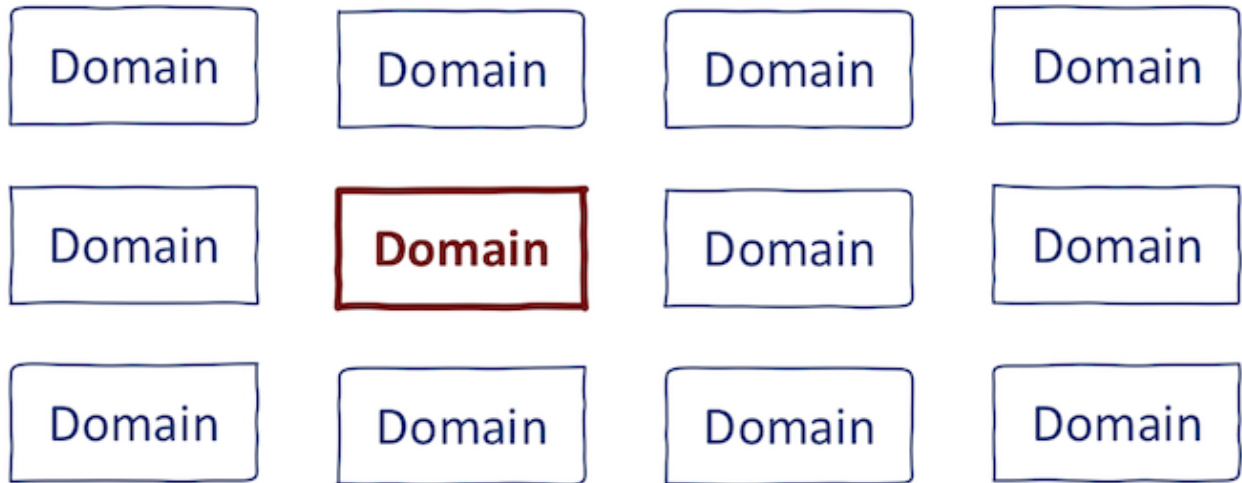


翻译文章，原文链接：<https://0xpatrik.com/osint-domains/>

在这篇文章中，我将解释如何尽可能多地查找有关域的信息。该文章没有解决查找相关域的枚举部分，而是查找特定于域的数据，例如域名持有人，信誉或DNS设置。这篇



先知社区

注意：这是此OSINT入门的第一个版本。我将使用新的工具和技术逐步更新它。

在深入研究具体技术或工具之前，我想简要谈谈思维方式。通常，我有以下目标之一：

- 该域名是我的目标的主要域名，我想尽可能多地获取信息。请注意，在这种情况下，我通常会搜集一切有用的东西。
- 域名可能是恶意的，我想证实我的假设，看看它是什么。
- 域似乎是一个潜在的攻击媒介，以收集最初的攻击点。具体来说，它正在托管一些可以被利用的服务。我想看看有关这些服务的详细信息。

请记住，你应该始终有一个明确的目标。这能防止你做不必要的事情。

请注意，域上存在的域和服务略有重叠。在某些情况下，我将解释影响服务的技术。

WHOIS

你应该掌握的第一个技术是WHOIS查找。WHOIS用于查询存储域名，IP块或ASN的注册用户的数据库。你可以使用CLI工具：

```
$ whois DOMAIN
```

或选择某些Web服务，例如[ICANN WHOIS](#)。

WHOIS数据提供有关注册域名的实体信息。请记住，某些域可能隐藏了WHOIS信息，有些域可能提供错误数据。

WHOIS数据提供了该域名与某个特定组织相关联的线索。虽然这在枚举步骤中更有用，但WHOIS数据可以在某些特定情况下提供帮助：例如，如果你遇到试图模仿某个特定

域分析

有时，你希望全面了解域管理员所做的域信息或决策。

我的[首选](#)工具之一是[Robtex的DNS查找](#)。它提供了有关域的大量信息。我特别喜欢共享部分，它们为你提供有关其他相关域的概述（是的，这与枚举阶段有关，原谅我一次

