# Coast Guard's commitment to Cyber  Resiliency

"The Coast Guard has authorities, capabilities, proficiencies, and a long history in leading responses to maritime disasters and incidents.

The Service's ability to operate within and bridge  between military, federal, state, local, and private sector response systems makes the Coast Guard an indispensable asset for ensuring national **resilience** in the maritime domain."

*– Commandant's Strategic Intent 2015-2019 June 2015*

## Cyber Resilience is all about managing security through a multi-layered approach that encompasses People, Processes, and Technology.

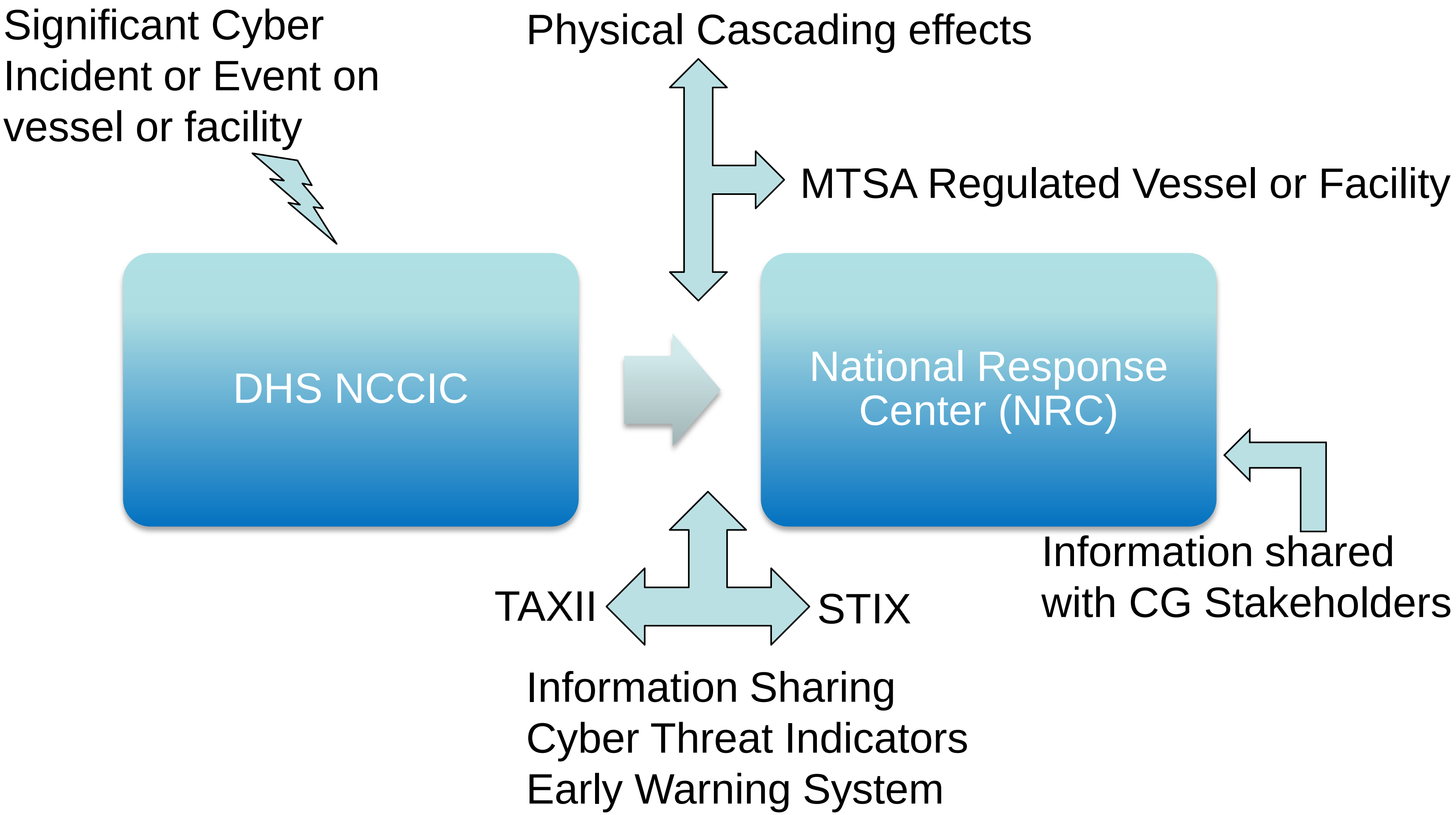
- Every organization should have a Cyber resilience Blueprint in order to adequately Respond and Recover from a major Cyber incident
- **Conduct as Asset Inventory**
  - Without an asset inventory, you cannot apply Cyber Risk Management in your organization
- **Develop and Test Incident Response Plans**
  - Many organizations have them, but very few run them
  - Backup data sets must be tested for reliability
- **Train and empower your employees**
  - Cyber Readiness and Resiliency Demands a focus on People
  - Cyber security MUST become the Social Norm inside the business

