NDHIMSS Spring 2017 Conference

transforming health through IT™

Dan Friedrich, CISSP

Healthcare Security From a Hacker's Perspective

Why, How, and What Now

COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT

WHY ME?

- Cyclops Lab (First ever NSA agreement with a public academic Institution)
  - DSU holds 3 National Security Agency (NSA) and Department of Homeland Security (DHS) Academic Centers of Excellence designations.
    - Cyber Operations, Information Assurance Education, and Information Assurance Research
    - Cyber Corps
  - CAHIT (Center for Advancement of Health IT)
    - History of National and Statewide projects
      - HISPC, SDEHRA, CMS EHR Demonstration
      - Regional Extension Center ONC P&S CoP Advisory Panel
      - CMS TCPI PTN, Statewide HIE
    - Performing Healthcare specific Pen Tests for 5 years
    - 1 provider offices, CAHs, and large Integrated Delivery Networks

COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT

Why Is Healthcare Information Becoming Increasingly Valuable on the Dark Web

- 2014-2016 chip card and Pin in financial industry moves financial fraud to 4 year low.
- 2009 ARRA and the HITECH ACT moved EHR adoption from
  - Hospital 9% to 84%
  - Providers 42% to 83%
- Health Breaches are more difficult to detect (twice as long) FBI brief
- Information can't be changed
- 22% of Acute Care and 10% of non-Acute providers DO NOT have a FIREWALL (HIMSS 2016 Security Survey)

COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT

DSU DAKOTA STATE

healthPOINT SECURITY services

COMPASS Practice Transformation Network

healthPOINT at Dakota State University

CAHIT

PRIVACY TIP FOR DEEP WEB USERS: Use a VPN with Tor. Don't fall into a false sense of security by believing that Tor is enough to protect you. If you want the very best anonymity and privacy while on the Deep Web then you need to be using a VPN with Tor. It is an extremely valuable tool in your fight for anonymity. Click here to find the best VPN for privacy on the Deep Web.

INVITE / REFERRAL ONLY MARKETS

This category is for markets that require an invite code or a referral link in order to register. We have included valid links that will enable registration. Please note: safety is not guaranteed! For the highest level of security, use multisig markets.

Filter

ALPHABAY

AlphaBay Market

★★★☆☆ 3.13 (615 REVIEWS)

Top Markets! MultiSig Or Trusted Invite Markets

Marketplace url:
http://pwoah7foa6au2pul.onion/register.php?aff=41211

Marketplace Forum Url:
http://pwoah7foa6au2pul.onion/forum/

Sub reddit:
http://www.reddit.com/r/AlphaBay/

Market Is Up (Green) Or Down (Red)?
AlphaBay - 98.12%

DeepDotWeb's Darknet Dictionary

QUICK NEWS

Prison Librarian Researched Rhys Jones Murder
22 Sep 2016

Hong Kong Customs Reports Drug Smuggling Increased Fourfold From 2013
21 Sep 2016

Blackmailer Warned Supermarket He Put Cyanide In Food, Wanted £2 Million
15 Sep 2016

Blockchain & Bitcoin Conference will reveal prospects and risks of cryptocurrency exchanges
10 Sep 2016

Source Code Of HL7 Software Maker PilotFish For Sale On Dark Web
29 Aug 2016

CATEGORIES

ARTICLES	FEATURED
MEMES & FUNNY	NEWS
NEWS UPDATES	VIDEOS

Hansa Market - 99.31%

INVITE / REFERRAL MARKETS

Python Market - 93.74%
Acropolis Market - 99.63%
T•chka Free Market - 95.68%
Apple Market - 98.99%

MARKETS

Darknet Heroes League - 98.32%
Zocalo - 99.7%
House Of Lions - 99.73%
TheRealDeal Market - 72.8%
DarkRabbit Market - 99.63%
The Majestic Garden - 96.95%
Bloomsfield - 99.14%
TheDetox Market - 98.28%
Crypto Market - 95.43%
Silk Road 3 - 97.68%
Minerva Market - 99.94%
The Trade Route - 98.61%
RsClub Market - 98.45%
Fantasia Market - 98.15%

VENDOR SHOPS

Megapack - 99.01%
Gammagoblin - 96.8%
The French Connection - 98.17%
CharlieUK - 94.15%
ToYouTeam - 93.91%
EuroPills - 98.55%
Fight Club - 98.82%
Darkmarket - 98.22%
MaghrebHashish - 94.28%

Home / Fraud Related / Documents & Data / Bulk pack of 50! USA FULLZ - Personal Info SSN + DOB

Bulk pack of 50! USA FULLZ - Personal Info SSN + DOB

USD 30.00

Ƀ 0.0492

In stock

Vendor	ednorton [+0|0] Level 1 (0)
Class	Digital
Delivery	⏭ Instant Delivery

⚠ This vendor only accepts 2-of-3 multi-signature orders. Click here to set it up. It is really easy and only takes a minute and protects you from being scammed.