SHARED

IP numbers 198.100.177.181 1 results shown.	Name servers ns1.eff.org ns2.eff.org 2 results shown.	Sharing name servers certbot.com reclaiminvention.com democracy.io manilapinciples.net noteviltrack.net teachingcopyright.net https-rulesets.org 7 results shown.	Partially sharing name servers freerangekitten.com projectsecretidentity.com soundcopyright.eu ifightsurveillance.net studentinnovation.net do-not-tracker.org globalchokepoints.org openwireless.org stopthespying.org donottrack.us 10 results shown.	IP numbers of the name servers 173.239.79.201 206.189.70.183 2 results shown.	Mail servers dummy1.eff.org dummy2.eff.org mail2.eff.org 3 results shown.	Sharing mail servers ifightsurveillance.com standagaintspyng.com eviltrack.net internetslowlane.net standagaintspyng.net defendinnovation.org httpsnow.org privacybadger.org stopsesta.org donottrack.us 10 results shown.	Partially sharing mail servers electionawareness.com savecrypto.net eff-ctf.org electionawareness.org openwireless.org lists.eff.org 7 results shown.
IP numbers of the mail servers 173.239.79.193 173.239.79.204 173.239.79.223 3 results shown.	Sharing mail servers under another name electiondayreport.com jailbreakthelaw.com panoptick.com surveillanceselfdefense.com eff.net surveillanceselfdefense.net electiondayreports.org freeyourphone.org https-rulesets.org surveillanceselfdefense.org 10 results shown.	Subdomains/Hostnames Domains or hostnames one step under this domain or hostname. certbot.eff.org docker4.eff.org gw-unwired.eff.org lib1.eff.org mail.eff.org ns6.eff.org openwireless.eff.org ssd-staging.eff.org web2.eff.org www.eff.org 10 results shown.	Siblings Siblings are domains or hostnames on the same level, under the same parent level. Not necessarily related in any other way. dearfcc.org eff-ctf.org electronicfrontierfoundation.org globalchokepoints.org jailbreakingsnotacrime.org necessaryandproportionate.org projectsecretidentity.org standagaintspyng.org teachingcopyright.org troublingeffects.org 10 results shown.				
On other TLDs and domains This sub section shows this name on other top level domains. eff.cn eff.email eff.info eff.net eff.store eff.vn eff.ics.ioan eff.tjg.ioan eff.tqj.ioan eff.com.vn 10 results shown.				Similar start This sub section shows this names that begin almost the same. fef.br fef.co fef.dk ffe.hu fef.it fef.me ffe.net ffe.pl ffe.supply ffe.us 10 results shown.			

Robtex提供了更多信息（例如，SEO详细信息，信誉……），但通常在有限的范围内。我尝试使用其他来源获取具体细节。Robtex为我提供了高层次的视角。我强烈建议在那

接下来，我想使用domain_analyzer为我提供更多域设置的信息。这个工具甚至可以抓取网站来发现电子邮件等等。我喜欢以更有限的方式使用它：

```
python domain_analyzer.py -d DOMAIN -w -j -n -a
```

想直接判断此输出中哪些数据有用是很困难的。但它曾多次帮助过我。我喜欢存储输出的数据并在分析过程中多次使用它。

被动数据

检查过去的域名服务很有用。有两种类型的被动域数据：

- 被动DNS - 过去DNS记录值是什么
- 被动“内容” - 过去在此域名托管上的Web服务是什么

对于被动DNS，我喜欢使用RiskIQ社区版。界面非常简单，搜索结果会直接显示：

RISKIQ Q eff.org

First Seen 2009-09-01 Registrar Gandi SAS
Last Seen 2018-07-08 Registrant Electronic Frontier F... Categorize

TERS (9 / 9)

- 198.100.177.181 1
- 23.235.40.201 1
- 64.147.188.10 1
- 64.147.188.11 1
- 64.147.188.3 1

ow More...