# Cyber Resiliency in the Marine Transportation System (MTS)

- **Cyber Resilience is being able to prepare for, withstand, rapidly recover, and learn from deliberate or accidental attacks in the Cyber domain.**

- **Identify all MTS Critical Infrastructure and Key Resources**
- **Address Supply Chain and Intermodal linkages**
  - Supply Chain Priorities (think NIST 1.1 update)
  - MTS Infrastructure linkages
  - Intermodal Transportation linkages
  - Critical Infrastructure Dependencies & Interdependencies & Cascading Effects (Physical and Cyber)
- **Understanding Economic Risks and Setbacks to Global Economy**
- **Operational & Business Continuity (Loss of business revenue)**

# Cyber Incident Reporting Process



Significant Cyber Incident or Event on vessel or facility

Physical Cascading effects

MTSA Regulated Vessel or Facility

DHS NCCIC

National Response Center (NRC)

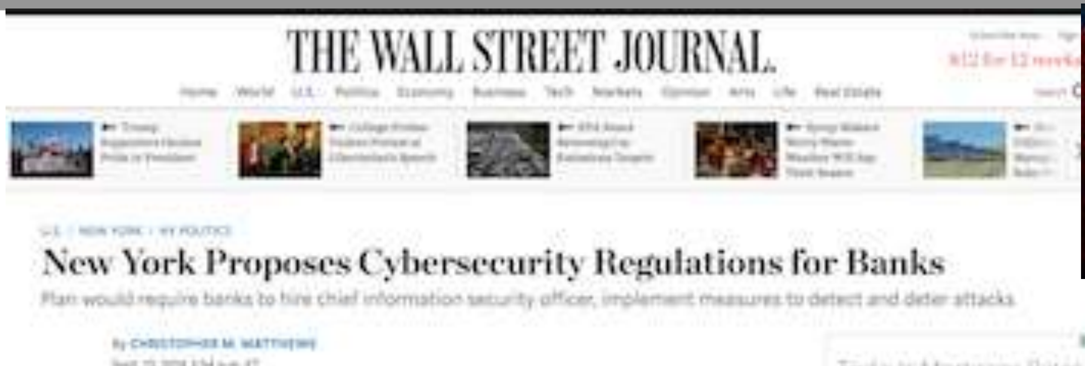
TAXII

STIX

Information shared with CG Stakeholders

Information Sharing
Cyber Threat Indicators
Early Warning System

# Top Trending Items in the Cyber World



THE WALL STREET JOURNAL.

$12 for 12 weeks

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

U.S. / NEW YORK / NY POLITICS

New York Proposes Cybersecurity Regulations for Banks

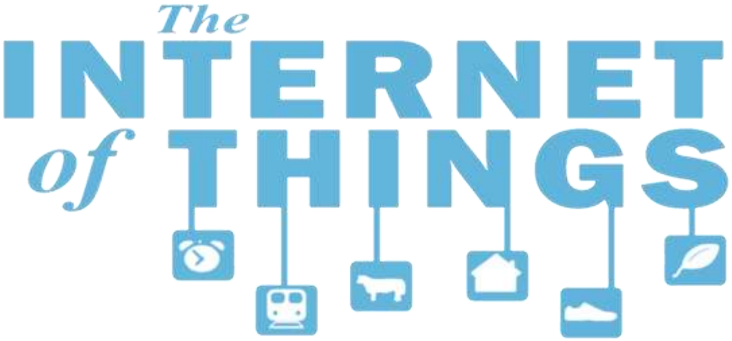
Plan would require banks to hire chief information security officer, implement measures to detect and deter attacks

By CHRISTOPHER M. MATTHEWS

New York Gov. Andrew Cuomo and the state's top ba

Tuesday that would be among the first in the U.S. to r

cybersecurity programs.



