VIRGINIA IT AGENCY

WELCOME TO THE July 13, 2022,

ISOAG MEETING

with

Virginia Cyber Security

Partnership and RVATech

AGENDA	
Welcome	Ed Miller/VITA
Virginia Cyber Security Partnership/RVA Tech	Bob Austin
IT Security in Hybrid World	Randy Marchany/Virginia Tech
MACH37	Mike McCoy
Problems, solutions, use cases and traction	MACH37 CoHort Presentations
From the trenches/call in from Kyiv, Ukraine	Hideez Inc
Upcoming Events	Ed Miller/VITA
Adjourn	

IT Security in the Hybrid World

Randy Marchany

Virginia Tech IT Security Office and Lab

Threats

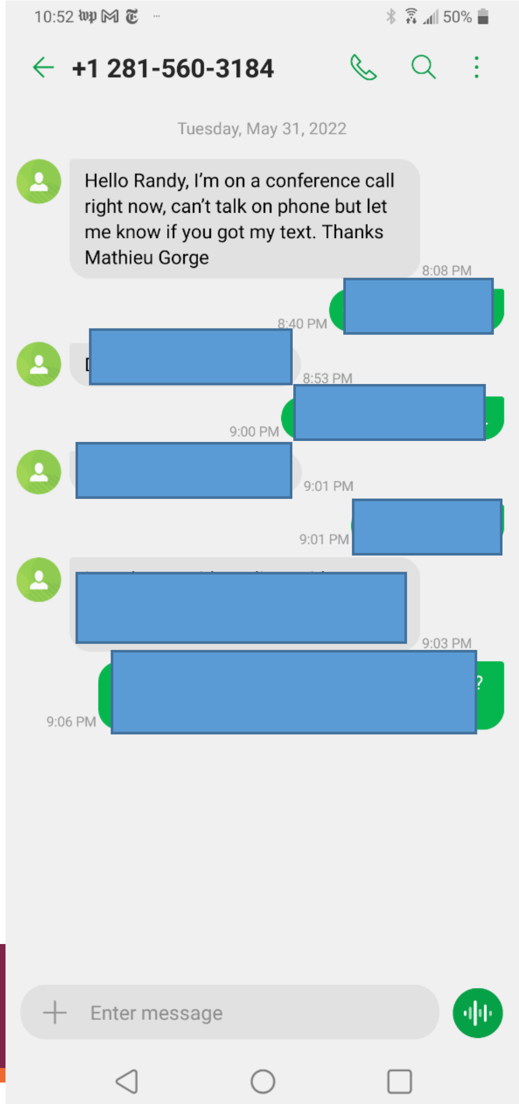
Hacker Attack Goals – over 30 years

Hacker attack goals are 1 or more of the following:

- **DATA theft/disclosure** aka data breaches
- **ATTACK** other sites using hacked assets
- **DESTRUCTION** of company data (deletion or ransomware).

- **DEFEND** accordingly

Anyone is a target…



10:52 50%

+1 281-560-3184

Tuesday, May 31, 2022

Hello Randy, I'm on a conference call right now, can't talk on phone but let me know if you got my text. Thanks Mathieu Gorge

8:08 PM

[redacted]

8:40 PM

[redacted]

8:53 PM

[redacted]

9:00 PM

[redacted]

9:01 PM

[redacted]

9:01 PM

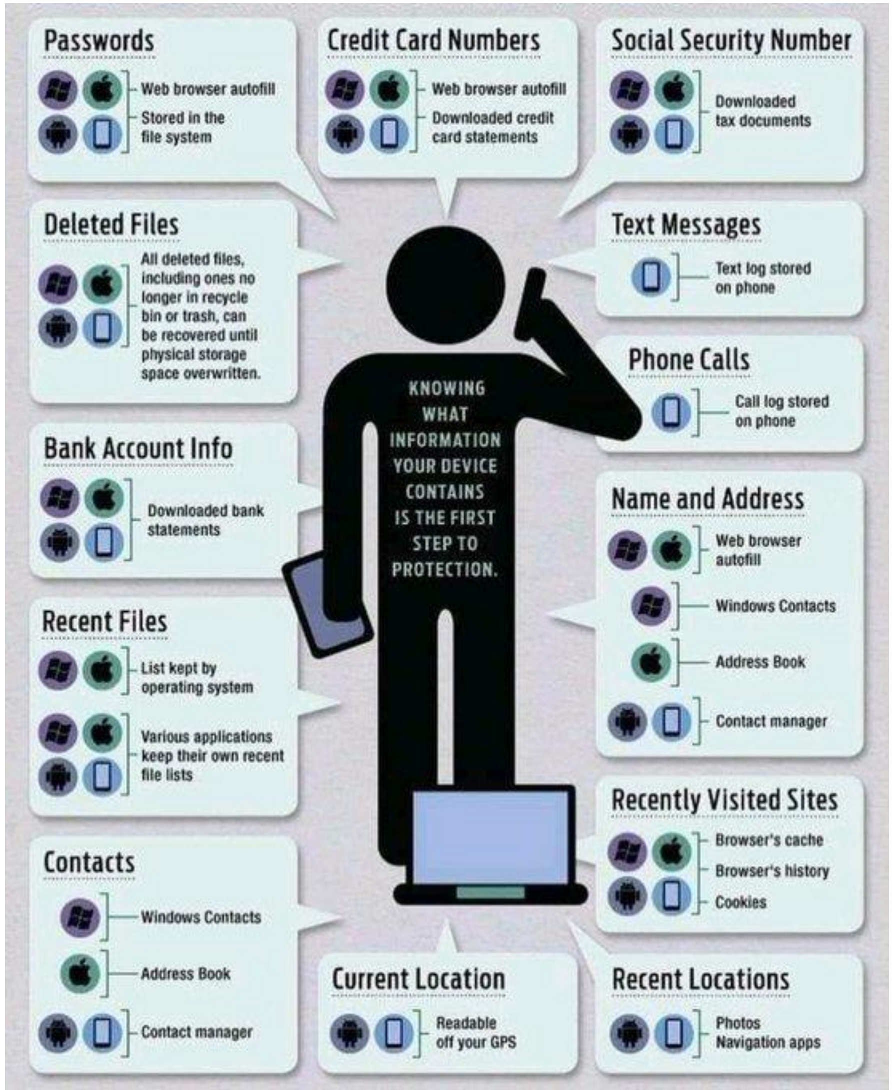
[redacted]

9:03 PM

[redacted]

9:06 PM

- Mathieu Gorge is the CEO, this isn't his phone #
- Tuesday, I got this text
- Reverse lookup of phone #
- Got an address, went to Google Maps



Passwords
- Web browser autofill
- Stored in the file system

Credit Card Numbers
- Web browser autofill
- Downloaded credit card statements

Social Security Number
- Downloaded tax documents

Deleted Files
- All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Text Messages
- Text log stored on phone

Phone Calls
- Call log stored on phone

KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.

Bank Account Info
- Downloaded bank statements

Name and Address
- Web browser autofill
- Windows Contacts
- Address Book
- Contact manager

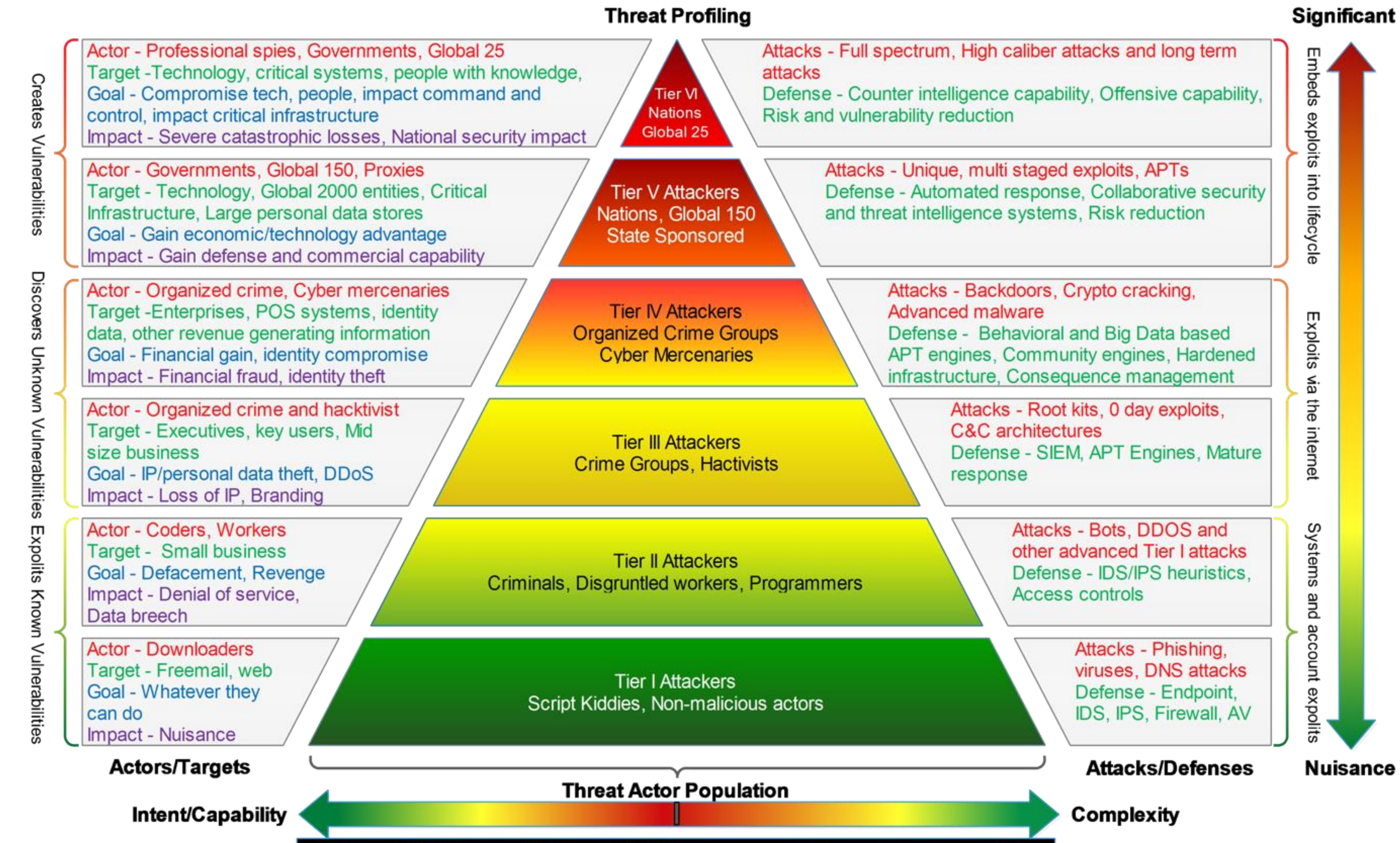
Recent Files
- List kept by operating system
- Various applications keep their own recent file lists

Recently Visited Sites
- Browser's cache
- Browser's history
- Cookies

Contacts
- Windows Contacts
- Address Book
- Contact manager

Current Location
- Readable off your GPS

Recent Locations
- Photos
- Navigation apps



Threat Profiling

Significant

Creates Vulnerabilities

Discovers Unknown Vulnerabilities

Exploits Known Vulnerabilities

Actor - Professional spies, Governments, Global 25
Target -Technology, critical systems, people with knowledge,
Goal - Compromise tech, people, impact command and control, impact critical infrastructure
Impact - Severe catastrophic losses, National security impact

Tier VI
Nations
Global 25

Attacks - Full spectrum, High caliber attacks and long term attacks
Defense - Counter intelligence capability, Offensive capability, Risk and vulnerability reduction

Actor - Governments, Global 150, Proxies
Target - Technology, Global 2000 entities, Critical Infrastructure, Large personal data stores
Goal - Gain economic/technology advantage
Impact - Gain defense and commercial capability

Tier V Attackers
Nations, Global 150
State Sponsored

Attacks - Unique, multi staged exploits, APTs
Defense - Automated response, Collaborative security and threat intelligence systems, Risk reduction

Actor - Organized crime, Cyber mercenaries
Target -Enterprises, POS systems, identity data, other revenue generating information
Goal - Financial gain, identity compromise
Impact - Financial fraud, identity theft

Tier IV Attackers
Organized Crime Groups
Cyber Mercenaries

Attacks - Backdoors, Crypto cracking, Advanced malware
Defense - Behavioral and Big Data based APT engines, Community engines, Hardened infrastructure, Consequence management

Actor - Organized crime and hacktivist
Target - Executives, key users, Mid size business
Goal - IP/personal data theft, DDoS
Impact - Loss of IP, Branding

Tier III Attackers
Crime Groups, Hactivists

Attacks - Root kits, 0 day exploits, C&C architectures
Defense - SIEM, APT Engines, Mature response

Actor - Coders, Workers
Target - Small business
Goal - Defacement, Revenge
Impact - Denial of service, Data breech

Tier II Attackers
Criminals, Disgruntled workers, Programmers

Attacks - Bots, DDOS and other advanced Tier I attacks
Defense - IDS/IPS heuristics, Access controls

Actor - Downloaders
Target - Freemail, web
Goal - Whatever they can do
Impact - Nuisance

Tier I Attackers
Script Kiddies, Non-malicious actors

Attacks - Phishing, viruses, DNS attacks
Defense - Endpoint, IDS, IPS, Firewall, AV

Embeds exploits into lifecycle

Exploits via the internet

Systems and account expoilts

Actors/Targets

Attacks/Defenses

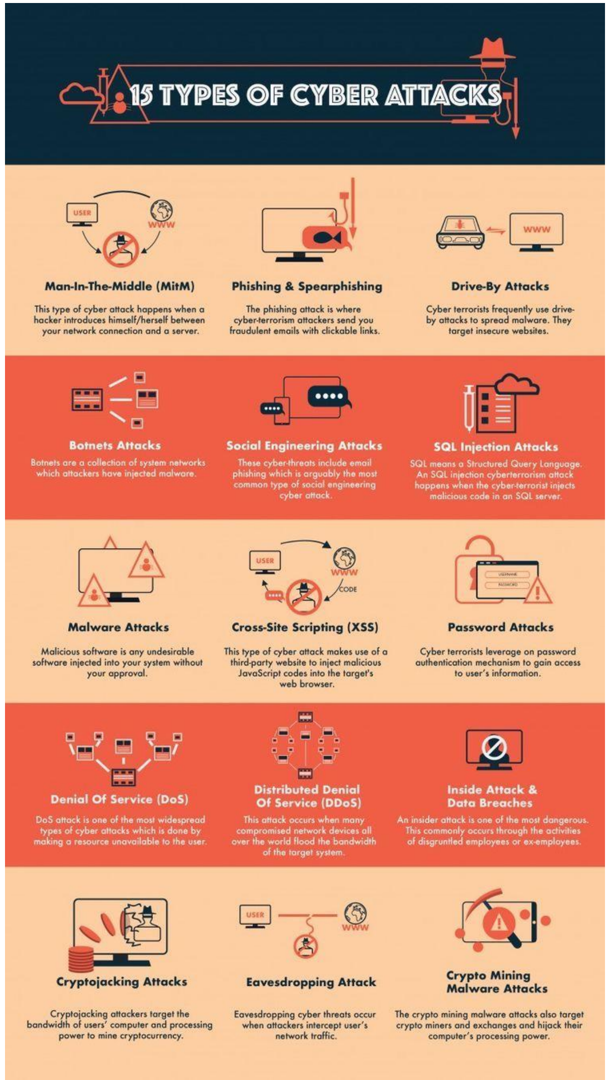
Nuisance

Threat Actor Population

Intent/Capability

Complexity

Commitment	Intensity	Low	Medium	High	Fanatical	Multiple, Scopes	Multiple, Multiple Sources	Multiple, Single Source	One	Components	
	Timing Sensitivity	Days	Weeks	Months	Years						
	Stealthiness	Noisy			Undetectable						
Capability	Personnel	Ones	Tens	Tens of Tens	Hundreds	High	Medium	Low	Low	Funding (Impact)	Multipliers
	Knowledge	Limited	General	Specialized	Multi Scope	High	Medium	Low	NA	Assets	
	Access	None	Through Others	Indirect	Direct	Low	Medium	Low	NA	Technology	



15 TYPES OF CYBER ATTACKS

Man-In-The-Middle (MitM)

This type of cyber attack happens when a hacker introduces himself/herself between your network connection and a server.

Phishing & Spearphishing

The phishing attack is where cyber-terrorism attackers send you fraudulent emails with clickable links.

Drive-By Attacks

Cyber terrorists frequently use drive-by attacks to spread malware. They target insecure websites.

Botnets Attacks

Botnets are a collection of system networks which attackers have injected malware.

Social Engineering Attacks

These cyber-threats include email phishing which is arguably the most common type of social engineering cyber attack.

SQL Injection Attacks

SQL means a Structured Query Language. An SQL injection cyberterrorism attack happens when the cyber-terrorist injects malicious code in an SQL server.

Malware Attacks

Malicious software is any undesirable software injected into your system without your approval.

Cross-Site Scripting (XSS)

This type of cyber attack makes use of a third-party website to inject malicious JavaScript codes into the target's web browser.

Password Attacks

Cyber terrorists leverage on password authentication mechanism to gain access to user's information.

Denial Of Service (DoS)

DoS attack is one of the most widespread types of cyber attacks which is done by making a resource unavailable to the user.

