OSINT Resources for 2019

mss**** / 2018-12-31 10:00:00 / 浏览数 3273

原文：https://medium.com/@micallst/osint-resources-for-2019-b15d55187c3f

无论您是OSINT(公开资源情报)方面的新手，还是在自己的职业生涯中经常使用它进行侦察、威胁情报收集或调查方面的老手，鉴于该领域最近发展迅猛——无论是在OSIN

首先，让我们来点基础性的知识。

如果您是新手，或者技术水平不是非常深厚的话，那么，最好先设法掌握一些基础性的资源，以便打下一个坚实的基础，这样，不仅可以帮助您更好地利用本文后面提到的其

- DNS:借助于host、dig和nslookup等命令工具，可以查询各种类型的DNS记录(A、CNAME、NS、MX、TXT等）、使用的备用名称服务器等。例如，您知道Quad9的D

```
$ nslookup m-tesla.pw 9.9.9.9
Server:       9.9.9.9
Address:      9.9.9.9#53
Non-authoritative answer:
Name:   m-tesla.pw
Address: 127.0.0.1
```

- Whois：也许大家都知道如何对域名进行Whois查询，但是您知道也可以对IP地址、网络和ASN执行Whois查询吗？比如，我们不妨看看谁拥有地址8.8.8.8——是的，是

```
$ whois 8.8.8.8
...
NetRange:       8.0.0.0 - 8.127.255.255
CIDR:           8.0.0.0/9
NetName:        LVLT-ORG-8-8
NetHandle:      NET-8-0-0-0-1
Parent:         NET8 (NET-8-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Level 3 Parent, LLC (LPL-141)
RegDate:        1992-12-01
Updated:        2018-04-23
```

```
Ref:            https://rdap.arin.net/registry/ip/8.0.0.0
OrgName:        Level 3 Parent, LLC
OrgId:          LPL-141
Address:        100 CenturyLink Drive
City:           Monroe
StateProv:      LA
PostalCode:     71203
Country:        US
RegDate:        2018-02-06
Updated:        2018-02-22
...
NetRange:       8.8.8.0 - 8.8.8.255
CIDR:           8.8.8.0/24
NetName:        LVLT-GOGL-8-8-8
NetHandle:      NET-8-8-8-0-1
Parent:         LVLT-ORG-8-8 (NET-8-0-0-0-1)
NetType:        Reallocated
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2014-03-14
Updated:        2014-03-14
Ref:            https://rdap.arin.net/registry/ip/8.8.8.0
...
```

端口扫描器(
Nmap、masscan、...)：打开的端口能够帮我们弄清楚服务器已经公开了哪些服务。端口443通常用于HTTPS服务，端口22通常用于SSH服务，等等。端口扫描器可以自

谷歌的搜索语法：很多书籍都对此进行了广泛的讨论(甚至有一本书是专门讨论这一主题的)，所以，这里就不再多费口舌了，不过，这并不是说它并不重要——大家只要
Hacking Database(GHDB)，您心里就会有数了。

Python：早晚有一天，大家都会遇到一些独一无二的需求，这时，就需要为自己特定的场景集成不同的工具和API。之所以单独提及Python，因为它不仅是一种平易近人
Seitz（Hunchly软件的作者）编写的在线课程，或者直接看这里的Python教程——其可读性好到令人发指。

