CYBER THREATS IN THE STATE OF NH

… AND BEYOND

OCTOBER 23, 2024

Rick Rossi
CSA - New Hampshire

WHAT DOES TODAY'S CYBER THREAT LANDSCAPE LOOK LIKE?

Today's Themes...

- **Data as a Commodity**
- **Hacking as a Service (HaaS)**
  - **Ransomware, DDOS**
  - **Initial Access Brokers**
- **Ubiquity of Malicious Tools**
  - **Ease of Use**
  - **Destructive Capabilities**
- **Targets of Opportunity**
- **Supply Chain Campaigns and Zero Day Markets**
  - **External Dependency Management**

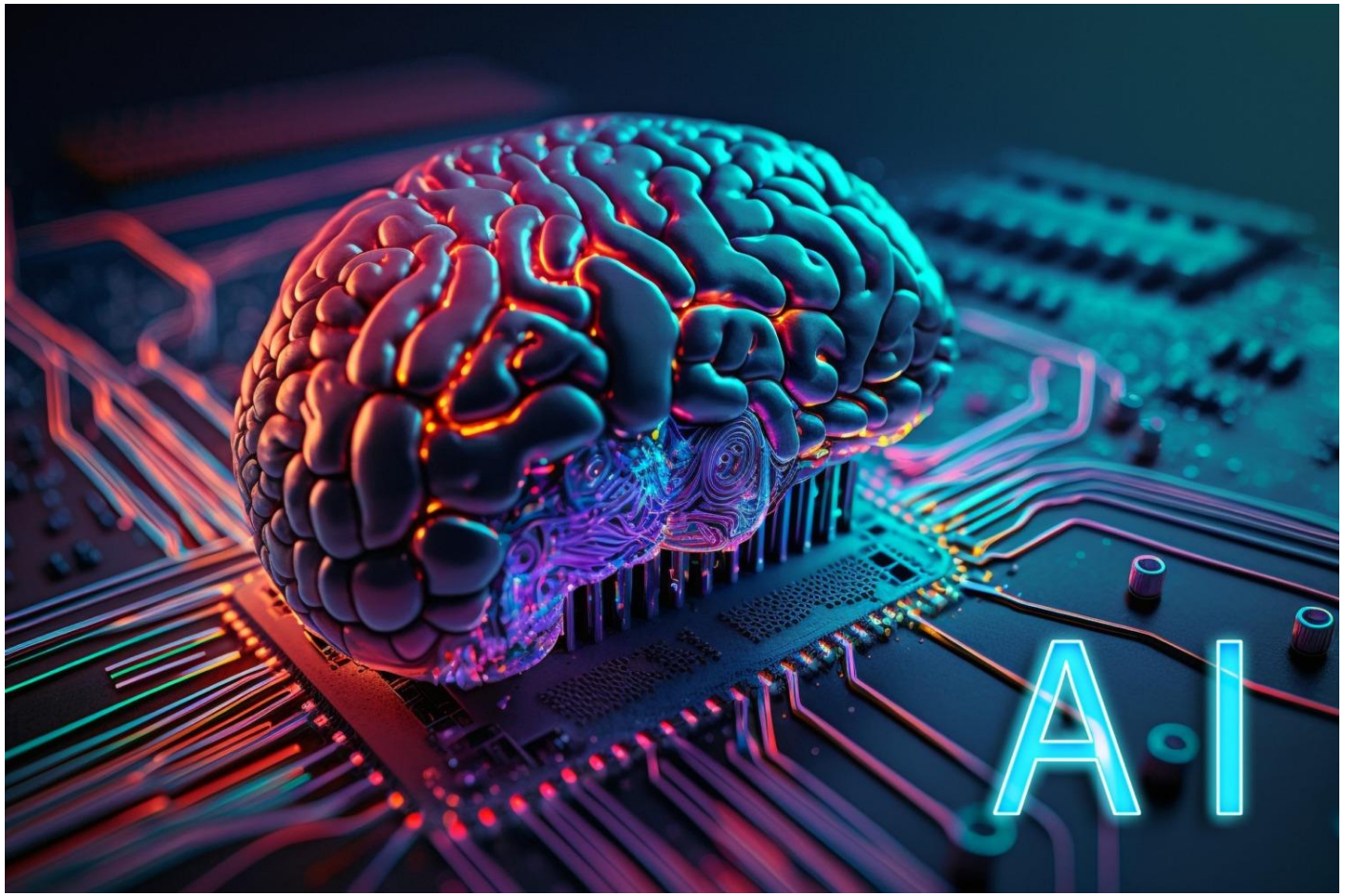
An Ever Expanding Attack Surface...

