OSINT Primer：组织（第3部分）

请吃栗子吧 / 2019-04-02 09:50:00 / 浏览数 3900 渗透测试 渗透测试 顶(1) 踩(0)

翻译文章，原文链接：https://0xpatrik.com/osint-organizations/

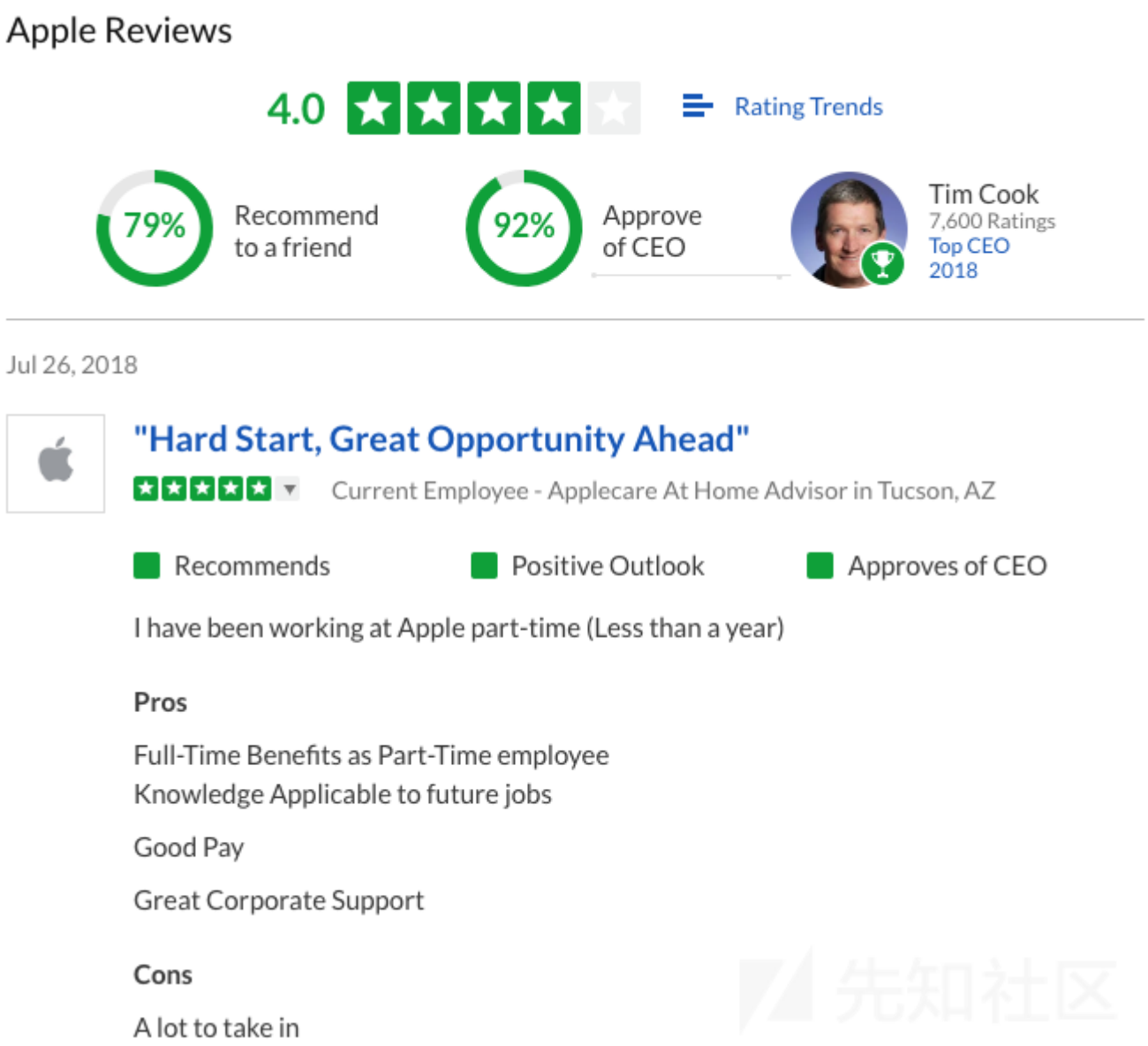
原文作者：Patrik Hudak

在之前的文章中，我介绍了很多关于OSINT的内容。然而，仍有一些技术和想法未被公开。我将它们放在了这篇文章中，因为我觉得它们大多与组织有关。话虽如此，不要

- 我正在与组织面谈/合作/做生意; 我想找到一些有关它们的信息。