❤ Favorite | ? Question | ⚑ Report

ℹ Details | 💬 Feedback

Listing Details

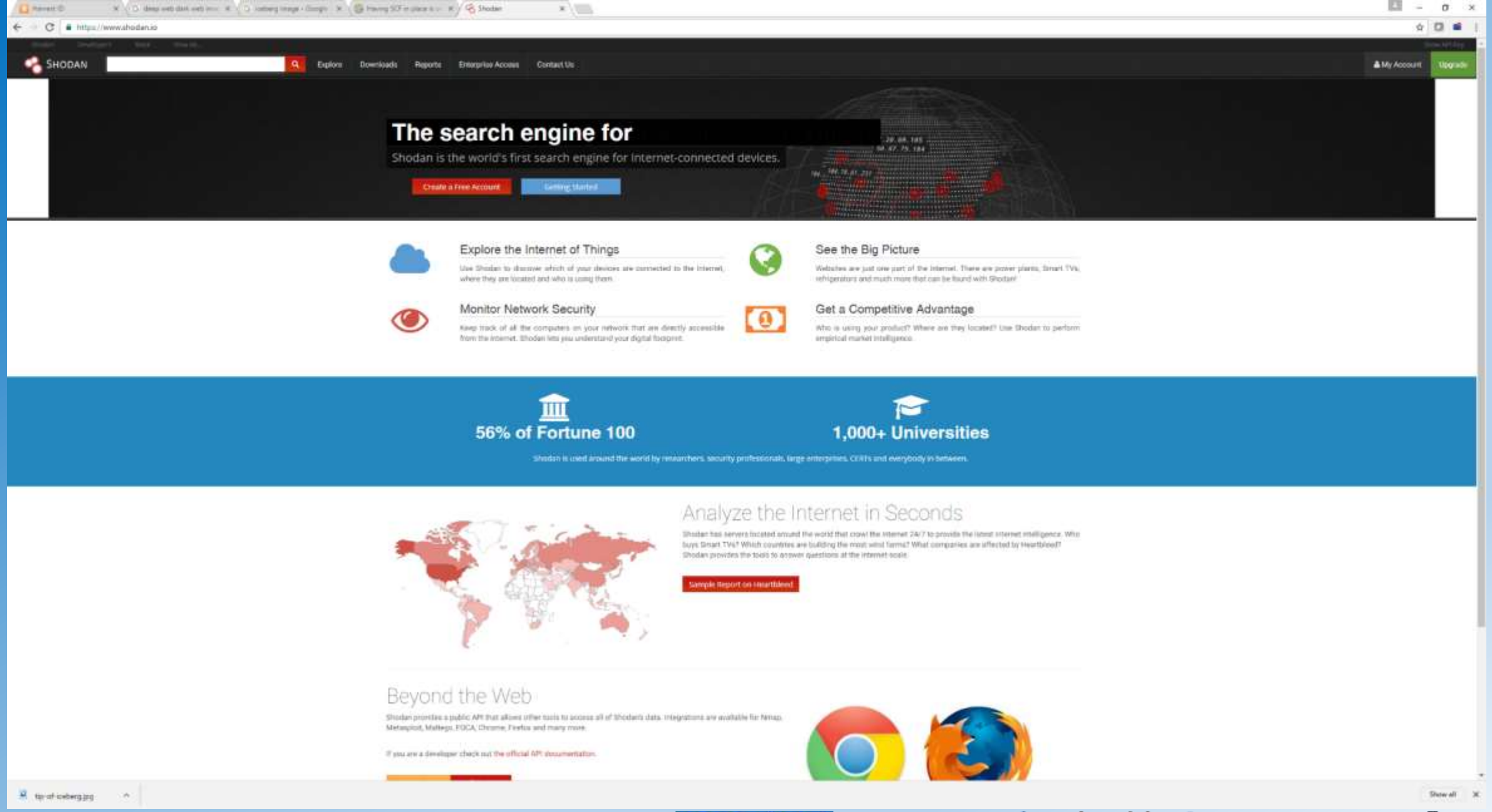
United States NEW FULLZ 2016

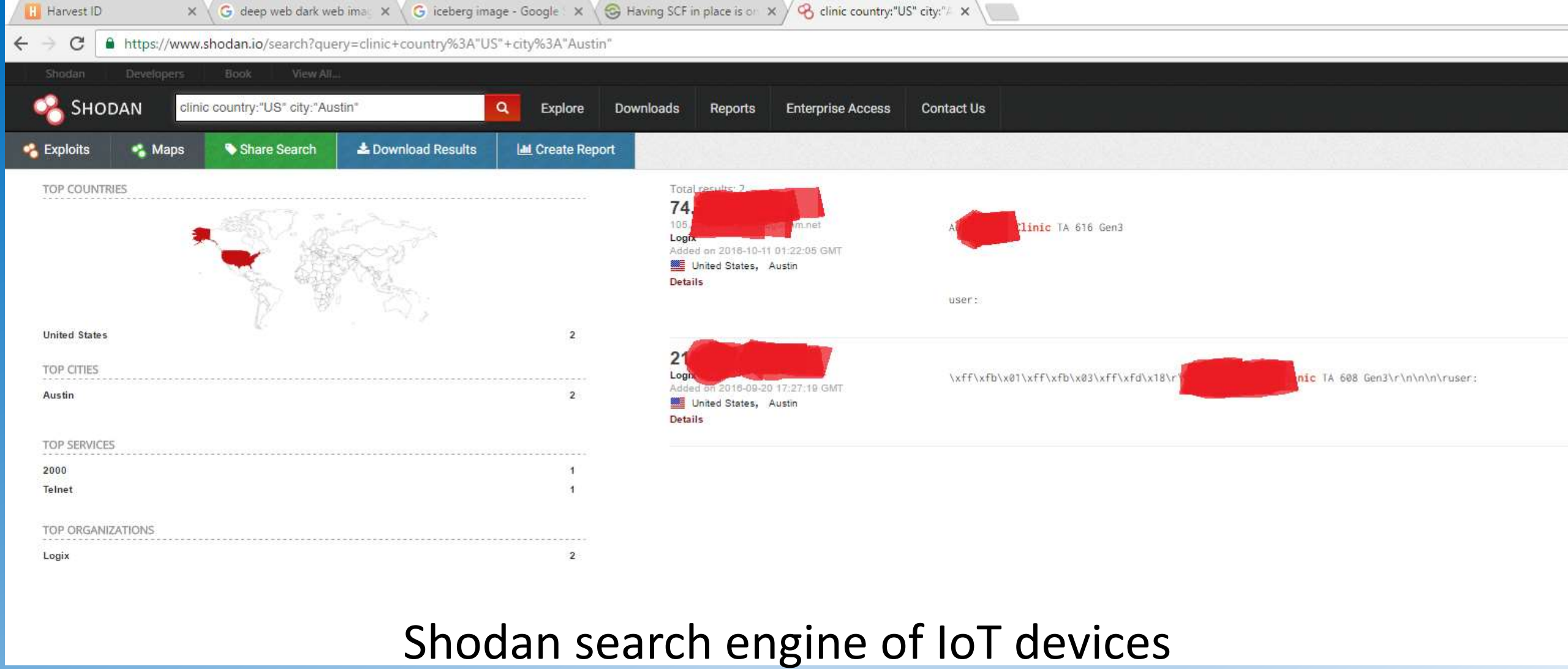
SSN, GENDER, DOB, FULL NAME, HOME PHONE, CELL PHONE, ADDRESS CITY STATE ZIP

Comes in the following format:
"SSN","GENDER","DOB","FULL NAME","HOME PHONE","CELL PHONE","FULL ADDRESS"

Example:
"333445555","F","1980-01-01","HALEY J BARNER","3095452266","","","19 GRANDVIEW DR,JACKSONVILLE,FL,,32200"

COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT


https://www.shodan.io
SHODAN
Explore
Downloads
Reports
Enterprise Access
Contact Us
My Account
Upgrade
The search engine for
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.
56% of Fortune 100
1,000+ Universities
Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.
Analyze the Internet in Seconds
Sample Report on Heartbleed
Beyond the Web
Shodan provides a public API that allows other tools to access all of Shodan's data. Integrations are available for Nmap, Metasploit, Maltego, FOCA, Chrome, Firefox and many more.
If you are a developer check out the official API documentation.
top-of-iceberg.jpg
Show all

