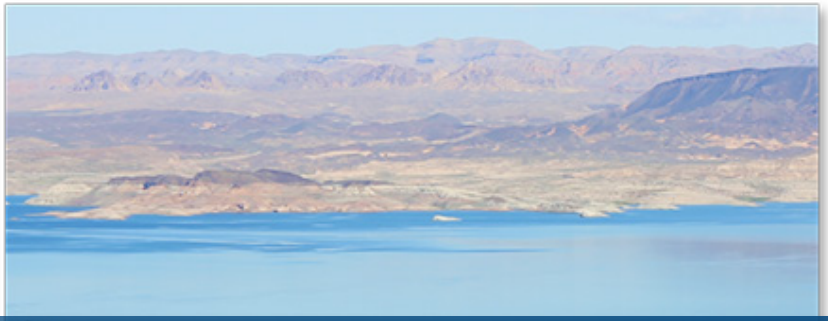


Western Area Power Administration

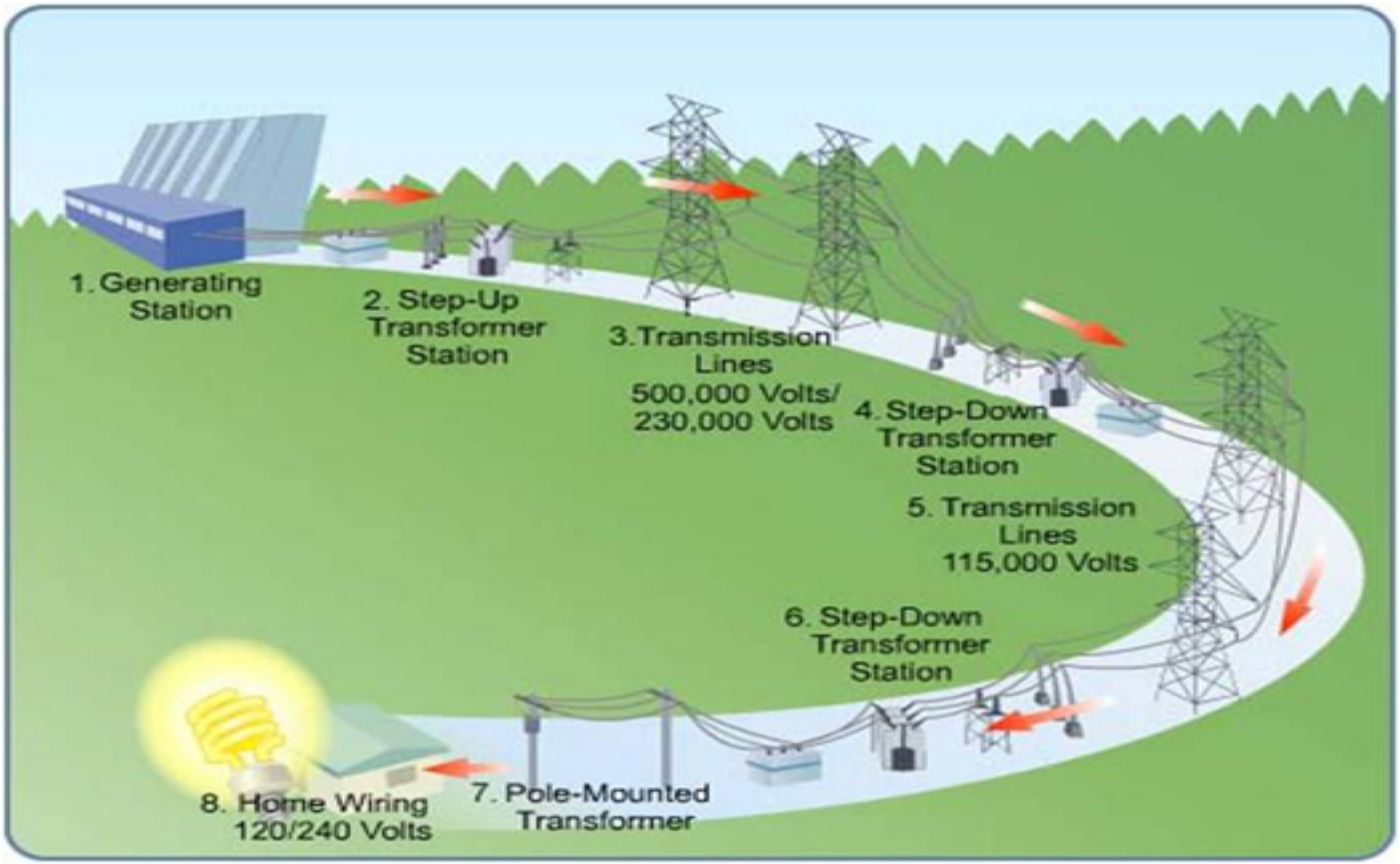
Cyber Security update

Dawn Roth Lindell, Senior Vice President and Chief Information Officer

