。 一旦安装了, 恶意软件可以使犯罪分子监视您的在线活动, 窃取您的密码或文件, 或使用您的系统来攻击他人。 恶意软件甚至可以控制你所拥有的文件, 在然后要求你支付赎金, 才可赎回你的文件。 许多人认为恶意软件只是在Windows计算机才出现问题。 遗憾的是, 恶意软件可以感染任何设备, 从苹果电脑电脑和智能手机到DVR甚至安全摄像头。 网络罪犯感染的电脑和设备越多, 他们赚的钱就会越多。 因此, 每个人都是目标对象, 包括你在内。

保护自己-停止恶意软件

你可能认为所要做的只是安装一个安全程式, 例如防病毒软件, 那么以后你就安全不会受到感染。 遗憾的是, 防毒產品无法阻止所有恶意软件。 网络犯罪分子不断开发新的和更复杂的恶意软件, 便可以逃避检测。 反过来, 病毒软件供应商亦不断更新其产品, 以检测恶意软件的新功能。 在许多方面, 它已经成为一个军备竞赛, 然而坏人通常会抢先一步。 由于您无法单靠依赖病毒软件, 所以有些额外步骤, 您应采用来保护自己:

网络罪犯经常利用你的软件漏洞来感染计算机或设备。 你的软件越多, 系统的漏洞就会越少, 网络罪犯去感染病毒的难度也就越大。 请保持您的操作系统、应用程序、浏览器和浏览器插件以及设备确保更新, 並且是最新的。 确保这一点的最简单方法是尽可能启用自动更新模式。

网络罪犯感染计算机或移动设备的一种常见方式是创建假冒的计算机程式或移动应用程序，将它们张贴在互联网上，然后诱使您下载和安装一个程序。 只从受信任的在线商店下载和安装程式或应用程序。此外，远离品牌新的移动应用程序，很少有积极的评论，绝少更新或很少有人下载的应用程序。 已经不再使用的计算机程序或移动应用程序？ 删除它

网络罪犯经常欺骗人们来为他们去安装恶意软件。 例如，他们可能会向您发送一封看似合法并且包含附件或一个带有链接的电子邮件。 也许电子邮件似乎是来自你的银行或朋友。 然而，如果要打开附加的文件或单击该链接，则会激活在系统上安装恶意软件的恶意代码。 如果一条消息产生强烈的紧迫感，或者好得令人难以置信，这个可能是一种攻击。 保持怀疑，基本常识便是你的最佳防御。

定期将系统和文件备份到基于云的服务，或将备份存储在脱机状态，比如在断开连接的外部驱动器上。这样可以保护您的备份，以防恶意软件试图加密或删除它们。 备份是重要的关键，它们通常是从恶意软件感染了，要恢复的唯一方法。

最终，抵御恶意软件的最佳方法是保持所有软件和设备为最新状态，尽可能安装可信任的防病毒软件，并警惕任何试图诱使您感染您系统的人。 当所有其他操作失败时，常规备份通常是您用来恢复操作的唯一方法。

特邀编辑

Lenny Zeltser 他通过在密涅瓦实验室和在SANS学院任教时，创建了端点安全产品並用於进行打击恶意软件。 Lenny在Twitter上活跃名为 @lennyzeltser 他还编写安全博客，可参阅以下纲址 zeltser.com.

资源

勒索软件: https://www.sans.org/u/EdI
备份: https://www.sans.org/u/EdN
停止网络钓鱼: https://www.sans.org/u/EdS