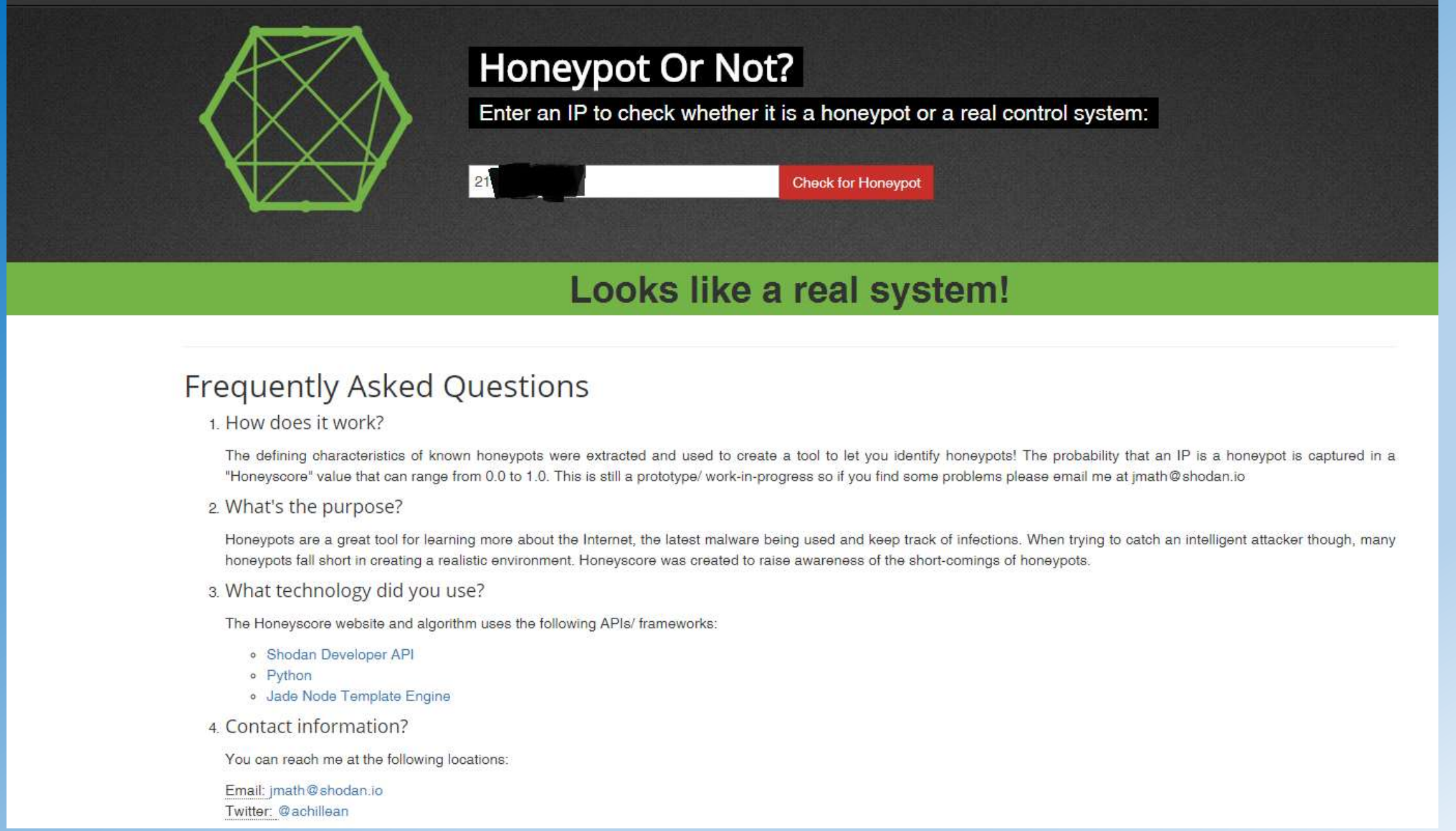


Shodan search engine of IoT devices

Crawls entire web space looking for devices

Enumerates services and captures banners

COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT


Honeypot Or Not?
Enter an IP to check whether it is a honeypot or a real control system:
21
Check for Honeypot
Looks like a real system!
Frequently Asked Questions
1. How does it work?
The defining characteristics of known honeypots were extracted and used to create a tool to let you identify honeypots! The probability that an IP is a honeypot is captured in a "Honeyscore" value that can range from 0.0 to 1.0. This is still a prototype/ work-in-progress so if you find some problems please email me at jmath@shodan.io
2. What's the purpose?
Honeypots are a great tool for learning more about the Internet, the latest malware being used and keep track of infections. When trying to catch an intelligent attacker though, many honeypots fall short in creating a realistic environment. Honeyscore was created to raise awareness of the short-comings of honeypots.
3. What technology did you use?
The Honeyscore website and algorithm uses the following APIs/ frameworks:
Shodan Developer API
Python
Jade Node Template Engine
4. Contact information?
You can reach me at the following locations:
Email: jmath@shodan.io
Twitter: @achillean

Total results: 2

[redacted]

10[redacted]xcom.net

Logix

Added on 2016-10-02 20:40:01 GMT

United States, Austin

Details

[redacted] Clinic TA 616 Gen3

user:

2[redacted]

Logix

Added on 2016-09-20 17:27:19 GMT

United States, Austin

Details

\xff\xfb\x01\xff\xfb\x03\xff\xfd\x18\r\[redacted]clinic TA 608 Gen3\r\n\n\n\ruser:

Ports

23 2000

Services

23
tcp
telnet

[redacted]TA 616 Gen3

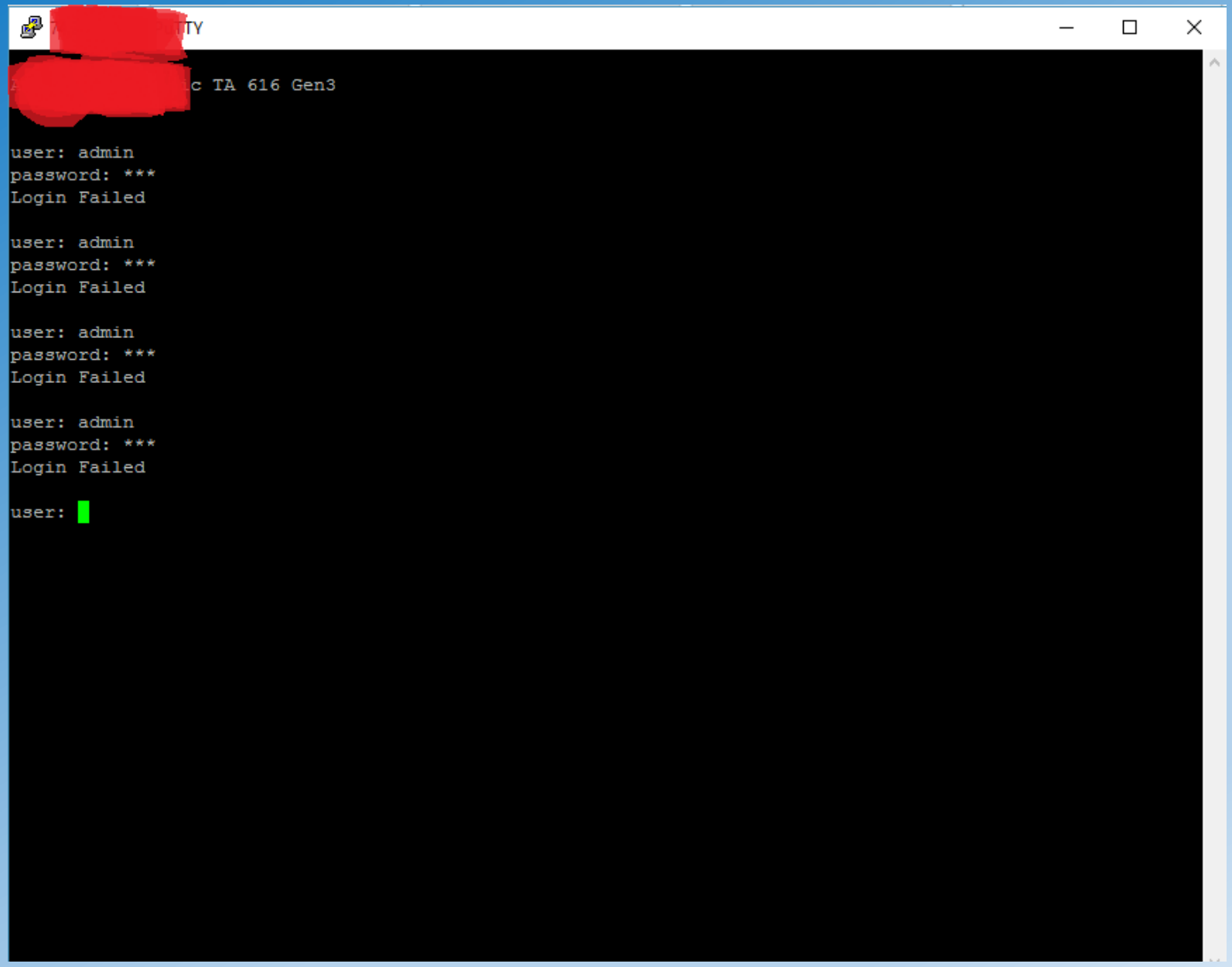
user:

2000
tcp
ikettle

\xff\xfb\x01\xff\xfb\x03\xff\xfd\x18\r\[redacted]A 616 Gen3\r\n\n\n\ruser:

Now…. This is interesting

- Http://www.makeuseof.com/tag/ikettle-hack-worry-even-dont-one/



COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT

Total Access 616, T1 TDM (3rd Gen)