August 30, 2017

Mountain Plains Intergovernmental Audit Forum

Analyzing cyber risk on the grid



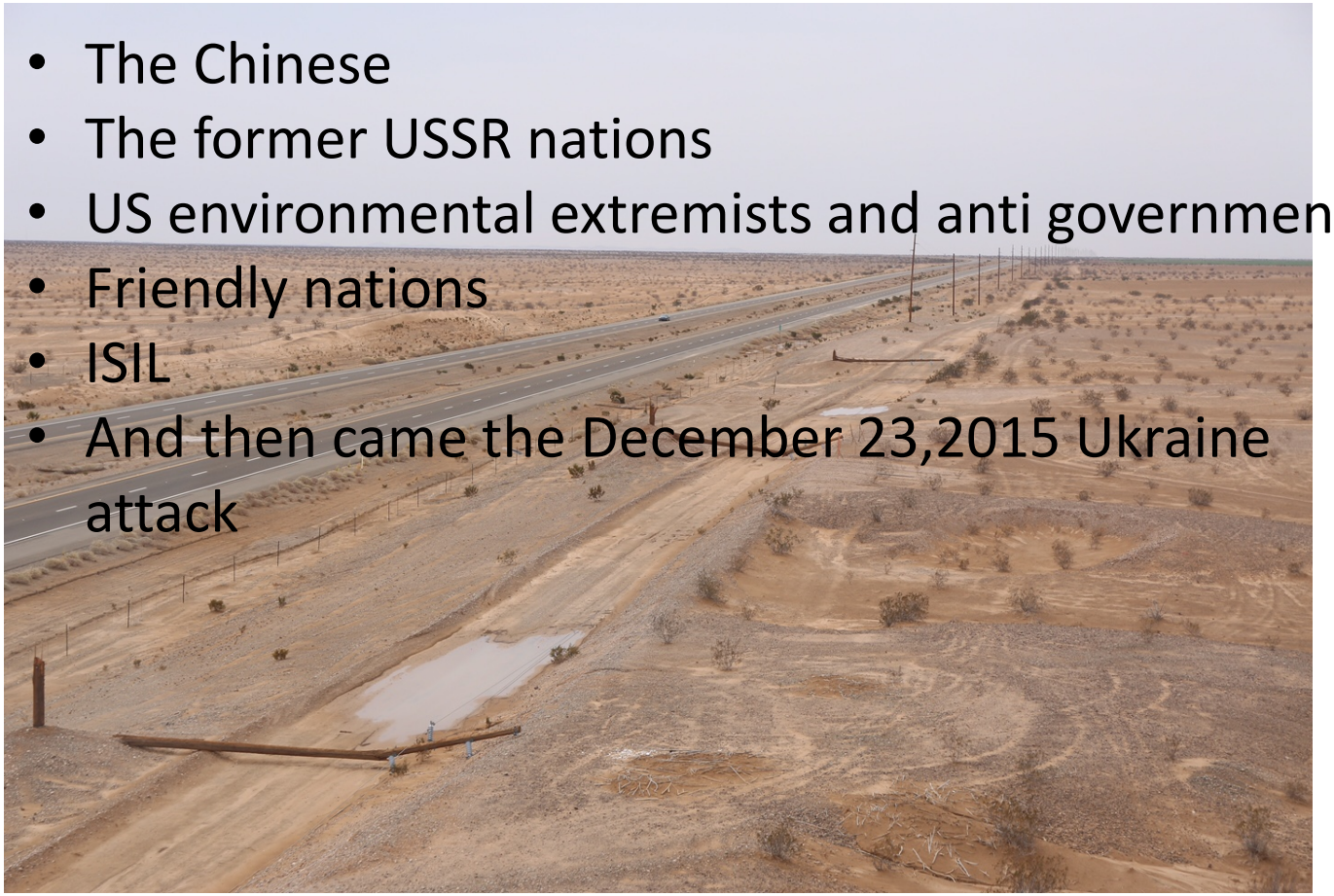
What happens when the power goes out – indefinitely?

