Unplug Your Refrigerator...

Entering the Internet of Things (IoT) space and looking at its implications on cybersecurity using Shodan.io

By:

Diante Jackson, CougarCS InfoSec Workshop Lead

Amani Jackson, Fortune 100 Cyber Strategy Consultant

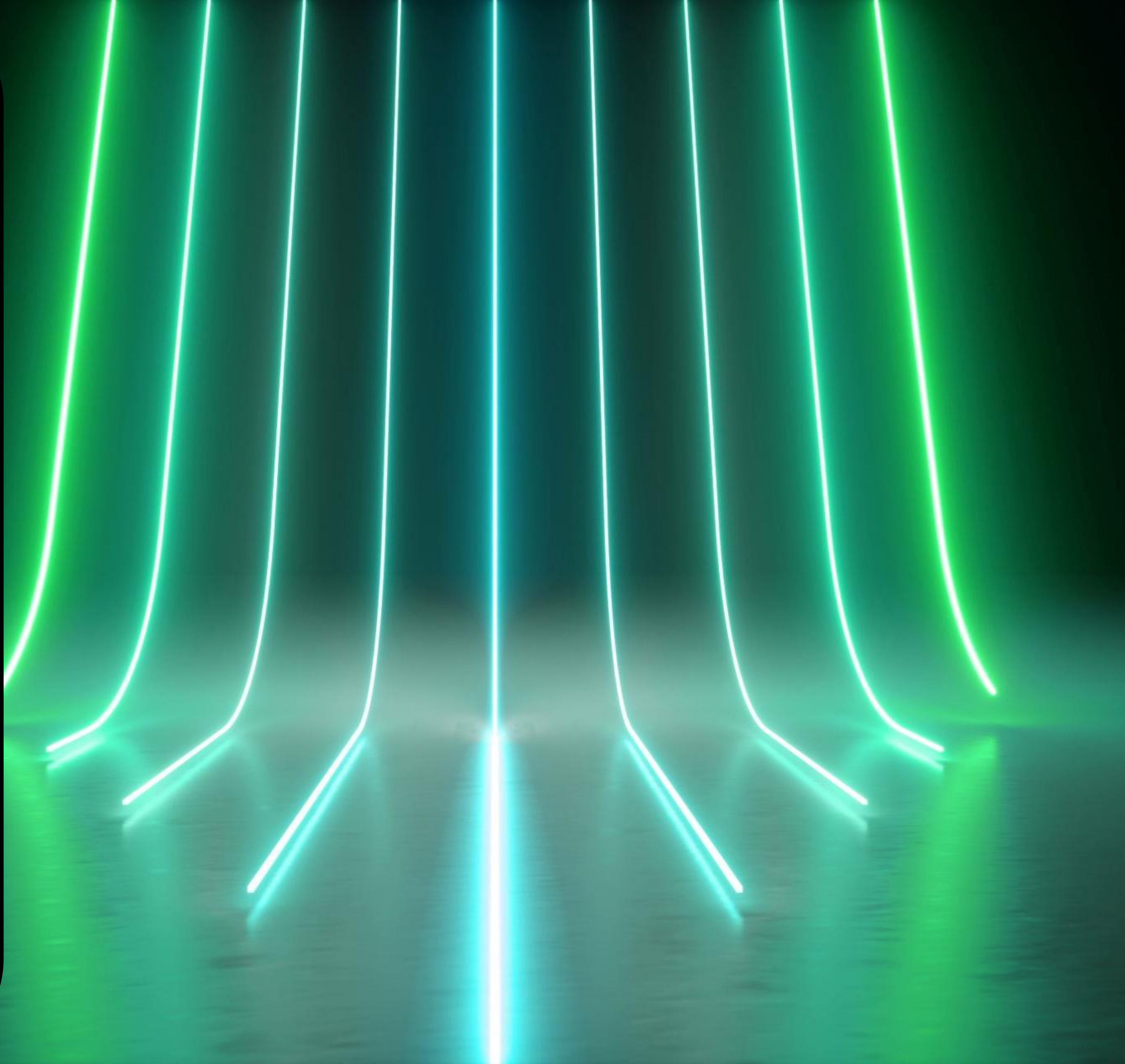


Table of Contents

Intro

- What is IoT?
- What is Shodan?