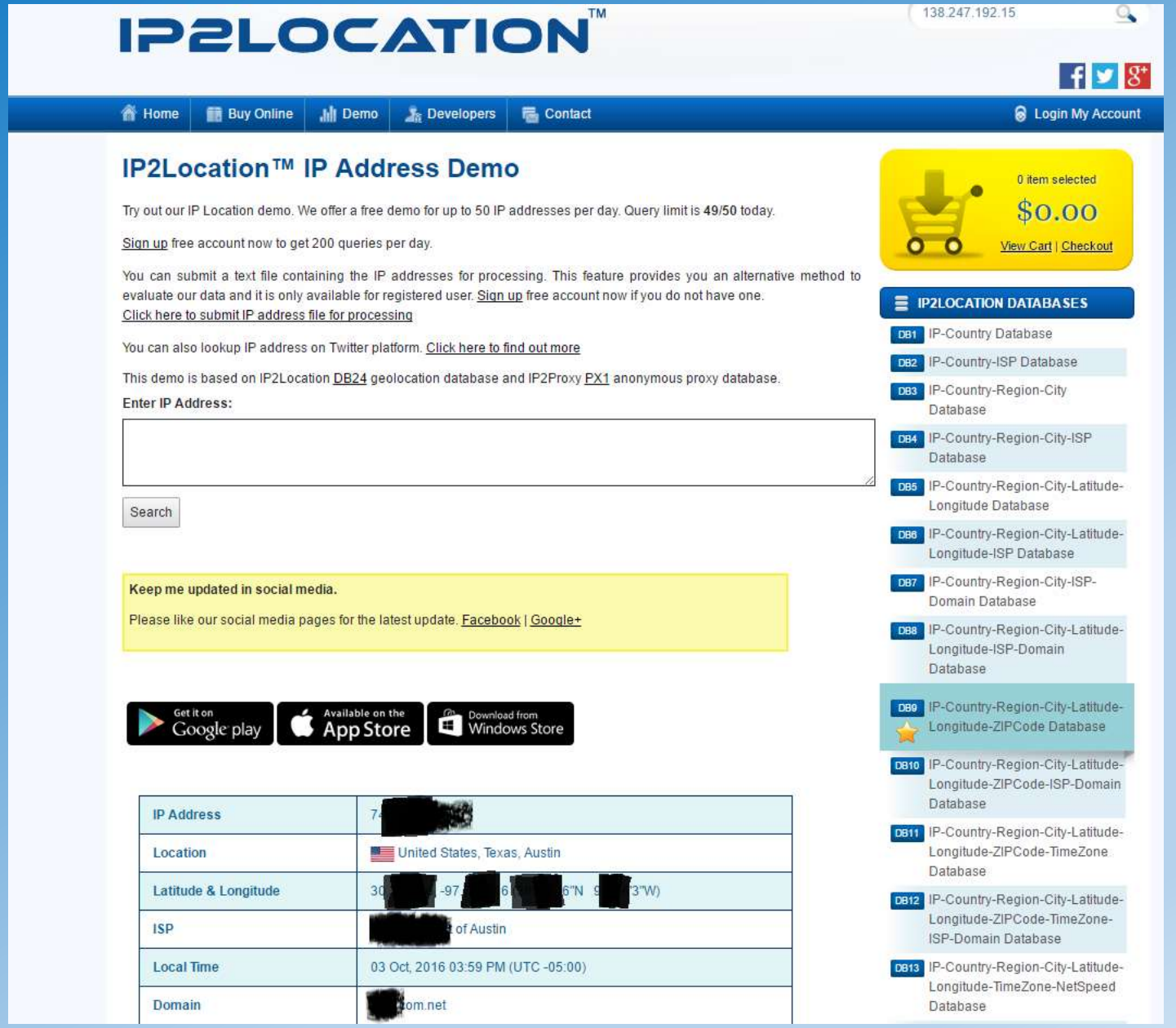
Related

Integrated Ac

Part Number: 4203616L1#TDM

The Total Access 616 (T1 TDM) is a fixed-port Integrated Access Device (IAD) providing a single T1 network interface, 16 analog FXS interfaces, V.35 serial port and 10/100Base-T IP router.

- Pre-configured with TDM software
- Intuitive menu-driven configuration
- Integral IP router supports DHCP, NAT/PAT, packet filtering, RIP V1/V2, Layer 2 PPP, and Frame Relay
- 50-pin female Amphenol connector for Carrier Class analog POTS (FXS) interfaces
- Migration path to packet-based technologies such as ATM and IP (MGCP-only) with software download
- Industry-leading 5-year North American warranty