- 我正在对组织进行安全评估/漏洞奖励; 我想找一些技术细节。

员工评价

一个组织和员工一样好。话虽如此，员工也喜欢写他们公司的匿名评价。当你考虑加入公司或寻找期望的薪水范围时，这尤其有用。最受欢迎的网站是Glassdoor Company Reviews。请注意，在查看所有评价之前，你需要先登录。一个类似的评价网站是Indeed。



如图，在Glassdoor.com上评论Apple Inc。

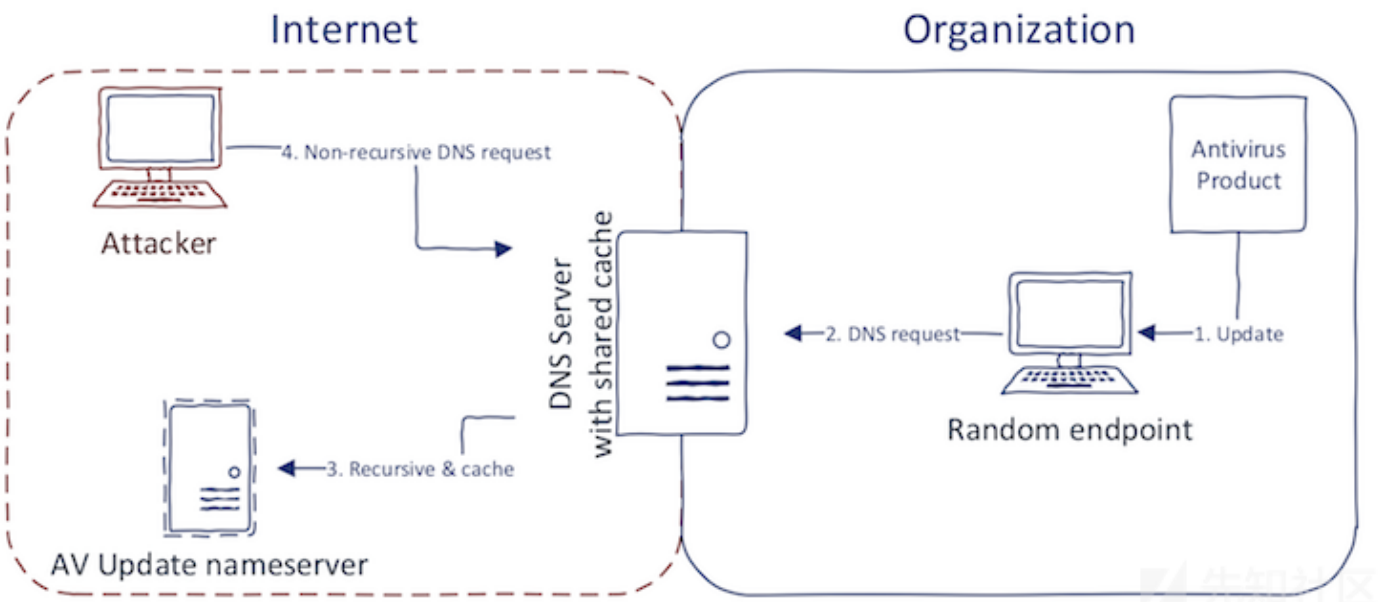
关于公司的商业类型信息往往是针对其注册国家的，所以我决定不大量关注这个文章。有一些聚合器，如opencorporates.com。我建议检查OSINT框架作为特定搜索提供