Demos

- North Korea
- I C U ^_^
- Passwords? Nah I'm Good

Serious Implications

Outro

Introduction to IoT

IoT

The **Internet of Things** (IoT) refers to the online networks of interconnected devices which communicate with other devices in their surrounding environments. These connections are remotely facilitated via data centers, resulting in increased reactivity and responsiveness.

What is Shodan and Why Use It?

Shodan, short for **Sentient Hyper-Optimized Data Access Network**, is a search engine for internet-connected devices. From routers and servers to energy plants and transportation systems, Shodan can provide details on the device's location, what organization owns it, protocols in use, and other technical measures.

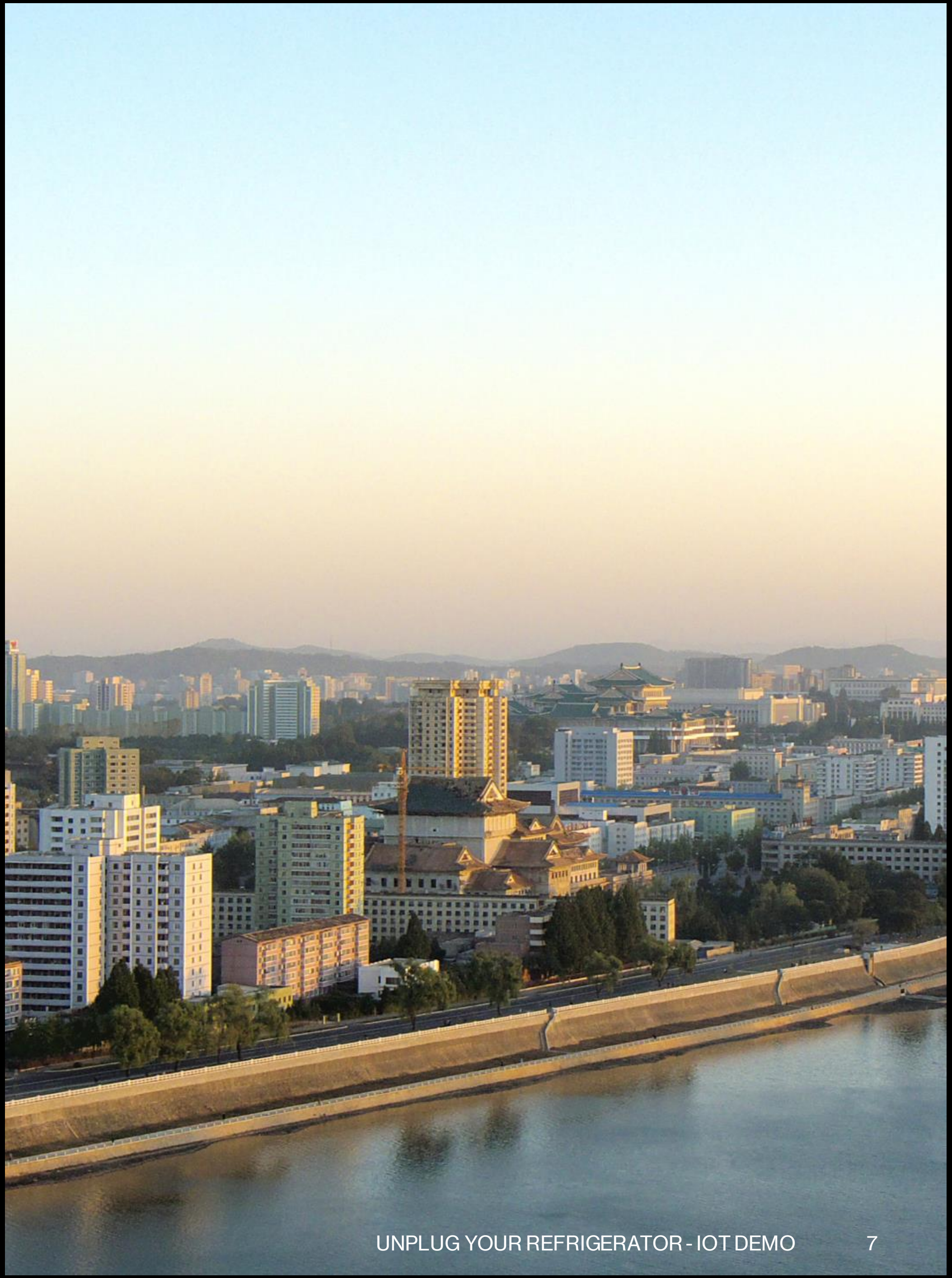
Cybersecurity professionals may leverage Shodan to discover vulnerable devices on the web. When dealing with corporate networks, the time it would take to run scans manually is greatly reduced. When dealing with zero-day vulnerabilities, researchers may use Shodan to gather large-scale information on impacted devices with minimal impact.