ETWORK (4 / 9)

- 69.50.224.0/19 4
- 64.147.160.0/19 3
- 198.100.160.0... 1
- 23.235.40.0/24 1

IN (3 / 9)

- 13332 5
- 15203 3
- 54113 1

RESOLUTIONS (1)

Show: 25 1-9 of 9 Sort: Last Seen Descending

Resolve	Location	Network	ASN	First	Last	Source	Tags
198.100.177.181	US	198.100.160.0/19	13332	2018-04-30	2018-07-08	pingly, riskiq	Nephoscale-Inc. Routable
69.50.232.54	US	69.50.224.0/19	13332	2012-06-08	2018-04-30	pingly, riskiq	Nephoscale-Inc. Routable
23.235.40.201	US	23.235.40.0/24	54113	2016-04-29	2016-04-29	riskiq	Fasty Routable
69.50.225.155	US	69.50.224.0/19	13332	2013-11-15	2016-04-29	riskiq	Nephoscale-Inc. Routable
69.50.232.155	US	69.50.224.0/19	13332	2013-11-15	2013-11-15	riskiq	Nephoscale-Inc. Routable
69.50.232.52	US	69.50.224.0/19	13332	2011-03-10	2013-11-15	riskiq	Nephoscale-Inc. Routable
64.147.188.3	US	64.147.160.0/19	15203	2009-12-14	2011-03-10	riskiq	Mhmr Routable
64.147.188.11	US	64.147.160.0/19	15203	2009-09-01	2010-07-29	riskiq	Mhmr Routable
64.147.188.10	US	64.147.160.0/19	15203	2009-09-01	2010-01-01	riskiq	Mhmr Routable

1-9 of 9

尽管RiskIQ

CE旨在成为域的整体分析平台，但我专门使用它来获取被动DNS数据。与本文的许多其他方面一样，你可以自行决定是使用一个源还是使用多个源来处理不同的数据。我喜

在RiskIQ CE之外，我也喜欢使用VirusTotal：

Categories ⓘ

Alexa	advocacy_organizations
BitDefender	computersandsoftware
Forcepoint ThreatSeeker	advocacy groups
TrendMicro	politics

Passive DNS Replication ⓘ

Date resolved	IP address
2018-07-08	198.100.177.181
2018-04-29	69.50.232.54
2013-12-06	69.50.225.155
2013-09-28	69.50.232.52

Whois Lookup ⓘ

```
Domain Name: EFF.ORG
Registry Domain ID: D2234962-LROR
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2018-03-08T02:19:58Z
Creation Date: 1990-10-10T04:00:00Z
Registry Expiry Date: 2022-10-09T04:00:00Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
```

同样，你将获得比被动DNS更多的数据。根据我自己的经验，RiskIQ倾向于为被动DNS提供更多数据。

最后，我将提到[CIRCL.LU的被动DNS](#)，我很幸运能够访问它。我有时用它来交叉关联上面两个来源。请注意，CIRCL.LU被动DNS不向公众开放。

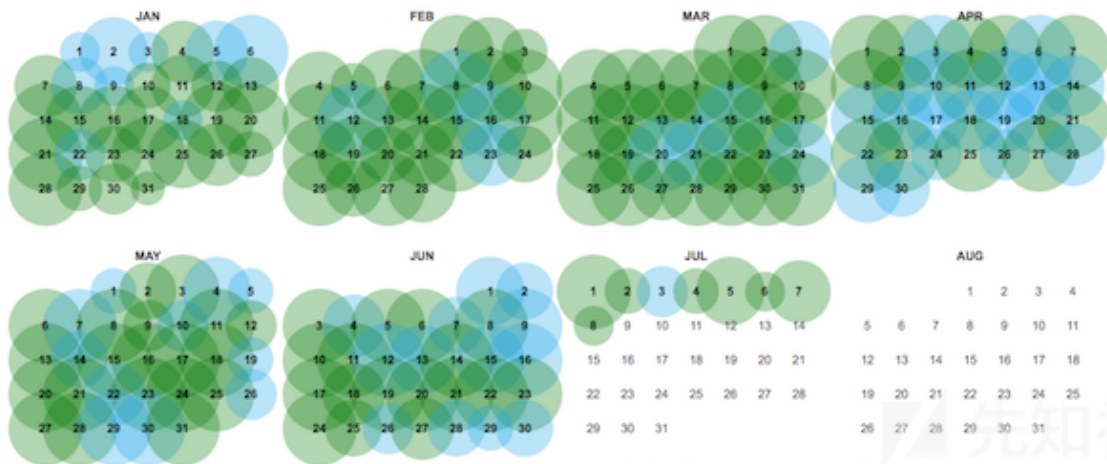
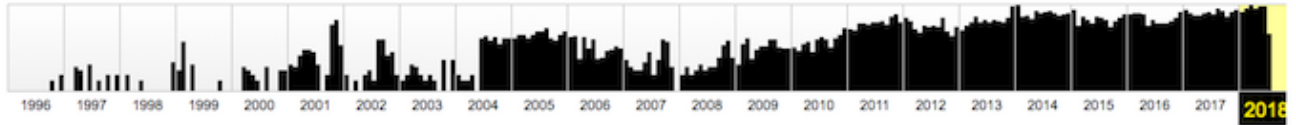
更多被动DNS来源：