IOT and IIOT Devices

Employee and guest-owned devices

Personal Accounts

Artificial Intelligence Use in Hacking



Some Current Uses

- Improving colloquiality of phishing emails

- Vishing using the voice of senior executives and IT personnel

- Significantly lowers the barrier of entry for developing custom scripts and malware

- Greatly speeds up laborious steps in the hacking process

TARGETING OF CRITICAL INFRASTRUCTURE

Critical Infrastructure: Overview

The term critical infrastructure is tossed around a lot. What does it really mean?

Critical Infrastructure

Definition: systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on:

- security;
- national economic security;
- national public health or safety;
- any combination of those matters.

*** 42 U.S. Code § 5195c**

Threat Environment

https://www.youtube.com/watch?v=TH-2Ae5E1zE

Who’s responsible for securing the critical infrastructure your organization relies on?

So… Is it just China?

Short answer is a resounding NO!

FBI, CISA, and partnering agencies assess that cyber actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) are responsible for computer network operations against global targets for the purposes of espionage, sabotage, and reputational harm since at least 2020.

Whether through offensive operations or scanning activity, Unit 29155 cyber actors are known to target critical infrastructure and key resource sectors, including the government services, financial services, transportation systems, energy, and healthcare sectors of NATO members, the EU, Central American, and Asian countries.

Is it just China and Russia?

Short answer is a resounding NO!

The IRGC is an Iranian military organization that the United States designated as a foreign terrorist organization in 2019. IRGC-affiliated cyber actors using the persona “CyberAv3ngers” are actively targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs). These PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and are additionally used in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare. The PLCs may be rebranded and appear as different manufacturers and companies.

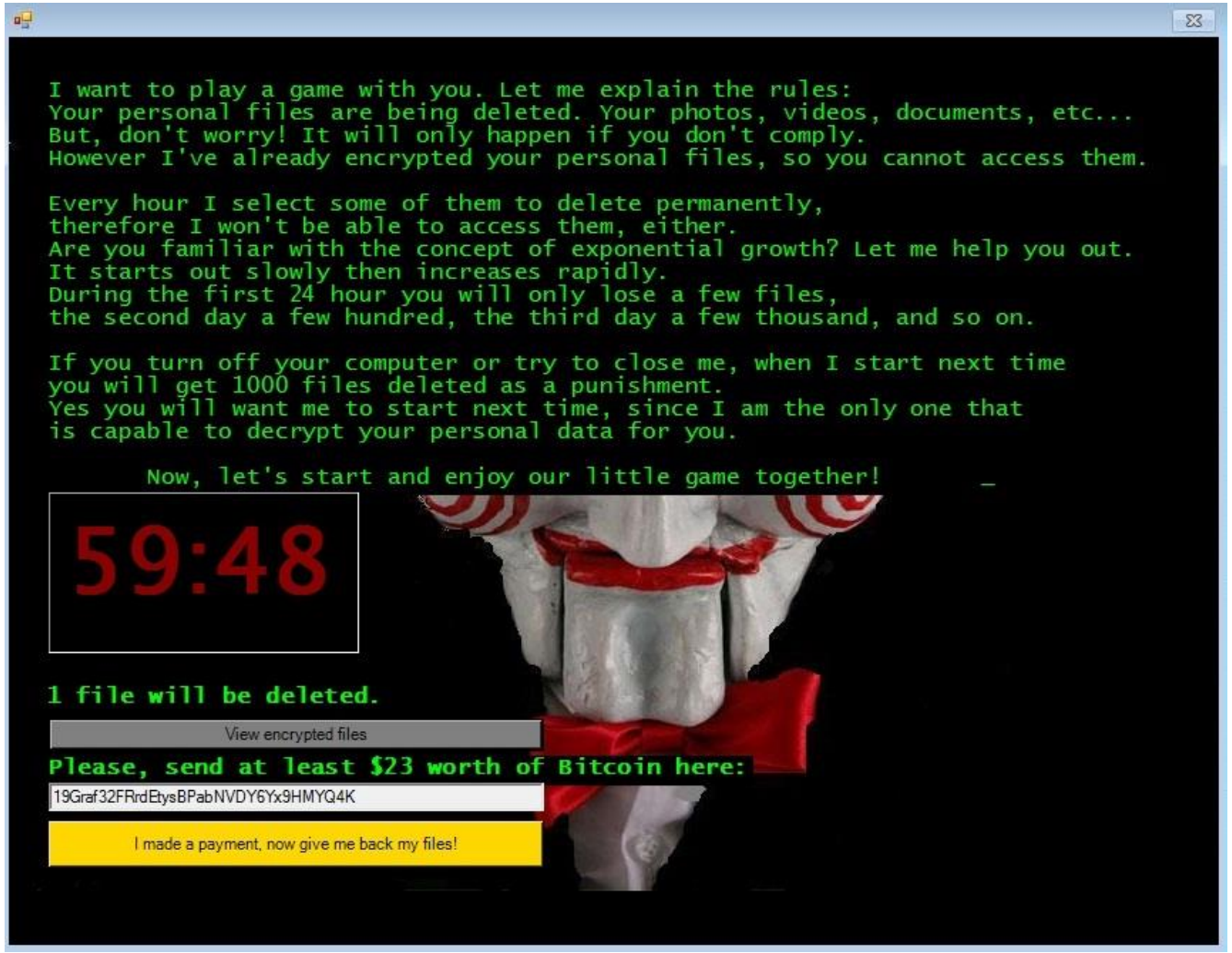
Is it just China, Russia, and Iran?