But surely “they” can restore the power, right?

Cyber attacks to date have not resulted in large outages

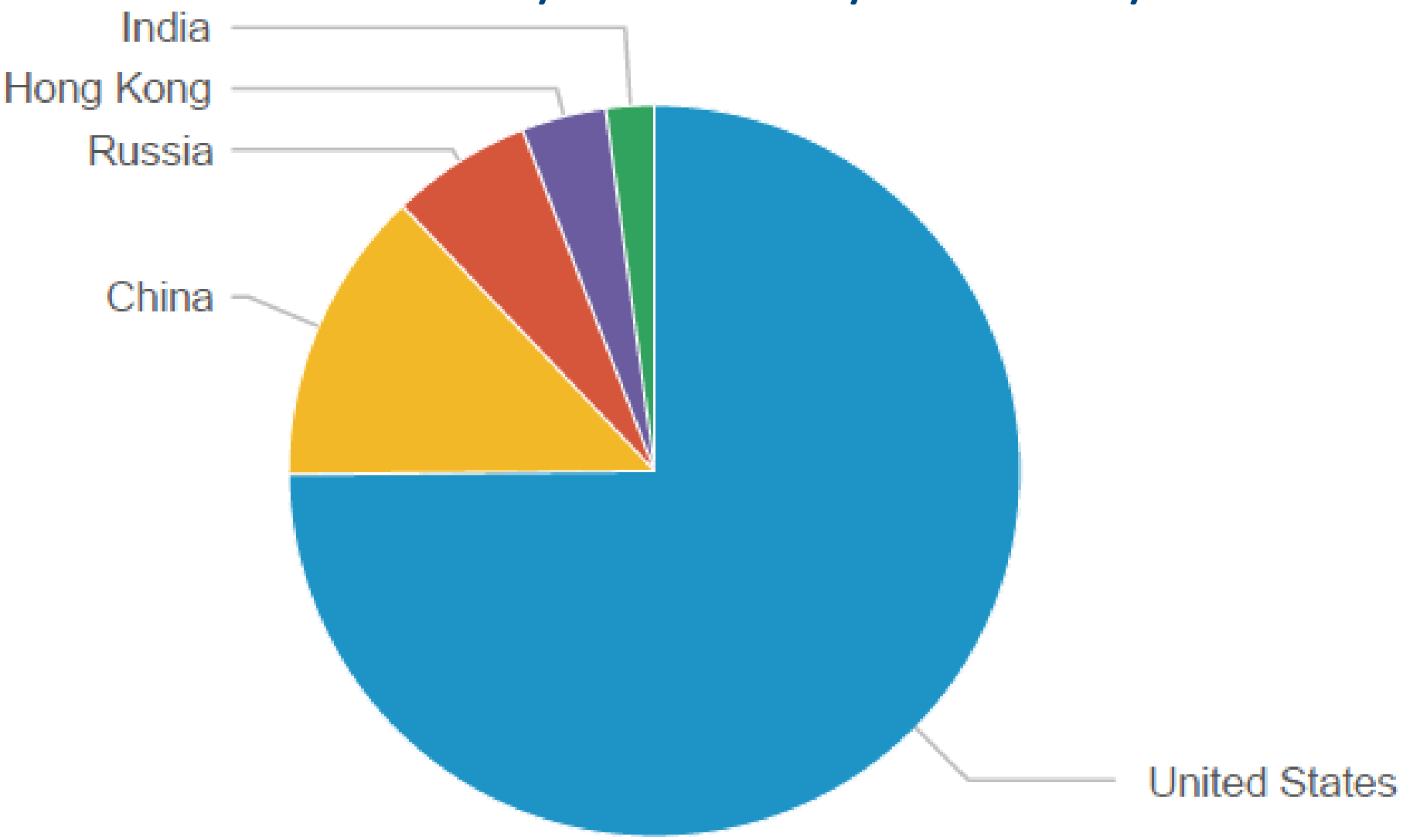
intention

capability

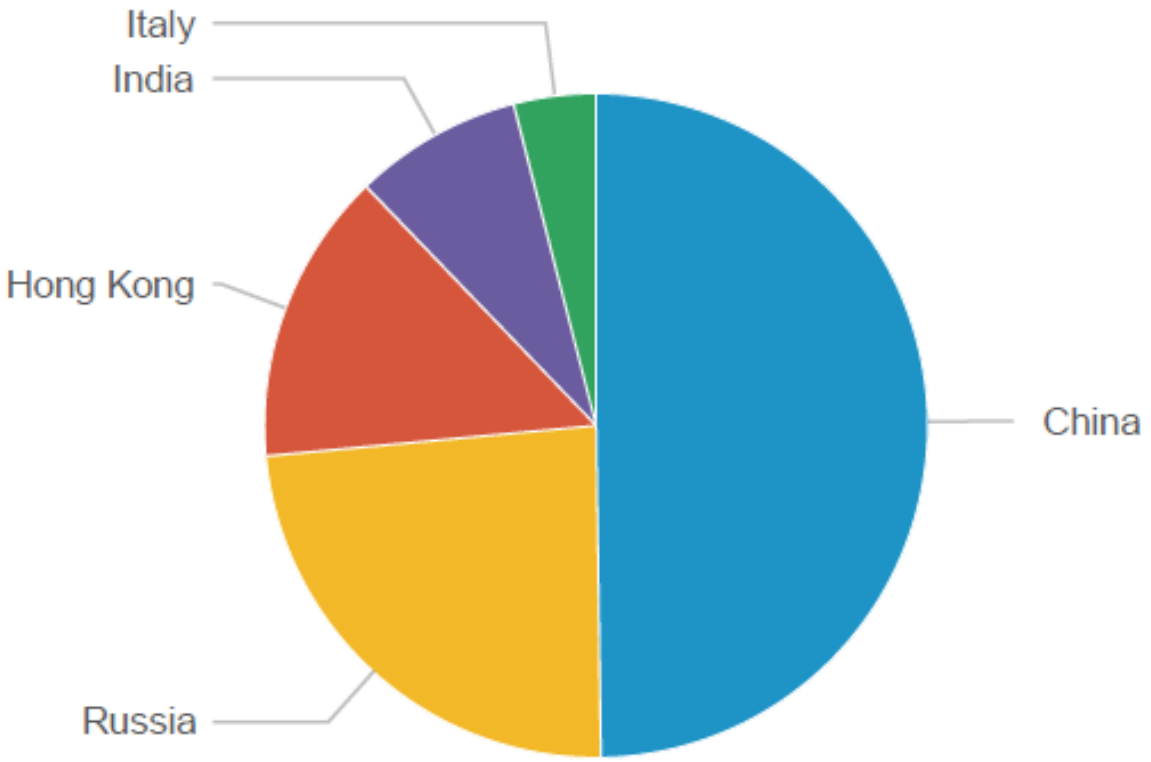


- The Chinese
- The former USSR nations
- US environmental extremists and anti government
- Friendly nations
- ISIL
- And then came the December 23,2015 Ukraine attack

WAPA Blocks by Country for July 2017



WAPA Blocks by Country- July exclude U.S.