- [mnemonic](#)
- [DNSTrails](#)

我的被动内容工具是[Wayback Machine](#)。它提供大多数网站过去的快照。通常有多个快照，因此你甚至可以选择要查看的快照日期：

DONATE

Saved 17,673 times between October 20, 1996 and July 8, 2018.

[Summary of eff.org](#) · [Site Map of eff.org](#)

快照的频率取决于网站的受欢迎程度。最后，我想使用简单的Google Dork从Google数据库中检索网址，如下所示：

cache:https://eff.org/

This is Google's cache of <https://www.eff.org/>. It is a snapshot of the page as it appeared on Jul 7, 2018 13:04:39 GMT. The current page could have changed in the meantime. [Learn more.](#)

[Full version](#) [Text-only version](#) [View source](#)

Tip: To quickly find your search term on this page, press Ctrl+F or ⌘-F (Mac) and use the find bar.



FEATURED UPDATE

After More Than a Decade of Litigation, the Dancing Baby Has Done His Part to Strengthen Fair Use for Everyone

The leading nonprofit defending digital privacy, free speech, and innovation.



FEATURED UPDATE

Victory! Supreme Court Says Fourth Amendment Applies to Cell Phone Tracking

内容分析

你可能需要检查域中当前服务的是什么Web服务器。在处理潜在的恶意软件站点时，有必要遵循基本的OPSEC指南。当你没有VPN或虚拟机的保护时，你不应该直接访问这

www.eff.org 2a04:4e42:1b::201 

Lookup

Go To

Report

Rescan

Submitted URL: http://eff.org
Effective URL: https://www.eff.org/
Submission: On July 08 via manual (July 8th 2018, 2:54:04 pm)

Summary

HTTP 42

Links 23

Behaviour

IoCs

DOM

Content

Related

JSON

API

42

1

0

100%

33%

1

3

2

2

1,184kB

1,754kB

0

Requests

Ad-blocked

Malicious

HTTPS

IPv6

Domains

Subdomains

IPs





Countries

Transfer

Size

Cookies

This website contacted 2 IPs in 2 countries across 1 domains to perform 42 HTTP transactions. Of those, 42 were HTTPS (100 %) and 33% were IPv6. The main IP is 2a04:4e42:1b::201, located in European Union and belongs to FASTLY - Fastly, US. The main domain is www.eff.org. It took 2.375 seconds to load this page.

IP/ASNs	IP Detail	(Sub)Domains	Domain Tree	Links	Certificates
	IP Address		AS Autonomous System		
2 → 2	198.100.177.181 	13332 (HYPEENT-SJ - Hype Enterprises)			
41	2a04:4e42:1b::201 	54113 (FASTLY - Fastly)			
1	173.239.79.196 	32354 (UNWIRED - Unwired)			
42	2				

Screenshot (click to see full image)

Expand Image



Detected technologies

Drupal (CMS)

jQuery (JavaScript Frameworks)

PHP (Programming Languages)

Nginx (Web Servers)

Varnish (Cache Tools)

Website

Website

Website

Website

Website

有时，你想要检测某些网站上的视觉变化。当处于关闭状态的域可能在将来更改为不同的域时，这非常有用。为此，我喜欢使用[visualping.io](#)。一旦某个域的内容发生变化，从内容的角度来看，短网址通常被用来伪装恶意软件/钓鱼网站，发送给受害者。名为checkshorturl.com的工具用于自动将短网址恢复到其原始形式。

CheckShortURL

Your shortened URL expander

[ShortURL Expander](#) [ShortURL Customizer](#) [CheckShortURL Blog](#) [Statistics](#)