1. Ransomware
2. Elaborate Phishing Campaigns
3. Internet of Things (IoT)
4. Cybersecurity Insurance
5. Consideration of Mandatory Cybersecurity standards in Maritime

# The Art of Ransomware…Why the Popularity?

**Def:**
**Ransomware is about denying you access to your data via encryption.**

- Fastest-growing Cybercrime epidemic in the world
- Proliferation of point and click tools are making extortion easy for anyone

Value of the encrypted data relies on 2 functions:

1. Intrinsic value of the data (irrespective of how many copies exist)

2. Extent of operations lost or disruptions in life or business

-The data does not have to be private, It just needs to be VALUABLE

-If there are no backups of the data, the value of the data skyrockets

# The Art of Ransomware…Cont.

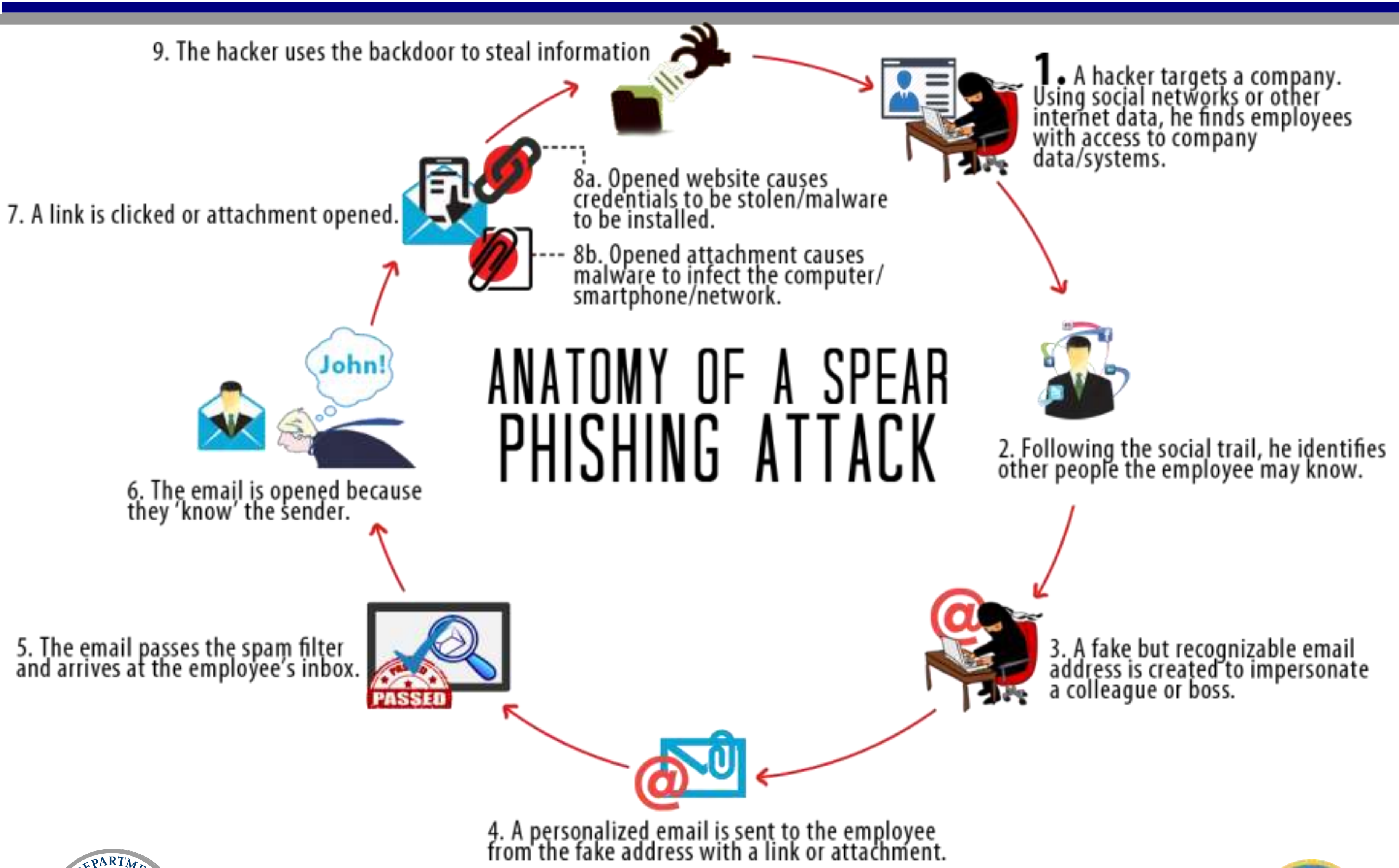
**The threat of release causes concern with:**

- Company trade secrets
- Human Resource (HR) sensitive information
- Consumer private data (think Supply Chain)
- Data about customers (Credit cards stored)
- Reputation as a company

https://www.youtube.com/watch?v=5WJ2KHoo5Fo

NOTE: Recent studies by the Gartner indicate that over 50 percent of Ransomware victims PAY the fee for their data to be restored!!

