电脑用户安全意识月刊

OUCH!

本期摘要

被攻击了，我该怎么办?

概述

每个人都非常注意保护自己电脑以及移动设备的安全，然而，无论你如何安全地使用这些科技产品，你早晚都有可能被攻击或者被危及。本期简报将告诉你如何判断自己的电脑或移动设备是否被攻击，以及如果被攻击该如何采取措施。通常来说，越早发现有问题出现并且越快做出反应，你受到的损失就很可能越小。

客座主编

Samantha Davison (@sam_e_davison) 是优步(Uber)公司安全意识和教育项目的主管，负责向其分布在全球超过350个城市的员工进行安全培训。

被攻击的线索

判断是否自己被攻击了并不是一件容易的事情，因为并没有一个简单易行的方法来帮助你判断。相反，攻击者通常会留下一系列的蛛丝马迹。在以下所列举的迹象中，你的系统符合的条数越多，那么你已经被攻击的可能性就越大。

- 你的杀毒软件弹出系统已被感染的警告，特别是它无法移除或隔离受感染的文件。
- 你的浏览器主页被篡改或者你的浏览器自动打开你并没有点击的网页。
- 你的电脑或设备上出现了并非你所创建的新账户，或者运行了你没有安装的程序。
- 你的电脑或者应用程序频繁崩溃，不断弹出未知应用程序的图标或者陌生的窗口。
- 一个程序要求获取你的授权以对你的系统做更改，尽管你没有安装或者更新任何应用软件。
- 当你试图登录系统或者网上账户时发现密码失效，即便你确定输入了正确的密码。
- 被朋友们问起为什么要给他们的邮箱发垃圾邮件，但是你从来没有这么做过。
- 你的移动设备在你不知情的状况下向收费号码发送短信。

被攻击了，我该怎么办?

- 你的移动设备莫名其妙地消耗了大量的数据流量或者电量。

你的电脑或者设备多多少少都有可能被危及，发现并采取措施得越快越好。

我该怎么办

如果你认为你的电脑或者设备已经被攻击了，那么越快做出反应越好。如果该电脑或者设备是由公司提供的，或者被用于工作，那么不要试图自行解决问题。不仅是有可能造成更大的损失，而且还有可能破坏有关调查的宝贵证据。相反，应该立即向你的雇主反应情况，通常是联系你的帮组台、安全小组或者监管。如果出于某些原因你无法联系到相关部门，或者你担心来不及汇报，请即刻将你的电脑或者设备断开网络连接，然后开启休眠、暂停或者飞行模式。即便你并不确定是否被攻击，也可以马上汇报情况。不怕一万，就怕万一。如果你使用的是个人电脑或者设备，那么以下是你可以采取的几个措施。

- **更改密码**：除了更改你电脑或者移动设备的密码，还有你所有的网络账户的密码。确保不使用已被攻击的电脑来更改密码，而是使用一台不同的且安全的电脑或者设备。
- **杀毒软件**：如果你的杀毒软件提醒你有受感染的文件，请采取其推荐的措施，通常包括隔离、清理或者删除该文件。大部分杀毒软件都提供链接供你了解更多有关信息。如果有疑问，隔离该文件。如果无法进行隔离，就进行删除。
- **重建**：如果你无法修复系统或者你想要确保你的系统已经被修复，一个更安全的措施就是重建系统。对于电脑而言，请按照你的系统提供商的使用说明。通常情况下这意味着用内置的工具来重新安装操作系统。如果没有内置工具，或者这些工具已损坏或者被感染，请联系你的系统提供商寻求帮助或者访问其网页。不要通过你的备份重装系统，因为其很有可能包含同样的漏洞能够使黑客再一次控制你的电脑。备份应该仅被用来进行数据恢复。对于移动设备，请遵从你的设备制造商或者服务提供商的使用说明，一般都能够在其网站上找到。大多情况下，恢复

被攻击了，我该怎么办?

出厂设置即可。如果你觉得自己无法完成重装，请考虑向专业服务寻求帮助。或者，如果你的设备很老旧，可能换一个新设备更简单实惠。最后，一旦你重建或购买了新的电脑或设备，确保该设备已经升级到最新版本并开启自动更新。

- **备份**：你能够采取的最重要的自我保护措施就是提前进行日常备份。备份的频率越高越好。有些更新方案能够每小时自动备份新的或者更改的文件。无论拟采用哪种备份方案，请定期检查备份以确保你能够使用该备份恢复文件。通常从备份中恢复数据是你恢复损失的唯一途径。
- **法律途径**：如果你感觉到被威胁了，请向当地司法机构提起诉讼。

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

备份与恢复:	https://securingthehuman.sans.org/ouch/2015#august2015
密文:	https://securingthehuman.sans.org/ouch/2015#april2015
恶意软件:	https://securingthehuman.sans.org/ouch/2016#march2016
平板电脑安全使用手则:	https://securingthehuman.sans.org/ouch/2016#january2016

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

