AMPEX

The Dark Web and Why You Should Care

This Briefing is Proprietary and Competition Sensitive

What is the Dark Web

- The “Dark Web” is a part of the world wide web that requires special software to access.
- Much like the internet, the Dark Web is a network of websites, forums, and communication tools like email.
- What differentiates the Dark Web from the internet is that users are required to run a suite of security tools that help anonymize web traffic.

The Dark Web

- Though the name sounds ominous, the Dark Web did not hatch from some evil hacker lab.
- The Dark Web is simply a network of websites that require basic encryption technologies to be enabled before users can load content.
- These are the same technologies that protect passwords when users log on to bank portals and sites like Gmail and Facebook

What's the Big Deal?

However…….

- The Dark Web is used for both nefarious and reputable purposes.
- Criminals exploit the network's anonymity to sell
  - Personal Information
  - Banking information
  - Corporate information / access
  - Guns
  - Drugs
  - Human Trafficking

Examples of What is Sold

- Social Security number: $1
- Credit or debit card (credit cards are more popular): $5-$110
- Online payment services login info (e.g. Paypal): $20-$200
- Loyalty accounts: $20
- Subscription services: $1-$10
- Diplomas: $100-$400
- Driver's license: $20
- Passports (US): $1000-$2000
- Medical records: $1-$1000*
- Customized Exploits - Varies
- A recent study by Carnegie Mellon researchers Soska and Christin has calculated that drug sales on the dark net total US$100M

Dark Web and Cyber Security

- Consider the Ashley Madison hack. Vast amounts of account data, including real names, addresses and phone numbers ended up on the Dark Web f
- Exploits and attack code are complex to build from scratch. The dark web provides a marketplace that connects programmers with the needed skills with those with motivations to unleash them.
- Dr0p1t-Framework, a trojan that downloads other malware, and the Silent Word exploit, which converts a malicious .EXE file into an innocent-seeming .DOCor sale

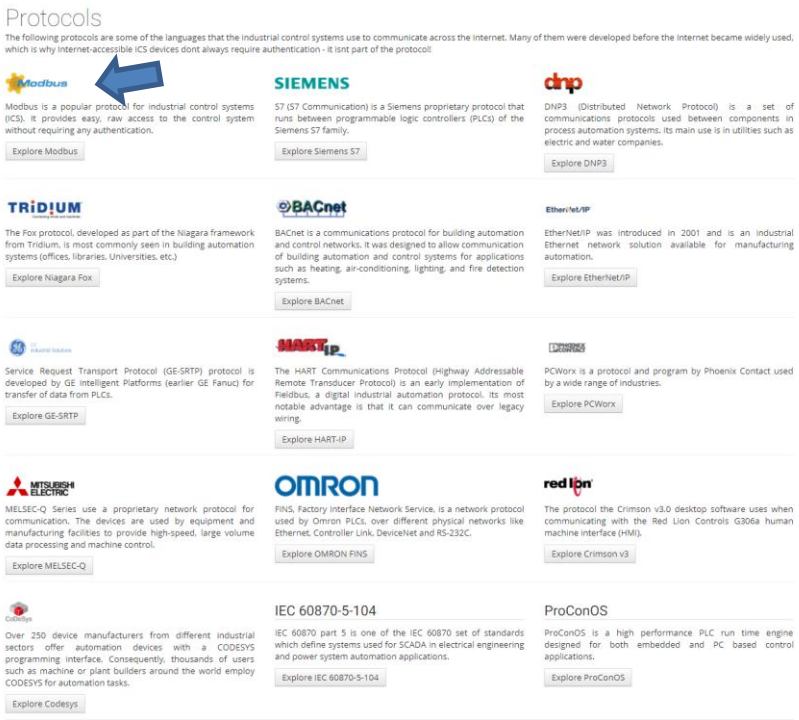
- Buyers of these exploits don't need to be master hackers themselves. There are guides on how to spread your malware, and also phishing and carding tutorials.“
- Dark Web paying corporate workers to leak info or for access
  - *staff at an unnamed bank were found to be helping hackers maintain a persistent presence on their corporate networks.*

Control Systems

- Control Systems (ICS, OT, SCADA) are used to run facilities like nuclear power stations, oil refineries and chemical plants, building automation, manufacturing and even airplanes so if cyber-criminals gained access to these netowrks, then the consequences could be lethal.

What's on the "ClearNet" - Shodan Tool

- Simple search for devices running Modbus that are connected to internet in U.S.



Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices dont always require authentication - it isnt part of the protocol!

Modbus

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

Explore Modbus

SIEMENS

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Explore Siemens S7

dnp

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Explore DNP3

TRIDIUM

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

Explore Niagara Fox

BACnet

BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

Explore BACnet

EtherNet/IP

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

Explore EtherNet/IP

Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

Explore GE-SRTP

HART-IP

The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

Explore HART-IP

PHOENIX CONTACT

PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

Explore PCWorx

MITSUBISHI ELECTRIC

MELSEC-Q Series use a proprietary network protocol for communication. The devices are used by equipment and manufacturing facilities to provide high-speed, large volume data processing and machine control.

Explore MELSEC-Q

OMRON

FINS, Factory Interface Network Service, is a network protocol used by Omron PLCs, over different physical networks like Ethernet, Controller Link, DeviceNet and RS-232C.

Explore OMRON FINS

red lion

The protocol the Crimson v3.0 desktop software uses when communicating with the Red Lion Controls G306a human machine interface (HMI).

Explore Crimson v3

Over 250 device manufacturers from different industrial sectors offer automation devices with a CODESYS programming interface. Consequently, thousands of users such as machine or plant builders around the world employ CODESYS for automation tasks.