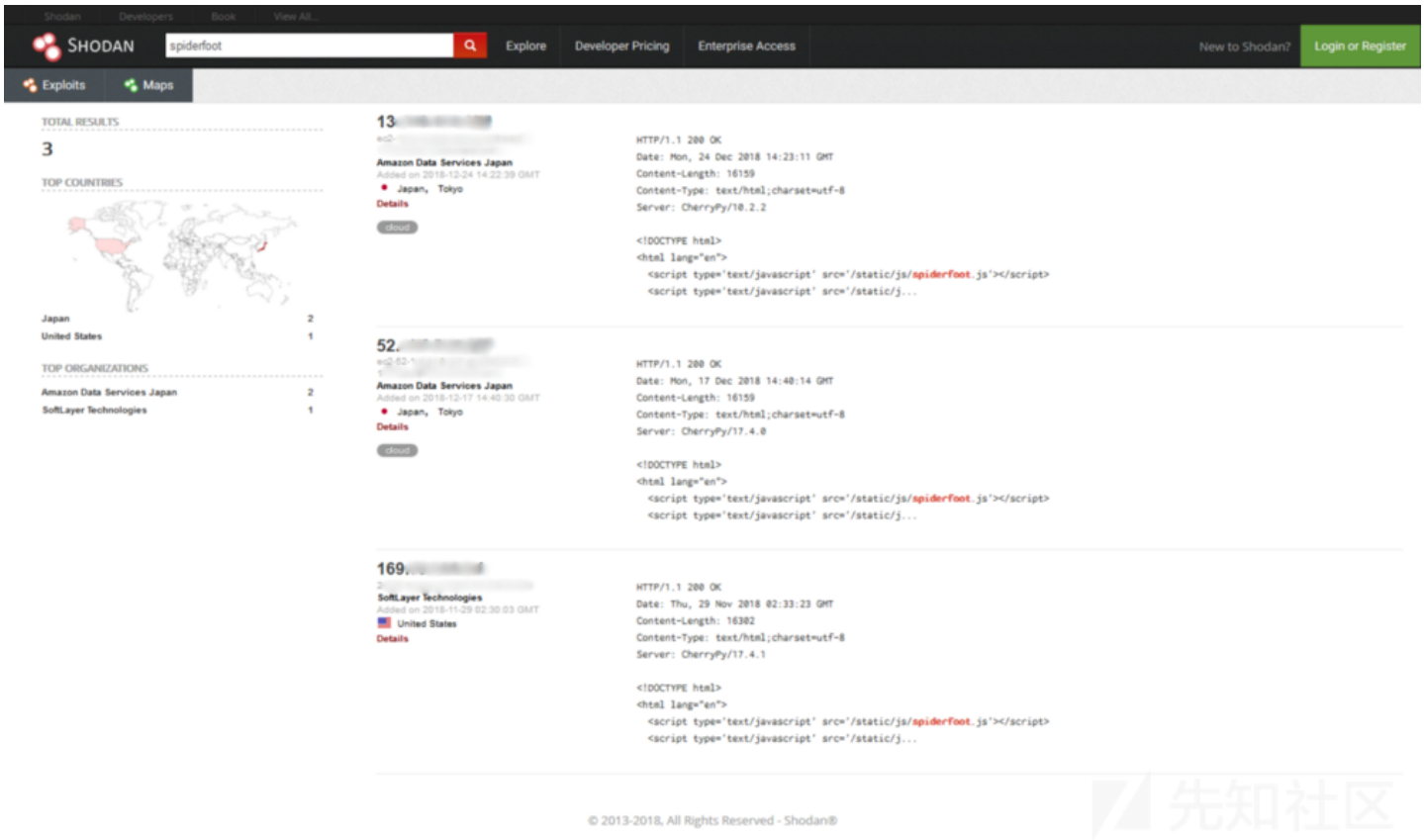
我们需要创造性地思考！我最喜欢OSINT的一点是，它通常是一个由松散连接（或经常是不连接）的组成部分构成的大拼图。如果您得到了一条信息，通常顺着又能得到另一

