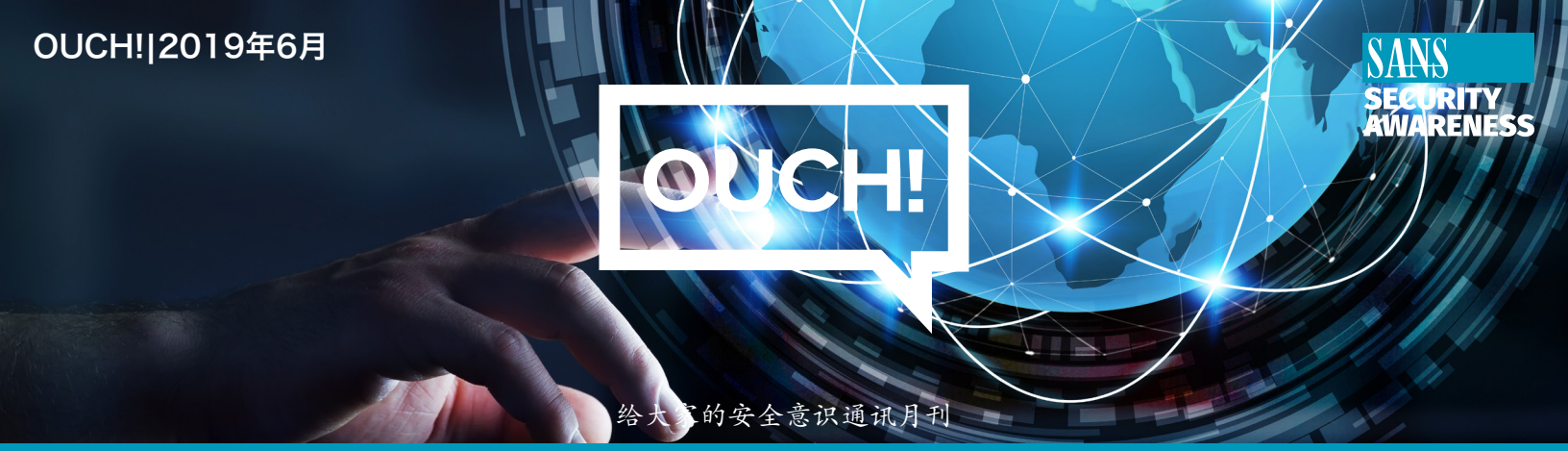

暗网

概述

你也许已经从别人或媒体那儿听过“暗网”这个词了，并且好奇什么是暗网，或是针对暗网，你是否应该做些什么。今天，我们将解释暗网是什么，以及对你来说意味着什么。

它是什么?

暗网由互联网上专门为安全、匿名地通信、分享信息而设计的系统构成。暗网不止一个，它不像 Facebook 那样由单一的组织来运营。取而代之的是，暗网由许多不同的人为不同的目的而管理的不同的系统构成。这些系统仍然与互联网连通，且是互联网的组成部分，然而你基本上不能通过正常的搜索引擎找到它们。你一般也需要特别的计算机软件来找到、访问它们。Tor 项目就是一个这样的软件。为了访问暗网，你下载、安装 Tor 浏览器。当你用 Tor 浏览器连接网站服务器的时候，你的加密流量会途径其它同样使用 Tor 的电脑。当你的流量在这些电脑间跳动的时候，源 IP 地址随之改变，这意味着当你的流量到达网站的时候，你的线上活动是匿名的。其它例子包括 Zeronet、Freenet 和 I2P。

谁使用它?

暗网的用户中有一大批是网络罪犯。为了使其购买毒品、售卖 GB 级泄露数据等犯罪行径完全匿名和安全，他们在暗网维护网站和论坛。例如，当网络罪犯入侵了一个银行或网店，他们会窃取尽可能多的信息，然后在暗网的网站上将其售卖给其它网络罪犯。

暗网也有合法的用处。例如，在监管猖獗的国度，人们可以用暗网来保护自身隐私、保持匿名的同时，分享信息，看世界上还发生了什么。记者、告密者和重视隐私的人可以用暗网来提升他们的匿名性，绕过监管。此外，这样的个人不仅可以用 Tor 浏览器这样的技术来访问暗网，还能匿名浏览常规的互联网。

我该做什么？

除非你有特定的理由访问暗网，我们建议你远离它。一些暗网网站被用于非法目的，其中有许多会在一个对等网络中，使用你的电脑来达成它们的目标，并且在某些情况下，你的电脑甚至还有可能被探测或攻击。一些公司提供监测服务，让你知道你的名字或其它信息是否已经被网络罪犯窃取，并且存在于暗网中。这些服务的实际价值有待商榷。保护你自己的最佳方式就是假定你的一些信息已经在暗网中被网络罪犯使用了。结果是……

- **对任务假装是官方组织并且迫使你采取交罚款等行动的电话和邮件保持怀疑。罪犯甚至可能会利用他们找到的关于你的信息来进行个性化攻击。**
- **监控你的信用卡和银行账单。或许甚至设置每日交易提醒。这样一来，你就能检测是否有财务诈骗正在发生。如果你检测到了，那就立马报告给你的信用卡公司或银行。**
- **冻结你的信用分。这不会影响你使用信用卡，并且是你能采取的避免身份窃取的最有效的方法之一。**

特邀编辑

Micah Hoffman （@WebBreacher）是 Spotlight Infosec LLC 的首席调查者、SANS Institute 的认证讲师和 SANS OSINT 课程的作者。Micah 对网络和开源情报的激情体现在他的项目、课件和教学方式中。

资源

个性化攻击:	https://www.sans.org/security-awareness-training/resources/personalized-scams
社会工程学:	https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering
身份窃取:	https://www.identitytheft.gov
信用冻结:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Tor 浏览器:	https://www.torproject.org/
SANS OSINT 课程:	https://sans.org/sec487