Distributed Denial Of Service (DDoS)

This attack occurs when many compromised network devices all over the world flood the bandwidth of the target system.

Inside Attack & Data Breaches

An insider attack is one of the most dangerous. This commonly occurs through the activities of disgruntled employees or ex-employees.

Cryptojacking Attacks

Cryptojacking attackers target the bandwidth of users' computer and processing power to mine cryptocurrency.

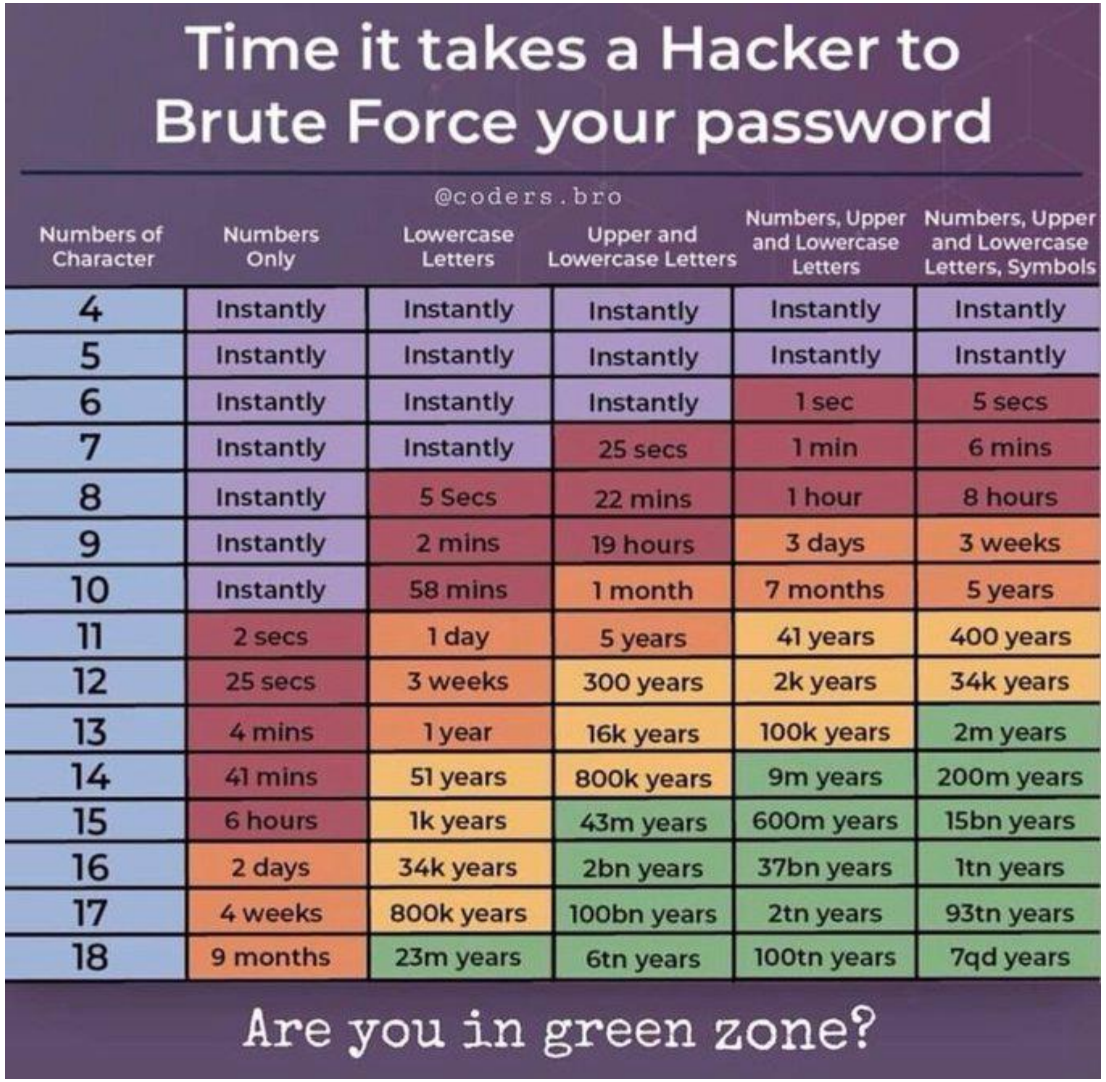
Eavesdropping Attack

Eavesdropping cyber threats occur when attackers intercept user's network traffic.

Crypto Mining Malware Attacks

The crypto mining malware attacks also target crypto miners and exchanges and hijack their computer's processing power.

USER
WWW
CODE
USERNAME
PASSWORD



Time it takes a Hacker to Brute Force your password

@coders.bro

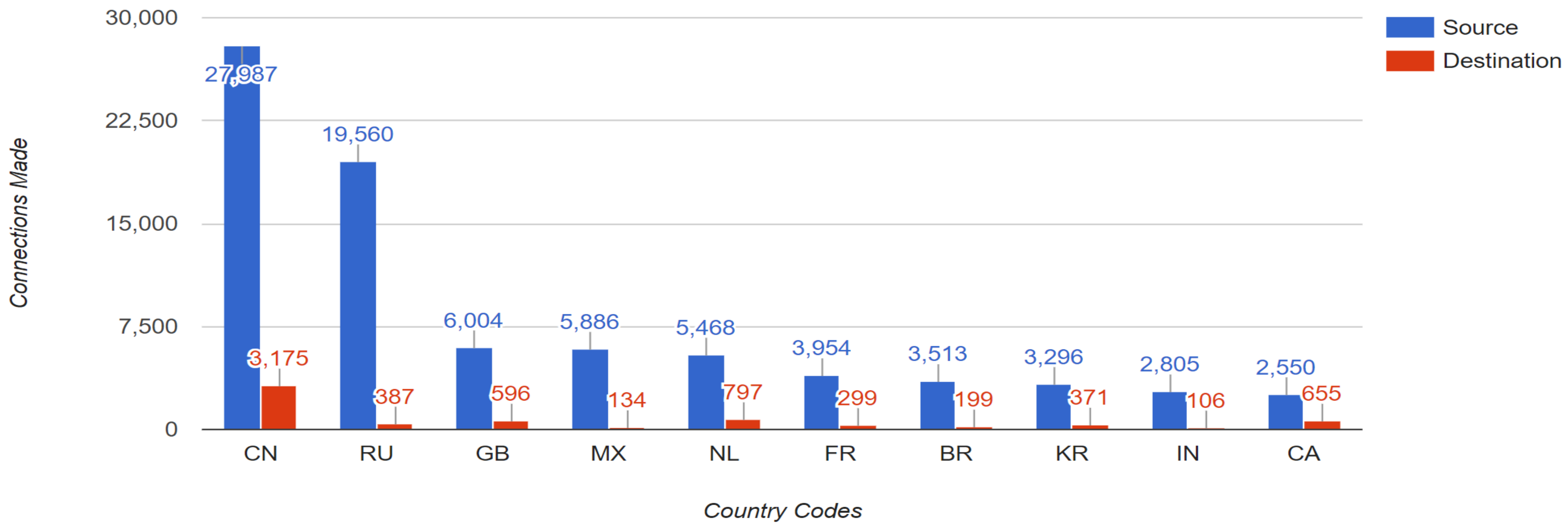
Numbers of Character	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 Secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Are you in green zone?

Sample In/Out Traffic Profile

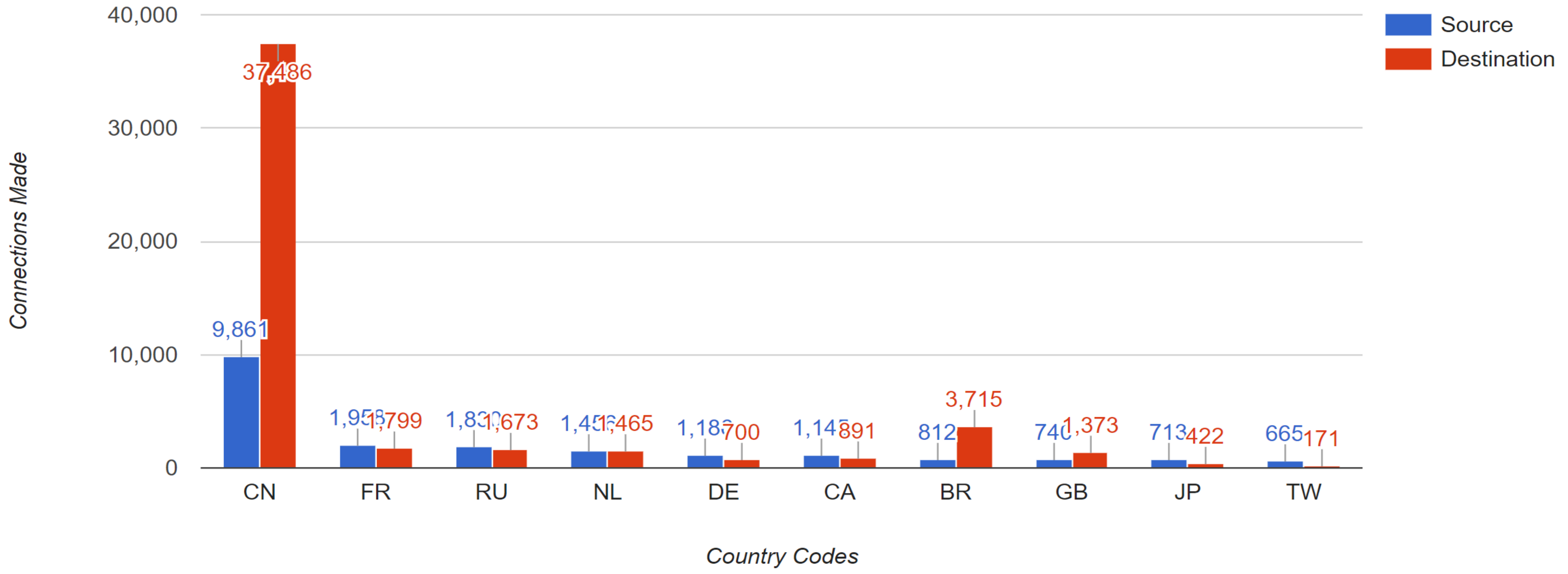
Top Source & Destination Countries - By Connection

Aug 01, 2017 to Aug 31, 2017 - ITSO Argus Data

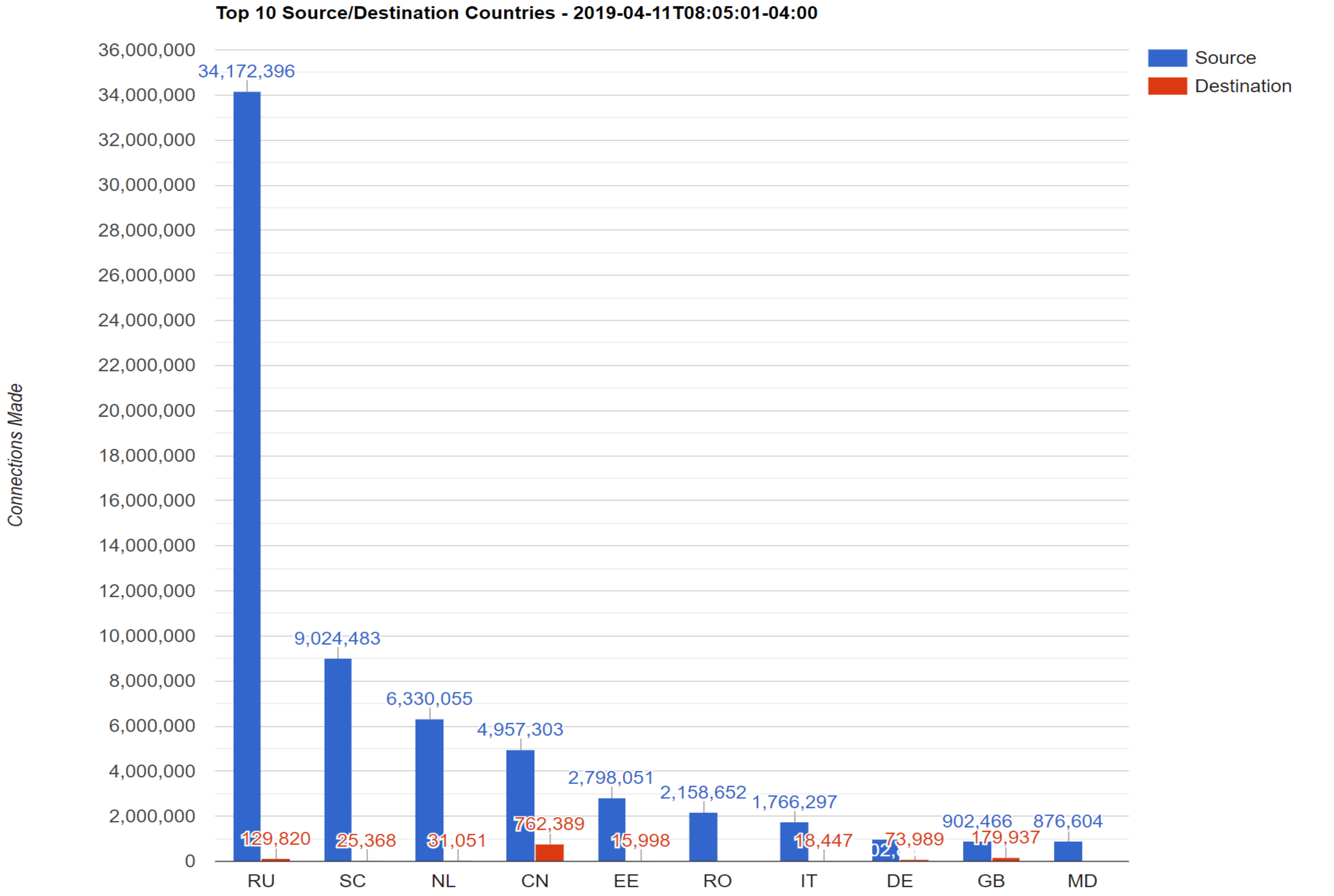


Country Code	Country Name	Source Count	Destination Count
US	United States	91396	206186

Nov 01, 2014 to Dec 01, 2014 - ITSO Argus Data



Country Code	Country Name	Source Count	Destination Count
US	United States	136701	104575


Top 10 Source/Destination Countries - 2019-04-11T08:05:01-04:00
Connections Made
36,000,000
34,000,000
32,000,000
30,000,000
28,000,000
26,000,000
24,000,000
22,000,000
20,000,000
18,000,000
16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
🟦 Source
🟥 Destination
34,172,396
129,820
RU
9,024,483
25,368
SC
6,330,055
31,051
NL
4,957,303
762,389
CN
2,798,051
15,998
EE
2,158,652
RO
1,766,297
18,447
IT
02,
73,989
DE
902,466
179,937
GB
876,604
MD

A Brave New World

Different Approach

- Data Protection is key
  - Find, Tag, Encrypt
- Data Flow
  - Where does our data go?
- Logs are crucial
  - Who, What, When, Where, How, Why
- Resilience
  - Can’t prevent ransomware attack
  - Recovery is key

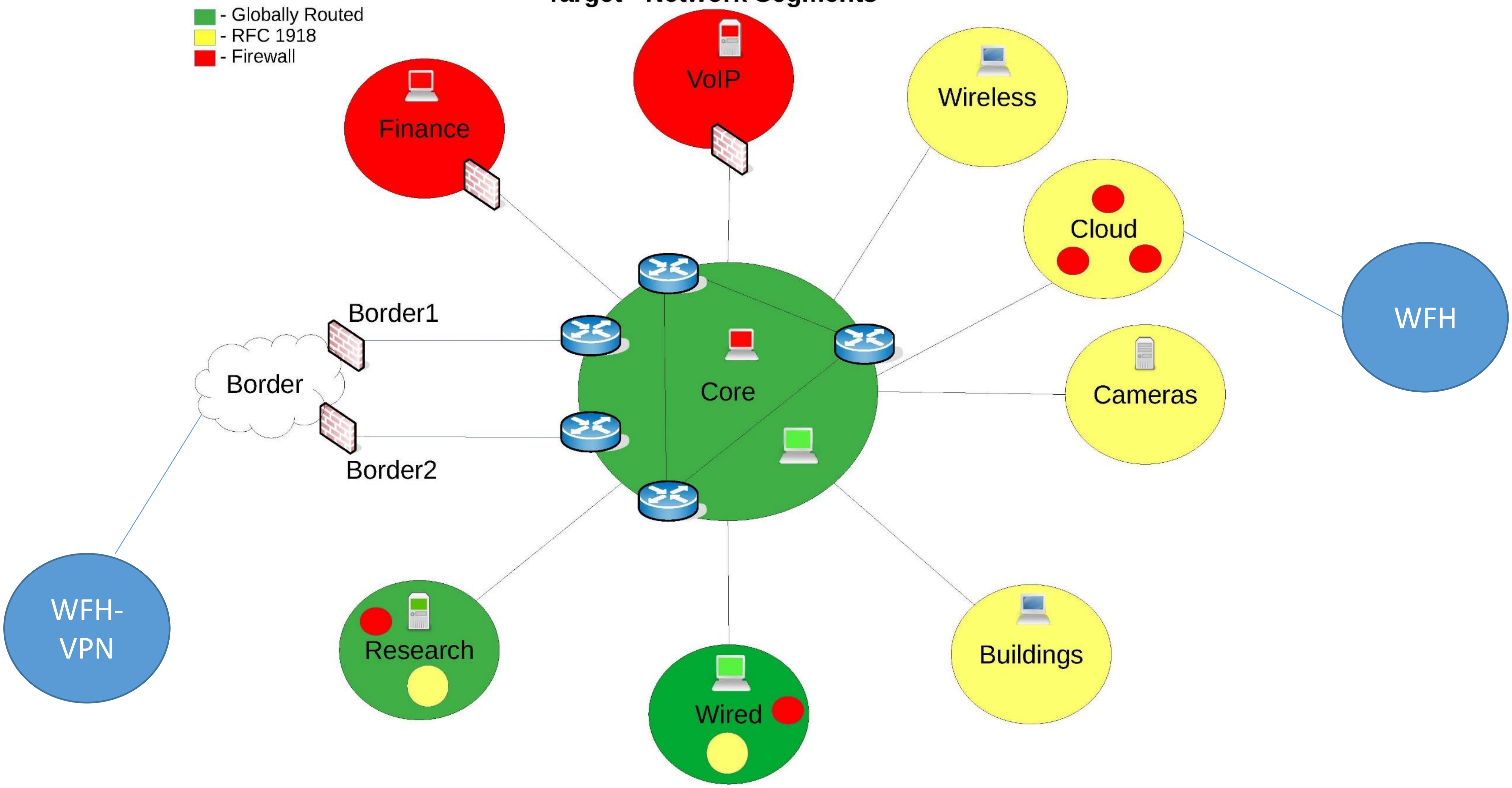
Border? What Border?