# Lets Go Phishing!!



## ANATOMY OF A SPEAR PHISHING ATTACK

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

6. The email is opened because they 'know' the sender.

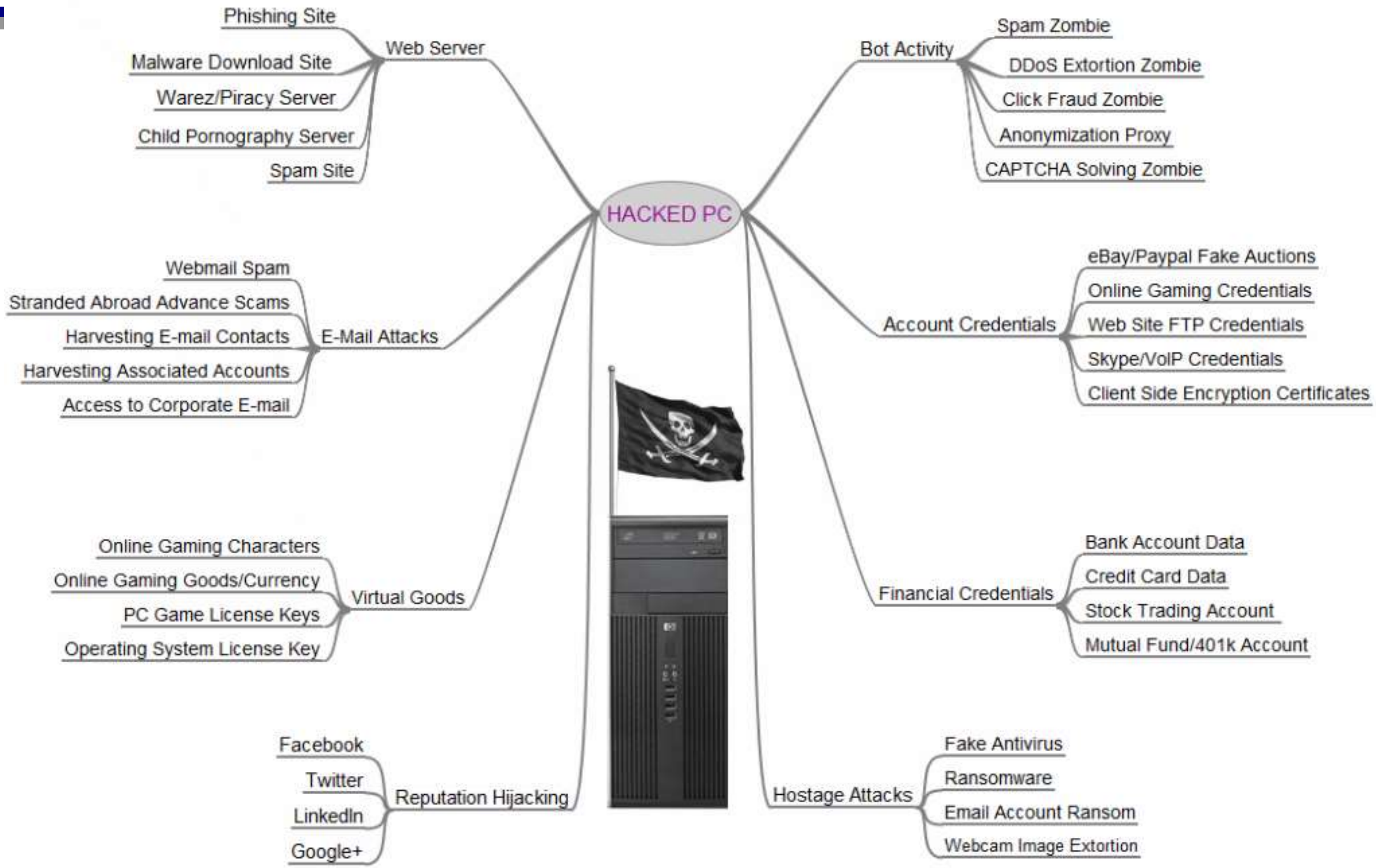
7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/ smartphone/network.

