

<https://www.darkreading.com/threat-intelligence/8-low-or-no-cost-sources-of-threat-intelligence-----/d/d-id/1330447>

11/27/2017
08:00 AM



Steve Zurier

8 Low or No-Cost Sources of Threat Intelligence

Here's a list of sites that for little or no cost give you plenty of ideas for where to find first-rate threat intelligence.



Image Source: BeeBright / Shutterstock.com

Organizations know they need to get serious about threat intelligence, but it's not always clear where to find credible information. While just about every security industry vendor website offers up information on the latest threats, some are better than others. Here, we'll point out the sites that are the most informative and useful.

We called on Roselle Safran, president of Rosint Labs, to work with us to build a meaningful list. Safran's extensive experience in cybersecurity includes several years

of service in the Executive Office of the President and Department of Homeland Security during the Obama administration.

Safran included some obvious choices from federal government sources, but she also struts her cybergeek sruff by offering up some lesser-known sites that track ransomware and malware. We combined forces with Safran to develop a list that will give novices the threat intelligence amuse-bouche they need while supplying some intel red meat for experienced security pros.

Go through the list. You'll find that there are many more than eight sites to choose from:



Department of Homeland Security, Automated Indicator Sharing

The Department of Homeland Security's free [Automated Indicator Sharing \(AIS\)](#) website was set up for private companies to share cyber threat indicators with the federal government. Typical threat indicators available are information such as malicious IP addresses or the sender address of phishing emails. DHS aims to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared with all AIS participants. Federal officials say while AIS won't eliminate sophisticated cyber threats, it will clear out the less sophisticated attacks, making it possible for the federal government and private companies to focus on the more pernicious targeted attacks.

Image Source: Carsten Reisinger / Shutterstock.com



FBI InfraGard Portal

The FBI's [InfraGard Portal](#) serves as a clearinghouse for the public and private sectors to share information to protect America's critical infrastructure. The government breaks critical infrastructure into 16 sectors ranging from the defense industrial base to manufacturing to dams. The site offers a news feed on events relevant to the 16 sectors, plus has Cyber Crimes and Cyber Fugitives links that contain information on the most recent attacks and potential threats being tracked by the FBI.

Image Source: Tiny Ivan/ Shutterstock.com



National Council of ISACs

National Council of Information Sharing and Analysis Centers

While the National Council of ISACs was formed in 2003, the ISAC concept was first introduced in 1998, almost 20 years ago. Today, there are 24 ISACs. Some of them, like the financial services ISAC (FS-ISAC), are expensive to join. But many of them offer low or no-cost threat intelligence. The basic idea is for each critical infrastructure sector to have its own organization that monitors and ferrets out threat information specific to that industry vertical. Most ISACs have 24x7 threat warning and incident reporting capabilities, and many also set the threat level for their sectors. Follow [this link](#) to look up the ISAC that applies to your industry.

Image Source: National Council of ISACs



Ransomware Tracker

Managed by [@abuse.ch](#), Ransomware Tracker is a Swiss security site that focuses on tracking and monitoring the status of domain names, IP addresses, and URLs that are associated with ransomware. This includes botnet command-and-control servers, distribution sites, and payment sites. According to the Ransomware Tracker website, by using data provided by the site, hosting, and ISPs, as well as national CERTs, law enforcement agencies and security researchers can receive an overview on infrastructure exploited by ransomware and whether these are actively being used by bad threat actors to commit fraud. The site also offers guidelines for mitigating ransomware as well as blocklists for stopping ransomware at the network edge.

Image Source: [zimmytws](#) / Shutterstock.com



The Spamhaus Project

Founded in 1998, [The Spamhaus Project](#) is an international non-profit based in Geneva and London that tracks spam and related cyber threats such as phishing, malware, and botnets. While it is best-known for publishing DNS-based blocklists, according to its website, Spamhaus produces special data for use with Internet firewall and routing equipment, such as the Spamhaus DROP lists, botnet C&C data, and the Spamhaus Response Policy Zone data for DNS resolvers, a tool that helps prevent millions of internet users from clicking on malicious links in phishing and malware emails.

Image Source: Tetiana Yurchenko / Shutterstock.com



Internet Storm Center

The [Internet Storm Center](#) was founded in 2001 following the collaboration that took place in the security community following the LiOn worm. Today, the ISC gathers millions of intrusion detection log entries every day, from sensors covering more than 500,000 IP addresses in more than 50 countries. The ISC is a free service supported by the SANS Institute from tuition paid by students attending SANS security education programs. The site offers numerous links to tools, educational podcasts, forums, and a job board for security professionals.

Image Source: SANS Institute



Free anti-malware sites

The [Verizon 2017 Data Breach Investigations Report](#) found that 51 percent of data breaches analyzed involved malware. Here are links to free sites that offer analysis of the leading malware infecting networks: [virustotal.com](#), [malwr.com](#) and [VirusShare.com](#).

Image Source: cifotart / Shutterstock.com



Vendor blogs

Vendors will always try to sell you product in the end, but that doesn't mean that they don't maintain informative blogs that serve as excellent sources to learn more about what the vendor has found about recent attacks and remedies for protecting your network. Here are some to consider: [Alien Vault](#), [Cisco Threat Research Blog](#), [CrowdStrike Research and Threat Intel Blog](#), [FireEye Threat Research Blog](#), [Palo Alto Networks Unit 42](#), [Recorded Future](#), and [Windows Security Blog](#).

Image Source: Aniwwhite via Shutterstock

https://www.darkreading.com/author-bio.asp?author_id=2460

Profile of Steve Zurier

Freelance Writer News & Commentary Posts: 94

Steve Zurier has more than 30 years of journalism and publishing experience, most of the last 24 of which were spent covering networking and security technology. Steve is based in Columbia, Md.