So… Let Me Show You Why This Matters!

Let's evaluate the inherent issues that Shodan allows us to observe!

North Korea is not safe from IoT...

- It's a common misconception that the DPRK has little to no modern infrastructure regarding the internet. You'd be shocked to find that not only do they possess many devices operating within their limited space, but that we can collect intelligence on those devices!
- Let's explore the results.



I C U ^_^ <3

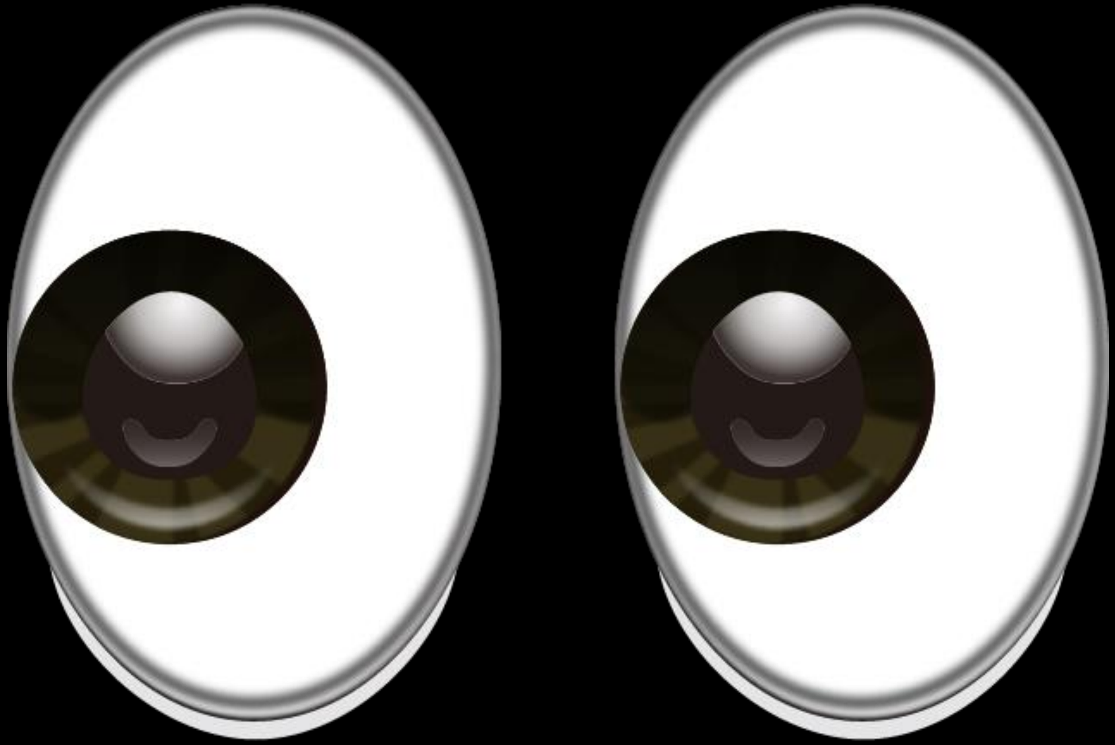
Yeah... Um... Cringe...