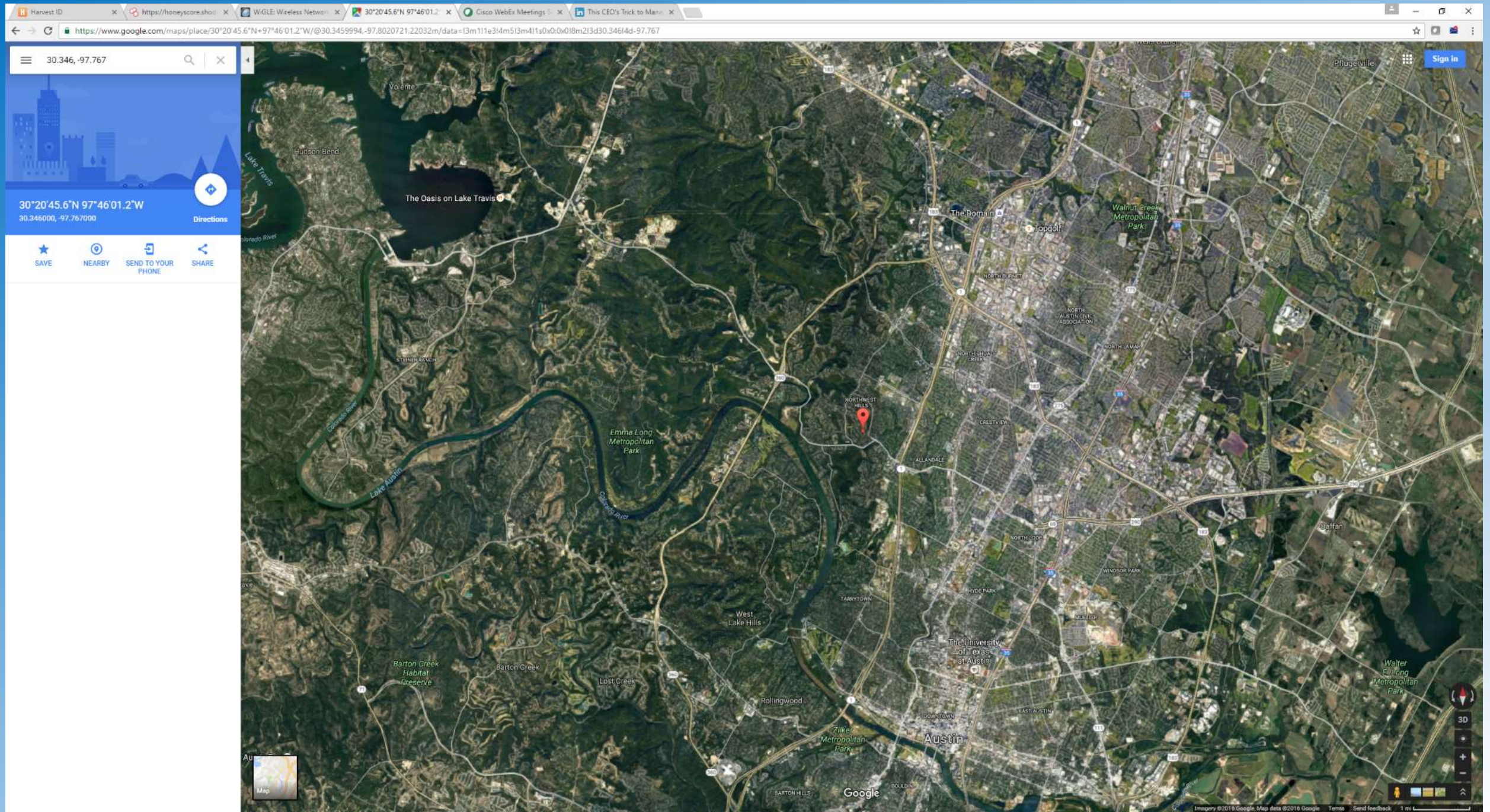
COMPASS Practice Transformation Network

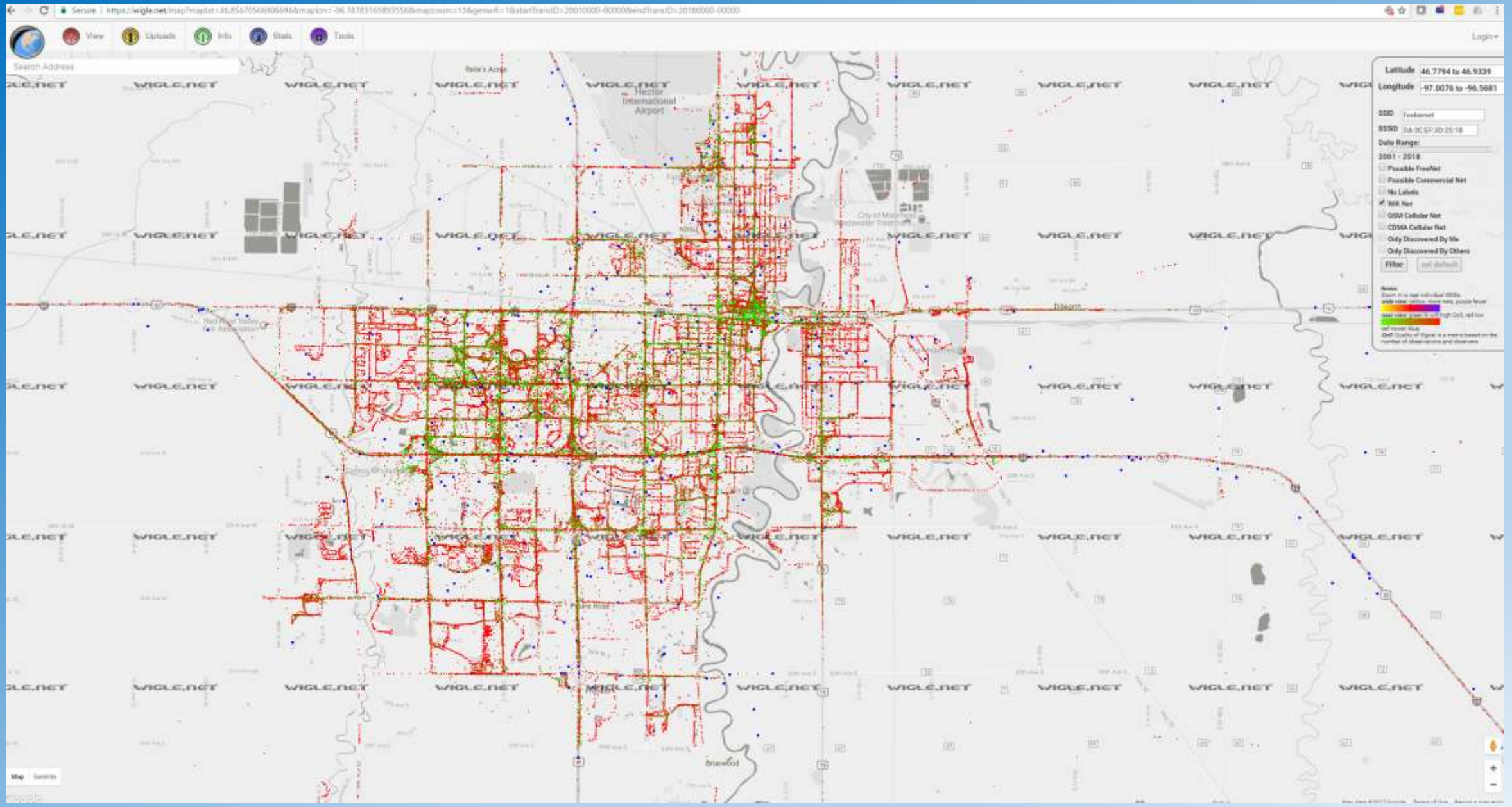
healthPOINT at Dakota State University

DSU DAKOTA STATE

healthPOINT at Dakota State University SECURITY services

CAHIT


Harvest ID
https://honeyscore.shod
WiGLE: Wireless Networ
30°20'45.6"N 97°46'01.2
Cisco WebEx Meetings
This CEO's Trick to Manu
https://www.google.com/maps/place/30°20'45.6"N+97°46'01.2"W/@30.3459994,-97.8020721,22032m/data=!3m1!1e3!4m5!3m4!1s0x0:0x0!8m2!3d30.346!4d-97.767
30.346, -97.767
30°20'45.6"N 97°46'01.2"W
30.346000, -97.767000
Directions
SAVE
NEARBY
SEND TO YOUR PHONE
SHARE
Sign in
Volente
Hudson Bend
Lake Travis
The Oasis on Lake Travis
Pflugerville
The Domain
Topgolf
Walnut Creek Metropolitan Park
NORTH AUSTIN CIVIC ASSOCIATION
NORTH LAMAR
NORTH LOOP
WINDSOR PARK
HYDE PARK
TARRYTOWN
STEINER RANCH
NORTHWEST HILLS
CRESTVIEW
ALLANDALE
Colorado River
Lake Austin
Emma Long Metropolitan Park
Clarksville
West Lake Hills
Barton Creek Habitat Preserve
Barton Creek
Lost Creek
Rollingwood
Zilker Metropolitan Park
The University of Texas at Austin
Austin
DOWNTOWN
EAST AUSTIN
Walter E. Long Metropolitan Park
BARTON HILLS
Google
Map
3D



COMPASS Practice Transformation Network

healthPOINT at Dakota State University

DSU DAKOTA STATE

healthPOINT at Dakota State University SECURITY services

CAHIT

COMPASS
Practice Transformation Network

healthPOINT
at Dakota State University

DSU
DAKOTA STATE

healthPOINT
at Dakota State University
SECURITY services

CAHIT

General IoT Bad News

- Bad news: A hacker has released source code for malware that can be used to automatically find and hack internet of things devices that use default accounts and passwords, then use them to launch distributed denial-of-service attacks.
- DDoS attacks and related tools have long been sold via cybercrime sites by groups such asLizard Squad, often labeled as stresser/booter services.
- Releasing for free the supposed source code for Mirai malware, which has been tied to massive DDoS attacks launched via hacked IoT devices.
- Dahua Technology (security cameras)

TOP THREE FINDINGS

- VPNs Implemented incorrectly
  - Usually PSK and Aggressive Mode enabled
- Ports open to the world that don't need to be open
- Bad Password Hygiene
  - Too Short
  - Too Common
- Reuse on multiple applications

Most Common Passwords of 2015

RANK	PASSWORD	CHANGE FROM 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	1 ↗
4	qwerty	1 ↗
5	12345	2 ↘
6	123456789	Unchanged
7	football	3 ↗
8	1234	1 ↘
9	1234567	2 ↗
10	baseball	2 ↘
11	welcome	NEW
12	1234567890	NEW
13	abc123	1 ↗
14	111111	1 ↗
15	1qaz2wsx	NEW
16	dragon	7 ↘
17	master	2 ↗
18	monkey	6 ↘
19	letmein	6 ↘
20	login	NEW
21	princess	NEW
22	qwertyuiop	NEW
23	solo	NEW
24	password	NEW
25	starwars	NEW