抱歉，我得把Brooklyn 99的资料偷偷带过来。

掌握了这些要素之后，您就可以通过使用他人创建的更复杂的工具和平台了，也就是站在巨人的肩膀上了；话说回来，这些工具和平台中的大部分也都是建立在上述基础之上

Internet扫描器

Internet扫描器带来的好处是，当您想要了解目标计算机公开了哪些服务（开放端口、协议、应用程序、内容）时，大部分的繁重工作可由它们代劳，因此，您只需要查询它



我利用SHODAN对关键词'spiderfoot'进行了一个简单的搜索，结果显示，有些人正在网上公开运行它。

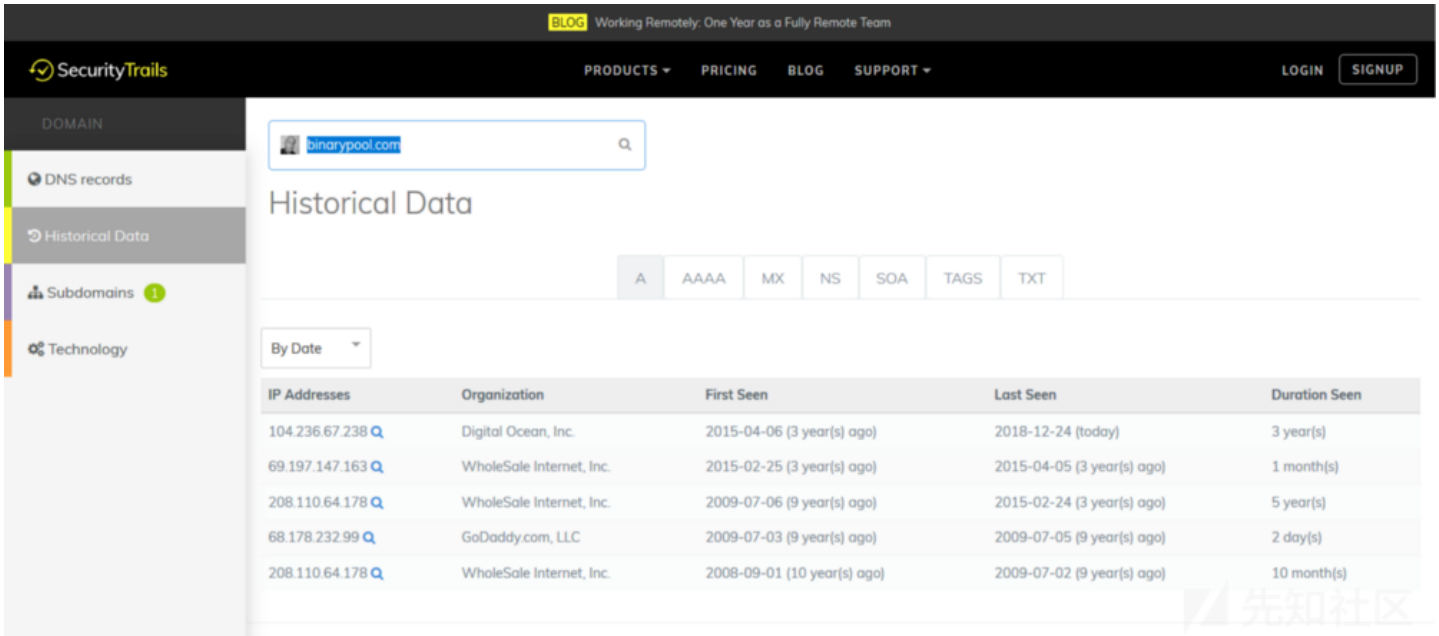
SHODAN：它是Internet扫描器之王，这一地位是无可争议的；它提供了丰富的查询语言、API，最重要的是，它还为我们提供了大量数据供筛选。

Censys：这个平台发展很快；它不仅提供了高质量的数据，同时，还提供了非常好用的界面和API。

BinaryEdge：有些家伙已经通过他们的平台发现了很多漏洞，最近还向公众开放了免费访问权限。另外，他们还提供了BitTorrent数据和相关的API。

被动型DNS

被动型DNS服务能够利用Internet
DNS流量来构建DNS解析的历史记录。我们知道，借助于DNS，我们可以将名称解析为相应的IP地址，或者将IP地址解析为相应的名称。但如果我们想找出解析到给定IP的