Get long URL from hundreds of URL shortening services

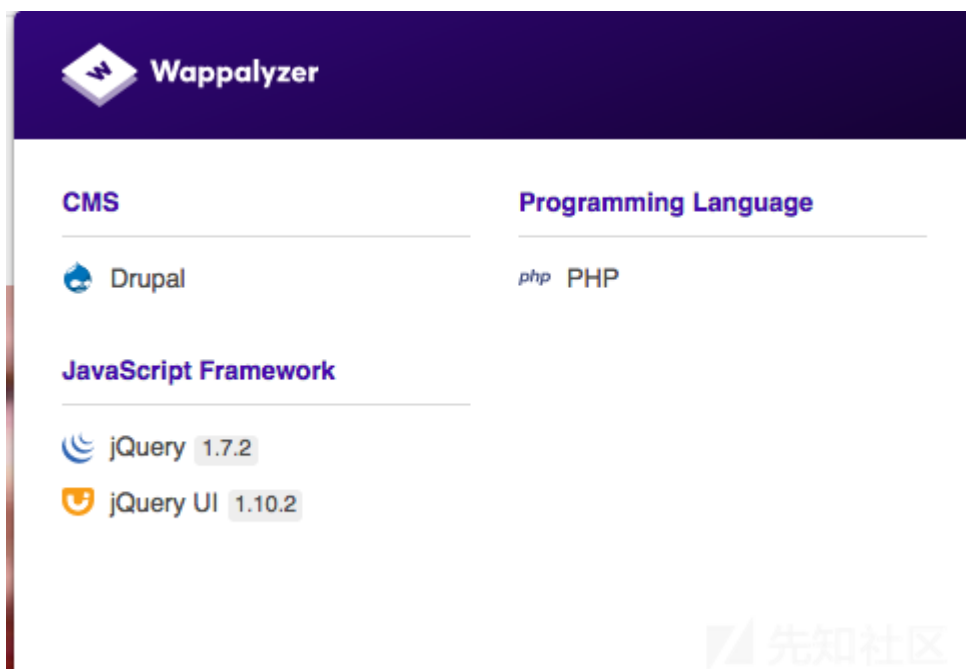
Ensure your safety and prevent unsuitable content while surfing on the World Wide Web

https://goo.gl/K89pem

Expand

Long URL	https://www.eff.org/
Delay	0.98 second(s)
Short URL	https://goo.gl/K89pem
Redirection	N/A