Source Geographic Country/Region	Count
United States	1,101,785
China	191,796
Russia	91,501
Hong Kong	54,984
India	31,547
Italy	15,415
United Kingdom	13,494
Vietnam	13,162
Germany	12,393
Republic of Korea	12,264
France	11,823
Canada	10,760
British Virgin Islands	10,445

WannaCry Ransomware, May 12, 2017

- What?
  - Worldwide attack
  - 200,000+ victims in 150 countries
  - Encrypts all data on the system, pay to unlock it

- How?
  - Phishing, visiting infected websites
  - Worm – spread using Eternal Blue, leaked NSA exploit
  - Infected machine scans subnet
  - Sends same malware to all other vulnerable machines

Source: “WannaCrypt Malware Analysis” reported on Blueliv.com on 5/15/2017

WannaCry Ransomware, May 12, 2017

- Who?
  - Perpetrators are likely North Korean
  - Hardest hit – Russia, Taiwan, Ukraine, India
  - Anyone with outdated, unsupported or pirated versions of MS Windows

Source: “WannaCrypt Malware Analysis” reported on Blueliv.com on 5/15/2017

What can we learn? STOP. THINK. Connect.

Four part cybersecurity plan

- Predict – perform exposure analysis
- Prevent – deploy defensive solution to reduce attack surface
- Detect – monitor infrastructure for intrusion, suspicious activity
- Respond – identify how attack happened, impact on system, remediation

Source: “Ransomware made you Wannacry? 10 things the Disaster Taught” by Cigniti.com on 5/21/2017

What can we learn? STOP. THINK. Connect. Audit Controls

1. Vulnerability assessment
   - Completed?
   - On what systems?
   - Report?
   - Programmatic corrections
2. Firewalls
   - Traffic in/out
   - Segmentation
3. Encryption
4. Monitoring

What can we learn? STOP. THINK. Connect.

- Open attachments with extreme caution
- Do not take fake tech support calls
- Use robust anti virus protection
- Keep everything patched and updated
- Clean the system of old stuff
- Dependable back up needed

2016 Key Attacks

- Unnamed Water Utility
  - Discovered during a vulnerability assessment
  - Hacktivist IP address connected to payment system
    - Stole 2.5 million customer records
  - Accessed SCADA
    - Altered water flow & treatment chemical ratio

Security Week, Verizon's Data Breech Digest, "Attackers Alter Water Treatment Systems in Utility Hack: Report", reported in 3/22/16 Security Week by Eduard Kovacs

How?

- Online connection to payment system
  - Exploited a **known** vulnerability
- Poor architecture
  - Same IBM AS/400 for financial & operational tech systems
- Old OT technology
- At least 4 separate connections in prior 60 days

Verizon's Data Breech Digest, "Attackers Alter Water Treatment Systems in Utility Hack: Report", reported in Mar. 22, 2016 Security Week by Eduard Kovacs

2016 Key Attacks

March 24, 2016

- Bowman Avenue Dam in Rye, NY, attacked by Iranians
  - Did not gain control
  - Did gain access to process/network diagrams

Tripwire Site Article, “3 ICS Security Incidents that Rocked 2016 & What We Should Learn from Them”, Oct. 31, 2016, reported by David Bisson

2016 Key Attacks

August 2016

- Operation Ghoul
  - Uncovered by researchers at Kaspersky Lab
  - 130 victims- Navy, other military, aerospace, petrochemical, machine industries
- Spear-phishing campaign targeting industrial organizations in the middle east
  - Email appeared to come from Emirates NBD (a bank)
  - Came with Hawkeye (malware) or with a link
    - ➢Collects keystrokes, clipboard data, other data

Tripwire Site Article, "3 ICS Security Incidents that Rocked 2016 & What We Should Learn from Them", Oct. 31, 2016, reported by David Bisson

How?

