Hunting Cobalt Strike C2 with Shodan

michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2

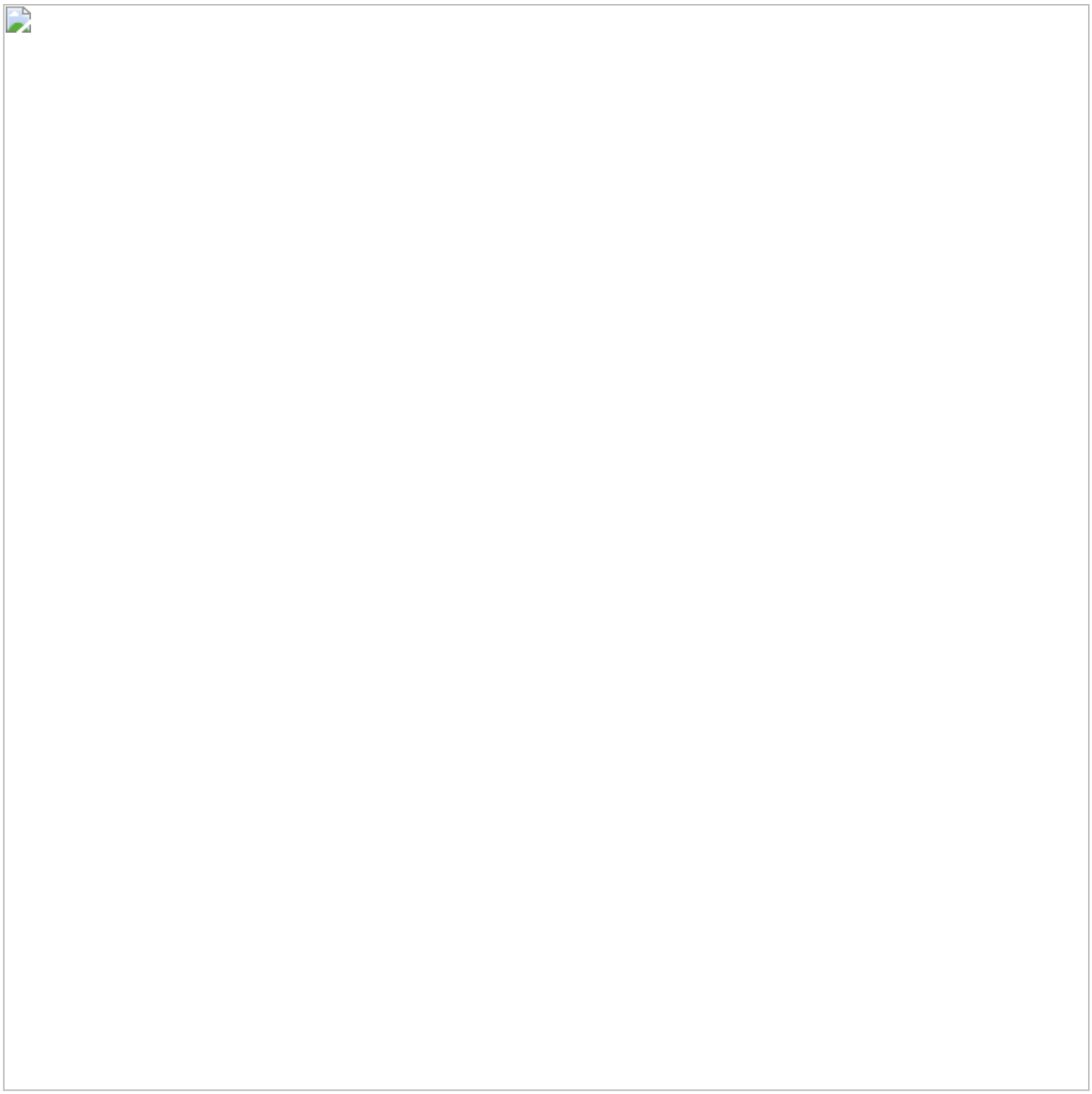
Michael Koczwara September 25, 2021

Michael Koczwara

Sep 7, 2021

.

2 min read



Cobalt Strike C2 Hunting

Four techniques:

- Default certificate.
- Hash + 50050 port (FP filtering is required).
- JARM (FP filtering is required).
- ASN/ISP scanning (this one is handy for subnet pivoting).

You can read my Twitter thread where I explained the logic behind each technique.

--

Try Knowable

Recommended from Medium


Tatiania Isleana

{UPDATE} 장기도사 Hack Free Resources Generator


Erin M. Nanasi

We’re RICH!



Chris Gebhardt

Penetrating Testing is Dead as We Now Know It