Short answer is a resounding NO!

The FBI, CISA, NSA, and authoring agencies assess North Korea conducts ransomware attacks on critical infrastructure to fund malicious cyber activities. The authoring agencies assess that an unspecified amount of revenue from these cryptocurrency operations supports DPRK national-level priorities and objectives, including cyber operations targeting the United States and South Korea governments—specific targets include Department of Defense Information Networks and Defense Industrial Base member networks.

Is it just China, Russia, Iran, and DPRK?

Short answer is a resounding NO.



Ransomware gangs constantly attack Critical Infrastructure (CI), but many attacks go unreported, particularly when no ransom is paid.

Ransomware is a national security threat often compared to terrorism. Like terrorism, ransomware focuses on soft targets like civilian critical infrastructure, but unlike terrorism, it is primarily financially motivated.

Advanced Cyber Campaigns

Who is the Target?

Staging Targets

- **Smaller organizations** with less sophisticated networks
- **Pre-existing relationships** with intended targets
- **Deliberately selected**, not targets of opportunity
- Examples: **vendors, integrators, suppliers,** and **strategic R&D partners**
- Used for **staging tools** and **capabilities**

Intended Targets

- **Small, medium,** and **large organizations**
- U.S. targets focused within the **Energy Sector**, specifically power generation, transmission, and distribution
- **Sophisticated networks** with more defensive cyber tools

THE PERSISTING PROBLEM

Threat Actors Are Sophisticated…

But They Often Don't Need To Be

DARKReading

91% Of Cyberattacks Start With A Phishing Email

Phishing remains the number one attack vector, according to a new study that analyzes why users fall for these lures.

The majority of cyberattacks begin with a user clicking on a phishing email. Ever wondor why users continue to fall for phishing emails?

According to a new report from PhishMe that found that 91% of cyberattacks start with a phish, the top reasons people are duped by phishing emails are curiosity (13.7%), fear (13.4%), and urgency (13.2%), followed by reward/recognition, social, entertainment, and opportunity.

"Fear and urgency are a normal part of every day work for many users," says Aaron Higbee, co-founder and CTO of PhishMe. "Most employees are conscientious about losing their jobs due to poor performance and are often driven by deadlines, which leads them to be more susceptible to phishing."

Higbee says PhishMe based the study on more than 40 million simulation emails by about 1,000 of its customers around the world. The study took place over an 18-month span from January 2015 through July 2016.