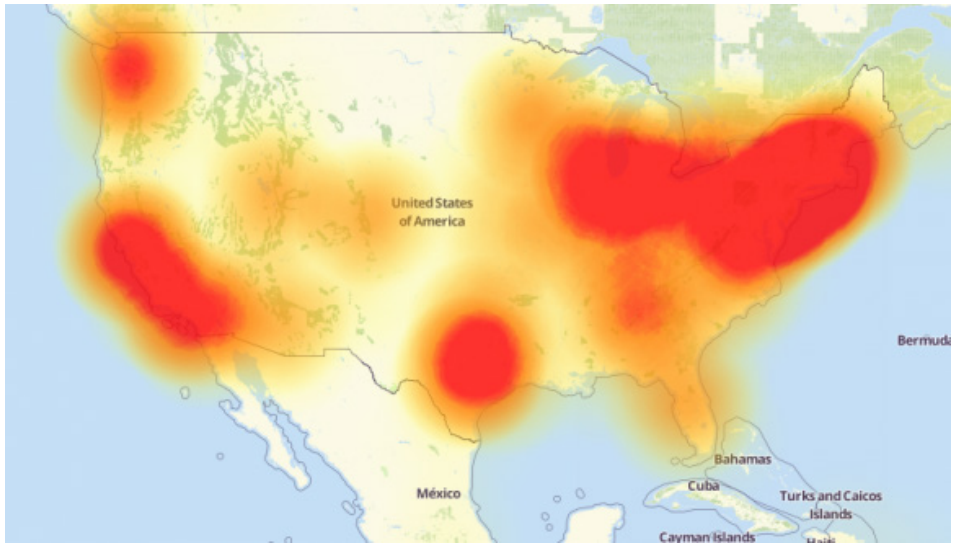
- Exploit the human – spear phishing
- Commercial off the shelf malware

Tripwire Site Article, “3 ICS Security Incidents that Rocked 2016 & What We Should Learn from Them”, Oct. 31, 2016, reported by David Bisson

2016 Key Attacks

October 21, 2016

- Attack on Dyn- Internet infrastructure company
- Provides critical tech services to Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix among others
- DDOS
- Mirai Malware



Krebs on Security, “Hacked Cameras, DVRs Powered Today’s Massive Internet Outage”, October 21, 2016, by Brian Krebs

How?

Mirai Malware via the internet

- Creator released source code
- Looks for IoT with factory default usernames/passwords
  - DVR's
  - Cameras- especially with components from XiongMai Technologies
  - Password is hardcoded into the firmware- web credentials
- Gains access, uploads DDOS flood

Krebs on Security, "Hacked Cameras, DVRs Powered Today's Massive Internet Outage", October 21, 2016, by Brian Krebs

How?

Researchers at Flashpoint scanned the internet on

Oct 6, 2016

- Found 515,000+ instances with the vulnerability
- Backdoor to network

WAPA: 37 cameras with the default passwords

Krebs on Security, “Hacked Cameras, DVRs Powered Today’s Massive Internet Outage”, October 21, 2016, by Brian Krebs

2016 Key Attacks

December 18, 2016

- Ukraine outage or UkrEnegro “North” substation
  - Removed 1/5 of Kiev’s energy
  - 75 minute outage

- Note: in Nov, Dec 2016, 6500 Russian attempts on Ukrainian State Institutions per Ukrainian President

Washington Post, “Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say”, Dec. 31, 2016. Alice Crites, Carol Morello and Ellen Nakashima contributed to this report, also By Juliet Eilperin and Adam Entous

How?

- Initial assessment points to cyber attack
  - SCADA logs show “close” then “open” commands to breakers
  - Ukraine blames Russia

Washington Post, “Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say”, Dec. 31, 2016. Alice Crites, Carol Morello and Ellen Nakashima contributed to this report, also By Juliet Eilperin and Adam Entous

2017 Petya/Netya attack

- Occurred June 27, 2017 in the Ukraine
  - Banks, ministries, newspapers, electricity firms
  - Also hit France, Germany, Italy, Poland, Russia, U.K., U.S., Australia
- Threat vector
  - Originated from an update to a Ukrainian tax accounting package called MeDoc
  - Used by 90% of Ukrainian domestic firms
  - Via Eternal Blue exploit in older, unpatched MS Windows

Wikipedia, “2017 Cyber Attack on Ukraine”, Wikipedia Foundation Inc.

2017 Petya/Netya attack

- Impact:
  - Petya encrypts Master File Table
  - Requires $300 bitcoin to “unlock”
  - Promulgates to other computers on network – including remote login
  - Netya (NotPetya) encrypts additional files
  - Netya intercepts passwords and allows admin functions
    - Wipes hard drives
- Attribution: Security Service of Ukraine (USB) identifies Russia – same attacker as Dec 2016

Wikipedia, “2017 Cyber Attack on Ukraine”, Wikipedia Foundation Inc.