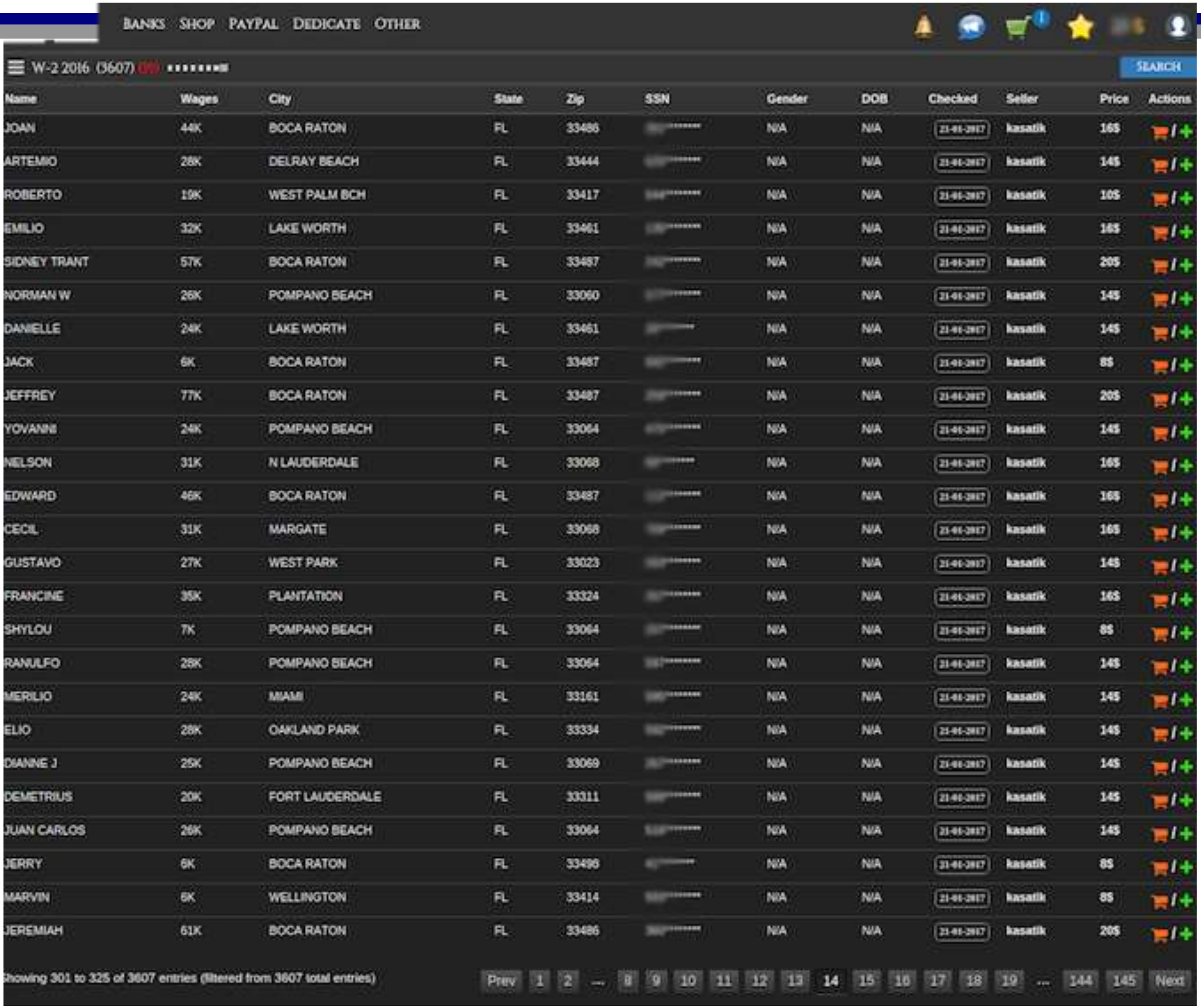
9. The hacker uses the backdoor to steal information

# Phishing…Cont



- HACKED PC
  - Web Server
    - Phishing Site
    - Malware Download Site
    - Warez/Piracy Server
    - Child Pornography Server
    - Spam Site
  - Bot Activity
    - Spam Zombie
    - DDoS Extortion Zombie
    - Click Fraud Zombie
    - Anonymization Proxy
    - CAPTCHA Solving Zombie
  - E-Mail Attacks
    - Webmail Spam
    - Stranded Abroad Advance Scams
    - Harvesting E-mail Contacts
    - Harvesting Associated Accounts
    - Access to Corporate E-mail
  - Account Credentials
    - eBay/Paypal Fake Auctions
    - Online Gaming Credentials
    - Web Site FTP Credentials
    - Skype/VoIP Credentials
    - Client Side Encryption Certificates
  - Virtual Goods
    - Online Gaming Characters
    - Online Gaming Goods/Currency
    - PC Game License Keys
    - Operating System License Key
  - Financial Credentials
    - Bank Account Data
    - Credit Card Data
    - Stock Trading Account
    - Mutual Fund/401k Account
  - Reputation Hijacking
    - Facebook
    - Twitter
    - LinkedIn
    - Google+
  - Hostage Attacks
    - Fake Antivirus
    - Ransomware
    - Email Account Ransom
    - Webcam Image Extortion

