

OUCH!








给大家的安全意识通讯月刊

我被黑客攻击了吗？

概述


不管你如何防备，就像开车一样迟早会发生意外。 以下是帮助你找出你是否被黑客攻击的线索，以及如果是的话，那该怎么办。 你越早发现坏的事情发生了，你就越有可能解决这个问题。


你被黑客攻击时出来的线索

-  您的防病毒程序会产生一个系统已被感染的警报。 请确保它是您的防病毒软件从网产生成的警报，而不是一个从网站弹出窗口，试图欺骗你去打一个电话或安装其它东西。 不确定吗？ 打开您的防病毒程序。
-  你会得到一个弹出窗口，说你的电脑已被加密，你必须支付赎金来找回你的文件。
-  您的浏览器正在带您到不是您想去的各种网站。
-  您的电脑或应用程序不断崩溃，有未知的应用程序或奇怪的窗口弹出的图标。
-  即使您知道正确密码，您的密码也不再有效。
-  朋友问你为什么你正在发送垃圾邮件给他们，而你知道你从来没有发送。
-  您的信用卡有不明消费或从您的银行帐户中有不该有的提款。


如何应对


如果你怀疑自己被黑客入侵了，你越早行动越好。 如果被黑客入侵的部份是与工作相关，不要试图自己解决问题，立马回报。 如果是个人系统或帐户已被黑客攻击，以下是您可以采取的一些步骤

 **更改你的密码:** 这不仅包括更改您的电脑和移动设备上的密码, 而且还包含您的在线帐户。 不要使用黑客攻击过的电脑去更改你的密码, 而是使用您知道安全的其它不同系统。 如果你拥有多个帐户, 首先便要从最重要的开始。 无法追踪您的所有密码, 请使用密码管理器。

 **金融理财:** 对于您的信用卡或任何财务帐户上的问题, 请立即致电您的银行或信用卡公司。 使用受信任的电话号码来调用他们, 例如从您的银行卡背面、财务报表或从受信任的电脑参观其网站。 此外, 考虑对您的信用档案进行信用冻结。

 **防病毒:** 如果您的防病毒软件通知您受感染的文件, 请按照它建议的操作。 大多数防病毒软件都有链接您可以跟随了解有关特定感染的更多信息。

 **重新安装:** 如果您无法修复受感染的电脑, 或者您想要更确定您的系统是否安全, 请重新安装操作系统。 不要从备份中重新安装, 而备份只应用于恢复您的个人文件。 如果重建让您觉得不舒服, 请考虑使用专业服务来帮助您。 或者, 如果您的电脑或设备是旧的, 购买一套新的可能更容易。 最后, 一旦您重新构建了系统或购买了一套新设备, 请确保它已更新, 尽可能启用自动更新。

 **备份:** 保护自己的一个关键步骤是, 提前准备定期备份。 许多解决方案将每天甚至每小时自动备份你的文件。 无论您使用哪种解决方案, 定期检查您是否能够还原这些文件。 通常, 恢复数据备份是唯一可以从被黑客攻击中恢复的方法。

 **求助执法部门:** 如果您觉得有任何威胁, 请向当地执法部门举报该事件。 如果您是身份盗窃的受害者, 并设在美国, 则访问<https://www.identitytheft.gov>。

特邀编辑

Dr. Johannes Ullrich ([@johullrich](https://twitter.com/johullrich))是SANS技术研究所研究院长, SANS网络风暴中心的主任和SANS研究员。 他创造了DSShield协作传感器网络, 并主持了互联网风暴中心的每日网络安全新闻播客。



资源

备份: <https://www.sans.org/u/JGP>
口令句: <https://www.sans.org/u/JGU>
密码管理器: <https://www.sans.org/u/JGZ>
恶意软件是什么: <https://www.sans.org/u/JH4>
信贷冻结: <https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/>

OUCH! 由SANS SecurityAwareness出版, 并以 [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) 许可证分发。只要您不修改内容, 您可以随意分发本通讯, 或者将其用于您的安全意识项目。有关翻译或更多信息, 请联系 www.sans.org/security-awareness/ouch-newsletter。编辑委员会: Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley | 翻译: Kathy Lee McClean