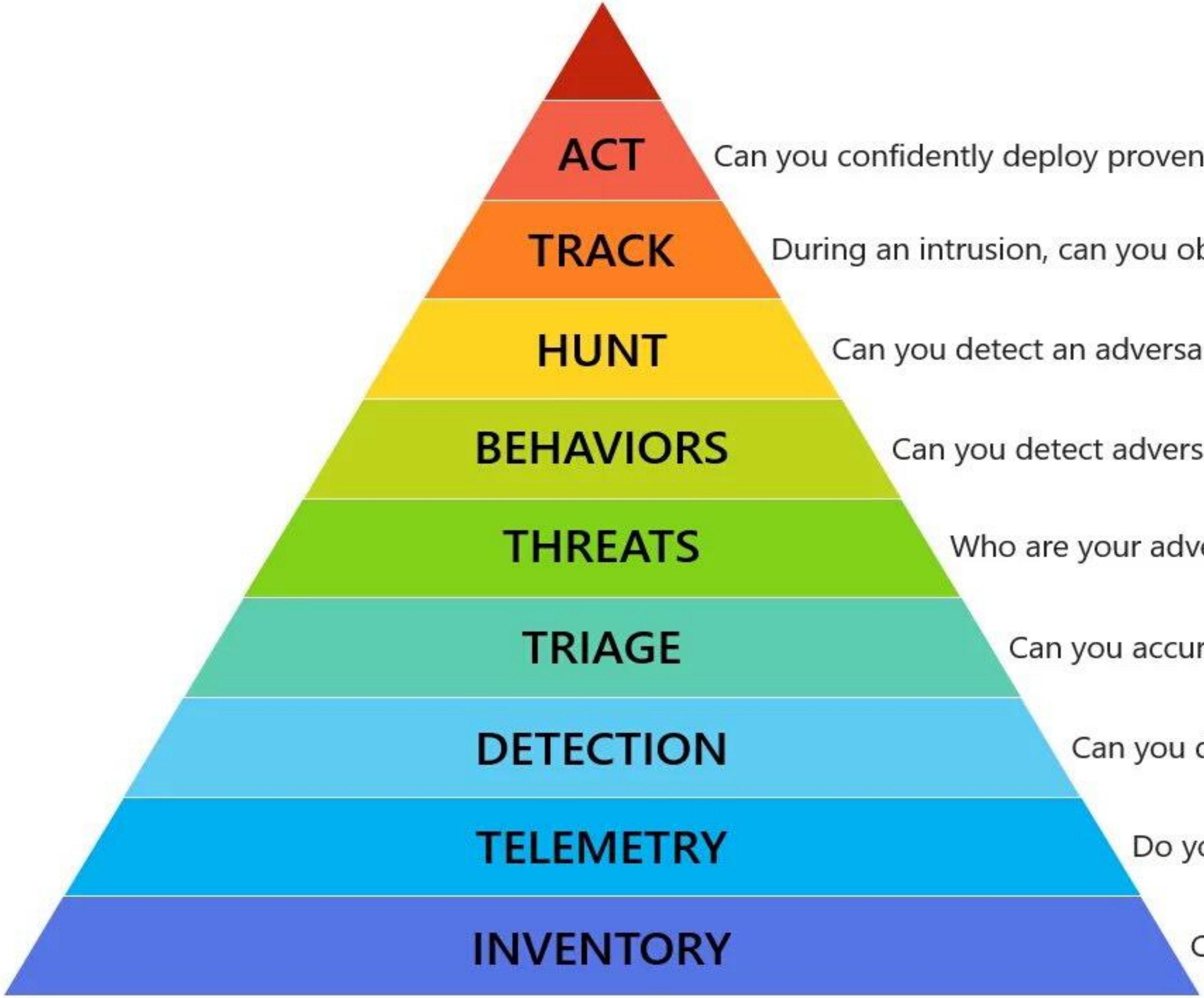
- Internet 1.0 – static servers, endpoints
- Internet 2.0 – static servers, mobile endpoints
- Internet 3.0 – mobile servers (containers, serverless),
  mobile endpoints (laptops, phones,tablets, IoT, ICS)
- Internet 3.5 – Work From Home (WFH)
- **The new border is data, not the device or the network**

Times are a'changing – Gartner Predictions

- **"Through 2023, government regulations requiring organizations to provide consumer privacy rights will cover 5 billion citizens and more than 70% of global GDP.“**
- **"By 2025, 80% of enterprises will adopt a strategy to unify web, cloud services and private application access from a single vendor's SSE platform.“**
- **"Sixty percent of organizations will embrace zero trust as a starting point for security by 2025. More than half will fail to realize the benefits.“**
- **"By 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements.“**
- Source: https://campustechnology.com/articles/2022/06/23/gartners-top-8-cybersecurity-predictions-for-the-coming-year.aspx?s=ct_nu_050722

Target - Network Segments





ACT Can you confidently deploy proven countermeasures to evict and recover?

TRACK During an intrusion, can you observe adversary activity in real-time?

HUNT Can you detect an adversary that is already embedded?

BEHAVIORS Can you detect adversary activity within your environment?

THREATS Who are your adversaries? What are their capabilities?

TRIAGE Can you accurately classify detection results?

DETECTION Can you detect unauthorized activity?

TELEMETRY Do you have visibility across your assets?

INVENTORY Can you name the assets you are defending?

Source: https://holisticinfosec.blogspot.com/2016/12/the-dfir-hierarchy-of-needs-critical.html
Figure source: https://github.com/swannman/ircapabilities

Zero Trust Networks(ZTN) Characteristics*

Vendors usually don’t mention the 1st 3 Pillars

- Pillar 1: The network is always assumed to be **hostile**
- Pillar 2: Assume the hostiles are already **inside your network**
- Pillar 3: Network locality (segmentation) is **not sufficient** for deciding trust in a network
- Pillar 4: **Every** device, user and network flow is authenticated and authorized
- Pillar 5: **Policies** must be dynamic and calculated from as many sources of data as possible

** “Zero Trust Networks: Building Secure Systems in Untrusted Networks”, Evan Gilman, Doug Barth*

What’s Changing?

- Border Monitoring
  - Line Speeds >100Gb, moving to 300-400Gb in 5 years
    - Bad News:Inline IDS/IPS/DLP not practical w/o impacting performance
    - Good News: some vendors are adjusting
- Vulnerability Scanning
  - ISP may interfere thinking it’s an attack and block it
- Incident Response
  - Cutting off net access no longer under your control
- Cloud
  - Email, File sharing, Incident response, high risk data inventory affected

What’s Changing?

- VPN
  - Not necessarily a “security” feature
  - Home system may still be accessed from the net
  - Does force your packets to go thru your net
  - What services require VPN
    - ERP, etc.?
  - What services don’t require VPN
    - Email, Slack, Zoom, Teams?

A New Strategy

Sensitive Data Protection Strategy

- Create data management framework
- Create data classification framework

- Create Sensitive Data Search framework
- Create Sensitive Data Protection framework

- Create Sensitive Data Breach framework

Data Management Framework

- No one gets access to data w/o Data Owner approval
  - Data Owners/Trustee
  - Data Steward
  - Data Expert
- Example: www.policies.vt.edu/7100.pdf

Data Classification Framework

- **HIGH RISK**
  - Protection of the data is required by law/regulation **and**
  - Virginia Tech is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed
  - The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

- Data level determines security level of asset storing the data

- High Risk Data encrypted in Transit and at Rest

Data Search Framework

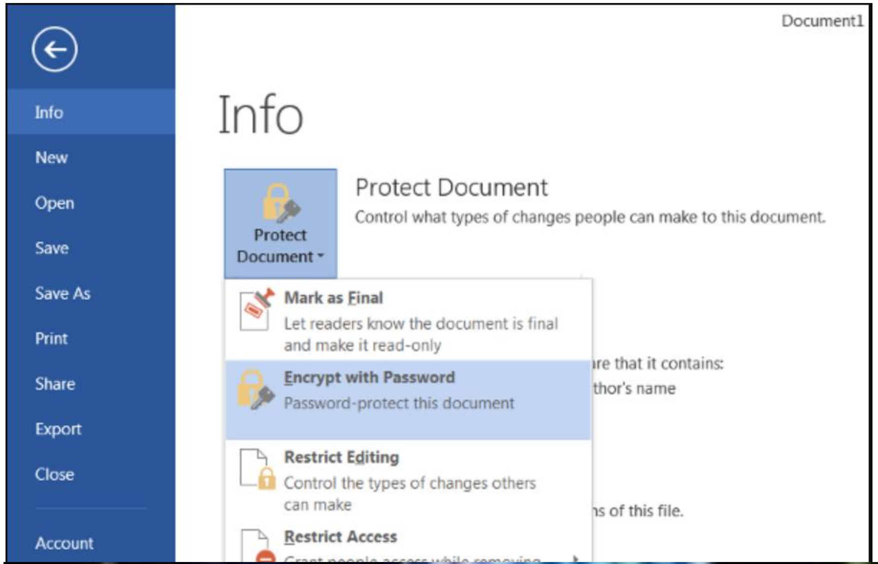
- Before you protect, you must detect

- Commercial or Freeware
- Spirion (former IdentityFinder), Find_SSN (Freeware)

- Run on ALL systems
- Do you need this data for your job
- yes? Encrypt at rest, in transit
- no? Delete the file

Data Protection

- Office Encryption
- PDF Encryption
- Veracrypt

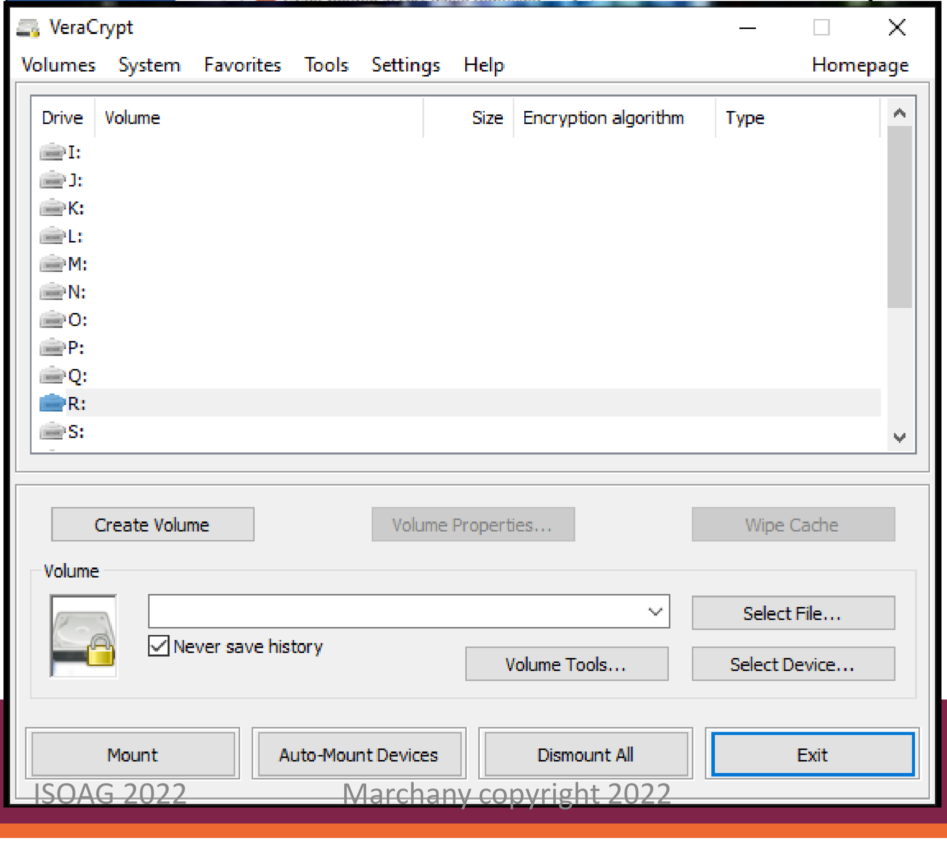


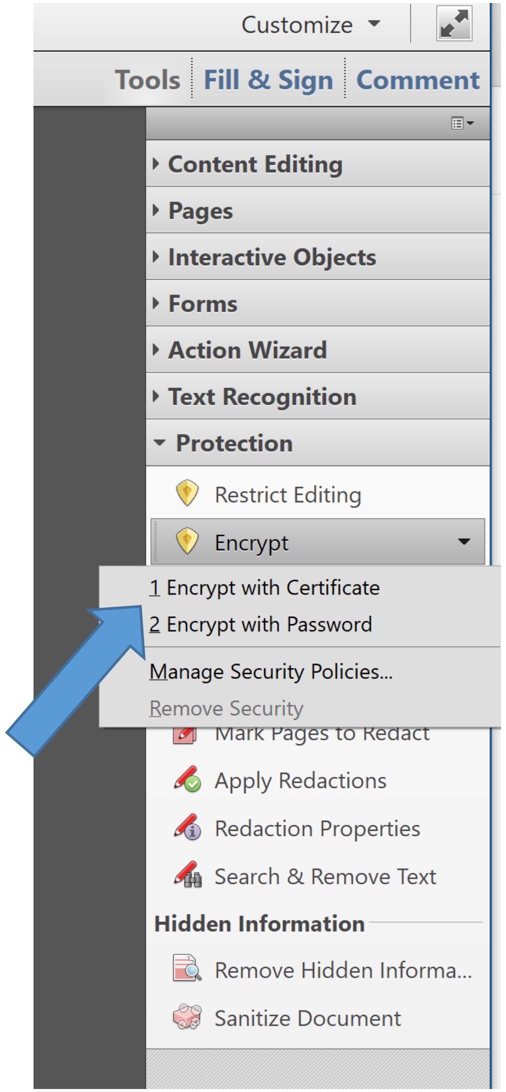
Control what types of changes people can make to this document.

Let readers know the document is final and make it read-only

Password-protect this document

Control the types of changes others can make





Data Breach Framework

- What to do in the event of a data breach
  - what sensitive data was on the target?
  - who attacked the machine, when and how?
  - Was data exfiltrated outside of your net?

- Have notification templates ready
- https://security.vt.edu/content/dam/security_vt_edu/downloads/forms/data_exposure/data_exposure_v1.1.pdf

Net Access isn't Equal

- Some areas have no internet access
- Some areas have poor internet access
  - https://it.vt.edu/resources/home-internet-tips.html
- ISP rate based charge structure

- EDITORIAL COMMENT – My Opinion only (Flame Retardant Suit On)
  - #WFH shows the Net has become a utility.
  - It should be regulated as such.
  - 21st Century version of Rural Electrification Project

Where Does It Go When It Goes Home?

- PROBLEM: Once data is on your home net, you lose data visibility
- Home systems become exfil targets
  - Infostealer class malware looks for PII
  - Attacker dumps from the home system
  - We don’t know if/when/where it went but the home ISP may
- SOLUTIONS (?)
  - TAG your data files (web bug)
  - File phones home instead of computer
  - Lot of work to implement

Your Work Computer Became Your Home Computer

- Hopefully not!
- WFH not new but # of WFH computers has INCREASED
- Will your company tools work outside of your work network?
  - Active Directory?
  - Authentication? 2 factor?
  - Software Licensing?
  - Virtual Private Network (VPN)?

Your Home Computer Became Your Work Computer - 1

- If you use your home computer for work, you must follow your office's security requirements on it.

- **Create a separate userid for work stuff.** Keeps personal separate from work.
  - Browser history, photos, personal sensitive data vs. work sensitive data. Can limit ransomware damage.
- When you're done #WFH, you can delete that account

And Now Some Geek-Speak

- Can your IT scan computers at your house?
  - Probably not. May be blocked by your ISP
- Can you “disconnect” a host from your network?
  - ISP will get abuse complaints not your org.