我在SecurityTrails上搜索自己的个人网站binarypool.com，竟然能够看到2008年的DNS记录！

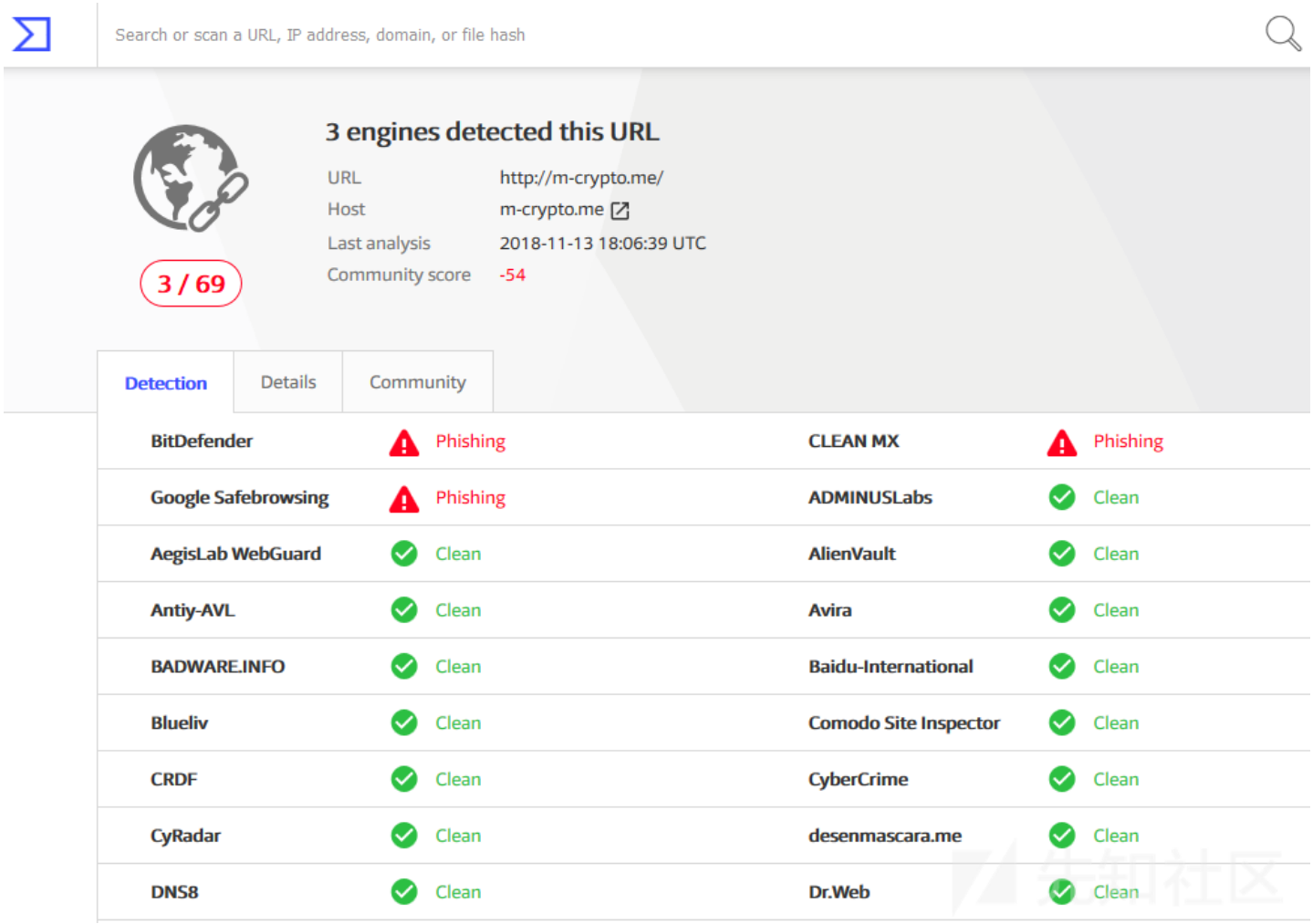
SecurityTrails：实际上，将SecurityTrails归入被动型DNS类别确实有点保守，因为，它们的用途远不止于被动型DNS。它们不仅提供了巨量的数据，还提供了丰富的AP

Robtex：Robtex是本人第一次接触到的被动型DNS服务，让我非常着迷。目前，几乎所有的OSINT工具都在使用它，毕竟，它已经存在了很长时间了，并且是免费的，

HackerTarget：这是另一个具有丰富的免费被动型DNS数据源，同时，我们也可通过API获得相应的数据。此外，他们还提供了许多其他方面的免费工具，这些工具也值