关于内容，我通常想检查一些网站上使用了什么技术。我使用Wappalyzer作为浏览器插件。Wappalyzer会自动识别你浏览到的每个网站上的技术：

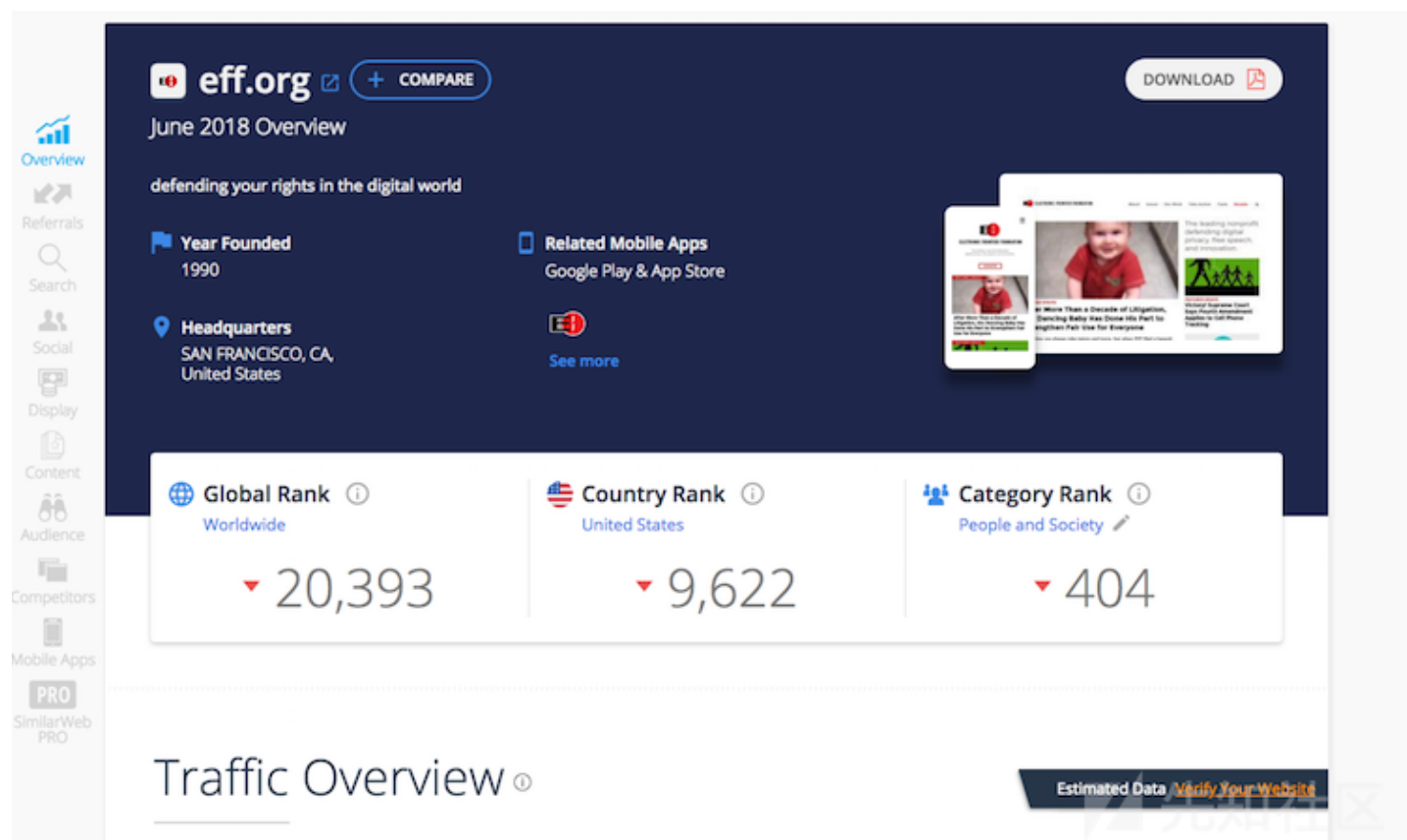


Wappalyzer的结果使我能够在这种情况下触发一些漏洞扫描工具，例如[droopescan](#)。如果你想要使用基于CLI的工具，我建议[使用stacks-cli](#)。

流量分析

在内容分析之后，我想检查网站在网络上如何推广。我使用了几种SEO分析工具：

- [SimilarWeb](#)
- [moz Link Explorer](#)
- [SEMRush](#)
- [moonsearch](#)
- [Alexa](#)