# Phishing…Cont.



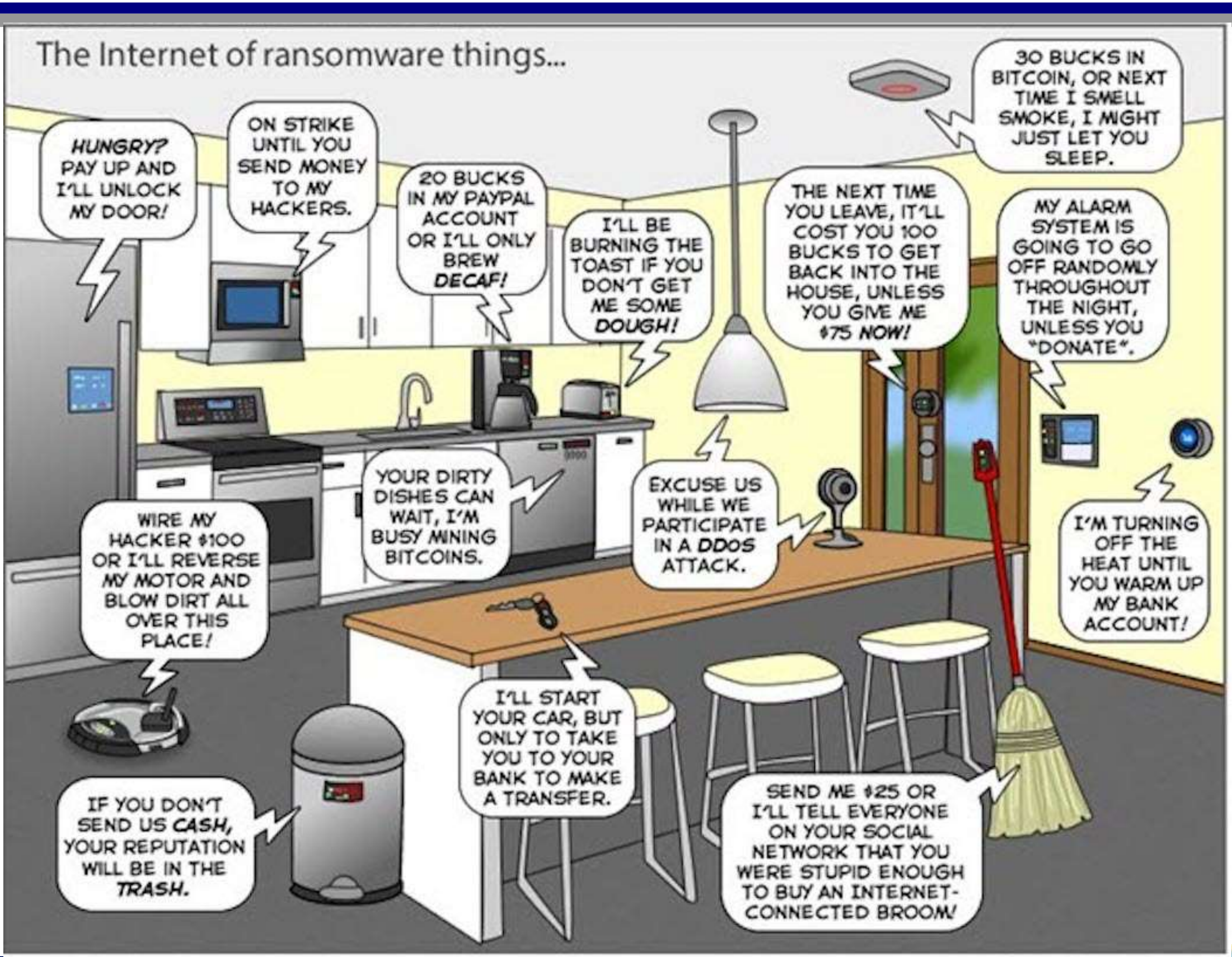
W-2 2016 (3607)