- What network traffic visibility exists from computers at your house?
  - None probably unless you require VPN.
- What type of logs will you need to collect in this new WFH environment?

Simple Steps to Protect Your Computer

- Password protect your userid, screen lock
- Update your OS & software
- Think before click
- You have a firewall already
- Adjust browser security, privacy settings

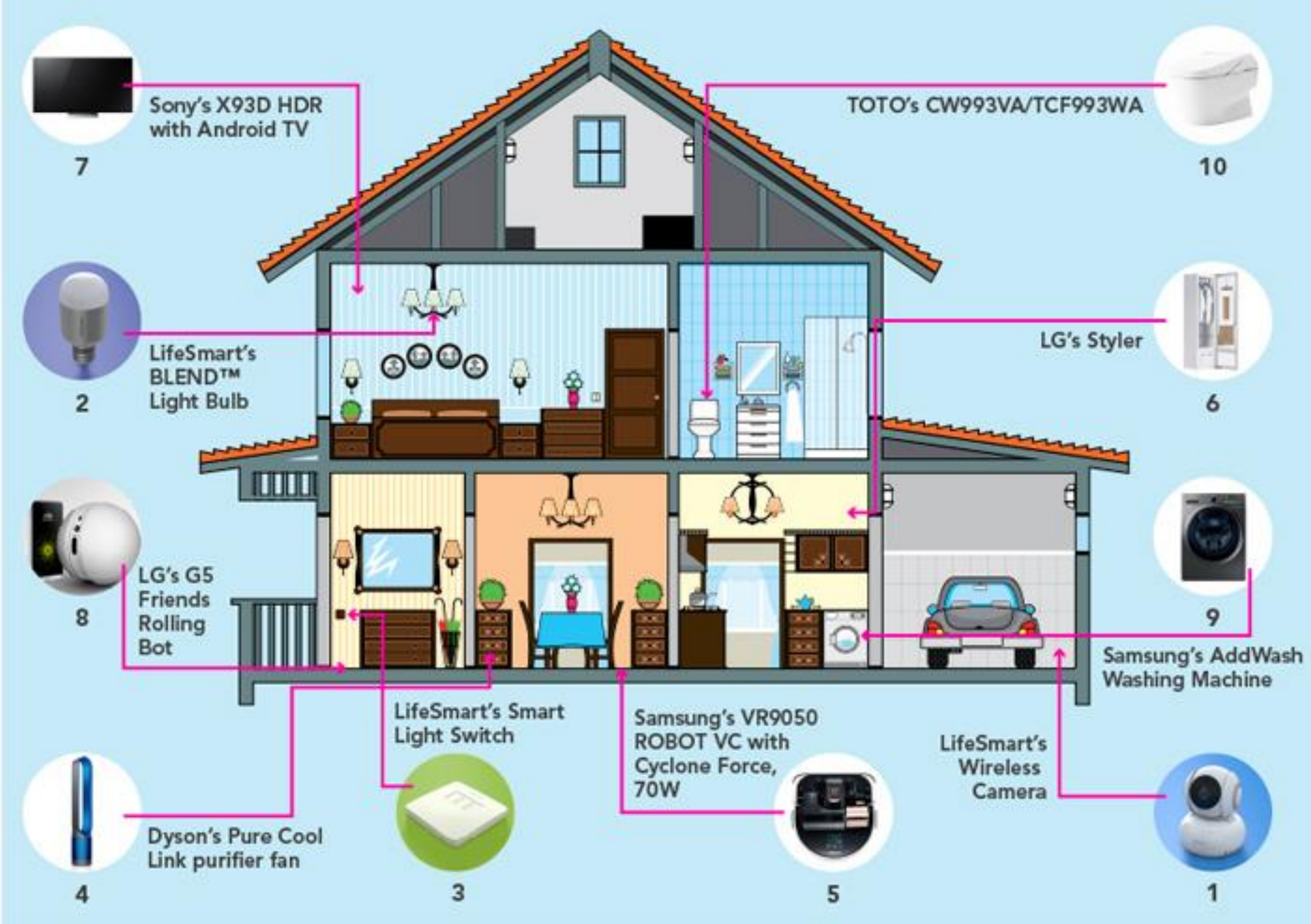
- Encrypt sensitive data
  - Use Microsoft Office tool
  - Remember your password!
- https://www.us-cert.gov/ncas/tips/ST15-002 "How to Secure Your Home Network"
- https://privacy.net/how-to-secure-your-computer/

https://privacy.net/how-to-secure-your-computer/

Your Home Network and Work Network

- Your home network is an extension of the work network

- Does your home **computer** meet any regulatory requirements imposed on the data you use?
- Does your home **network** meet any regulatory requirements imposed on the data you use?


Sony's X93D HDR with Android TV
7
TOTO's CW993VA/TCF993WA
10
LifeSmart's BLEND™ Light Bulb
2
LG's Styler
6
LG's G5 Friends Rolling Bot
8
9
Samsung's AddWash Washing Machine
LifeSmart's Smart Light Switch
Samsung's VR9050 ROBOT VC with Cyclone Force, 70W
LifeSmart's Wireless Camera
Dyson's Pure Cool Link purifier fan
4
3
5
1

WFH, IoT, Mobile, Oh My!

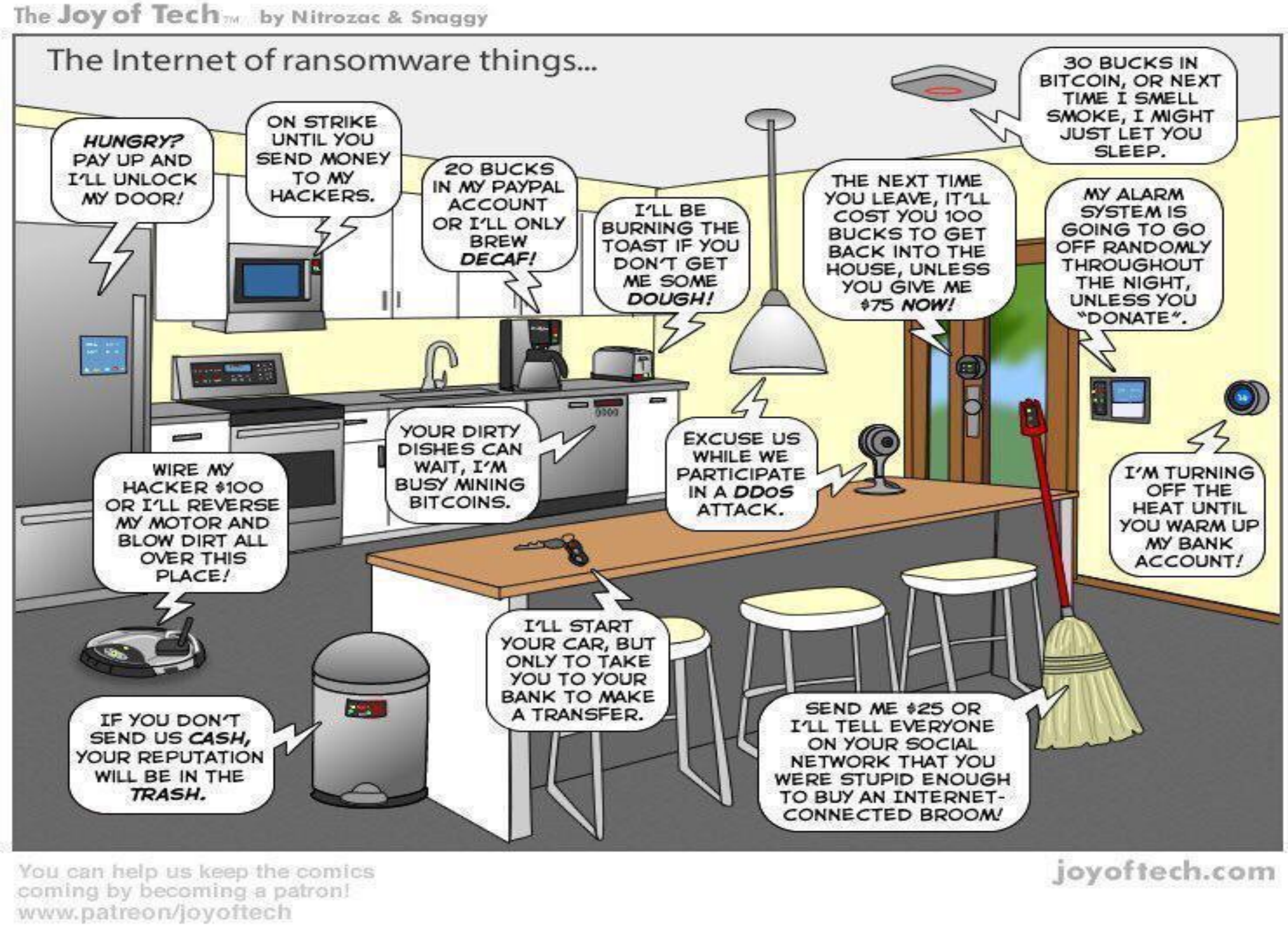
Times are a’changing – Gartner Predictions

- **"By 2025, threat actors will have weaponized operational technology environments successfully to cause human casualties."**
- **"Through 2025, 30% of nation states will pass legislation that regulates ransomware payments, fines and negotiations…"**
- **"By 2025, 70% of CEOs will mandate a culture of organizational resilience to survive coinciding threats from cybercrime, severe weather events, civil unrest and political instabilities.“**
- **"By 2026, 50% of C-level executives will have performance requirements related to risk built into their employment contracts.“**
- Source: https://campustechnology.com/articles/2022/06/23/gartners-top-8-cybersecurity-predictions-for-the-coming-year.aspx?s=ct_nu_050722

What’s a Thing?

- A Thing is physical object that contains 1 or more devices
- Sensor – sense the physical environment
  - Thermometers, Thermostats, weight scales
  - Measure something
- Actuator – affect the physical environment
  - Brakes, pedals, pistons
  - Does something

  - https://www.cosic.esat.kuleuven.be/school-iot/slides/IoTChallenges.pdf

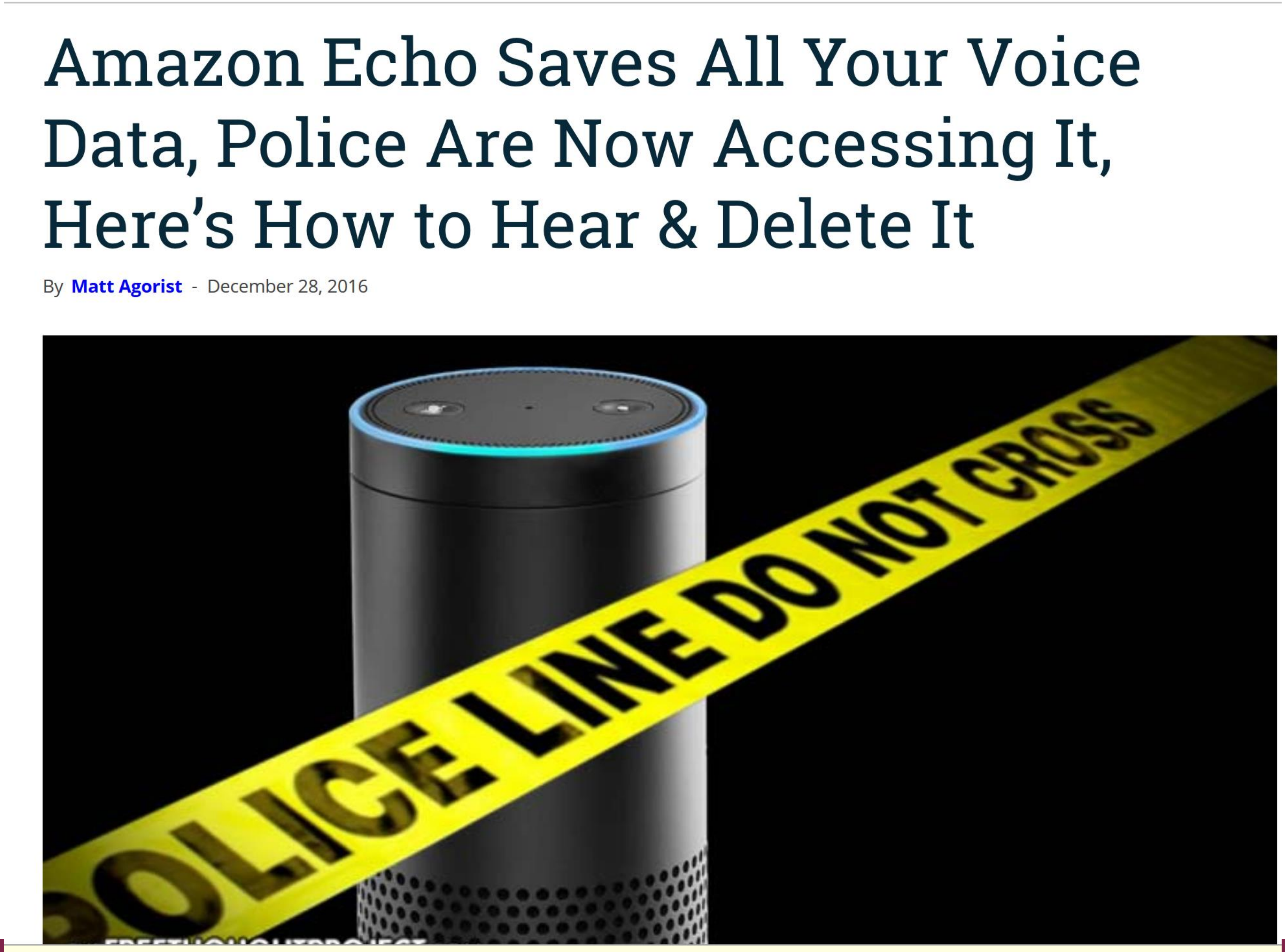

The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

1
2
3
4
5
6
7
8
9
*
0
A

Schneier's Example – Car Attack*

- Confidentiality, Availability, Integrity
- Confidentiality
  - Know who you are so we target your car
- Availability
  - Disable your car's brake system
- Integrity
  - Change the settings on your car's "stay in lane" feature
  - Tell it to be 2 ft to the left of the center line

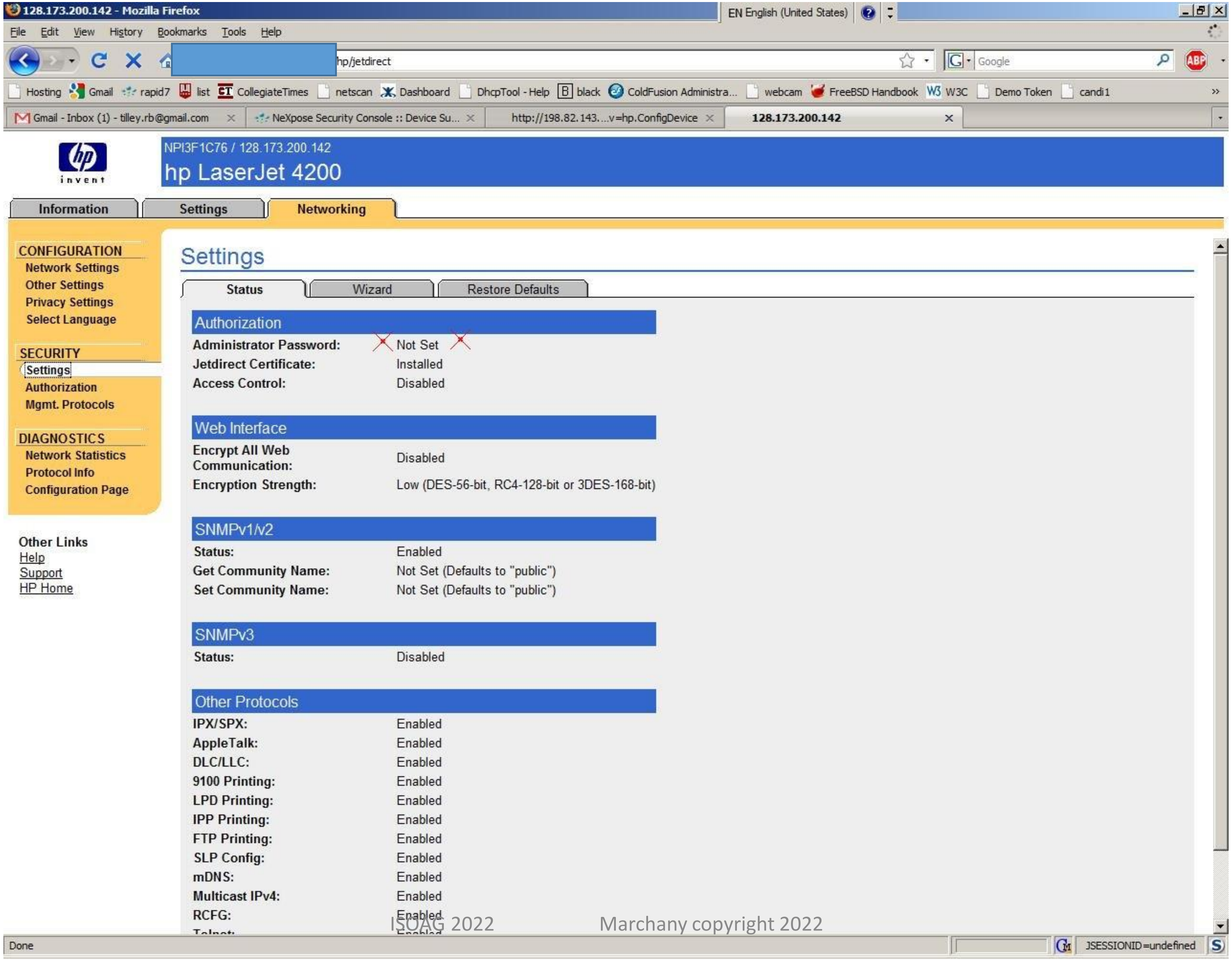
- *"Click Here to Kill Everybody", by Bruce Schneier, ISBN: 978-0-393-60888-5