技术架构

从pentester的角度来看，了解组织的技术架构是一件有价值的事情。你希望最大限度地提高工作效率，因此了解公司使用的防病毒或出站代理可能有助于你构建攻击。我喜

- 关注招聘启事。他们通常包括职位所需的技能或经验。关注技术职位。你可以通过多种方式查看职位发布。一个好主意是LinkedIn Jobs。还有像Indeed或Monster Job这样的招聘网站。我建议使用Google dork查找所有可能的网站："<ORG_NAME>" intext:career | intext:jobs | intext:job posting。公司通常会在其网站上列出招聘信息。这种技术背后的想法很简单：组织倾向于保持一致，并在整个公司范围内部署相同的产品。
- 与之前的技术类似，在LinkedIn上查找组织的（技术）员工（查看上一篇文章）。他们很可能会拥有最新的认证和技能。请注意，可以在之前的演出中获取认证，因此我
- 检查stackshare.io。一些（主要是技术）公司公开分享其架构。
- 使用搜索引擎。你不应该把自己局限在招聘启事上。StackOverflow或员工关于特定产品的其他类似网站可能存在问题。这些步骤将需要更深入的OSINT。
- 元数据。组织通常在其网站上公开共享文档。你可以利用这一事实，默认情况下，Microsoft Office或Adobe Reader等流行的商业产品会将元数据附加到文件中。此元数据包含作者姓名，日期以及最重要的软件类型和版本等内容。你可以使用客户端漏洞利用某些软件的旧版本。Carnogursky撰写的这篇文章。
- 你希望在脱离网络的情况下找出网络内部正在运行的内容（请注意，外部扫描很可能不会告诉你正在部署的Web代理）。有一种方法，我仍然将其标记为实验性的。该方