CSO FROM IDG

Home > Information Security

ANALYSIS

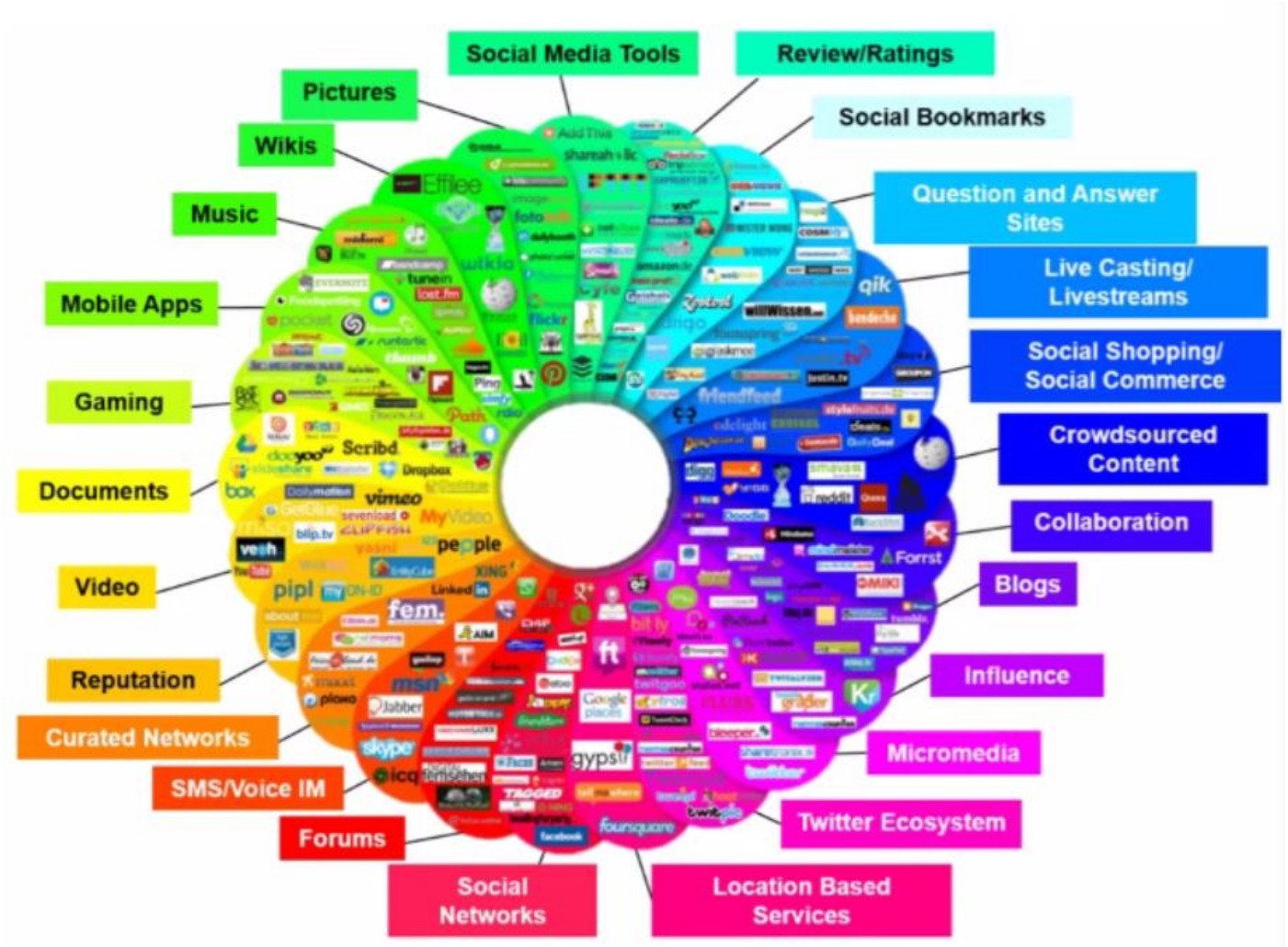
Zero-days aren't the problem -- patches are

Everyone fears the zero-day exploit. But old, unpatched vulnerabilities still provide the means for malicious hackers to carry out the vast majority of hacks