Amazon Echo Saves All Your Voice Data, Police Are Now Accessing It, Here's How to Hear & Delete It

By **Matt Agorist** - December 28, 2016

Meet a Spammer


128.173.200.142 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
[redacted]hp/jetdirect
Hosting Gmail rapid7 list CollegiateTimes netscan Dashboard DhcpTool - Help black ColdFusion Administra... webcam FreeBSD Handbook W3C Demo Token candi1
Gmail - Inbox (1) - tilley.rb@gmail.com
NeXpose Security Console :: Device Su...
http://198.82.143....v=hp.ConfigDevice
128.173.200.142
NPI3F1C76 / 128.173.200.142
hp LaserJet 4200
Information
Settings
Networking
CONFIGURATION
Network Settings
Other Settings
Privacy Settings
Select Language
SECURITY
Settings
Authorization
Mgmt. Protocols
DIAGNOSTICS
Network Statistics
Protocol Info
Configuration Page
Other Links
Help
Support
HP Home
Status
Wizard
Restore Defaults
Done
JSESSIONID=undefined

Settings

Authorization

Administrator Password:	Not Set
Jetdirect Certificate:	Installed
Access Control:	Disabled

Web Interface

Encrypt All Web Communication:	Disabled
Encryption Strength:	Low (DES-56-bit, RC4-128-bit or 3DES-168-bit)

SNMPv1/v2

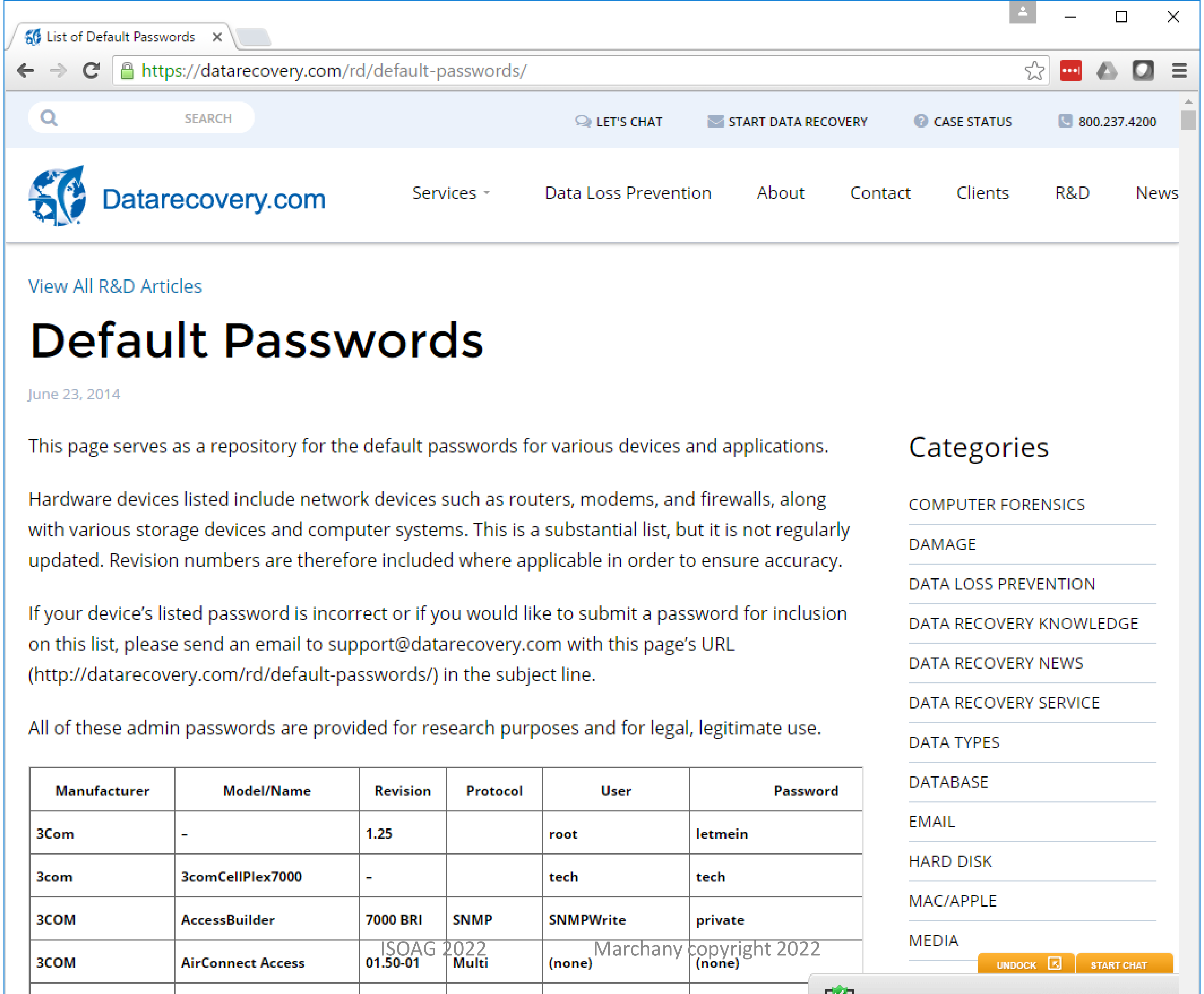
Status:	Enabled
Get Community Name:	Not Set (Defaults to "public")
Set Community Name:	Not Set (Defaults to "public")

SNMPv3

Status:	Disabled

Other Protocols

IPX/SPX:	Enabled
AppleTalk:	Enabled
DLC/LLC:	Enabled
9100 Printing:	Enabled
LPD Printing:	Enabled
IPP Printing:	Enabled
FTP Printing:	Enabled
SLP Config:	Enabled
mDNS:	Enabled
Multicast IPv4:	Enabled
RCFG:	Enabled
Telnet:	Enabled



View All R&D Articles

Default Passwords

June 23, 2014

This page serves as a repository for the default passwords for various devices and applications.

Hardware devices listed include network devices such as routers, modems, and firewalls, along with various storage devices and computer systems. This is a substantial list, but it is not regularly updated. Revision numbers are therefore included where applicable in order to ensure accuracy.

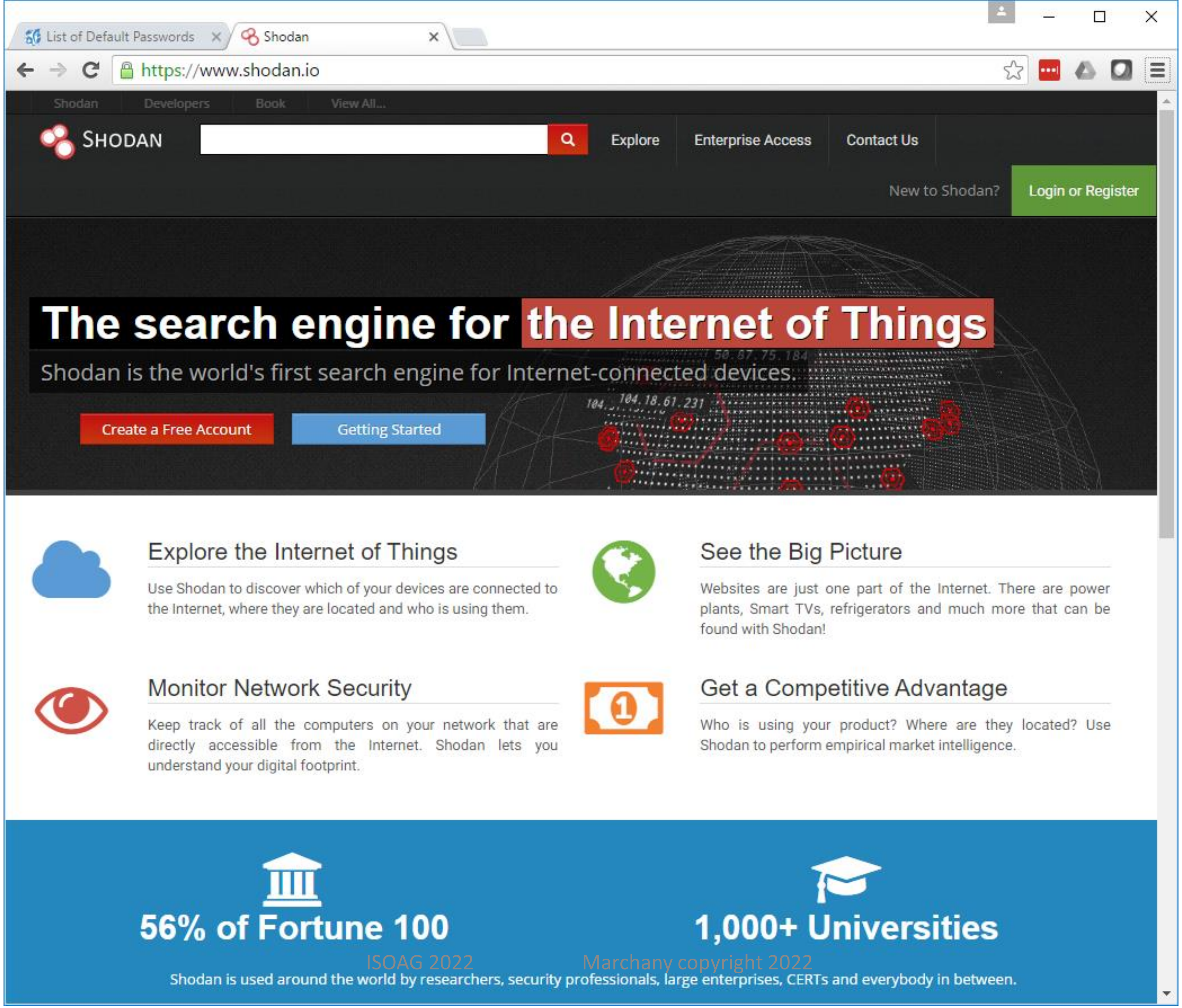
If your device's listed password is incorrect or if you would like to submit a password for inclusion on this list, please send an email to support@datarecovery.com with this page's URL (http://datarecovery.com/rd/default-passwords/) in the subject line.

All of these admin passwords are provided for research purposes and for legal, legitimate use.

Manufacturer	Model/Name	Revision	Protocol	User	Password
3Com	-	1.25		root	letmein
3com	3comCellPlex7000	-		tech	tech
3COM	AccessBuilder	7000 BRI	SNMP	SNMPWrite	private
3COM	AirConnect Access	01.50-01	Multi	(none)	(none)

Categories

- COMPUTER FORENSICS
- DAMAGE
- DATA LOSS PREVENTION
- DATA RECOVERY KNOWLEDGE
- DATA RECOVERY NEWS
- DATA RECOVERY SERVICE
- DATA TYPES
- DATABASE
- EMAIL
- HARD DISK
- MAC/APPLE
- MEDIA



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

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

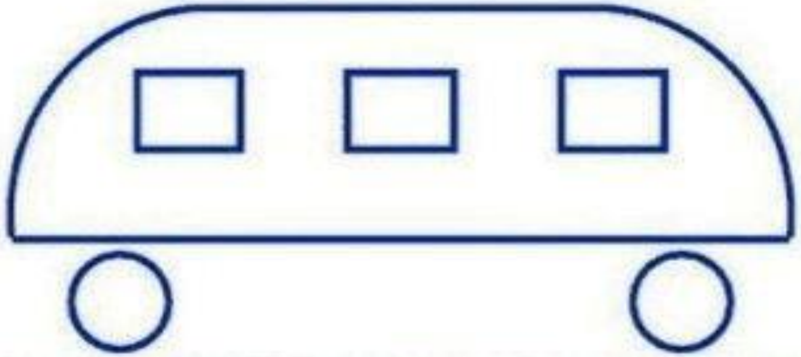
Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Summary

- Data Protection is key
  - Find, Tag, Encrypt
- Data Flow
  - Where does our data go?
- Logs are crucial
  - Who, What, When, Where, How, Why
- Resilience
  - Can’t prevent ransomware attack
  - Recovery is key

Which way is the bus going?

Right or left?

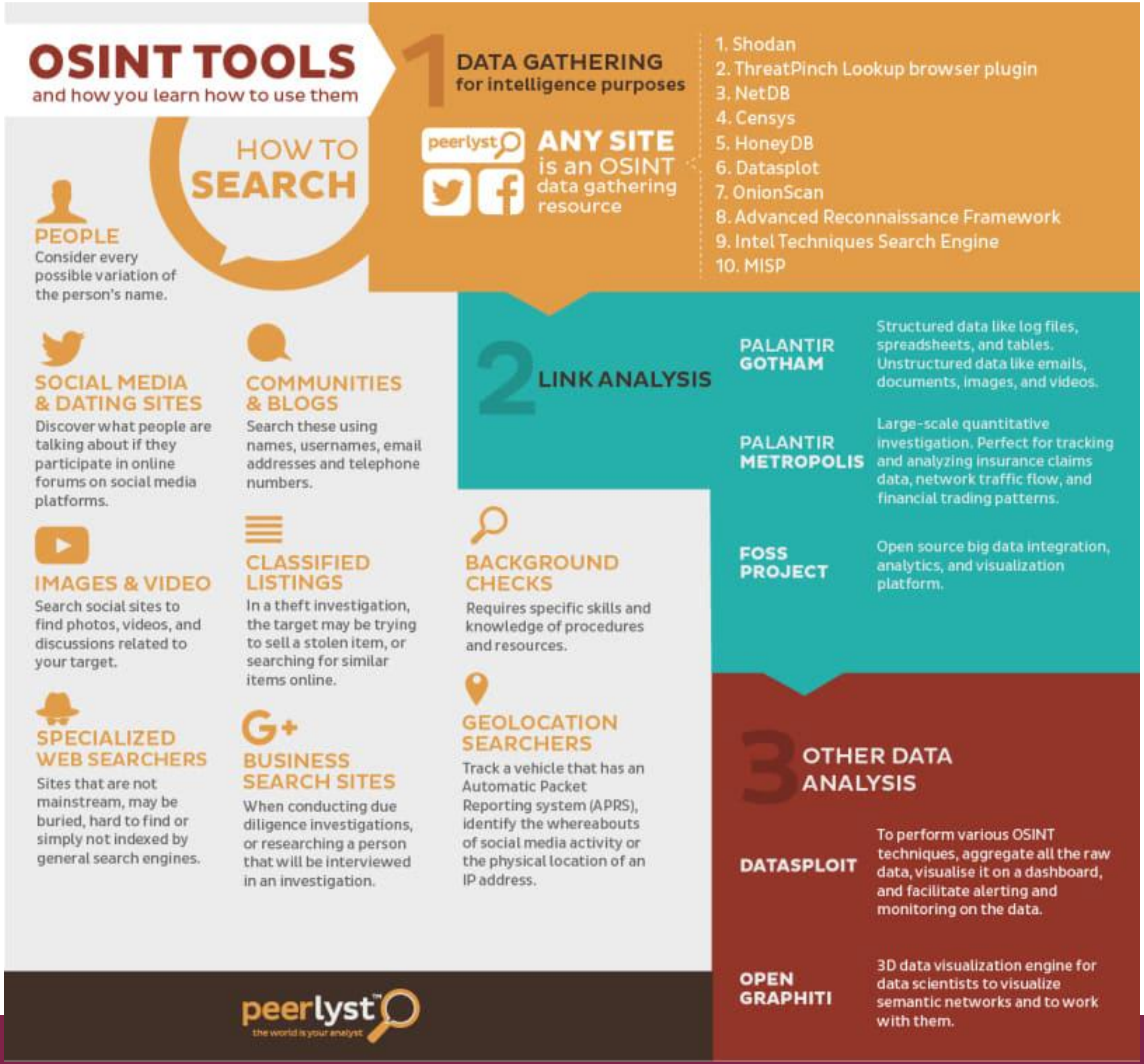


Contact information

- Randy Marchany, Marchany@vt.edu, 540-231-9523 (direct line), 540-231-1688 (office), Twitter: @randymarchany, Blog: randymarchany.blogspot
- http://security.vt.edu

References

- https://github.com/RUB-NDS/PRET
- https://www.nationalcyberscholarship.org/
- https://security.vt.edu
- https://foundation.mozilla.org/en/privacynotincluded/



OSINT TOOLS

and how you learn how to use them

HOW TO SEARCH

PEOPLE

Consider every possible variation of the person's name.

SOCIAL MEDIA & DATING SITES

Discover what people are talking about if they participate in online forums on social media platforms.

COMMUNITIES & BLOGS

Search these using names, usernames, email addresses and telephone numbers.

IMAGES & VIDEO

Search social sites to find photos, videos, and discussions related to your target.

CLASSIFIED LISTINGS

In a theft investigation, the target may be trying to sell a stolen item, or searching for similar items online.

BACKGROUND CHECKS

Requires specific skills and knowledge of procedures and resources.

