



## 八个低成本或免费威胁情报来源

哈尔滨安天科技集团股份有限公司



Steve Zurier

2017年11月27日

组织知道他们需要认真对待威胁情报，但是对于去哪里找可靠的信息并不是很清楚。虽然几乎所有的安全行业厂商网站都提供最新威胁的信息，但是有些网站的内容更好一些。在本文中，我们将推荐八个信息最丰富、最有用的网站。

我们邀请 Rosint Labs 总裁罗塞尔·萨夫兰（Roselle Safran）与我们一起总结网站清单。萨夫兰在网络安全方面拥有丰富的经验，曾在奥巴马政府的总统行政办公室和国土安全部任职多年。

萨夫兰提供了一些联邦政府网站，还提供了一些鲜为人知的、追踪勒索软件和恶意软件的网站。我们与萨夫兰联手制定了一份清单，旨在帮助新手获取他们需要的威胁情报，并为经验丰富的安全专家提供一些有用的情报。

浏览列表之后，你会发现可以选择的网站远不止八个。



## 国土安全部：自动信标共享网站

国土安全部 (DHS) 成立了免费的[自动信标共享 \(AIS\)](#) 网站，便于私营公司与联邦政府共享网络威胁信标。典型的威胁信标是诸如恶意 IP 地址或钓鱼邮件的发件人地址等信息。国土安全部旨在创建这样一个生态系统：一旦有公司或联邦机构发现攻击企图，就会立即与所有 AIS 参与者共享威胁信标。联邦政府官员说，虽然 AIS 不能清除复杂的网络威胁，但它能够清除复杂程度较低的攻击，使得联邦政府和私营公司能够专注于更具危害性的针对性攻击。

## FBI: InfraGard 门户网站

联邦调查局 (FBI) 的[InfraGard 门户网站](#)是一个信息交换中心，公共和私营部门可在此共享信息，以保护美国的关键基础设施。政府将关键基础设施分为从国防工业基地、制造业到水坝等 16 个行业。该网站提供有关 16 个行业相关事件的新闻，另外还附有网络犯罪和网络逃犯的链接，其中包含最新的攻击和联邦调查局正在追踪的潜在威胁的信息。



## 信息共享和分析中心国家委员会

信息共享和分析中心 (ISAC) 国家委员会成立于 2003 年, ISAC 的概念是在 1998 年首次提出的。如今共有 24 个 ISAC, 其中一些, 如金融服务 ISAC (FS-ISAC), 加盟费很高。但是很多 ISAC 提供低成本或免费的威胁情报。其基本思想是: 每个关键基础设施部门都设有负责监视和发现该行业威胁信息的组织。大多数 ISAC 都提供全天候的威胁警报和事件报告, 许多 ISAC 也为其部门设置威胁级别。请点击[此链接](#)查找适用于您所在行业的 ISAC。

## Ransomware Tracker

[Ransomware Tracker](#) 是一个瑞士安全网站, 由 [@abuse.ch](#) 管理, 专注于追踪和监控与勒索软件相关的域名、IP 地址和 URL 的状态。它包括僵尸网络 C&C 服务器、传播站点和支付站点。通过使用由 Ransomware Tracker 网站提供的数据, 托管服务提供商、ISP、国家 CERT、执法机构和研究人员可以获得勒索软件所利用的基础设施的信息, 以及威胁源是否正在利用它们进行诈骗的信息。该网站还提供缓解勒索软件攻击的指导, 以及需要在网络边界



拦截的勒索软件列表。

## Spamhaus 项目

[Spamhaus 项目](#)成立于 1998 年,是一家位于日内瓦和伦敦的国际非营利组织,负责追踪垃圾邮件和相关网络威胁,如网络钓鱼、恶意软件和僵尸网络。虽然 Spamhaus 以发布 DNS 拦截列表为人所知,但是它还能够生成用于互联网防火墙和路由设备的特殊数据,如 Spamhaus DROP 列表、僵尸网络 C&C 数据以及 Spamhaus 响应策略区数据(用于 DNS 解析器,这是一种有助于防止数百万互联网用户点击网络钓鱼和恶意邮件中的恶意链接的工具)。

## 互联网风暴中心

[互联网风暴中心](#) (Internet Storm Center, ISC) 成立于 2001 年,是继 Li0n 蠕虫之后安全社区进行合作的结果。如今,ISC 每天从覆盖 50 多个国家的超过 50 万个 IP 地址的传感器中收集数以百万计的入侵检测日志条目。ISC 是由 SANS 研究所支持的免费服务,其资金源于参加 SANS 安全教育计划的学生支付的学费。该网站提供了许多工具、教育播客、论坛和安全专业人士工作板的链接。



## 免费的反恶意软件网站

威瑞信 [《2017 年数据泄露调查报告》](#) 发现，51% 的数据泄露涉及恶意软件。以下网站对感染网络的主要恶意软件进行分析，可免费访问：[virustotal.com](http://virustotal.com)，[malwr.com](http://malwr.com)，[VirusShare.com](http://VirusShare.com)。

## 厂商博客

厂商的最终目的是销售产品，但这并不意味着他们不会发布信息丰富的博客，这些博客是很不错的信息来源，可由此了解厂商发现的最新攻击和保护网络的措施。我们向您推荐以下厂商博客：[Alien Vault](#)、[思科威胁研究博客](#)、[CrowdStrike 研究和威胁情报博客](#)、[火眼威胁研究博客](#)、[Palo Alto Networks Unit 42](#)、[Recorded Future](#) 和 [Windows 安全博客](#)。