Guys. If you EVER have an IP camera... scratch that... ANY camera... please don't make it internet accessible.

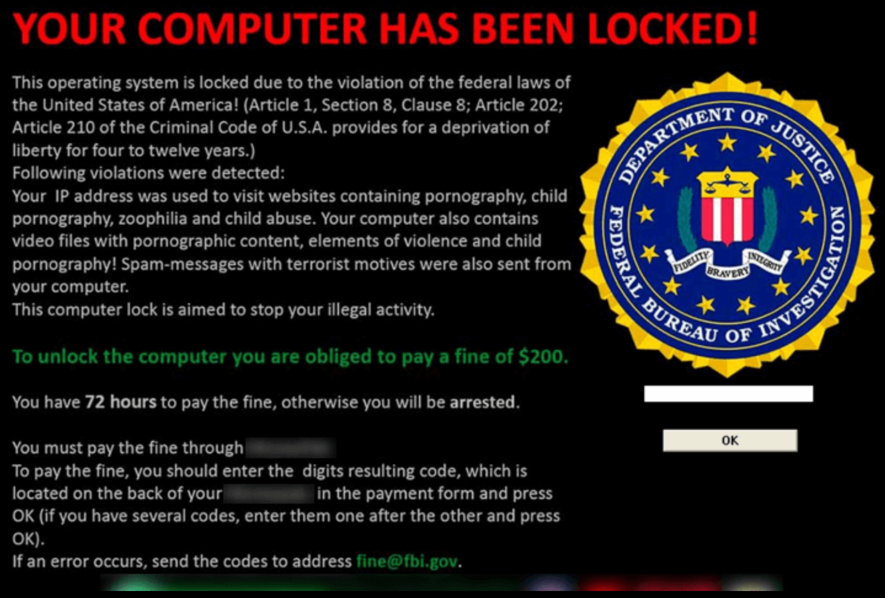
We can see you bruh...

I'm literally watching TV with you right now...

Let's watch other people now too! (in a totally non-illegal way I promise)



Doomed Desktops (guys... seriously... passwords...)



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Guys... I just told you quit making stuff accessible...

Leaving your Remote Desktop of ALL things not only accessible to IoT, but without a password or any form of authentication, is a surefire way to compromise your network.

Actually... Burn everything. Break your hard drives. By the time I see it on here you've already been hacked by half of the world.

Half of the middle east has been watching cooking tutorials with you...

Anyways, let's go be peeping toms again!