Splashdata annual poll

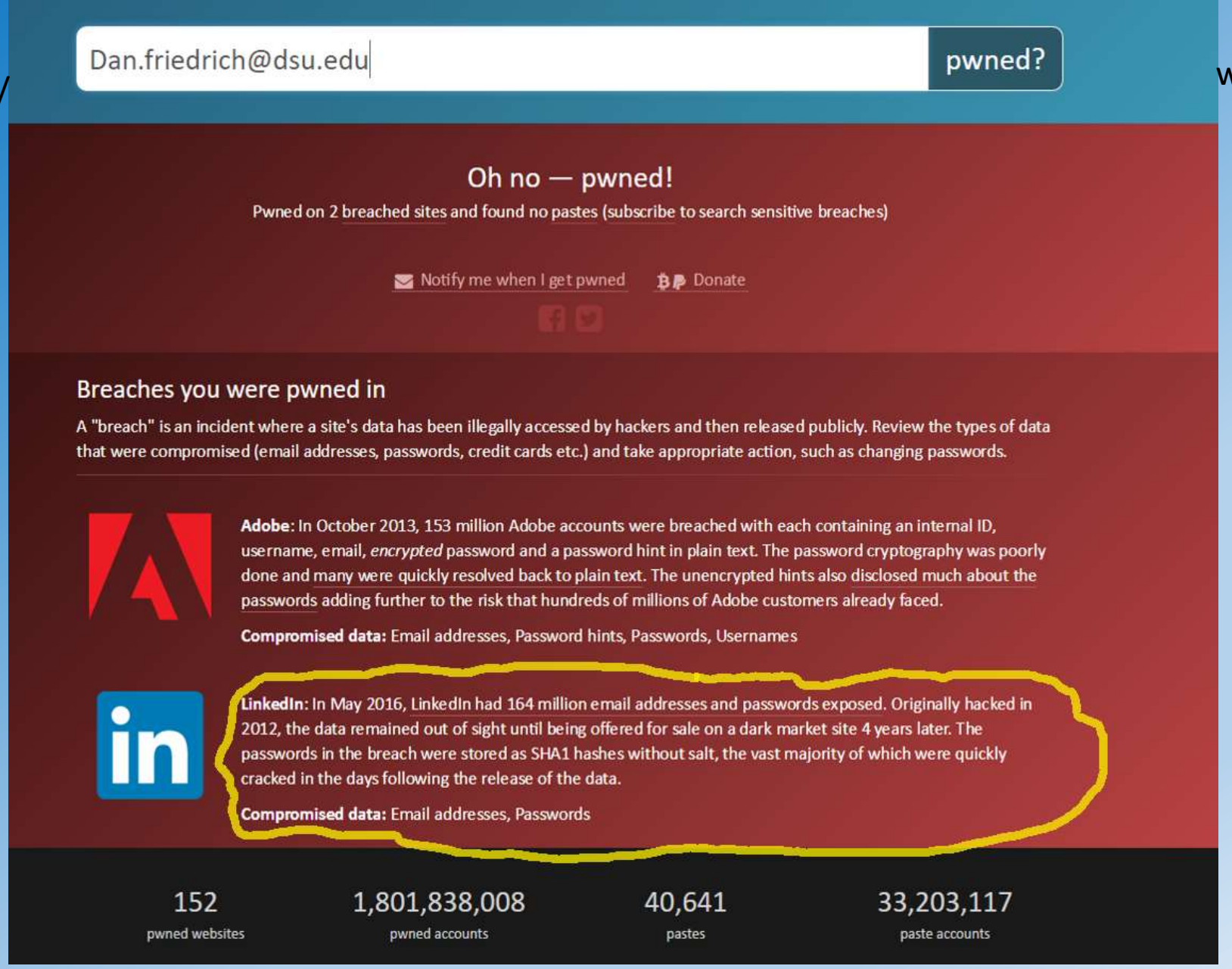
COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT

Password Reuse across multiple sites

- 50-59% reuse passwords across sites
- 61% more likely to share work passwords than personal passwords
- Most commonly shared passwords
  - Wi-fi 58%
  - Streaming 48%
  - Financial 43%
  - Email and communication 39%
  - Work 25%

haveibeenpwned.com/

www.leakedsource.com/



COMPASS Practice Transformation Network

healthPOINT at Dakota State University

DSU DAKOTA STATE

healthPOINT at Dakota State University SECURITY services

CAHIT

Linkedin
Badoo
Dropbox
Myspace
Imesh
Adobe
Tumblr

Email | Search

Username | Search

IP Address | Search

Myspace

Id	Email	Password	Password2
13361098	[redacted]	0x58DAF22A2B4B315F34390986C2C27E6A0FCDB5B8	"
20370666	[redacted]	0x5022D144CC0302E85DF1205802530AED25D537BE	"
296755359	[redacted]	0xE86EC3CEC059BC9B076859BE3F0E25A3B1F1AB6D	"
303157854	[redacted]	0xD9DEFA6EAE9AF64FC30F6F30A6C953FF690F4F2F	"
78919797	[redacted]	0xDCAD095CFC478036BA18945C8AA3DBC0E6617ABE	"

Adobe

Id	Email	Password	Hint
29942550	[redacted]	nK1toeqDal+/pprHjZdKAg==	
41232593	[redacted]	I7A/VHBaOU8=	
90691363	[redacted]	UYKTn2AAPCI=	MD