SPECIALIZED WEB SEARCHERS

Sites that are not mainstream, may be buried, hard to find or simply not indexed by general search engines.

BUSINESS SEARCH SITES

When conducting due diligence investigations, or researching a person that will be interviewed in an investigation.

GEOLOCATION SEARCHERS

Track a vehicle that has an Automatic Packet Reporting system (APRS), identify the whereabouts of social media activity or the physical location of an IP address.

1 DATA GATHERING for intelligence purposes

peerlyst **ANY SITE** is an OSINT data gathering resource

1. Shodan
2. ThreatPinch Lookup browser plugin
3. NetDB
4. Censys
5. HoneyDB
6. Datasplot
7. OnionScan
8. Advanced Reconnaissance Framework
9. Intel Techniques Search Engine
10. MISP

2 LINK ANALYSIS

PALANTIR GOTHAM Structured data like log files, spreadsheets, and tables. Unstructured data like emails, documents, images, and videos.

PALANTIR METROPOLIS Large-scale quantitative investigation. Perfect for tracking and analyzing insurance claims data, network traffic flow, and financial trading patterns.

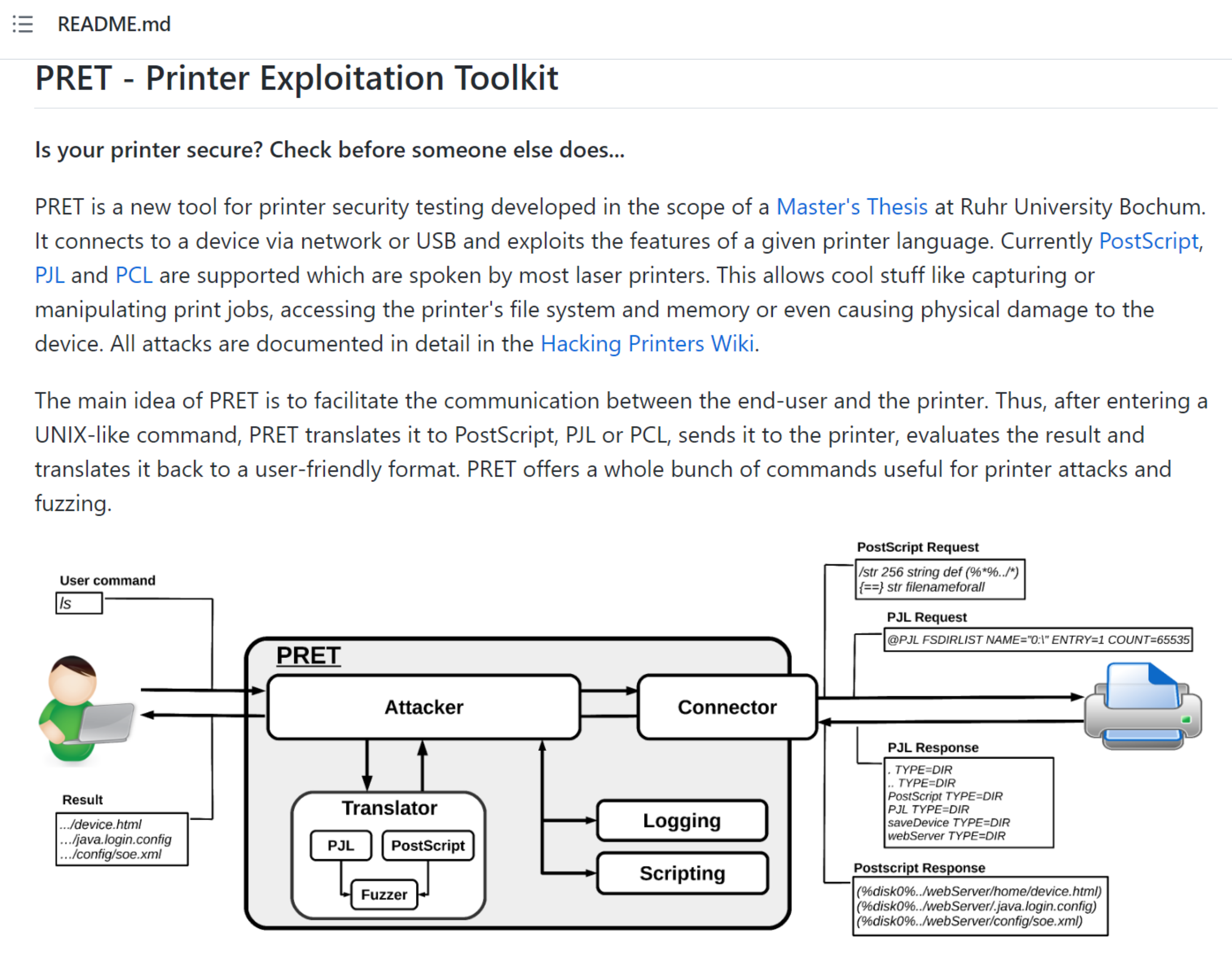
FOSS PROJECT Open source big data integration, analytics, and visualization platform.

3 OTHER DATA ANALYSIS

DATASPLOIT To perform various OSINT techniques, aggregate all the raw data, visualise it on a dashboard, and facilitate alerting and monitoring on the data.

OPEN GRAPHITI 3D data visualization engine for data scientists to visualize semantic networks and to work with them.

peerlyst
the world is your analyst



README.md

PRET - Printer Exploitation Toolkit

Is your printer secure? Check before someone else does...

PRET is a new tool for printer security testing developed in the scope of a Master's Thesis at Ruhr University Bochum. It connects to a device via network or USB and exploits the features of a given printer language. Currently PostScript, PJL and PCL are supported which are spoken by most laser printers. This allows cool stuff like capturing or manipulating print jobs, accessing the printer's file system and memory or even causing physical damage to the device. All attacks are documented in detail in the Hacking Printers Wiki.

The main idea of PRET is to facilitate the communication between the end-user and the printer. Thus, after entering a UNIX-like command, PRET translates it to PostScript, PJL or PCL, sends it to the printer, evaluates the result and translates it back to a user-friendly format. PRET offers a whole bunch of commands useful for printer attacks and fuzzing.

User command

```
ls
```

Result

```
.../device.html
.../java.login.config
.../config/soe.xml
```

PostScript Request

```
/str 256 string def (%*%../*)
{==} str filenameforall
```

PJL Request

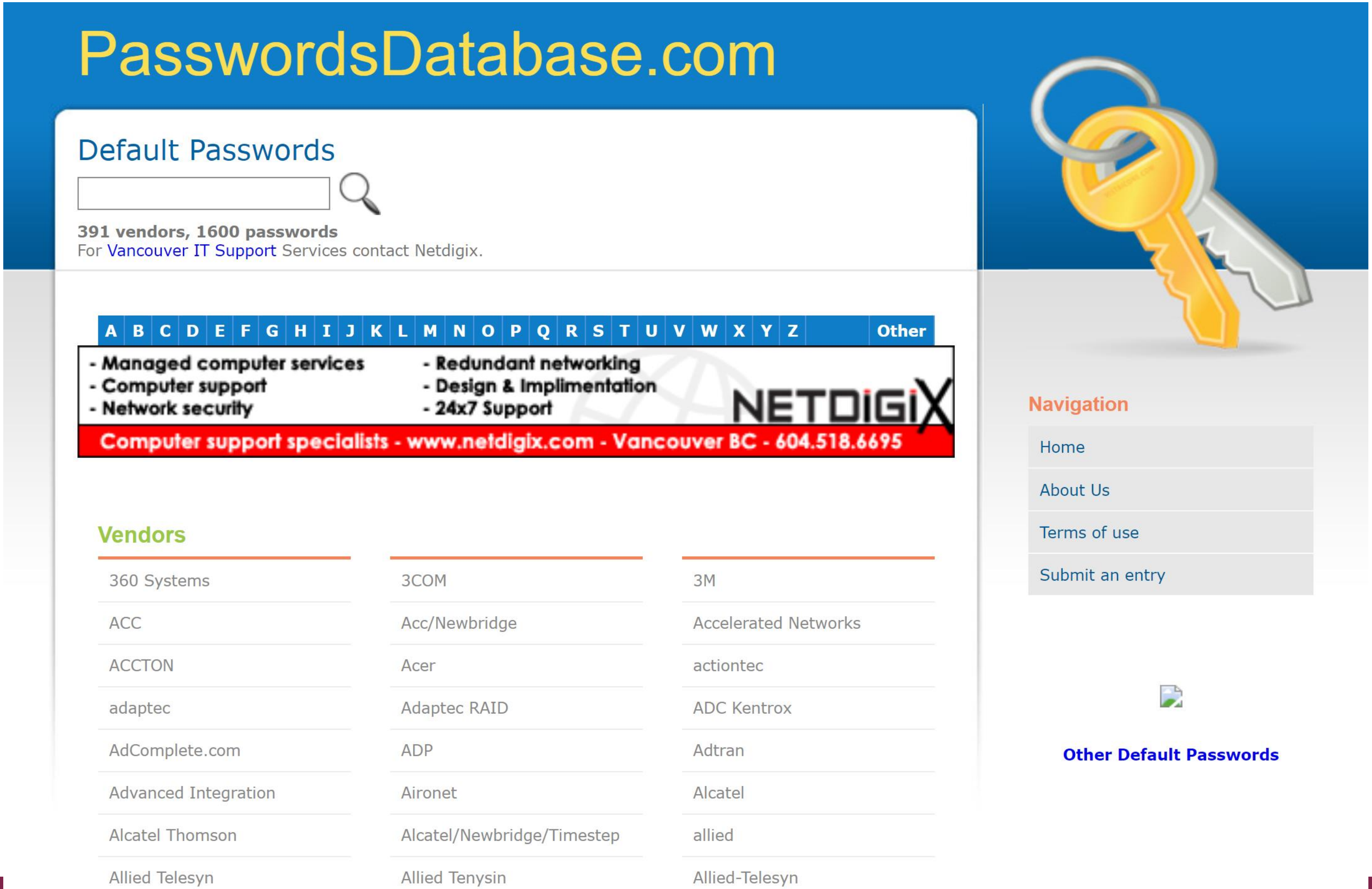
```
@PJL FSDIRLIST NAME="0:\" ENTRY=1 COUNT=65535
```

PJL Response

```
. TYPE=DIR
.. TYPE=DIR
PostScript TYPE=DIR
PJL TYPE=DIR
saveDevice TYPE=DIR
webServer TYPE=DIR
```

Postscript Response

```
(%disk0%../webServer/home/device.html)
(%disk0%../webServer/.java.login.config)
(%disk0%../webServer/config/soe.xml)
```



PasswordsDatabase.com

Default Passwords

391 vendors, 1600 passwords
For Vancouver IT Support Services contact Netdigix.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Other

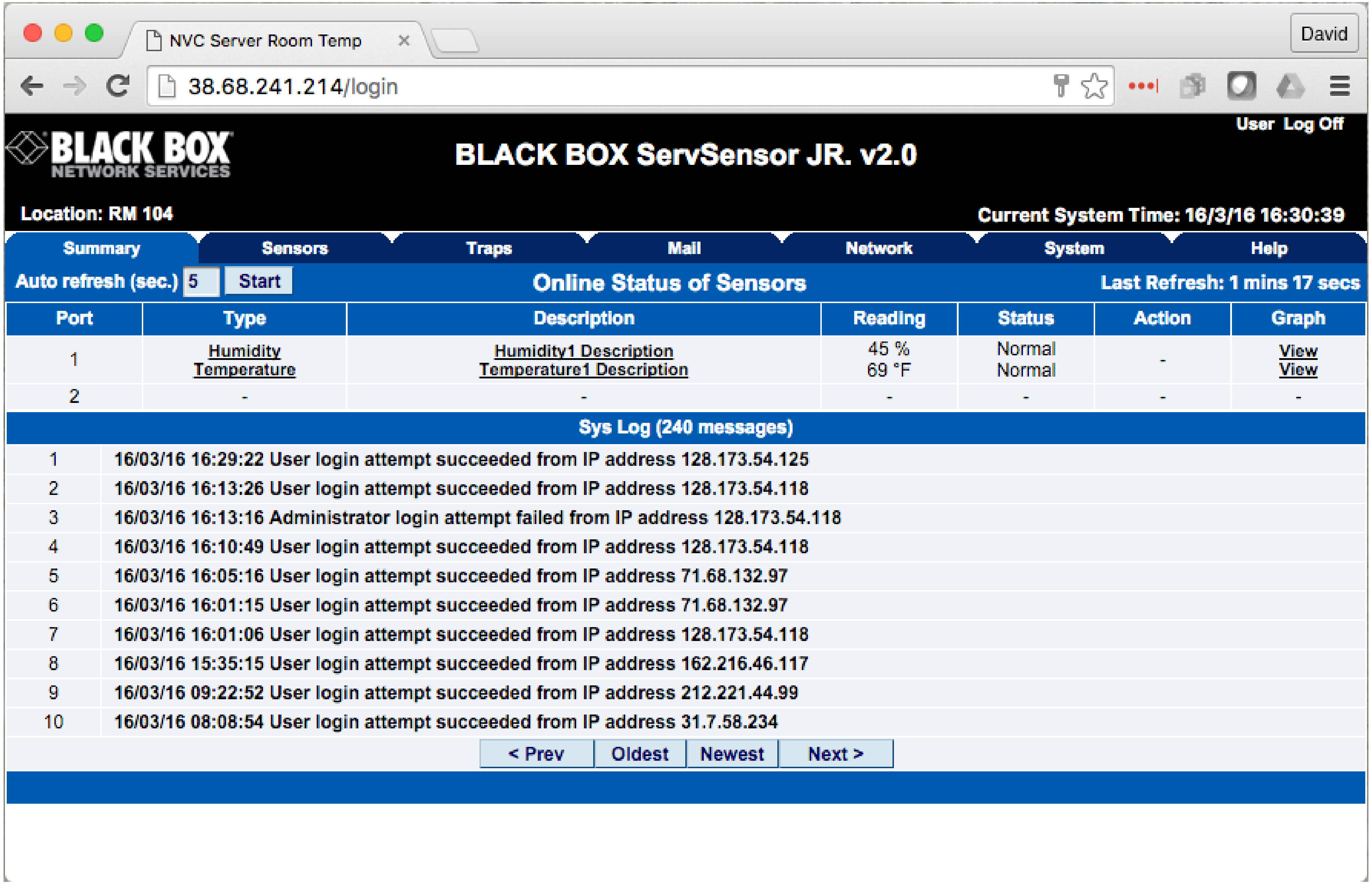
Vendors

360 Systems	3COM	3M
ACC	Acc/Newbridge	Accelerated Networks
ACCTON	Acer	actiontec
adaptec	Adaptec RAID	ADC Kentrox
AdComplete.com	ADP	Adtran
Advanced Integration	Aironet	Alcatel
Alcatel Thomson	Alcatel/Newbridge/Timestep	allied
Allied Telesyn	Allied Tenysin	Allied-Telesyn

Navigation

- Home
- About Us
- Terms of use
- Submit an entry

Other Default Passwords



BLACK BOX ServSensor JR. v2.0

Location: RM 104

Current System Time: 16/3/16 16:30:39

Auto refresh (sec.) 5

Online Status of Sensors

Last Refresh: 1 mins 17 secs

Port	Type	Description	Reading	Status	Action	Graph
1	Humidity Temperature	Humidity1 Description Temperature1 Description	45 % 69 °F	Normal Normal	-	View View
2	-	-	-	-	-	-

Sys Log (240 messages)

```
1    16/03/16 16:29:22 User login attempt succeeded from IP address 128.173.54.125
2    16/03/16 16:13:26 User login attempt succeeded from IP address 128.173.54.118
3    16/03/16 16:13:16 Administrator login attempt failed from IP address 128.173.54.118
4    16/03/16 16:10:49 User login attempt succeeded from IP address 128.173.54.118
5    16/03/16 16:05:16 User login attempt succeeded from IP address 71.68.132.97
6    16/03/16 16:01:15 User login attempt succeeded from IP address 71.68.132.97
7    16/03/16 16:01:06 User login attempt succeeded from IP address 128.173.54.118
8    16/03/16 15:35:15 User login attempt succeeded from IP address 162.216.46.117
9    16/03/16 09:22:52 User login attempt succeeded from IP address 212.221.44.99
10   16/03/16 08:08:54 User login attempt succeeded from IP address 31.7.58.234
```

MACH37™
CYBER ACCELERATOR

Owned and operated by:

VENTURESCOPE™
Strategies · Investments · Causes

VIRGINIA IT AGENCY

ISOAG
Information Security Officers Advisory Group

July 13, 2022

Mike McCoy
Director of Operations & Platform Engineering

Agenda

1) Learn about MACH37 Cyber Accelerator

2) Startup Showcase : Learn of emerging technology

3) From the Trenches : Live from Kyiv, Ukraine

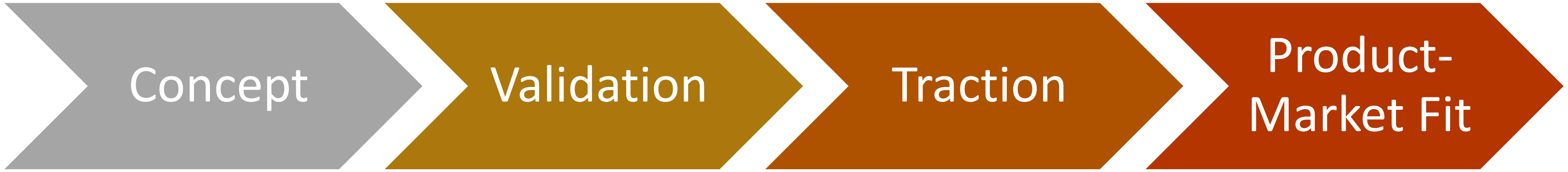
   How a Ukraine cybersecurity startup is helping defend critical infrastructure from Russian cyber attacks.