基本思路是：你将检查组织的DNS缓存，以查看之前是否有对某个特定域的请求。为什么有用？想象一下杀毒软件。它会定期下载新签名。例如，某些来自McAfee的更新来



你可以使用以下dig命令执行非递归DNS查询：

```
dig @DNS_SERVER -t A DOMAIN_TO_CHECK +norecurse
```

通过外部 DNS服务器，我主要是指为组织的网站提供服务的DNS服务器，换句话说：

```
dig -t NS MAIN_DOMAIN
```

另一个问题是你需要知道产品的域名（即snooping签名）。有一个项目，如DNSSnoopDogg。但是它们已有一段时间没有更新。

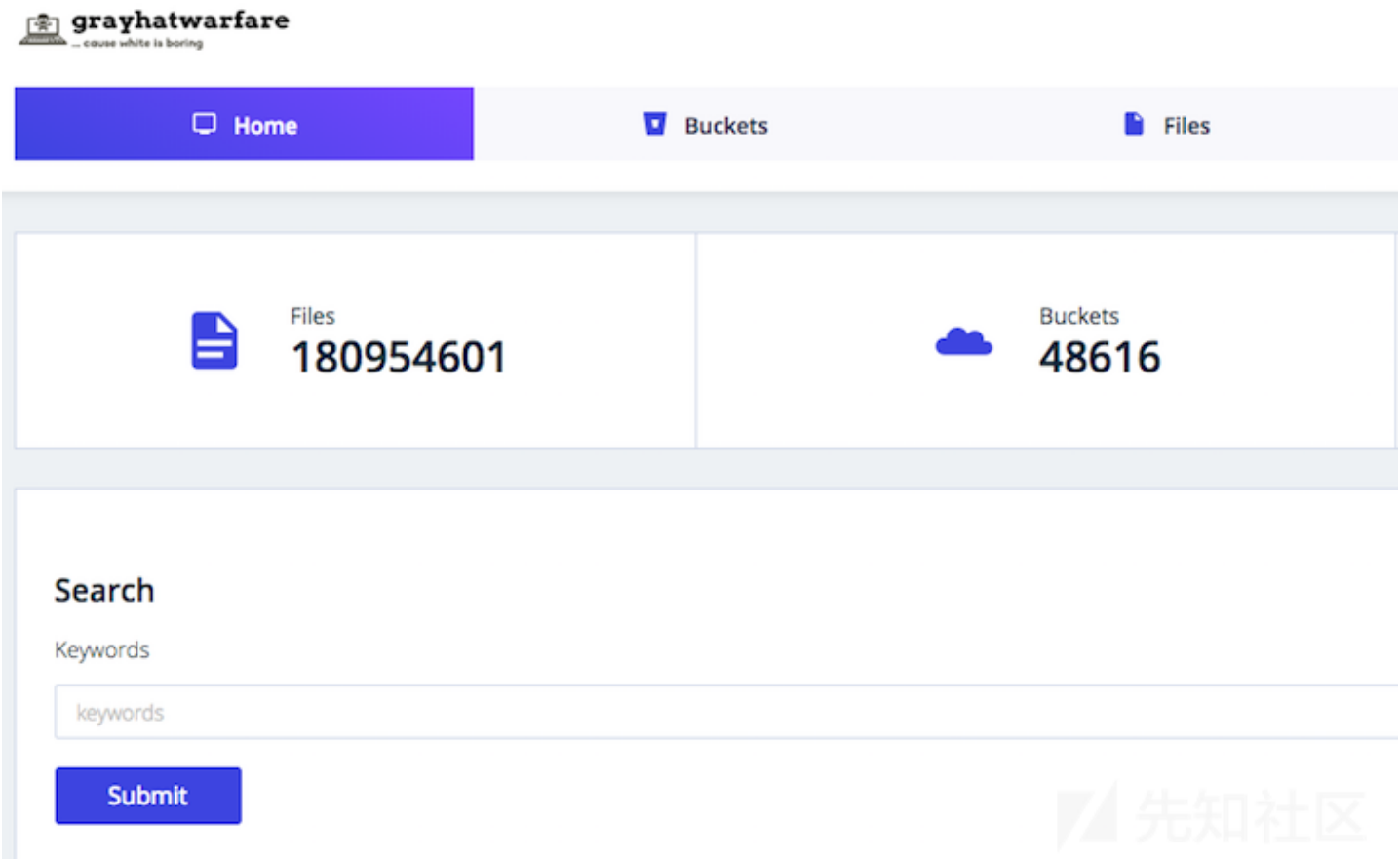
公开机密

这篇文章的最后一篇，也是我最喜欢的一篇，是公开机密。令人难以置信的是，组织在没有意识到的情况下公开分享。事实上，这篇文章已经涵盖了两个类别：元数据和公开

但是，还有其他类型的公开机密。首先，有一些机密被提交给git存储库。当开发人员使用在源代码中硬编码的API密钥或密码的代码时，通常会发生这种情况。当此类代码提

同样，粘贴网站是机密数据的金矿。开发人员倾向于使用这些站点共享代码，并且他们不倾向于查看安全方面 - 通常提交包含机密的代码。如果你想深入研究这个，我推荐使用PasteHunter。这是一个定期检查流行的粘贴网站并运行YARA签名来检查它是否包含有趣字符串的项目。或dorks：`site:pastebin.com ORG_DOMAIN`.

最后，我想提一下公共S3 buckets。最近出现了敏感信息托管在公共S3 buckets中的多种 案例 。可以将S3 buckets配置为公共的，开发人员通常会选择这种bucket，因为它更易于使用。问题是一旦发现了bucket名称，任何人都可以看到所有内容而无需身份验证。从工具中，我推 for S3 - buckets.grayhatwarfare.com。



OSINT Primer的第4部分将涉及证书。请继续关注Twitter以获取它。

点击收藏 | 1 关注 | 2

上一篇：NVIDIA GeForce Ex... 下一篇：Struts漏洞 S2-045 调试学习

1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板