linkedin

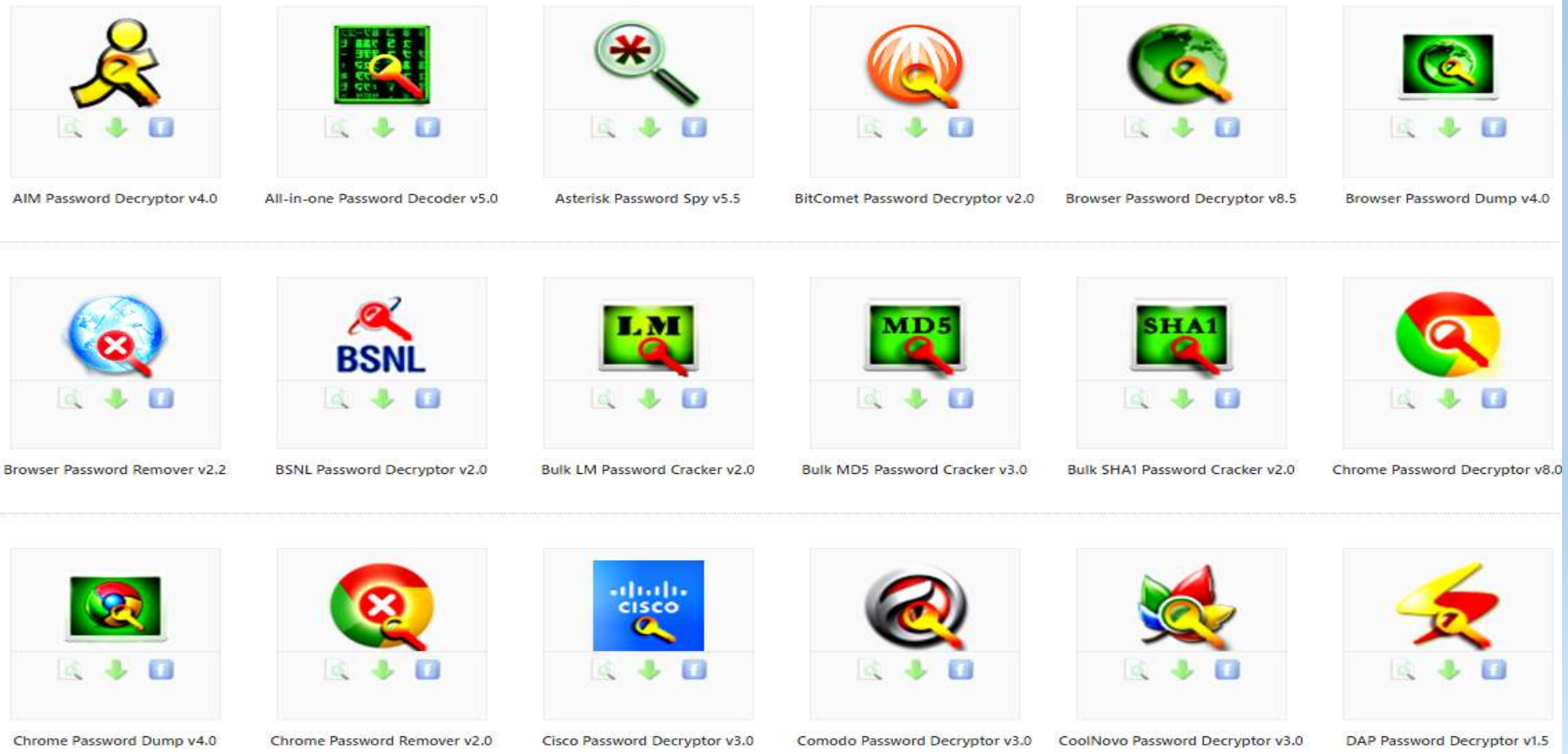
Id	Email	Password
33094717	[redacted]	1d40d154ec4b308c7cf773057bc97ef588f81891
41277871	[redacted]	ff1d3b70603a4dc2b03c5d158c0c95312488461c
70727250	[redacted]	3eb5378468c8b0ec96278ce8291720baa6f834e
70818629	[redacted]	xxx
82445473	[redacted]	d8a62834e1193a6a381b154badd61f79b6269e1a

Dropbox

Id	Email	Password	Hash Type
33201739	[redacted]	ee91d440cf0bcc97428cd8e147f418591e25294b	sha1
52452008	[redacted]	c5dbec988aee77465c4e3acf66e488c0d3a343a46	sha1

securityxploded.com/

Free Password Recovery Tools



COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT

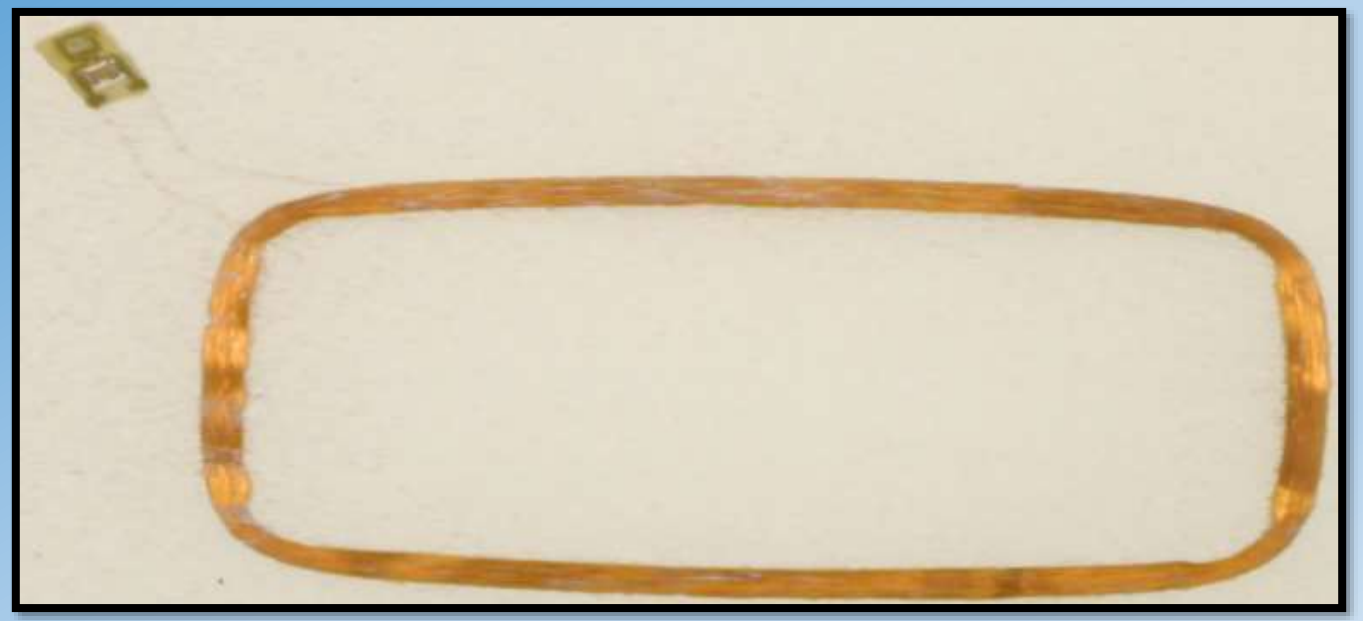
RFID Hacking

Tastic RDIF Thief

COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT

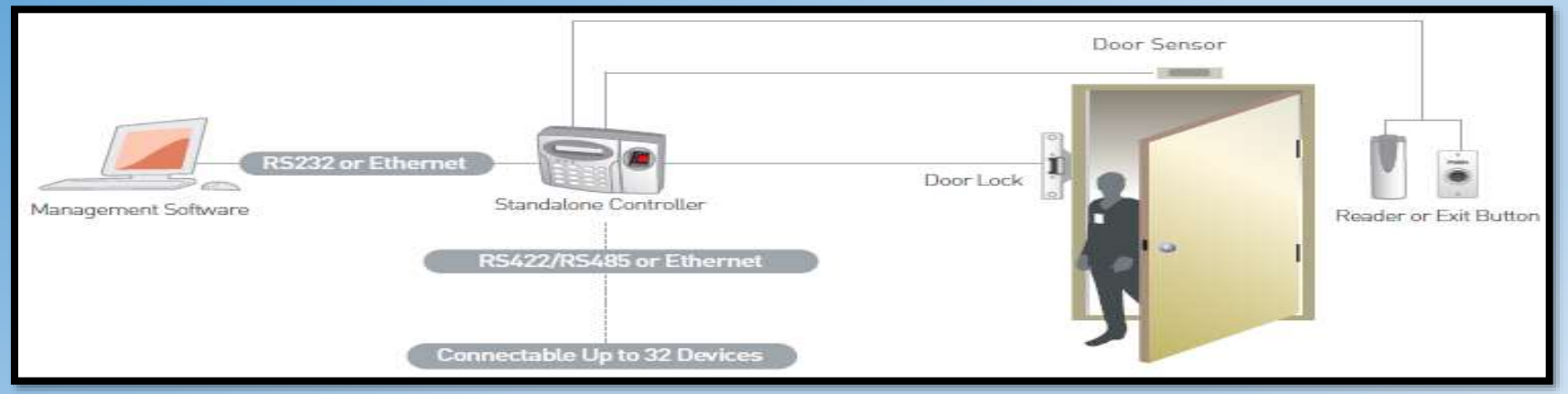
How Proximity cards Work

- Proximity reader transmits low-level radio frequency(RF)
  - A small coil in the proximity card absorbs the radio frequency which is used to power the card
- Once the card is powered it will transmit the code to the reader.