Explore Codesys

IEC 60870-5-104

IEC 60870 part 5 is one of the IEC 60870 set of standards which define systems used for SCADA in electrical engineering and power system automation applications.

Explore IEC 60870-5-104

ProConOS

ProConOS is a high performance PLC run time engine designed for both embedded and PC based control applications.

Explore ProConOS

TOTAL RESULTS

3,407

TOP COUNTRIES

United States	3,407

TOP CITIES

Atlanta	130
New York	54
Marietta	27
Tulsa	26
Long Beach	21

TOP ORGANIZATIONS

Verizon Wireless	1,609
AT&T Wireless	236
Comcast Business	155
Sprint PCS	119
Time Warner Cable	96

TOP OPERATING SYSTEMS

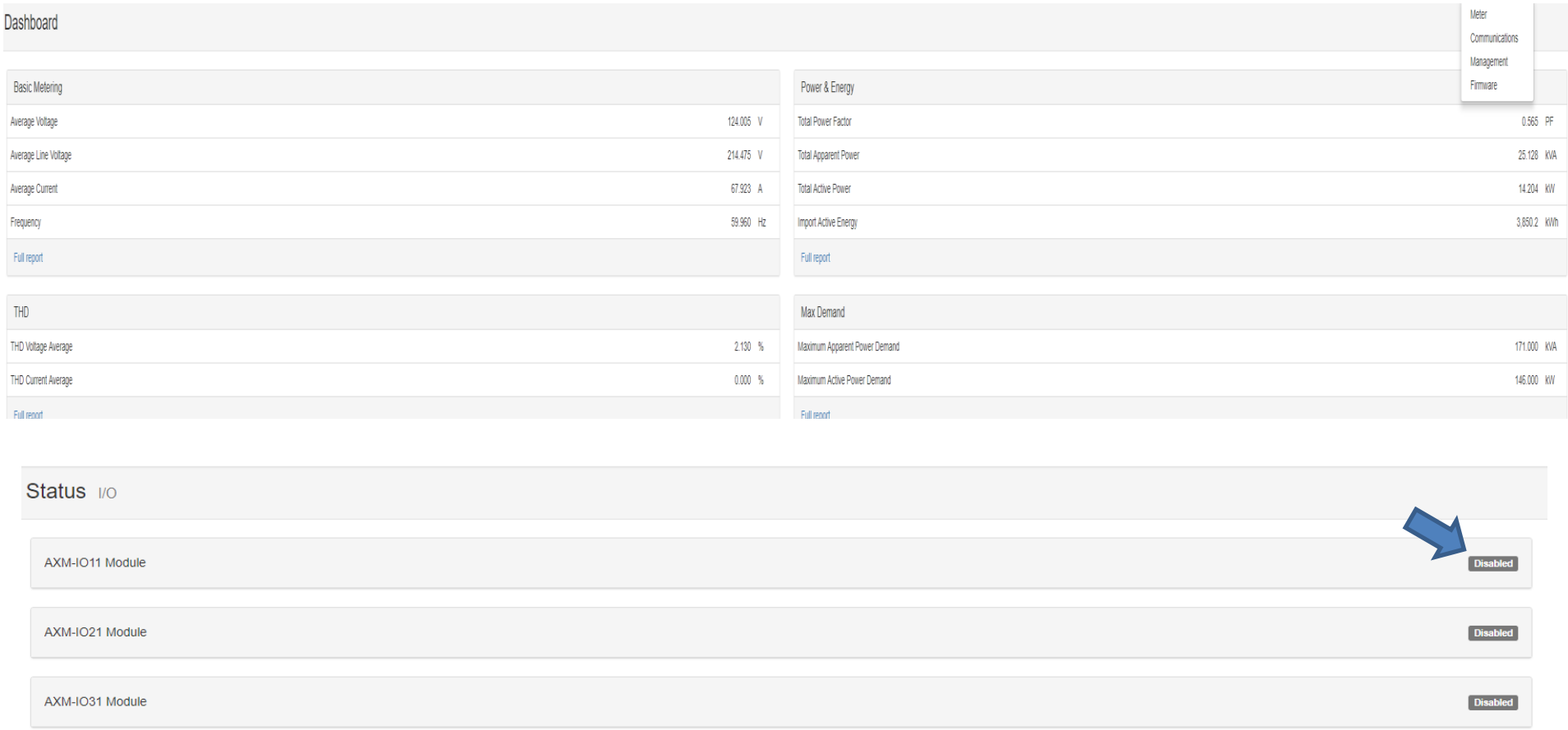
Linux 2.4-2.6	18
Windows 7 or 8	11
Linux 2.6.x	5
Windows XP	4
Linux 3.x	4

TOP PRODUCTS

BMX P34 2020	98
BMX NOE 0100	58
171 CBU 98090	26
NF3000	20
TM241CEC24T_U	19

Just found A Device

- Default credentials passwords



Known Data Breaches

- Known breaches
  - Equifax
  - Target
  - Macy's
  - Atlanta city government systems down due to ransomware attack
  - Oregon tax agency employee copied personal data of 36,000 people
  - Kansas Department for Aging and Disability Services Notifies 11,000 Consumers About Breach of Protected Health Information
  - Officials: 2 ex-Florida Hospital employees stole, sold patient records
- And the lists goes on and on

How Do We Protect

- The bad guys know and are trained on current defensive tools and strategies
- Must be better than they are
  - Faster, Outside the Box thinking and solutions
- Machine Learning defensive solutions for companies
- Understand your “Digital Footprint” and do things to minimize it

Questions