Let's Get Serious

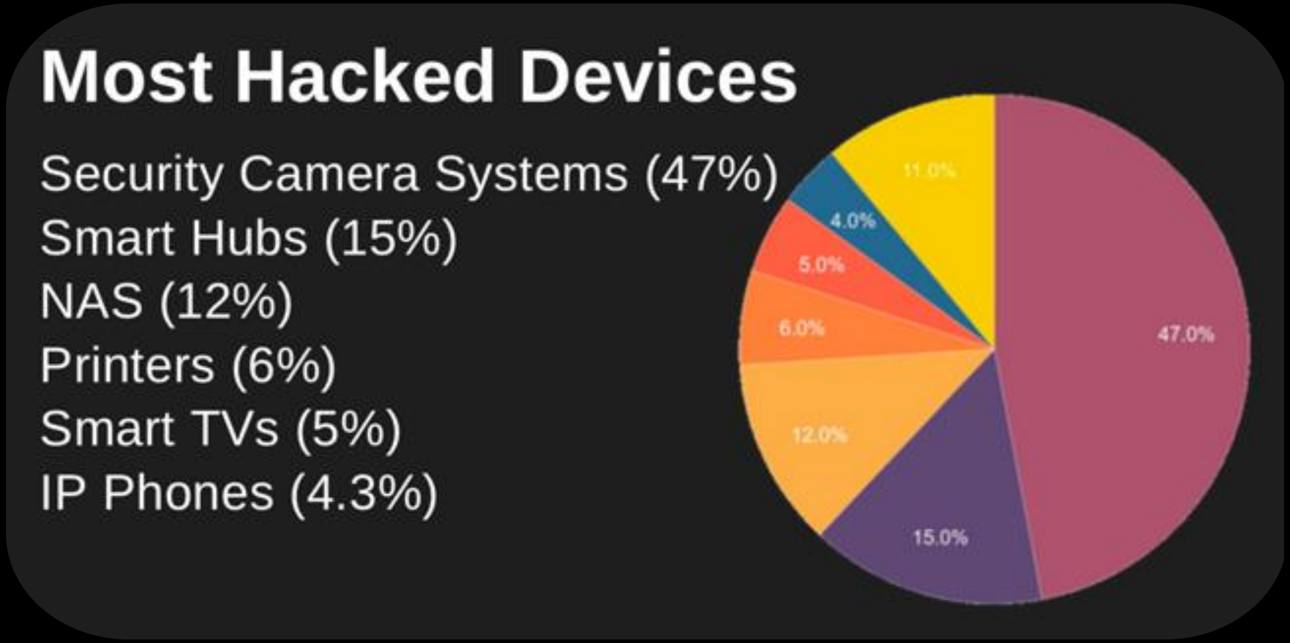
- Although we have been joking about spying and peeping on unsuspecting victims, it's still a very serious topic. There have been numerous instances of so-called "smart homes" and "security systems" being leveraged against themselves and exposing one's family, assets and secrets to surveillance that you would **NEVER** expect.
- As a security professional, these risks go further than just simple surveillance. Let's look further.

Exposing Assets

- Apache Directory Listing Dorks
  - When an index(.html/.php) file is not present, Apache lists directory contents by default, presenting an opportunity for attackers to search for specific filenames/types and attack.
- SMB (Samba File Share) (most common port[s]: 445, 139)
  - Samba is a file share protocol which is ***EXTREMELY*** dangerous to leave unsecured, as it can be enumerated to give critical system information as well as potentially leaking sensitive files.
- WordPress Misconfigurations:
  - Misconfigurations or human error during WordPress installations can lead to a leak of database credentials and code execution.
- Telnet (most common port: 23) ***IMPORTANT!!!***
  - Telnet is a protocol used for terminal-to-terminal communication, which commonly presents itself as an interactive shell. We can leverage this to completely control a system and/or network.

Outro

Are you using passwords yet??????



What have we learned?

- So…yeah. I hope you learned a little something about Shodan and think about just how secure the internet-connected devices all around us really are. ~~They aren't.~~
- Security professionals have been forced to adapt and are ~~failing~~ continuing to find ways to protect everyday individuals and corporations alike from the issues that arise from oversharing, human error, and poor policy enforcement.
- We also learned to stop port-forwarding and to use passwords! I hope… right?

Thanks To:

- Amani Jackson, Cyber Strategy Consultant and UTSA Alumna
  + Developed demonstrations.
  + Aided in presentation development.
- Jake Jarvis, https://github.com/jakejarvis/
  + Provided a GitHub repository for fun Shodan queries, on top of what we already knew. Check it out for more!
    - https://github.com/jakejarvis/awesome-shodan-queries

Thanks for participating!

Hack the Planet (in Minecraft) (also in GTA)!