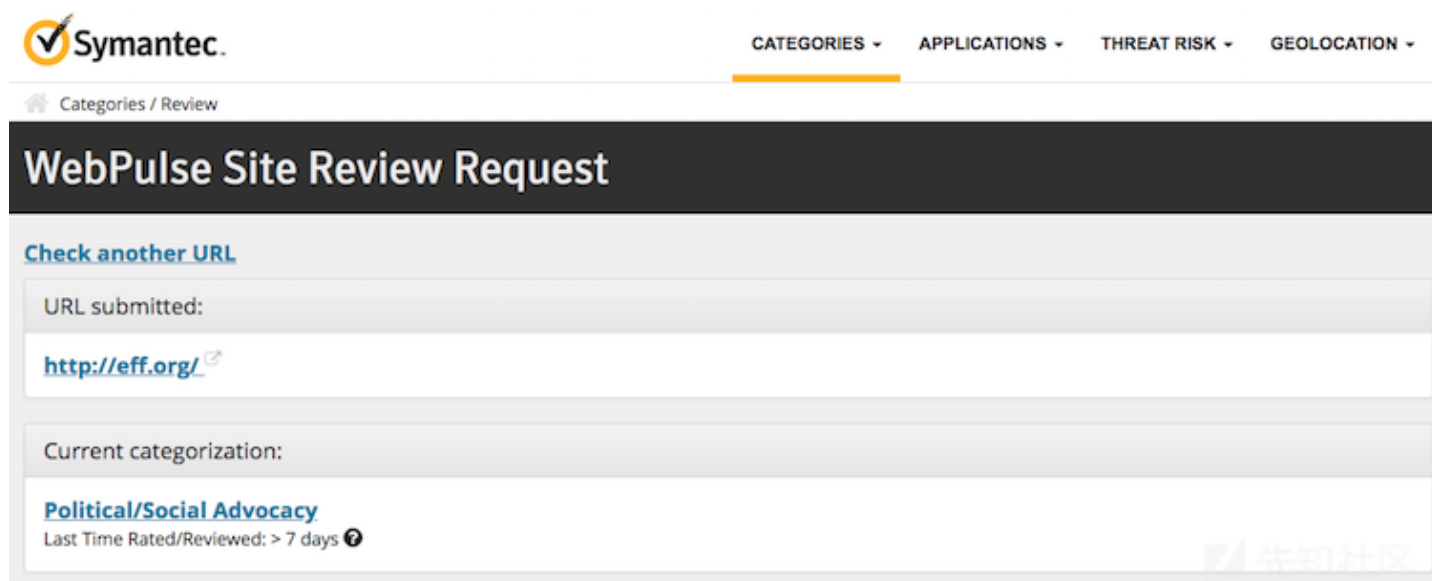


信誉

在事件响应或恶意软件分析期间，通常需要检查某个域信誉。信誉可能会让你知道该域名是否与某些恶意活动相关联。有许多免费服务可用于提供此信息。你应该始终检查 - 低信任域将包含可疑，恶意等类别广告。

我最常使用的信誉工具：

- [Bluecoat Sitereview](#)
- [Google安全浏览](#)
- [Sucuri Sitecheck](#)
- [ThreatMiner](#)
- [CyMon](#)
- [McAfee TrustedSource](#)



还有域黑名单，它是明确归类为恶意域的域列表。像CyMon这样的工具也会查看这些黑名单。这种黑名单的一个例子是Spamhaus Domain Blacklist(<https://www.spamhaus.org/lookup/>)。

OSINT自动化

如你所见，域相关数据有很多来源。当你需要收集数十或数百个域的信息进行广泛分析时，手动查询每个源可能会耗费精力。据我所知目前没有工具可以查询本文中提到的每个源。

```
p@eternity:~$ harpoon cache https://eff.org
Google: FOUND https://webcache.googleusercontent.com/search?num=1&q=cache%3Ahttps%3A%2F%2Feff.org&strip=0&vwsr=1 (2018-07-07 17:36:48+00:00)
Yandex: NOT FOUND
Archive.is: FOUND
-2012-12-20 17:36:48+00:00: http://archive.is/20121220173648/https://eff.org/
-2013-09-30 21:30:38+00:00: http://archive.is/20130930213038/http://eff.org/
-2014-01-27 14:55:32+00:00: http://archive.is/20140127145532/https://eff.org/
-2014-03-18 07:18:52+00:00: http://archive.is/20140318071852/http://eff.org/
-2014-03-29 01:59:16+00:00: http://archive.is/20140329015916/http://eff.org/
-2014-10-12 13:29:16+00:00: http://archive.is/20141012132916/http://eff.org/
-2014-11-18 05:30:31+00:00: http://archive.is/20141118053031/http://eff.org/
-2014-11-26 00:27:10+00:00: http://archive.is/20141126002710/http://eff.org/
-2015-01-06 05:16:11+00:00: http://archive.is/20150106051611/http://eff.org/
-2015-02-25 23:13:18+00:00: http://archive.is/20150225231318/http://eff.org/
-2015-04-03 12:32:17+00:00: http://archive.is/20150403123217/http://eff.org/
-2015-06-03 17:17:27+00:00: http://archive.is/20150603171727/http://eff.org/
-2017-01-16 17:29:46+00:00: http://archive.is/20170116172946/https://eff.org/
-2017-02-20 20:15:58+00:00: http://archive.is/20170220201558/https://eff.org/
-2017-12-13 05:06:22+00:00: http://archive.is/20171213050622/http://eff.org/
-2017-12-17 21:18:37+00:00: http://archive.is/20171217211837/http://eff.org/
Archive.org: NOT FOUND
Bing: FOUND http://cc.bingj.com/cache.aspx?d=4505675932894641&w=enxY6wdkqMMA8cCOvykvjwxhAM6cEKCx (2018-06-07 00:00:00)
```

替代品（来源少，质量差）：

- [QRadio](#)
- [Automater](#)

..或者你可以使用 [datasploit](#)。要获得更多处理领域开放源代码软件的工具，你还应该查看开放源代码软件框架。

点击收藏 | 1 关注 | 2

[上一篇：CVE-2019-2000—and...](#) [下一篇：用ARM编写TCP Bind Shell](#)

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](#)