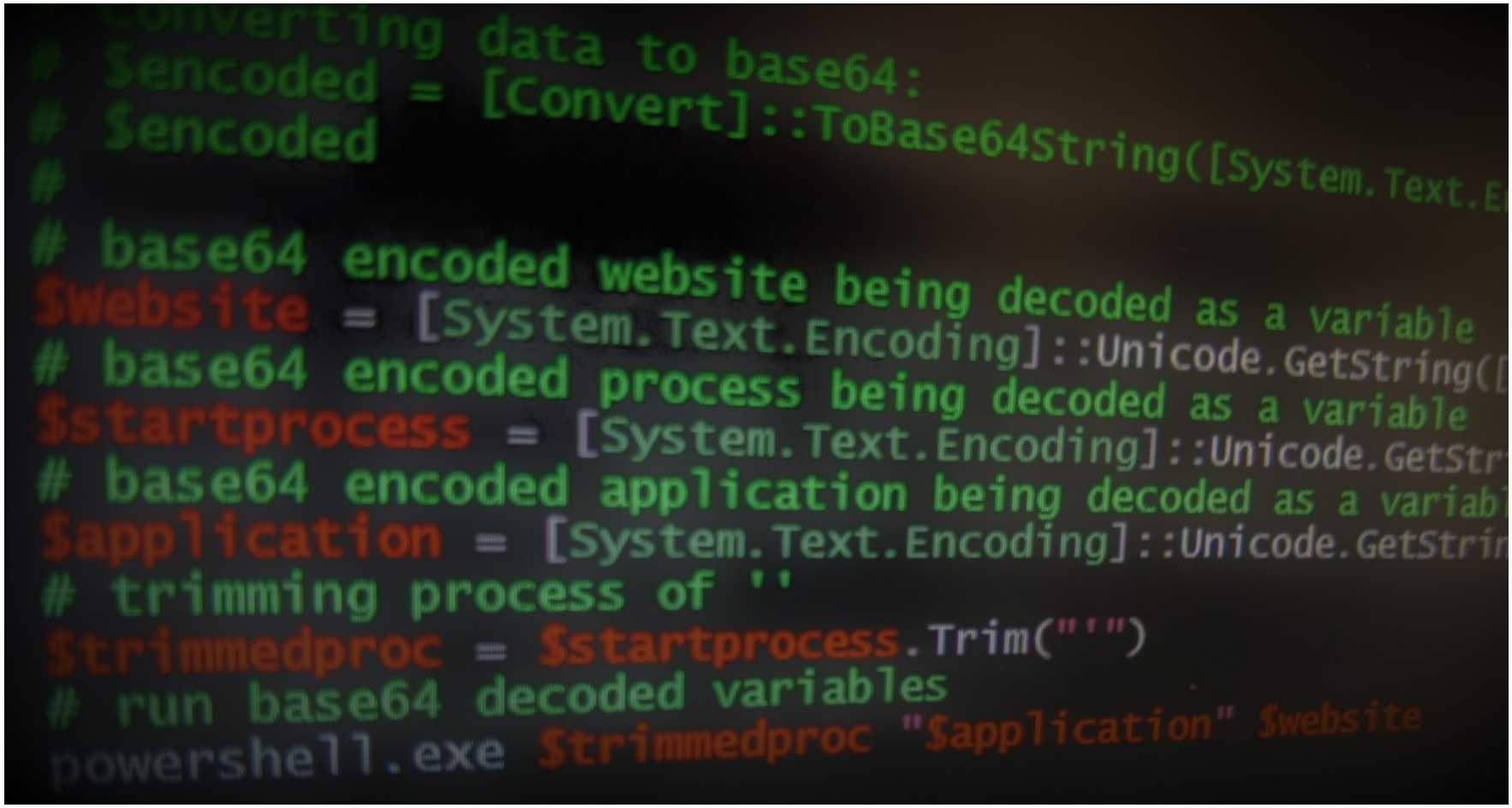

Building Better Queries in Shodan.io For Better Reporting

Published on April 1, 2020 Edit article View stats

Like Comment Share

6 ·

Messaging

Building Better Queries in Shodan.io for Better Reporting

By: Brad Voris

What is Shodan?

Below is Shodan's Description:

https://help.shodan.io/the-basics/what-is-shodan

Shodan is a search engine for Internet-connected devices. Web search engines, such as Google and Bing, are great for finding websites. But what if you're interested in measu which countries are becoming more connected? Or if you want to know which version Microsoft IIS is the most popular? Or you want to find the control servers for malware Maybe a new vulnerability came out and you want to see how many hosts it could affe Traditional web search engines don't let you answer those questions.

Shodan gathers information about all devices directly connected to the Internet. If a device is directly hooked up to the Internet then Shodan queries it for various publicly-available information. The types of devices that are indexed can vary tremendously: ranging from small desktops up to nuclear power plants and everything in between.

So what does Shodan index then? The bulk of the data is taken from **banners**, which are metadata about a software that's running on a device. This can be information about the server software, what options the service supports, a welcome message or anything else that the client would like to know before interacting with the server.