| Name | Wages | City | State | Zip | SSN | Gender | DOB | Checked | Seller | Price | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| JOAN | 44K | BOCA RATON | FL | 33486 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 16$ | 🛒 / + |
| ARTEMIO | 28K | DELRAY BEACH | FL | 33444 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| ROBERTO | 19K | WEST PALM BCH | FL | 33417 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 10$ | 🛒 / + |
| EMILIO | 32K | LAKE WORTH | FL | 33461 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 16$ | 🛒 / + |
| SIDNEY TRANT | 57K | BOCA RATON | FL | 33487 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 20$ | 🛒 / + |
| NORMAN W | 26K | POMPANO BEACH | FL | 33060 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| DANIELLE | 24K | LAKE WORTH | FL | 33461 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| JACK | 6K | BOCA RATON | FL | 33487 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 8$ | 🛒 / + |
| JEFFREY | 77K | BOCA RATON | FL | 33487 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 20$ | 🛒 / + |
| YOVANNI | 24K | POMPANO BEACH | FL | 33064 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| NELSON | 31K | N LAUDERDALE | FL | 33068 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 16$ | 🛒 / + |
| EDWARD | 46K | BOCA RATON | FL | 33487 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 16$ | 🛒 / + |
| CECIL | 31K | MARGATE | FL | 33068 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 16$ | 🛒 / + |
| GUSTAVO | 27K | WEST PARK | FL | 33023 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| FRANCINE | 35K | PLANTATION | FL | 33324 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 16$ | 🛒 / + |
| SHYLOU | 7K | POMPANO BEACH | FL | 33064 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 8$ | 🛒 / + |
| RANULFO | 28K | POMPANO BEACH | FL | 33064 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| MERILIO | 24K | MIAMI | FL | 33161 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| ELIO | 28K | OAKLAND PARK | FL | 33334 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| DIANNE J | 25K | POMPANO BEACH | FL | 33069 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| DEMETRIUS | 20K | FORT LAUDERDALE | FL | 33311 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| JUAN CARLOS | 26K | POMPANO BEACH | FL | 33064 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 14$ | 🛒 / + |
| JERRY | 6K | BOCA RATON | FL | 33496 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 8$ | 🛒 / + |
| MARVIN | 6K | WELLINGTON | FL | 33414 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 8$ | 🛒 / + |
| JEREMIAH | 61K | BOCA RATON | FL | 33486 | [redacted] | N/A | N/A | 21-01-2017 | kasatik | 20$ | 🛒 / + |