声誉系统（Reputation Systems）

如果从事OSINT的主要目标之一是威胁情报收集的话，那您运气不错，因为这方面的信息源不仅数量多，并且质量也很高，所以，我在这里夹带了一点私货，列出了我最喜欢



在VirusTotal中查找可疑域名，不仅能够找到相应的声誉信息，同时还能发现更多的信息。

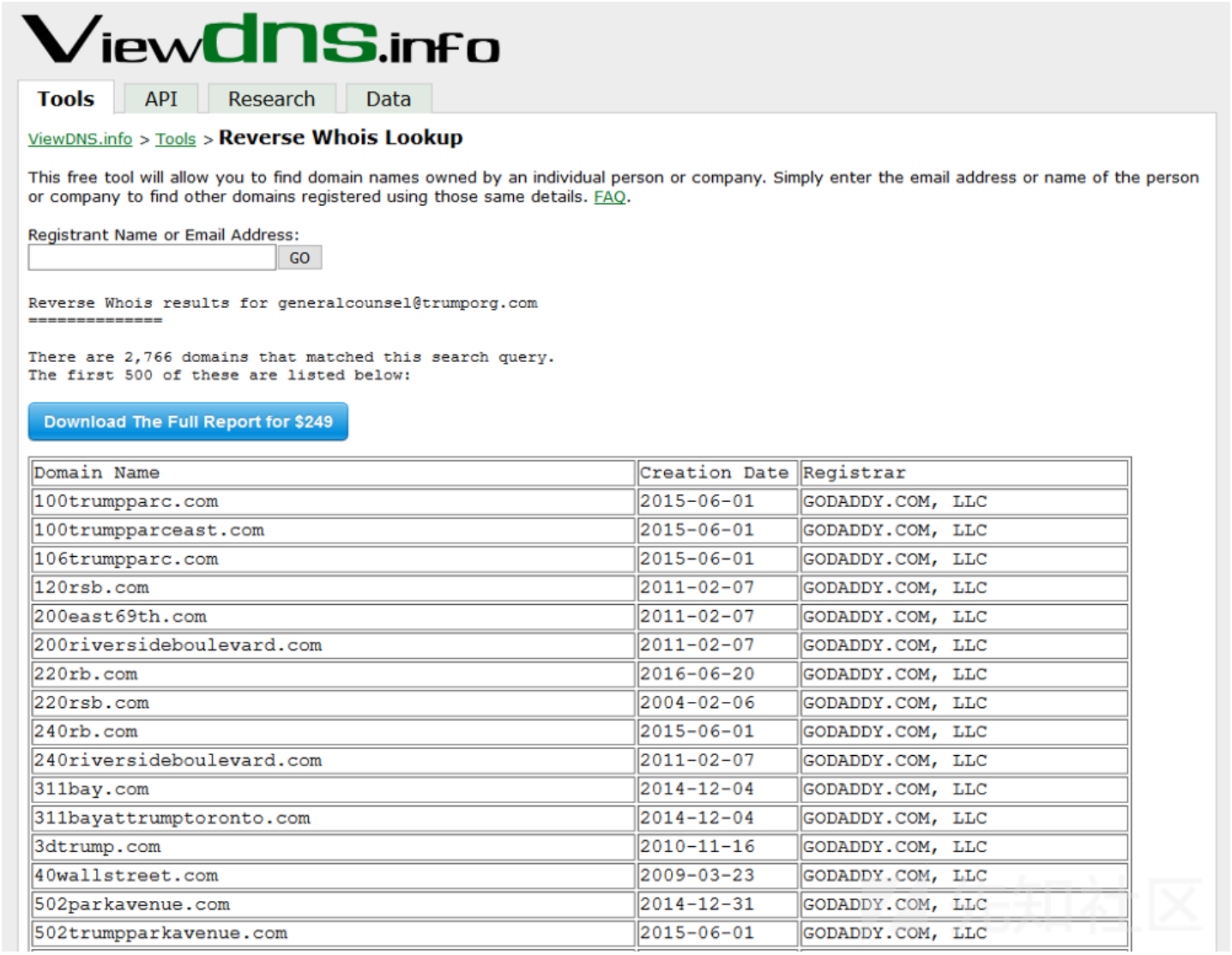
VirusTotal：在这个巨大的平台上，提供了巨量的声誉数据、被动型DNS数据，等等。虽然该平台的访问是免费的，但是在查询量方面具有严格的限制。不过，如果您只

Greynoise：这是一个新玩家，它更关注于识别Internet扫描器(例如上面提到的那些)。如果您正在调查可疑的IP地址，那么，这是一个消除误报("反威胁情报")的好去处。

FireHOL
IP清单:如其网站上所述，“其目标是创建一个足够安全得黑名单，可以在所有系统上使用，并提供了防火墙，以全面阻止对其列出的IP的访问。”他们还提供了历史数据维

反向Whois

反向Whois是我最喜欢的OCIT资源之一，因为它的功能非常强大，经常给我们带来惊喜。常规Whois只能提基于域名搜索结果，而反向Whois资源则允许我们根据名字、电
IT issues），或查找主域名完整的外围对象时，这会非常给力。



ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **Reverse Whois Lookup**

This free tool will allow you to find domain names owned by an individual person or company. Simply enter the email address or name of the person or company to find other domains registered using those same details. FAQ.

