针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 概览
- 入侵的迹象
- 如何响应

我被入侵了，怎么办？

概览

我们知道你对保护你的电脑和信息这一点十分关切，并且也采取了保护措施。然而，正如驾驶一样，无论你开得多么安全，迟早你还是可能遭遇事故。本期，我们将教你判断你的电脑是否被入侵，并且被入侵的话如何应对。归根到底，发现越早，响应越快，你就越能减小你的组织所遭受的侵害。

客座编辑

Jake Williams（@MalwareJake，malwarejake.blogspot.com）是CSRgroup Computer Security Consultants的首席科学家，还是SANS课程“内存取证（FOR526）”和“恶意软件逆向工程（FOR610）”的作者之一。

入侵的迹象

首先，你需要了解的是，在许多情况下，要判定你的电脑是否被入侵是不可能一蹴而就的；取而代之的是，通常会有多个迹象可供判断。如果你发现了其中的多个，这就说明你的电脑被入侵了。这里有一些例子：

- 反病毒软件报告你的电脑遭到感染，尤其当它说无法清除或者隔离被感染文件。
- 浏览器莫名其妙变了主页，或者它把你带到你本不想访问的网站。
- 你电脑上有新帐号，而你此前并未创建。
- 有新的程序在运行，而你此前并未安装。
- 你的电脑老是崩溃或者运行很慢。
- 你并未主动安装或更新任何程序，却突然有个程序跳出来向你请求系统修改权限。
- 防火墙报告一个程序正在请求互联网访问权限，而你并不认识这个程序。

我被入侵了，怎么办？

如何响应

如果你相信你的电脑已经被入侵了，那么你响应得越快就越好。如果你用的电脑是公司派发的或者用于工作的，就先不要尝试自己修复，也不要关机。一方面，你这一举动带来的损害可能比好处还要多；另一方面，你还可能毁坏可以用于调查的宝贵证据。取而代之的是，你应该把这一事件马上上报给公司——通常通过前台、安全团队或监理。如果由于某个原因你无法联系到你的组织，或者你担心会有延迟，那么就断开电脑的网络连接，并且将其置于睡眠、挂起或者休眠模式。即使你并不确定你是否被入侵了，以防万一，你最好还是现在就上报。你的组织极有可能有相关的程序和一个团队来处理这样的情况，让他们来处理。

你的电脑迟早都有可能被侵入，发现得越早，响应得越快，就越好。

如果你的电脑是供个人使用的，下面是你能采取的一些措施：

- **备份**：你能采取的最关键的措施就是靠备份来防患于未然。具体来说就是定期备份你的数据并检查你的备份看其是否有效。很多时候，当一台电脑被入侵后，唯一可做的就是清空硬盘，然后重装操作系统，或者购置一台新电脑。无论是哪种方式，你都需要备份来恢复你的个人数据。
- **更改你的密码**：务必更换你所有的密码——包括你电脑和移动设备的密码，还包括你的网上密码，且是要从一台不同的你知道是可信并且安全的电脑上更改你的网上密码。
- **反病毒**：如果你的反病毒软件告知你有一个文件被感染了，那么你可以按照它推荐的措施——通常包括隔离、清理或删除被感染文件——来操作。大多数反病毒软件还提供链接让你能了解特定的感染。如果心存疑虑，就隔离它；如果这不可能，就删除。

我被入侵了，怎么办?

- **重装**： 如果你无法用反病毒软件清理系统，那么最安全的恢复方式之一就是完全重装系统。首先，断开网络连接；然后，遵循你的系统厂商的说明——大多数情况下意味着用内置的恢复分区来重装操作系统。如果没有恢复分区，或者恢复分区损坏或被感染，那么就联系你的厂商，让他们给你寄一张系统恢复DVD。不要用备份来重装操作系统，你的备份可能还有一样的漏洞，正是这些漏洞让黑客当初得逞。使用备份的唯一地方应该是在恢复个人数据。另外，如果你的电脑老旧过时，那么问题可能就简单多了（或许还更实惠）——与其花数小时来重装系统，不如去买一台新的。
- **专业帮助**：如果你担心你被入侵，但是又觉得你没有相关的技能或知识来解决这一问题，你也许会想把你的电脑转交给专业人士来代为处理。比如，在被入侵之后，你可能发现你的备份不完整或者过时了，在此情况下你可能想把相片、文档、视频等关键文件从被感染的电脑拷到一台新电脑上；然而你可能还没有意识到，你的这一举动可能也把恶意软件传到新电脑并且让它也被感染了。一个安全得多的选择是把被感染电脑带到一个认证的技师那儿去，让他来安全地恢复这些文件，而不必冒以上风险。

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! 《备份》：	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! 《密码》：	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! 《什么是恶意软件》：	http://www.securingthehuman.org/ouch/2014#february2014
海报“检测邪恶势力”：	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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