How Proximity cards Work

- The reader will converts the card data to wiegand protocol
  - HID
  - Indala
- The reader passes the card data to the controller
  - Access Granted
  - Access Denied



Frequency

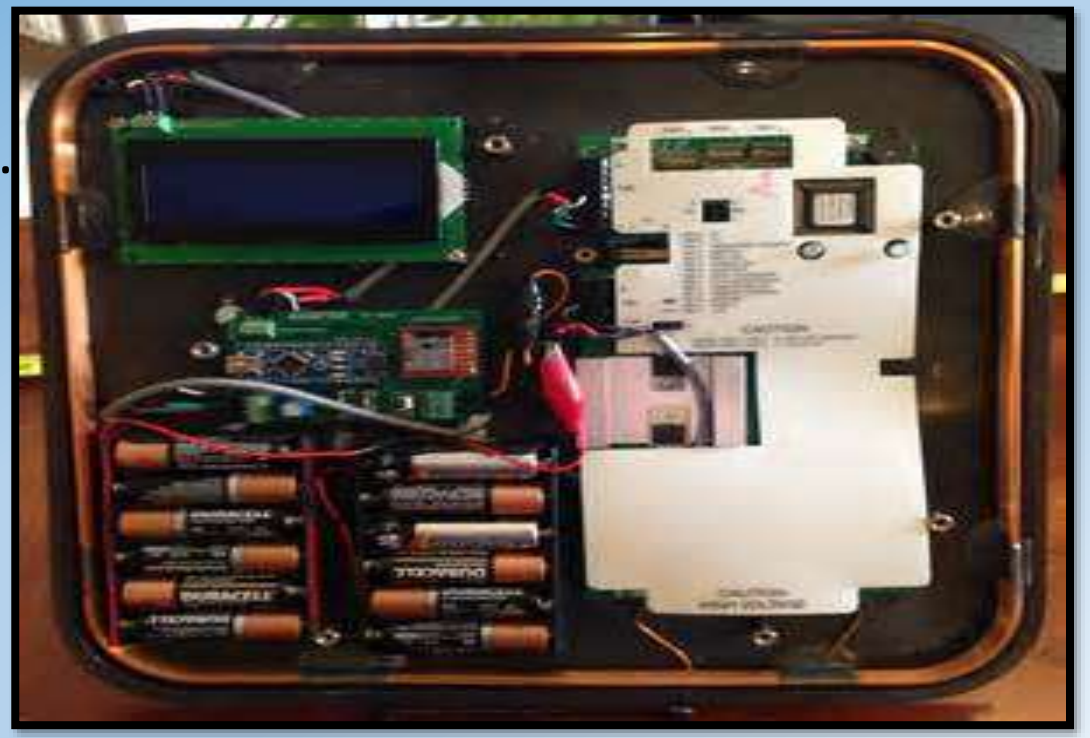
- Low Frequency (LF)
  - 120kHz – 140kHz
  - <3ft
  - What we will be hacking
- High Frequency (HF)
  - 13.56MHz
  - 3-10 ft
- Ultra-High Frequency (UHF)
  - 860-960 MHZ
  - 30ft

Products

- Disney world park bands
- Passport
- Animal rfid
- Security badges
- Credit cards
- Hotel key

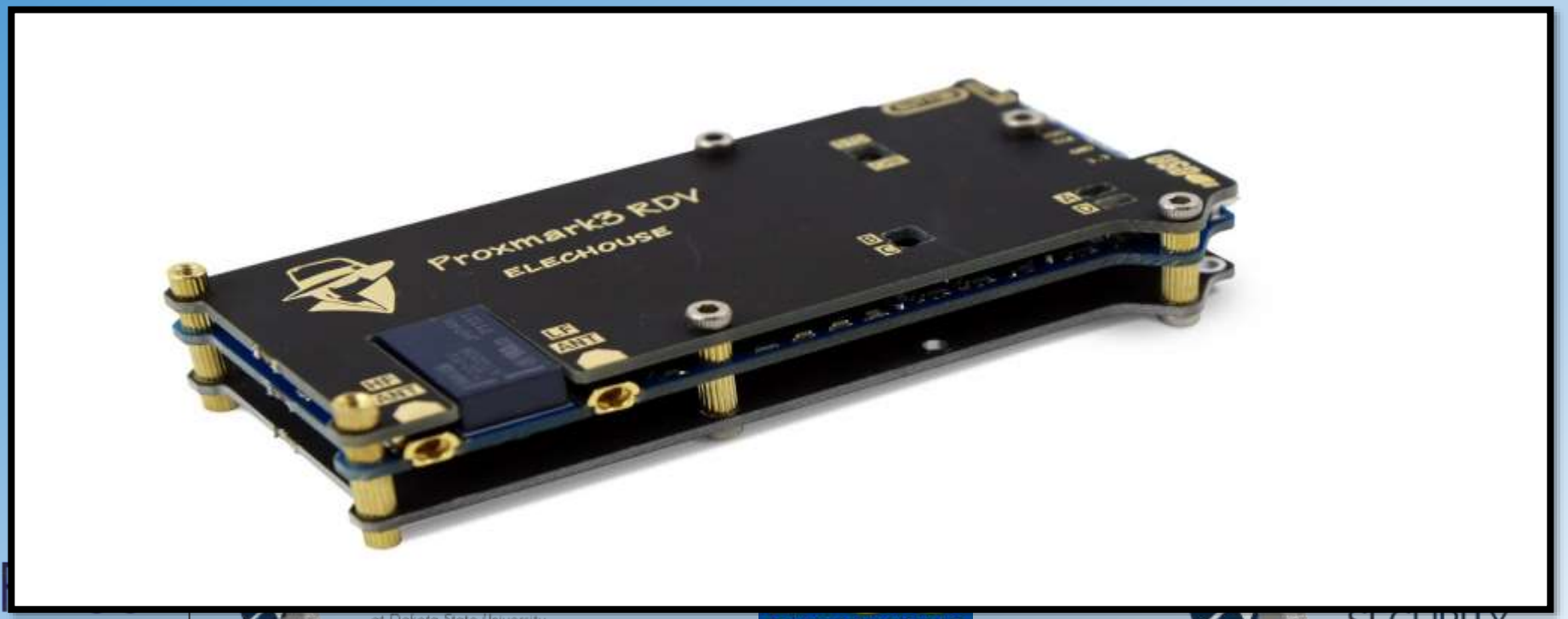
Tastic RFID Thief

- We use a commercial RFID reader and insert an Arduino that acts as the controller and intercepts the proximity cards code.
  - The reader powers the proximity card.
  - The proximity card sends the code to the reader (HID/INDALA).
  - The reader sends the code to the Arduino (Controller).
    - The Arduino records the code.
  - DEMO TIME



Card Cloning

- After we get the proximity cards code we have to clone it.
- Proxmark3
  - Can be used to clone cards



Attack scenario

- Put Tastic RFID Thief in backpack
- Walk to local Starbucks where employees get coffee
- Get within 5 feet of employee
  - Steal badge info
- Go home
  - Clone badge info to new card
- Walk into secure building using cloned card

Defense

- Multi Factor Authentication
  - Something you have
    - Proximity card
  - Something you know
    - Password
  - Something you are
    - Hair, eye, fingerprint

Presentation Links

- haveibeenpwned.com/
- www.leakedsource.com/
- www.shodan.io
- www.wiggle.net
- www.ip2location.com/
- securityxploded.com/
- icitech.org/

Thank You

- Dan.Friedrich@dsu.edu

COMPASS Practice Transformation Network | healthPOINT at Dakota State University | DSU DAKOTA STATE | healthPOINT at Dakota State University SECURITY services | CAHIT