4) Audience Feedback Survey

The Accelerator Purpose

To help improve a startup's chances of success.

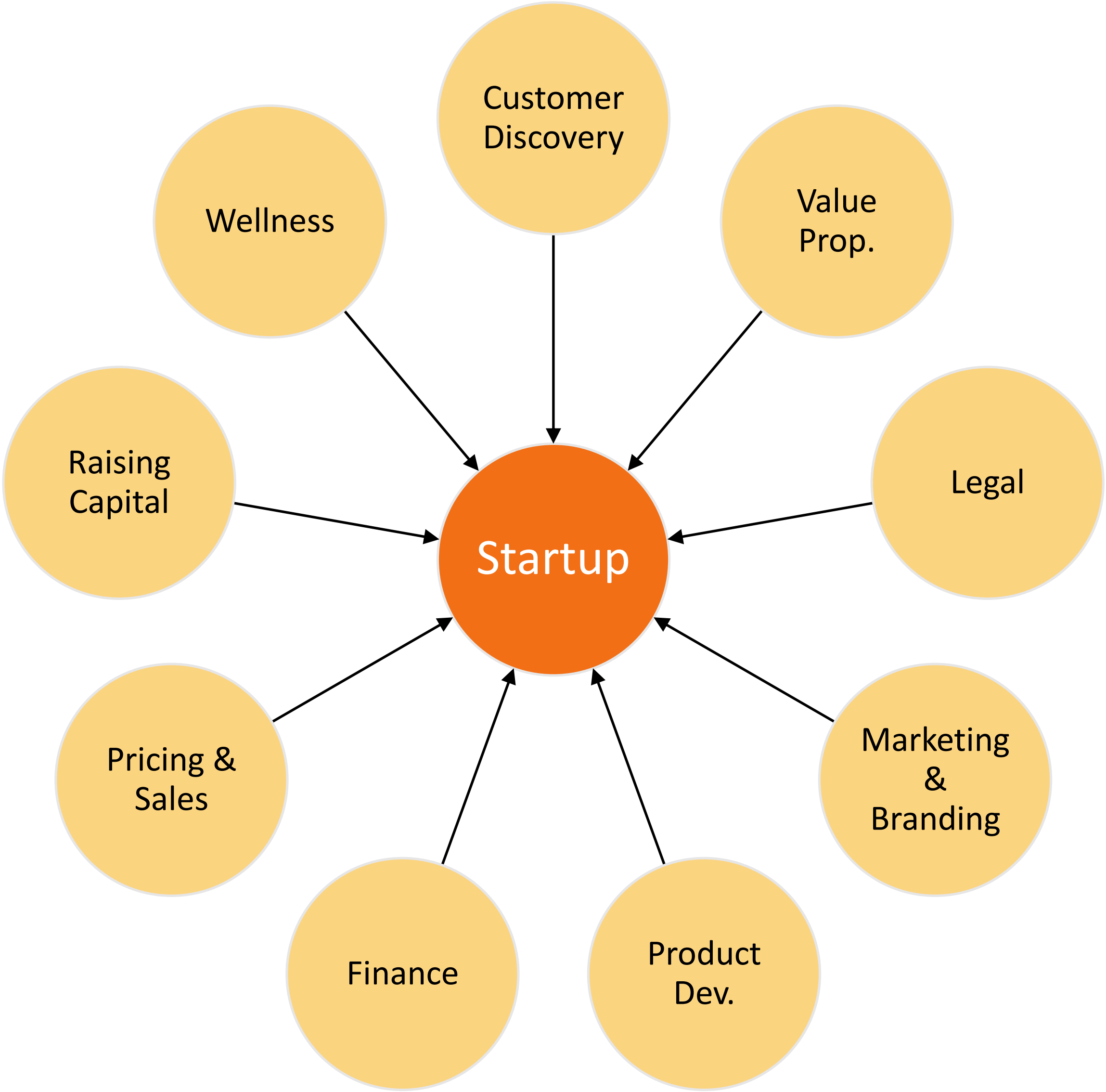
1. **Startup:** An organization formed in search for a repeatable and scalable business model. - Steve Blank
2. **Accelerator:** A mentor/expert-driven structured program that provides intense goals, guidance and support for 3 months.


Concept → Validation → Traction → Product-Market Fit

- Teach business acumen
- Stress-test founders, teams, and companies
- Perform investor due diligence

Connecting Startups w/Experts

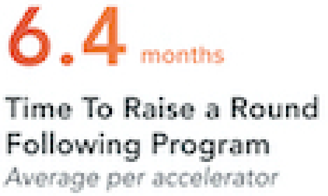
Sharing best practices to prevent common mistakes.



2021 Macro Startup Trends

*"Accelerated companies are 50% more likely to **raise seed funding** than non-accelerated companies.*

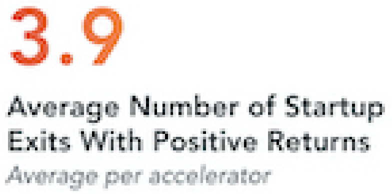
*38% of startups that pass through accelerator programs **raise Series A funding.**" - Failory.com*



6.4 months

Time To Raise a Round Following Program

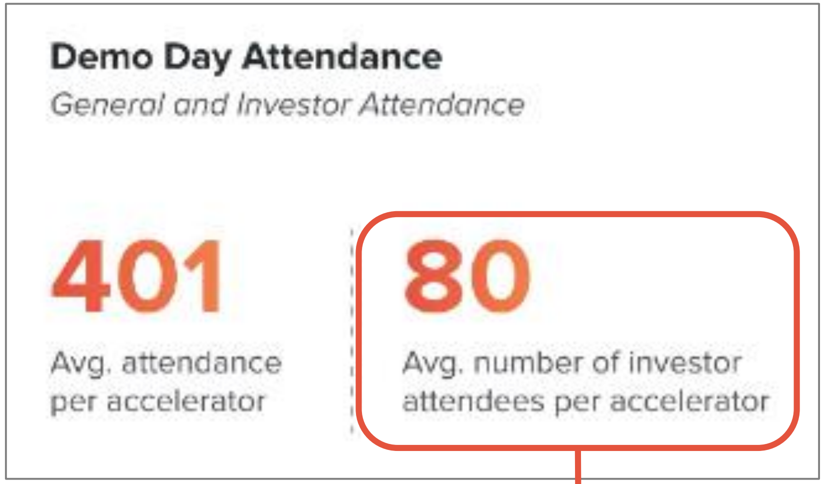
Average per accelerator



3.9

Average Number of Startup Exits With Positive Returns

Average per accelerator

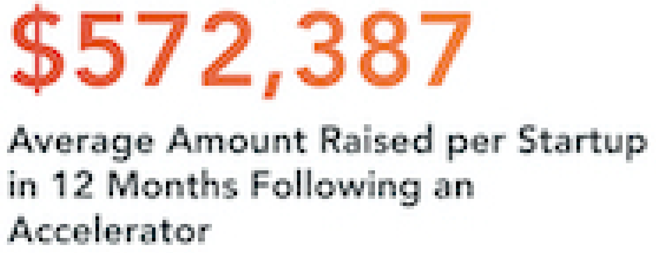


Demo Day Attendance

General and Investor Attendance

401	80
Avg. attendance per accelerator	Avg. number of investor attendees per accelerator

How long would it normally take for a startup to meet with 80 investors?



$572,387

Average Amount Raised per Startup in 12 Months Following an Accelerator

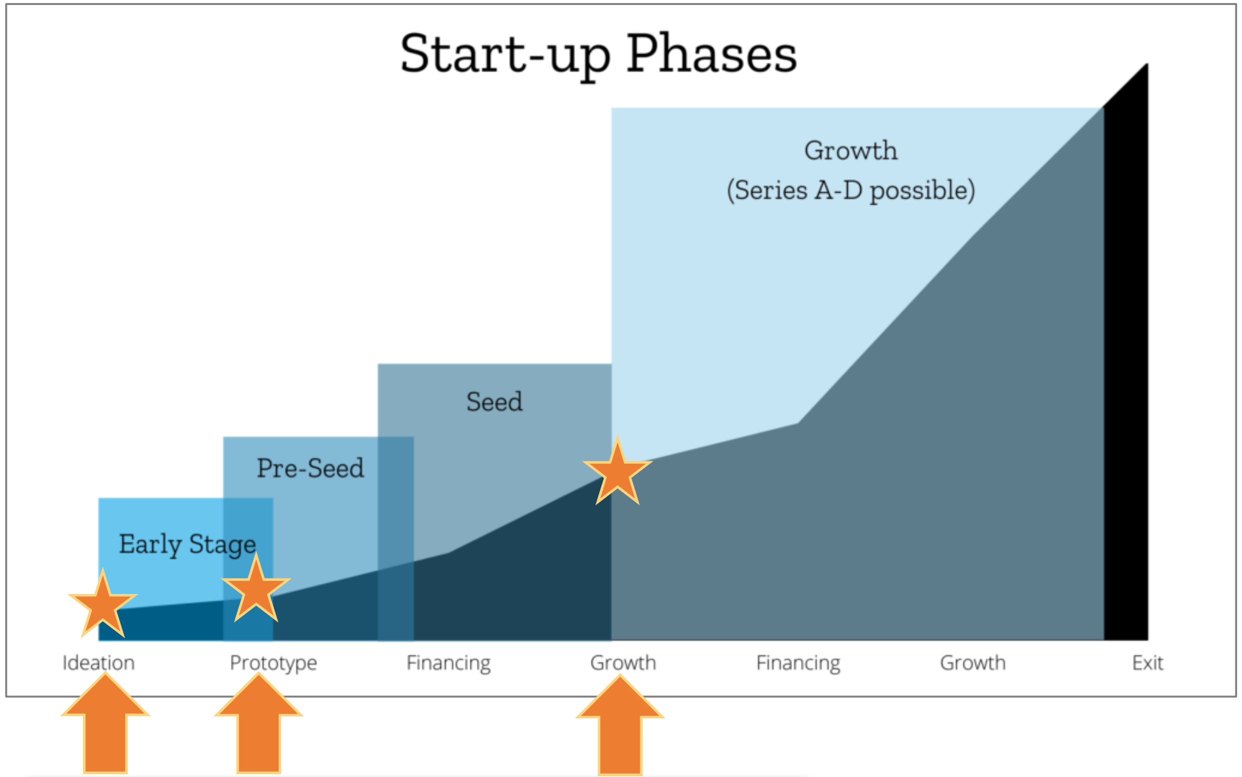
Source: Global Accelerator Network (GAN) 2021 Annual Report

MACH37 Statistics

Forbes

“the granddaddy” of cyber accelerators

- October 2020 article



3 different programs for early-stage companies

Founded in 2013

500+

Startups apply per year

8

Average cohort size
(Extremely selective)

400+

World-wide expert mentors

82

Companies launched

75%

Alumni still in business

64%

Raised investment
Post graduation

Events

- Accelerator cohorts (MACH37)
- Launch / Demo Day
- CISO Quarterly Round Table
- Cyber Coffee
- Cyber Salons
- Cyber Shark Tanks
- Cyber Summits
- Cyber week (Oct 17-21)
- Entrepreneur Expos
- Hackathons
- Happy Hour Networking & Meetups
- Local & National Conferences
- Startup Introductions and Match-Making
- Startup Week (Sept 12-16)
- Student Pitch Competitions
- Women in Cyber & Innovation

Ecosystem Supporters

NORTHERN VIRGINIA
CHAMBER OF COMMERCE

FAIRFAX COUNTY
ECONOMIC DEVELOPMENT AUTHORITY

Commonwealth
Cyber Initiative

nvtc
NORTHERN VIRGINIA
TECHNOLOGY COUNCIL

MARYLAND
TECH COUNCIL
ADVANCING LIFE SCIENCES AND TECHNOLOGY

GAN®

GLOBAL
STARTUP
STUDIO
NETWORK

University of Mary Washington

GEORGE MASON
UNIVERSITY

MARYMOUNT
UNIVERSITY

Blu Venture
INVESTORS

CYBER CAPITAL
PARTNERS

Partner with MACH37

- Send entrepreneurs & companies to MACH37
- Host events (private and public)
- Speak as an expert panelist
- Judge startup pitches
- Publish expert articles on our blog/newsletter
- Recruit highly skilled technologists & entrepreneurs

MACH37's Focus Areas

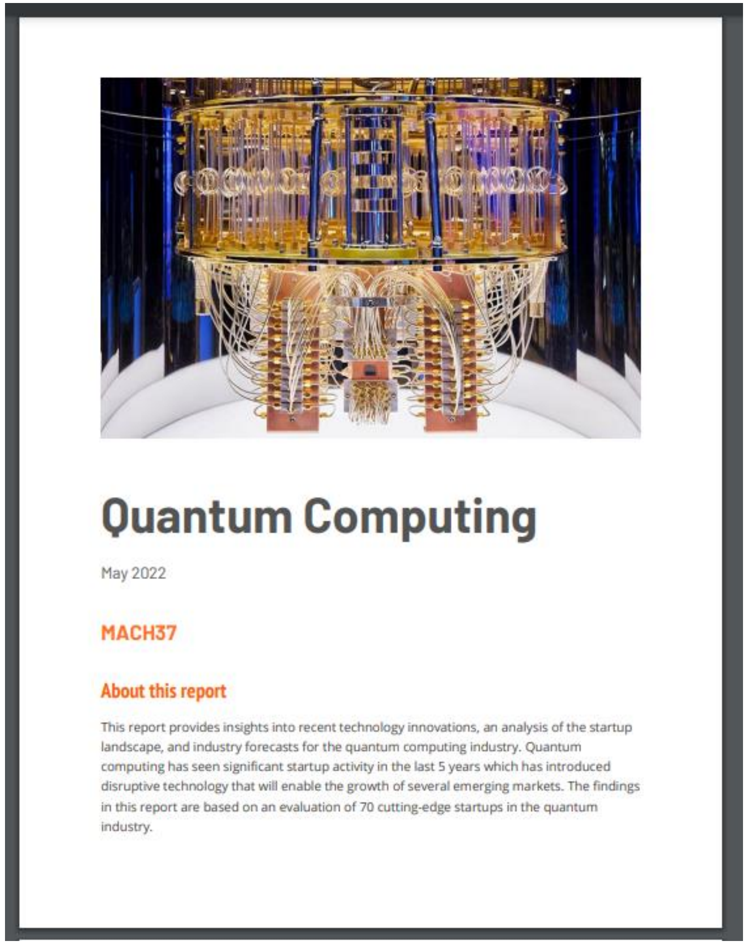
- Artificial Intelligence
- Cloud
- Critical Infrastructure
- Cyber Physical Systems
- Cyber Training
- DevSecOps Tools
- Distributed Finance (de-fi)
- Encryption & Cryptography
- Enterprise Security
- FinTech
- Identity
- Internet of Things (IOT)
- Industrial Controls
- Machine Learning
- Neural Networks
- Quantum Computing
- Security Compliance
- Smart Cities/Infrastructure
- Space tech

Interested in a specific tech? Let us know!

We find emerging technology companies.