Registrant Name or Email Address:

GO

Reverse Whois results for generalcounsel@trumporg.com

There are 2,766 domains that matched this search query.
The first 500 of these are listed below:

Download The Full Report for $249

Domain Name	Creation Date	Registrar
100trumpparc.com	2015-06-01	GODADDY.COM, LLC
100trumpparceast.com	2015-06-01	GODADDY.COM, LLC
106trumpparc.com	2015-06-01	GODADDY.COM, LLC
120rsb.com	2011-02-07	GODADDY.COM, LLC
200east69th.com	2011-02-07	GODADDY.COM, LLC
200riversideboulevard.com	2011-02-07	GODADDY.COM, LLC
220rb.com	2016-06-20	GODADDY.COM, LLC
220rsb.com	2004-02-06	GODADDY.COM, LLC
240rb.com	2015-06-01	GODADDY.COM, LLC
240riversideboulevard.com	2011-02-07	GODADDY.COM, LLC
311bay.com	2014-12-04	GODADDY.COM, LLC
311bayattrumptoronto.com	2014-12-04	GODADDY.COM, LLC
3dtrump.com	2010-11-16	GODADDY.COM, LLC
40wallstreet.com	2009-03-23	GODADDY.COM, LLC
502parkavenue.com	2014-12-31	GODADDY.COM, LLC
502trumpparkavenue.com	2015-06-01	GODADDY.COM, LLC

如果搜索generalcounsel@trumporg.com，则会显示在该地址下注册的其他域名。

ViewDNS.info：该网站上提供了许多免费工具，并且，API的定价也非常合理。即使不使用API，您仍然可以从网站上查询相当多的数据，并且这些数据可以追溯到很久

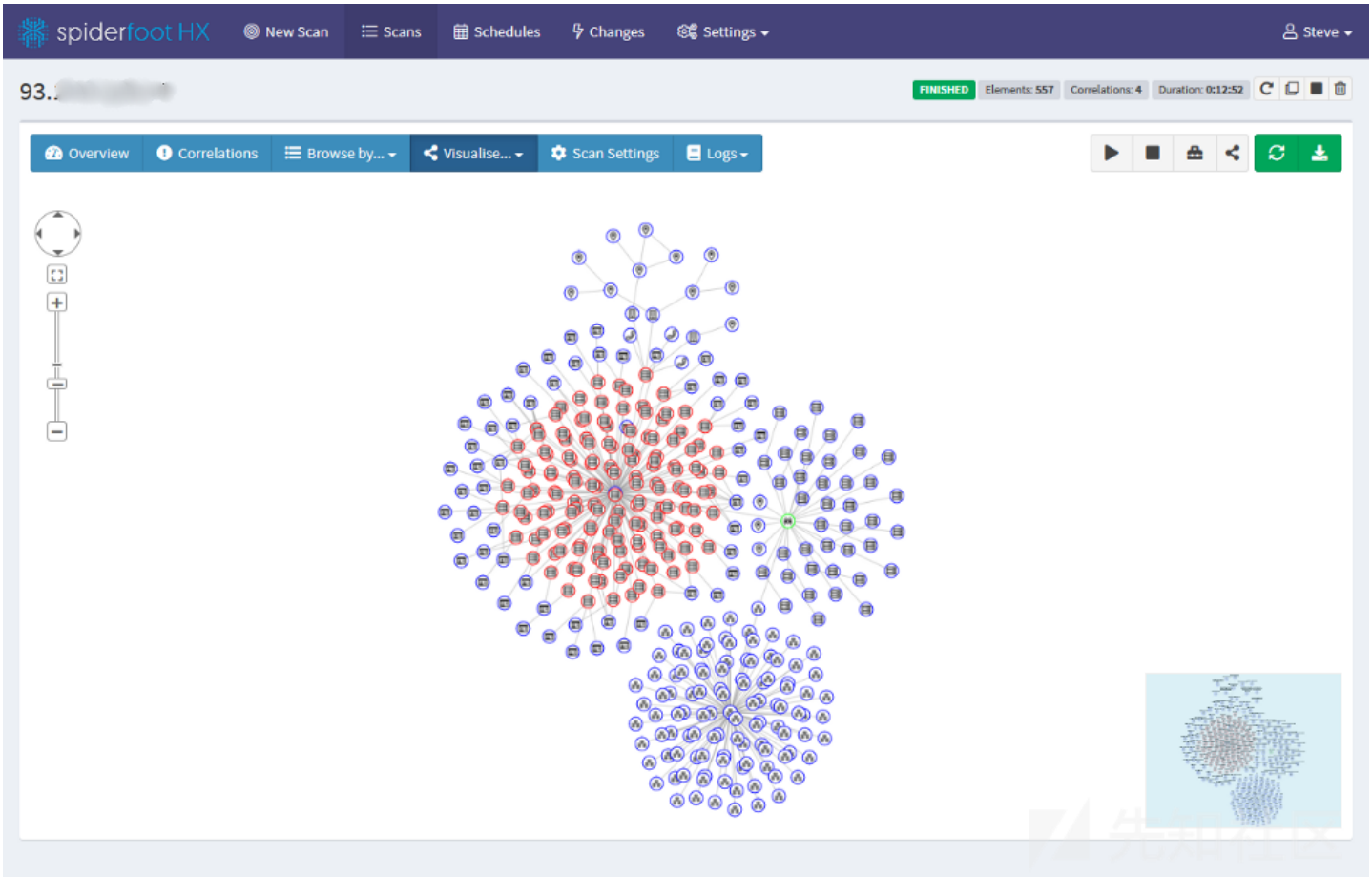
WhoXY：他们的数据覆盖范围超过了2000个TLD，可以通过API来批量获取。此外，您还可以以每1000个查询2美元的费率来购买查询流量。价格吗，还算公道吧。