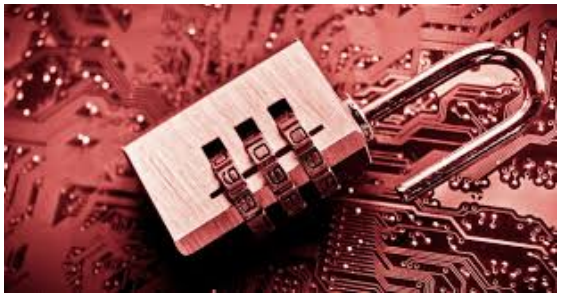
2017 The Fish Tank Hack

- North American casino
- Internet connected fish tank
  - Sensors for temperature, food, cleanliness
- Hackers accessed fish tank, then network
  - Sent out data
- Internet of things creates new risks

Washington Post, “How a fish tank helped hack a casino”, by Alex Schiffer

ICS Vulnerability Analyses

- Fire Eye Analysis, Jan 2000 – April 2016
- 123 vendors affected by vulnerability disclosures
  - 90% between 2011 – 2015
- 1,552 separate vulnerabilities



33% <u>still not</u> patched

Fire Eye, "Sight Intelligence 2016 ICS Vulnerabilities report, Overload: Critical Lessons from 15 Years of ICS Vulnerabilities" by Sean McBride, Jeffrey Ashcraft, & Nathan Belk

ICS Vulnerabilities

- Study by Positive Research Center, October 2015
- 146,136 ICS components web accessible
- Found 691 vulnerabilities in ICS components
  - 58% high severity
  - 39% medium severity
- By Vendor:
  - Siemens – 124
  - Schneider Electric – 96
  - Advantech – 51
  - GE - 31

So how do we tackle these issues?

First: SANS Top 20, #1, #2

- Inventory hardware
- Inventory software

IT and OT have the same cyber security needs.

So how do we tackle these issues?

Challenges:

- Collaboration required- mutual respect is critical
- Our OT technology is shockingly old
  - Identify first
  - Prioritize based on impact, simplicity of exploit, patchable?
- Embedded tech
  - Asset list
  - Actually embedded

- ICS vendors have been slow- we must **push**!

So how do we tackle these issues?

- Threat Intelligence is a must
  - APPA
  - LPPC
  - E- ISAC
  - Vendor service
  - WAPA pilot
  - FBI Infraguard

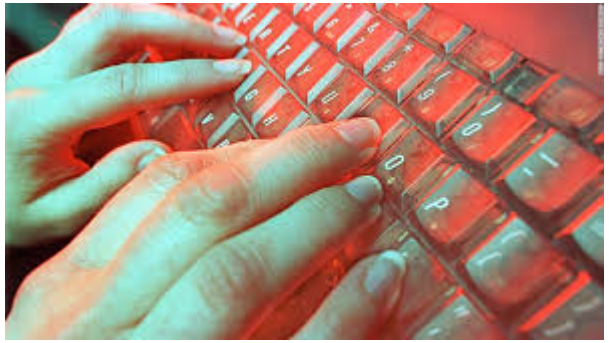
- Need analysis continuously
- Must address across industries
- Must share- there is NO shame

So how do we tackle these issues?

- Segment network
- WAPA: Secure Enclave Support Center for substations
  - Network considerations
  - Prioritize based on CIP

- Of course- separate business from SCADA network
  - Enforce this
  - Educate field folks
  - Data transfer

So how do we tackle these issues?



- Complete vulnerability assessment
  - WAPA results of our red team
  - Only way to truly know where your risk is
    - Physical
    - Cyber
  - Visibility to Internet
    - WAPA
      - old blog site
      - video conferencing equipment

So how do we tackle these issues?

- Inadvertent insider
  - Anti phishing campaigns
  - WAPA Results

Campaign	Sent	Users who clicked	Users who completed training
1	33	0	N/A
2	59	11	4
3	58	18	6
4	184	37	8

We, in this industry, must recognize we are:

- Vulnerable
- Under attack
- At risk
- Responsible to harden our assets
- In need of rapid information sharing

Questions?