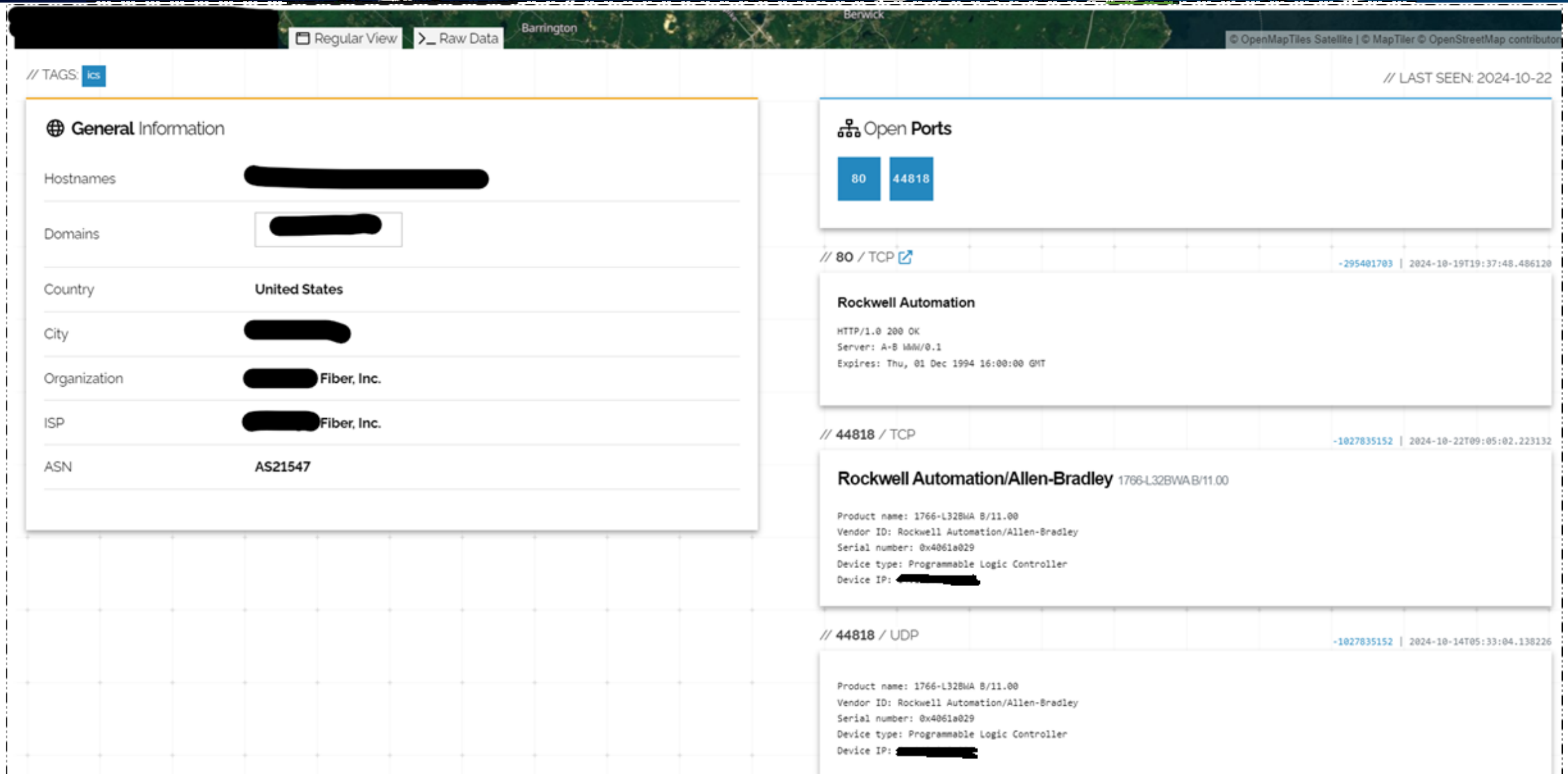
Most hackers follow the path created by a very few smart ones -- and zero days make up a very small percentage of attacks. It turns out that patching vulnerable software, if implemented consistently, would stop most hackers cold and significantly reduce risk.

But They Often Don't Need To Be

- Network Scans
- Information about the organization, employees, and executives found online.
- Discarded information
- Job Postings



But They Often Don't Need To Be...



Contact Information

CISA Team New Hampshire Contact Information

Rick Rossi **Cybersecurity Advisor**	**richard.rossi@cisa.dhs.gov** **+1 202-770-8991**
Joe Villers **Protective Security Advisor**	**joseph.villers@cisa.dhs.gov** **+1 771-217-6706**