SecurityTrails：在这里，我不得不再次提及SecurityTrails，因为他们也提供反向Whois数据。

自动化工具

随着OSINT数据源越来越多，所以，我们最终会走上自动化之路，这样，我们就不会将所有时间都花在浏览器窗口的切换、复制和粘贴上面，同时，还能降低人为出错的概率

眼下，已经有越来越多的工具进入OSINT领域，涵盖了子域枚举、社交媒体相关性等领域。有时，我们需要通用的广度覆盖工具（broad-coverage tool）来同时访问大量的数据点；另一些时候，我们却只需要一个涉及面很窄且专用的工具来处理某个数据点。此外，还有一个关键的维度，那就是新鲜度——我们要尝试和



SpiderFoot不仅提供了开源版本，还提供了云托管版本（SpiderFoot HX以上版本），目前处于Private Beta阶段。

SpiderFoot：作为SpiderFoot的作者，难免有失偏颇，所以，这里我们只能说该项目目前提供了基于Web的UI、CLI并且处于积极维护状态，并提供了150个以上的模块
HX Private Beta版本仍处于开放状态，所以，我们还将为其提供更多的功能。

Maltego：提供了社区版（免费）和商业版。Maltego具有令人印象深刻的可视化功能，并能够与OSINT的“transforms”模型一起工作，后者可以将一种类型的数据（例

theHarvester：一个非常流行的开源、纯CLI的OSINT工具，它集成了许多数据源，包括本文中之前提到的那些。

社区

在过去几年中，OSINT领域最让人高兴的事情之一就是社区的迅猛发展。现在，社区已经提供博客、聊天组、聚合资源列表甚至播客：

All Episodes

Subscribe

The OSINT Podcast

#13 - OSINT Weekly Rollup - Python is the Future, JungleScam v2, eCommerce Investigation, Asciinema, Deep Explorer, Facebook Anti-Scraping

December 09, 2018 Jake Creps

一个100%致力于传播OSINT的播客。

The OSINT Podcast：Jake Creps总能提供最新的主题，其中涵盖了新的OSINT资源和工具，以及对OSINT领域关键人物的采访。

Michael
Bazzell的网站（以及时事通讯！）：我们是该网站的常客，我经常通过该网站来寻找创建新SpiderFoot模块的灵感。该网站的主题更着重于调查方面，不过技术性较差，

OSINTcurio.us：一个最近才上线的博客，也是一个值得关注的博客。这里提供了许多有趣的文章，大多是有关人们是如何进入OSINT领域的，不过，将来会提供越来越

Awesome
OSINT：提供相关的OSINT资源链接。这里也许提供了人类已知的所有OSINT源，并且将其托管在Github上，所以，如果您想贡献内容，只需一个拉取请求就能搞定。

OSINT Rocket
Chat：随着数百（数千？）成员的加入，不久就会发展成一个由调查人员、信息安全人员、研究人员和业余爱好者组成的、有用且活跃的社区。

小结

就像所有这个方面的文章一样，这里真的只是触及了如今可用的OSINT资源的一点皮毛而已。尽管如此，我仍然希望本文能够对您有所帮助，同时，在后续文章中，我将介

上一篇：Cross-Browser-Tra... 下一篇：使用区块链技术来创建安全备份

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