

OUCH!

每月安全意识通讯

在网上搜索你自己

概述

你很有可能已经听说过保护你的隐私以及你在网上分享的信息有多么重要了。为了阐明这一点，我们这次将尝试一些新的东西，我们将向你展示如何调查自己，并发现有哪些关于你的信息是公开的。这一过程叫做 OSINT——“开放来源情报” (Open Source Intelligence) 的一种高级叫法。其意思是，通过调查网上的公开资源，看看你能了解到关于一个电脑 IP 地址、一个公司或甚至像你这样的一个人的多少信息。记住，网络攻击者使用的正是这些工具和技巧。攻击者越了解你，就越能发起针对性攻击。这个概念已经存在许多年了，但是网上最新的工具使实现它变得尤其简单。

如何找寻信息

你不会在一个网站上找到所有信息。取而代之的是，你从一个网站开始，了解一些细节，然后利用这些细节去继续搜索和从其它网站了解更多信息；然后，你通过对结果的结合与比较，来创建你的目标的个人信息或档案。一个不错的起点便是谷歌、必应、DuckDuckGo 等搜索引擎。每个搜索引擎都索引了你的不同信息，所以一开始要用不止一个搜索引擎来搜索。从输入你的名字，并将其用引号括起来开始，但在此之后，用我们称为运算符的东西来扩展你的搜索。运算符是一种你可以加到搜索里，从而更好地解释你的搜寻意图的特殊符号或文字。如果你的名字很常见，那么它尤其重要。你可能需要加上更多的信息，诸如你的电子邮箱或你所在的城镇。在文末的“资源”部分了解更多关于运算符和高级搜索技巧的东西。例子：



- 我能在网上找到的关于这个人的信息
- 查找可能和这个人关联的电子邮箱
- 任何含有这个人姓名的 Word 文档

还有些专门供你了解其他人的网站。 尝试一个这种类型的网站, 看看关于你有哪些信息是公开的。 记住, 这些网站不总是精确的, 并且可能只在特定的国家有用。 你可能需要搜索好几个网站来确认你找到的信息。



- <https://pipl.com>
- <https://cubib.com>
- <https://familytreenow.com>

最后, 还有许多其它网站你可以搜索来了解更多, 这些网站包括谷歌图片、谷歌地图、社交网站等。 如果你想得到一个能供你了解自己的各种网站的交互式列表, 我们推荐你看看“OSINT 框架” (<https://osintframework.com>)。

为什么要在网上搜索你自己?



1. 了解其他人或组织在网上收集、发布或分享的关于你的信息 (教堂、学校、运动俱乐部或其它本地社区的网站)。
2. 明白这些资源同样也对其他任何人开放, 其中就包括网络罪犯——他们能用这些信息来锁定你。 保持怀疑。 例如, 如果你接到了一个声称是你银行的紧急电话, 仅凭他们知道你的一些基本信息并无法证明电话真的是你银行打来的。 取而代之, 你应该礼貌地挂断电话, 然后回拨一个你知道的确认是你银行的电话的号码, 来确认刚刚确实是他们打来的。 同样的道理也适用于电子邮件, 仅凭一封电子邮件中有关于你的一些事实并不意味着这封邮件就是真的。
3. 考虑一下你公开分享的信息, 以及它们可能对你、你的家人和你的员工造成的影响。

特邀编辑

Nico Dekens ([@dutch_osintguy](https://twitter.com/dutch_osintguy)) 专攻 OSINT。 他的吃、睡、生活——一切的一切, 都与网络情报收集和分析有关。 Nico 是一位活跃于 OSINT、IoT 和运维安全等课题领域的国际讲师, 常在财富 500 强公司和政府授课。



资源

社会工程学: <https://www.sans.org/u/LW6>
有关社交媒体的重要提示: <https://www.sans.org/u/LWb>
搜索引擎运算符: <https://support.google.com/websearch/answer/2466433>
OSINT 框架: <https://osintframework.com/>
SANS OSINT 课程 (SEC487): <https://www.sans.org/u/LWZ>

OUCH! 由SANS SecurityAwareness出版, 并以 Creative Commons 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, Alan Waggoner, Cheryl Conley | 翻译: Kathy Lee McClean