Emerging Technology Research Products

Analytic Reports



Quantum Computing

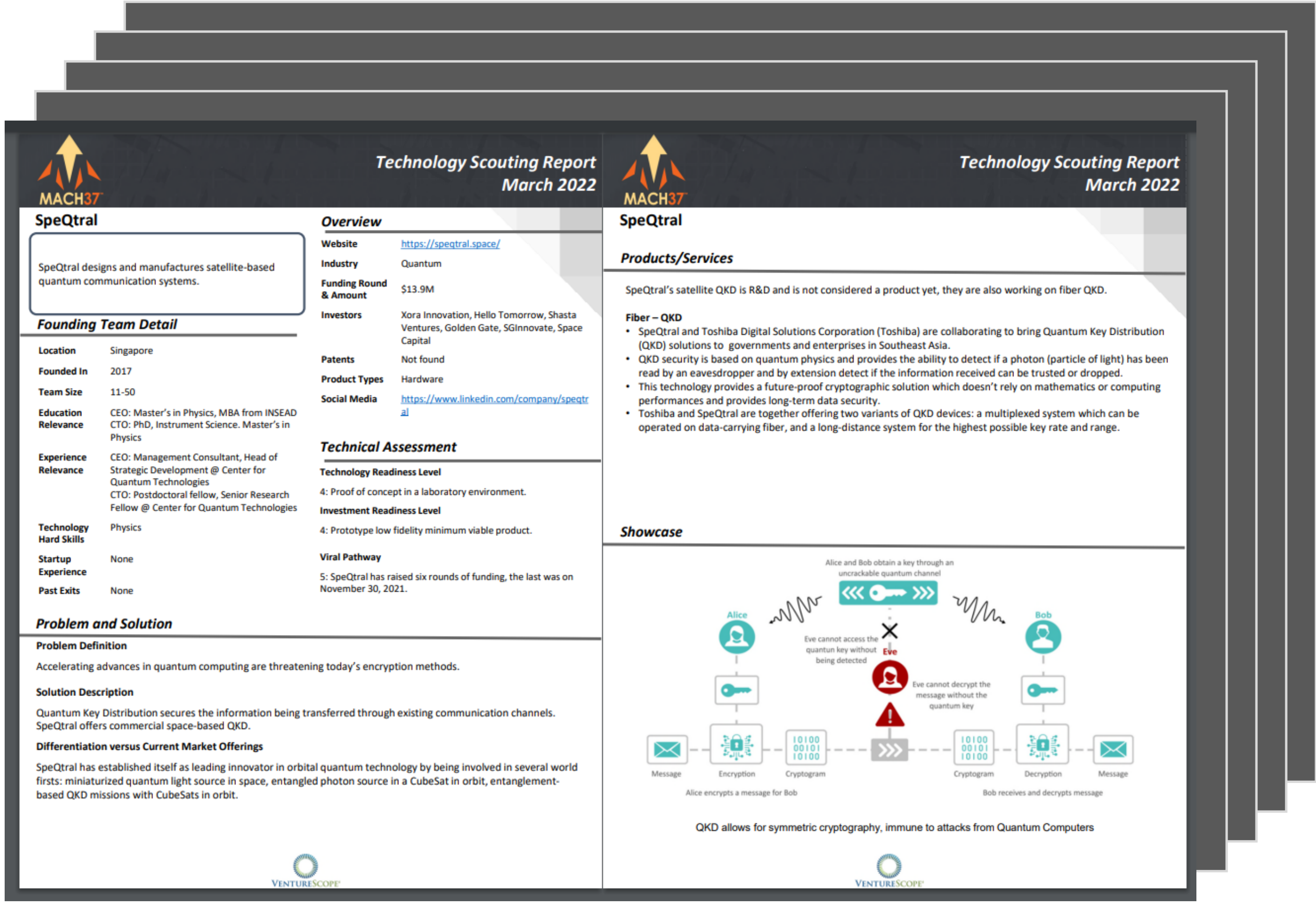
May 2022

MACH37

About this report

This report provides insights into recent technology innovations, an analysis of the startup landscape, and industry forecasts for the quantum computing industry. Quantum computing has seen significant startup activity in the last 5 years which has introduced disruptive technology that will enable the growth of several emerging markets. The findings in this report are based on an evaluation of 70 cutting-edge startups in the quantum industry.

Technology-Specific Company Profiles



MACH37

Technology Scouting Report
March 2022

SpeQtral

SpeQtral designs and manufactures satellite-based quantum communication systems.

Founding Team Detail

Location	Singapore
Founded In	2017
Team Size	11-50
Education Relevance	CEO: Master's in Physics, MBA from INSEAD CTO: PhD, Instrument Science. Master's in Physics
Experience Relevance	CEO: Management Consultant, Head of Strategic Development @ Center for Quantum Technologies CTO: Postdoctoral fellow, Senior Research Fellow @ Center for Quantum Technologies
Technology Hard Skills	Physics
Startup Experience	None
Past Exits	None

Overview

Website	https://speqtral.space/
Industry	Quantum
Funding Round & Amount	$13.9M
Investors	Xora Innovation, Hello Tomorrow, Shasta Ventures, Golden Gate, SGInnovate, Space Capital
Patents	Not found
Product Types	Hardware
Social Media	https://www.linkedin.com/company/speqtral

Technical Assessment

Technology Readiness Level

4: Proof of concept in a laboratory environment.

Investment Readiness Level

4: Prototype low fidelity minimum viable product.

Viral Pathway

5: SpeQtral has raised six rounds of funding, the last was on November 30, 2021.

Problem and Solution

Problem Definition

Accelerating advances in quantum computing are threatening today's encryption methods.

Solution Description

Quantum Key Distribution secures the information being transferred through existing communication channels. SpeQtral offers commercial space-based QKD.

Differentiation versus Current Market Offerings

SpeQtral has established itself as leading innovator in orbital quantum technology by being involved in several world firsts: miniaturized quantum light source in space, entangled photon source in a CubeSat in orbit, entanglement-based QKD missions with CubeSats in orbit.

VENTURESCOPE

MACH37

Technology Scouting Report
March 2022

SpeQtral

Products/Services

SpeQtral's satellite QKD is R&D and is not considered a product yet, they are also working on fiber QKD.

Fiber – QKD

- SpeQtral and Toshiba Digital Solutions Corporation (Toshiba) are collaborating to bring Quantum Key Distribution (QKD) solutions to governments and enterprises in Southeast Asia.
- QKD security is based on quantum physics and provides the ability to detect if a photon (particle of light) has been read by an eavesdropper and by extension detect if the information received can be trusted or dropped.
- This technology provides a future-proof cryptographic solution which doesn't rely on mathematics or computing performances and provides long-term data security.
- Toshiba and SpeQtral are together offering two variants of QKD devices: a multiplexed system which can be operated on data-carrying fiber, and a long-distance system for the highest possible key rate and range.

Showcase

Alice and Bob obtain a key through an uncrackable quantum channel
Alice
Bob
Eve cannot access the quantun key without being detected
Eve
Eve cannot decrypt the message without the quantum key
10100 00101 10100
Message
Encryption
Cryptogram
Cryptogram
Decryption
Message
Alice encrypts a message for Bob
Bob receives and decrypts message

QKD allows for symmetric cryptography, immune to attacks from Quantum Computers

VENTURESCOPE

Know where the hockey puck is going.

New Developments

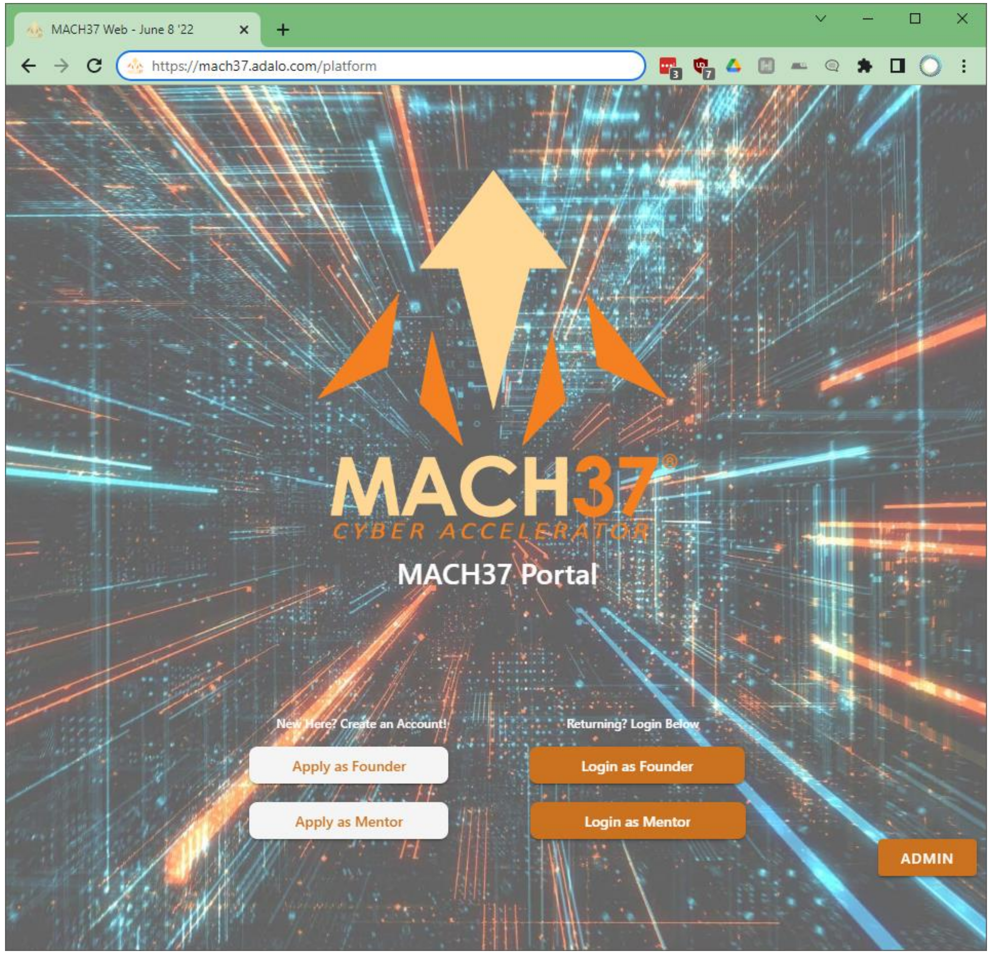
- Global startup participation:
  - India
  - Italy
  - Nigeria
  - Singapore
  - UK
  - Ukraine
- Partnering with International Accelerators
  - Canada
  - Ukraine
- Proprietary acceleration platform under development

Assist MACH37 Startups Directly

- Receive leads for new business.
- Share your expertise with startups!
- Grow your personal & company reputation.
- Expand your network.

✓Minimal time commitment

✓Flexible hours



Accepting new Mentor applications!

GET LAUNCHED

VENTURESCOPE™
Strategies · Investments · Causes

Innovation Consulting Services & Training:

- Accelerator Management
- Innovation Frameworks
  - Lean Startup
  - Lean Enterprise
  - Lean Analytics
  - Business Model Validation
  - Customer Discovery
- Design & Systems Thinking
  - Lean UX
  - Rapid Prototyping, Validation & Delivery
- Innovation Pipeline Design & Execution
- Advanced Agile System Development
  - Enterprise portfolio management
  - Agile contracting, estimating & projecting
  - Continuous DevOps

MACH37™
CYBER ACCELERATOR

Owned and operated by:

VENTURESCOPE™
Strategies · Investments · Causes

🚀Let's Connect! 🚀

- Mentoring
- Blog Posting
- Partner
- Sponsor
- Emerging Tech Research
- Entrepreneurship Training
- Innovation & Strategy Consulting

MACH37.com/contact

hello@mach37.com

Today's Startup Showcase

1)	FortMesa	Spring 2019
2)	BreachBits®	Fall 2019
3)	SylLab	Fall 2019
4)	CySecure	Spring 2020
5)	Obtego Cyber	Fall 2020
6)	HIDEEZ	Fall 2017

Group 1:

5 min overview

5 min Q&A

Conclusion:

25 mins

Live from Ukraine

MACH37™ CYBER ACCELERATOR

GET LAUNCHED

CySecure

Virginia Information Technology Agency

July 13, 2022

Candace Chandra
candace@cysecure.us

Passwords are the Problem

Data Breach Liability for Businesses

- Data breaches and cybercrime cost the global economy **$1.5 Trillion** in 2020 (World Economic Forum, Davos)
- 81% of data breaches are caused by compromised passwords
- $4.24 million average cost for a data breach

Current Passwordless Solutions Don’t Address Root Cause

- User’s personal information remains stored on company servers – a hacker’s dream world

Passwords Cause Negative Productivity and Stress

- 66% of users experience negative productivity
- 100+ passwords required for the average person

The Solution: Decentralized Identity

World Wide Web Consortium (W3C) Specification

Use Hyperledger (Blockchain) & DID for Identity Authentication

+

Put Users in Control of their Personal Identity (Self-Sovereign Identity)

=

No Passwords in the Entire Authentication Chain

CySecure Provides Next Generation Privacy Solutions

- Zero Trust passwordless authentication
- Operating on blockchain technology
- Utilizing Decentralized Identity and Verifiable Credentials global standards
- MFA built into CySecure solution
- Number of attributes are unlimited – definable by the enterprise and customizable by groups or users

CyVer™ – Passwordless Authentication with SSI

Painless User Experience

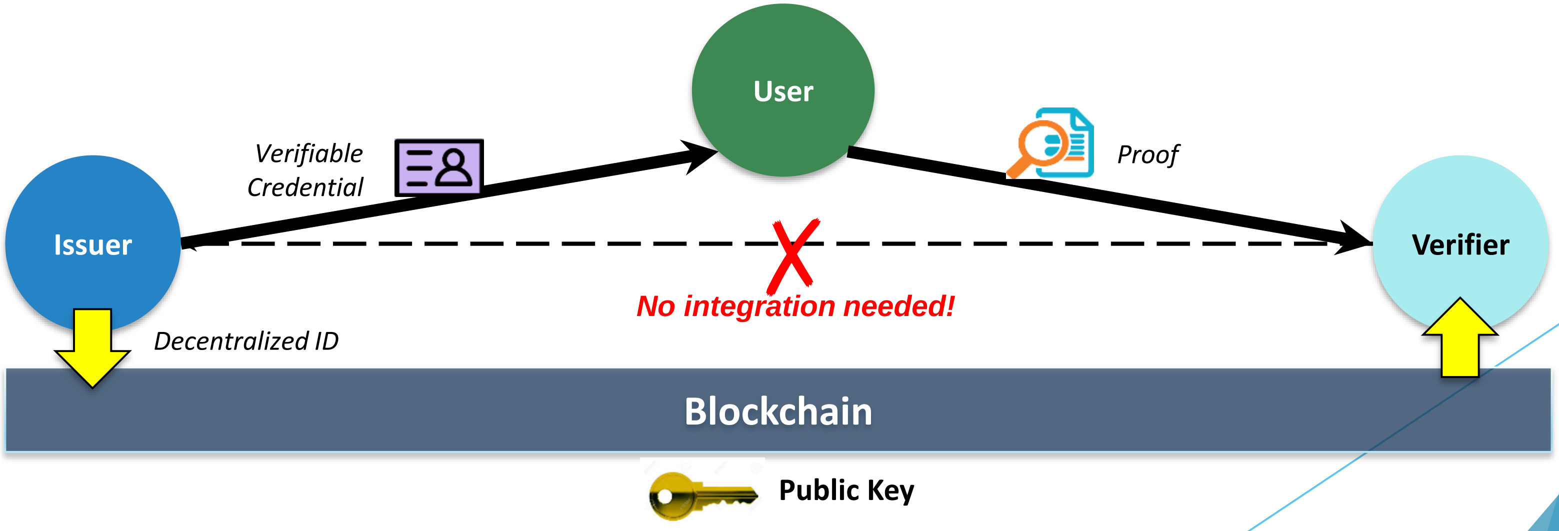
ACCESS GRANTED
ACCESS GRANTED

1 User opens the login screen and sees a QR code

2 User scans the QR code with CyWallet™

3 User access granted

Cryptographic Verification



User

Issuer

Verifier

Verifiable Credential

Proof

No integration needed!

Decentralized ID

Blockchain

Public Key

Progress Since MACH37 Graduation

- Based product architecture on open-source software
- Node Operator on global decentralized identity network
- Pivoted to SaaS business model
- Established partnerships with Indicio and IdRamp
- Completed product development – GA released
- CySecure digital wallet, CyWallet™ available for download in Apple's App Store and Google's Play Store
- Engaged with academic institutions and security companies as clients

CySecure Integrates with Existing Services

- No changes to the existing identity management services
- Authentication to services supporting standard protocols like SAML or OIDC
- Deploys quickly and easily
- Prepares enterprise for transition to Web3 services

CySecure’s key differentiators are user controlled PII and digital identity leading to Web3

Company	Passwordless	User Controls Personal Information	Web3 Enabled
CySecure	✓	✓	✓
Stych	✓	✗	✗
Trusona	✓	✗	✗
Transmit	✓	✗	✗
Hypr	✓	✗	✗
NuID	✓	✗	✗
Duo	✓	✗	✗
Beyond	✓	✗	✗

Be Secure With CySecure

Candace Chandra, Business Development

(703) 651-6838 – candace@cysecure.us

UPCOMING EVENTS

REGISTRATION IS OPEN

2022 COMMONWEALTH VIRTUAL INFORMATION SECURITY CONFERENCE – AUG. 18, 2022

HTTPS://WWW.VITA.VIRGINIA.GOV/INFORMATION-SECURITY/SECURITY-CONFERENCE/

VIRGINIA IT AGENCY

COMMONWEALTH OF VIRGINIA

INFORMATION SECURITY CONFERENCE

2022

VIRTUALLY, NOTHING IS IMPOSSIBLE:

SECURING THE HYBRID WORK ENVIRONMENT

COVITS – SAVE THE DATE

Commonwealth of Virginia Innovative Technology Symposium (COVITS)! September 7, 2022

Location:

Greater Richmond Convention Center

403 N 3rd Street

Richmond, VA 23219

Registration is now open:

COVITS 2022 - LIVE! (govtech.com)

ISOAG AUGUST MEETING

The next ISOAG meeting will be held on:

Aug. 3, 2022, at 1 p.m.

Presenters:

Blake Carpenter – Grant Thorton LLP

Raazi Zain, Peter Smith – Zscaler

Milty Brizan – Amazon Web Services

IS ORIENTATION

IS Orientation

Remote - WebEx

Sept. 29, 2022

Start time: 1 p.m.

End time: 3 p.m.

Instructor: Marlon Cole

https://covaconf.webex.com/covaconf/onstage/g.php?MTID=ecbe083f9321db08a0c81eca667f50575

IS COUNCIL COMMITTEE

The next scheduled meeting for the IS Council:

July 20, 2022

12 – 1 p.m. via Webex

If you would like an invite to the meeting, contact:

tina.gaines@vita.virginia.gov

VIRGINIA IT AGENCY

MEETING ADJOURNED