Know what results you are expecting from Shodan. Sounds easier said than done but i know what you are roughly looking for your search will be easier. Compile a list of yo search criteria and write it down prior to starting your search in Shodan.

Generic information about your search should be items like:

Application or product you are searching for, could include version I.E.: Microsoft-IIS

External or Public facing IP address or DNS name. I.E.: 8.8.8.8 or dns.google

Application ports that are being used and public facing. I.E.: Port 443 SSL/TLS

Location of where what you are looking for can be a country or a city. I.E.: US, Seattle

Organization's name that owns the resource. I.E.: Google

Starting your search:

To optimize your search results regardless of using the UI, CLI or API you will need to filter with search patterns.

We will start off with some generic searches to help you understand how and why it is important to filter your searches.

In Shodan I search for IIS. IIS is Microsoft's Web Application Server. Very Generic search criteria which presents with 9,159,942 public facing banners that can be identified wit

While this high level information is great for statistics its absolutely useless trying to g
down to an individual system or group of systems.

Let's refine the search for better criteria by including only port 80. Port 80 being the d
web application port for unencrypted traffic.

This time I search for IIS port:"80"

Ok that halved our results more or less from 9,159,942 to 5,085,603… So the search filtering was significantly better but the results still aren't earth shattering or helpful.

Lets refine the search again by adding country.

This time I search for IIS port:"80" country:"US"

Amazingly enough my search criteria resulted in nearly half the results again. Search results are down from 5,085,603 to 2,008,596. Lets refine our search again to see if we can get it even lower. I am going to change IIS to Microsoft-IIS/8.5 this being verify specific banner to IIS and its version.

Absolutely staggering to see results going from over 9 million results down to 460,364

Now let's refine our search to include the city of Seattle.

This time I search for Microsoft-IIS/8.5 port:"80" Country:"US" City:"Seattle"

Now we are getting somewhere. 3124 search results that get us very specific informati

Since the initial search results comprised Microsoft IIS 8.5 lets look at some even gran search results based on Operating System. Lets specify Windows Server 2008.

This time I search for Microsoft-IIS/8.5 port:"80" Country:"US" City:"Seattle" os:"Wi Server 2008"

Now we are down to some manageable results. Out of a total of 9,159,942 results we were able to get the search results down to 181.

Why break this down in such an elementary way? Because search results cost credits. The more we refine the results with filters the better the results will be. Fundamentally

time and effort.

Optimizing your search filters and results:

What are some other search filters I can use to get better results?

Excerpt from: **https://github.com/JavierOlmedo/shodan-filters**

Searching by Country codes Code list:

Excerpt taken from **https://github.com/postmodern/shodan-ruby**

Shodan Search Query Fundamentals

https://help.shodan.io/the-basics/search-query-fundamentals

Shodan Explore search queries shared by other users:

https://www.shodan.io/explore

Github PostModern Country Codes:

https://github.com/postmodern/shodan-ruby

GitHub JakeJarvis Awesome Shodan Queries

https://github.com/jakejarvis/awesome-shodan-queries

Computer Weekly Shodan Search Engine For Penetration Tests: How-to

https://www.computerweekly.com/tip/Shodan-search-engine-for-penetration-tests-How-to

YeahHub Shodan Search Examples

https://www.yeahhub.com/shodan-search-examples/

Daniel Miessler A Shodan Tutorial and Primer

Safety Detectives What Shodan Is and How to Use It

https://www.safetydetectives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/

Professional resources, like Cyber Forge Security, Inc are available to assist with establishing these plans and can work with you to evaluate technologies and plans, as
as assist with tabletop exercises to validate them and recommend appropriate changes.

#CyberSecurity #CyberForgeSecurity #InformationSecurity #CFS #CyberForgeSecuri
#PenetrationTesting #RedTeam #Security

Re

Published by

Brad Voris
CISSP, CCSK, Network+, MCP, MTA, VCA-DCV, NSE1, NSE2, ACE, 100W - OPSEC,
Trustee | (***I am not a purchasing authority***)
Published • 1y

Building better queries in Shodan.io for better reporting from a introductory perspective. If you are new to Shodan or you've been using it awhile to find systems this article provides some tips to minimize credit usage and optimize results.
#cybersecurity
#security
#cloudsecurity
#informationsecurity
#cyberforgesecurity

Reactions

0 Comments

Add a comment...

Brad Voris

CISSP, CCSK, Network+, MCP, MTA, VCA-DCV, NSE1, NSE2, ACE, 100W - OPSEC, Trustee | (***I am not a purchasing au

More from Brad Voris

HTTP Headers for the Security Professional

Brad Voris on LinkedIn

A Comparison of Different Online Password Vault/Manager Software Options

Brad Voris on LinkedIn

PowerShell Script Execution via Cmd.exe Relative Path PoC

Brad Voris on LinkedIn

Secu

Brad

See all 8 articles

Messaging