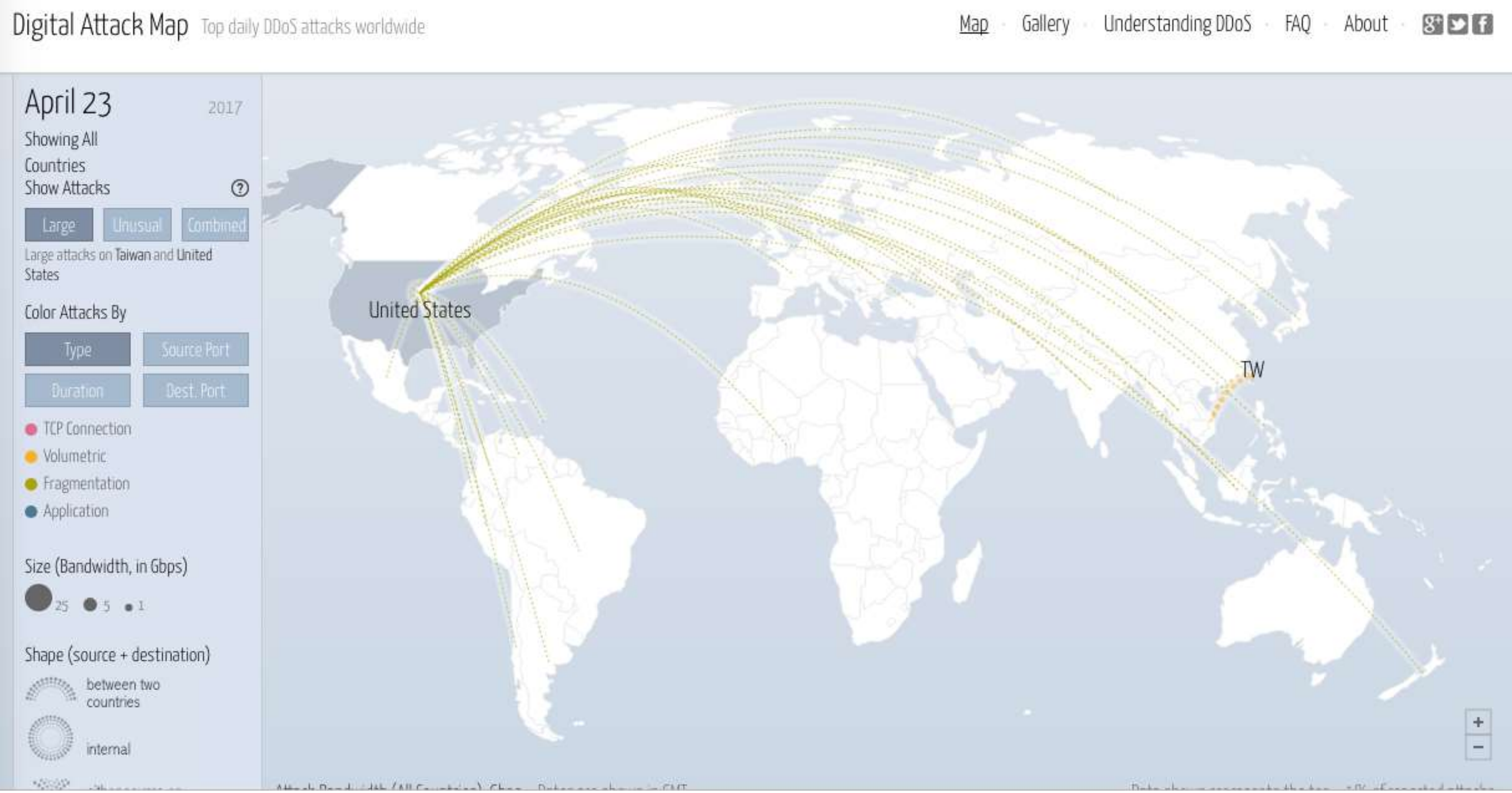
Showing 301 to 325 of 3607 entries (filtered from 3607 total entries)

Prev 1 2 ... 8 9 10 11 12 13 14 15 16 17 18 19 ... 144 145 Next

# The Internet of Things (IoT)


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.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
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!

# The Barrage of Attacks (IoT Devices)



Large attacks on Taiwan and United States

# Cybersecurity Insurance – Friend or Foe?

● Cyber insurance premiums are expected to grow from $2 billion in 2015 to an estimated $20 billion or more by 2025.

● Rates are growing astronomically for this line of business and really for good reason," said Jim Rice, senior business development executive at Uber. The potential is high for a widespread cyber event and underwriters are taking notice.

● Market immaturity and industry **lack of standardization** are two reasons why underwriting cyber products today make it challenging to be in the insurance world, says Timothy Zeilman, vice president of Hartford Steam Boiler.

● Exposures are technology based, but they're also human behavior based, Zeilman said. "Unlike most other kinds of insurance, you're not insuring against something that exists in nature. You're insuring primarily against criminal behavior by other human beings." And that can be risky.

# Maritime Cybersecurity Standards

## Some things to consider…

On Oct. 19, 2016, the Board of Governors of the Federal Reserve System (“Federal Reserve”), the Office of the Comptroller of the Currency (“OCC”) and the Federal Deposit Insurance Corporation (“FDIC,” collectively the “Agencies”) issued a joint advance notice of proposed rulemaking (“Notice”) inviting public comment on cybersecurity regulations and guidance designed to improve the safety and soundness of the U.S. financial system.

**Questions to ask…**

● Is there an appetite for a mandatory Maritime Cyber Framework?

● Will a major Cyber incident with physical cascading efforts be a precursor to consider a baseline Cyber standard to meet?

● Should there be an in-depth analysis to determine whether legislative updates are necessary to make progress in Maritime Cybersecurity?

# Future Coast Guard Efforts

- Cyber Risk Management (CYBER NVIC)
- Policy and Risk Development (NIST Profiles)
- Cyber Exercise Guidance, planning and standardization with AMSC’s
- Industrial Control Systems in the Maritime Domain
- Cyber Risk for Vessels and Waterfront Facilities (Vulnerabilities and Consequences)
- Research the IT/OT Convergence in the Maritime

# QUESTIONS?

Thank You for your time!

Further inquiries:

**Mr. Jason Warren**

CISSP, ITIL, CE|H, MCSE, CCNP, A+, Security+

Jason.s.warren@uscg.mil

202-372-1106