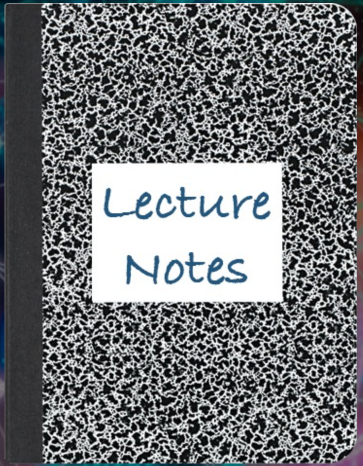
CS 419: Computer Security

Week 1: Part 3

Internet-Enabled Threats



Paul Krzyzanowski

The Internet Introduces Risks

> “The internet was designed to be open, transparent, and interoperable. Security and identity management were secondary objectives in system design. This lower emphasis on security in the internet’s initial design not only gives attackers a built-in advantage. It can also make intrusions difficult to attribute, especially in real time. This structural property of the current architecture of cyberspace means that we cannot rely on the threat of retaliation alone to deter potential attackers. Some adversaries might gamble that they could attack us and escape detection.”

– William J. Lynn III, Deputy Defense Secretary, 2010

http://archive.defense.gov/speeches/speech.aspx?speechid=1593

The Internet Makes It Easier To Attack

- **Security was not a design consideration**
  - This is not a bug but a design decision
- **Intelligence is at the edges of the network – distributed among many players**
  - Reliability, authentication, authorization, encryption, congestion notification, and quality of service are the responsibility of endpoints
- **Access and routing are not centrally managed**
  - Routing decisions distributed
  - DNS (domain name system) service is distributed too
  - No access control: any system can be added to the Internet
- **Bad actors can hide!**

How the Internet Creates Vulnerabilities

- **Action at a distance**
- **Asymmetric force**
- **Actors can be anonymous**
- **No borders or checkpoints**
  - Most countries do not control the flow of data to/from their country and rely on ISPs to enforce any policies
  - Exceptions include China, North Korea, Turkey, UAE, Iran, Egypt, and Vietnam
- **No distinction**
  - Hard to distinguish valid data from attacks
  - Can’t tell what code will be harmful until it’s executed

Action at a Distance

People can now be beyond our control or visibility.

Asymmetric Force

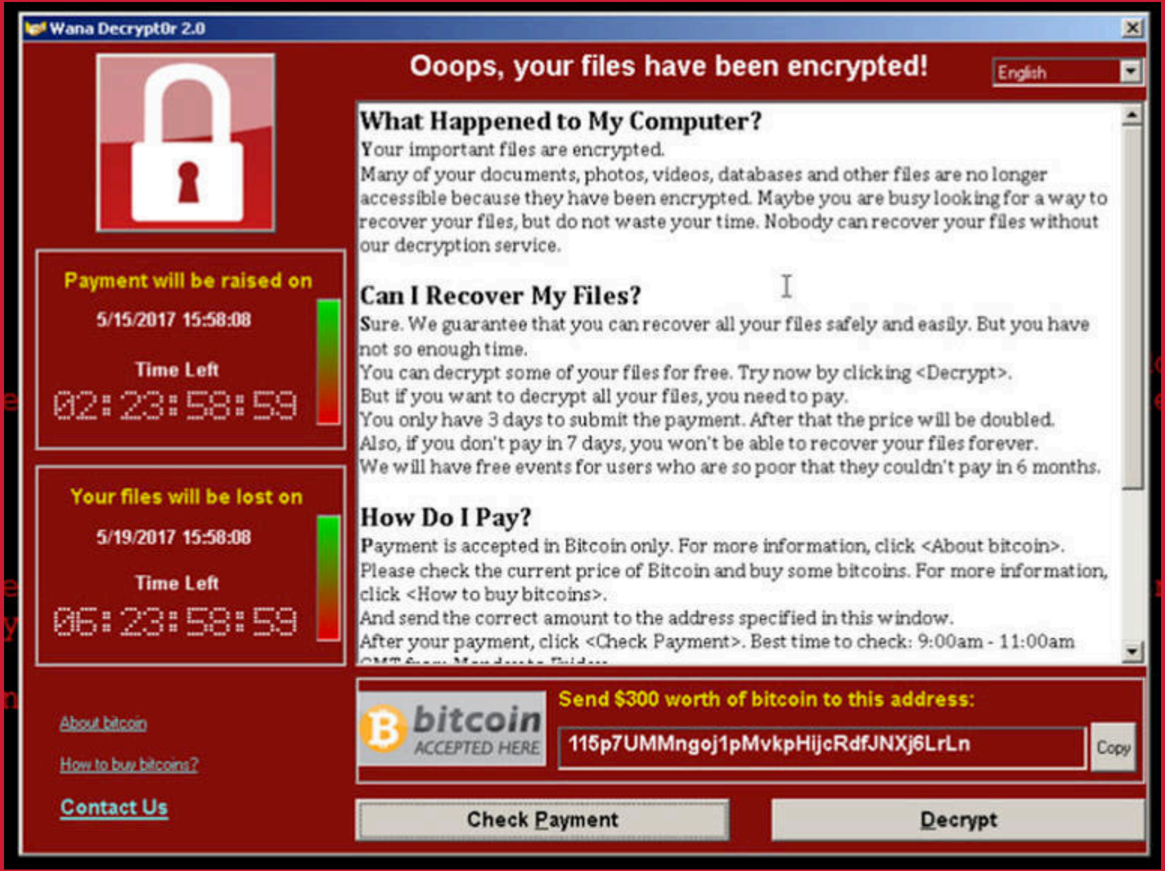
> Information Technology has "opened up a whole new asymmetry in future warfare"
>
> – *William J. Lynn III, Deputy Defense Secretary, 2010*

- Pentagon's 15,000 networks and 7+ million computers are being probed thousands of times daily
- Traditional deterrence models of retaliation do not apply in cyberspace

Asymmetric Force

- Actors can project or harness greater force. Low barriers to entry. Offense can be more effective than defense. A small number of actors can have a large effect.
- E.g., The Anonymous hacking group that tries to take down corporations or governments, people who send fraud or spam email, or those who send Facebook requests for money.
- Sending millions of messages costs almost nothing.
- Distributed Denial of Service (DDoS) attacks allow rogue actors to overwhelm large companies and nation states
  - Small countries can now inflict damage on countries like the US or China.

WannaCry Ransomware



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:58:59

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:58:59

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

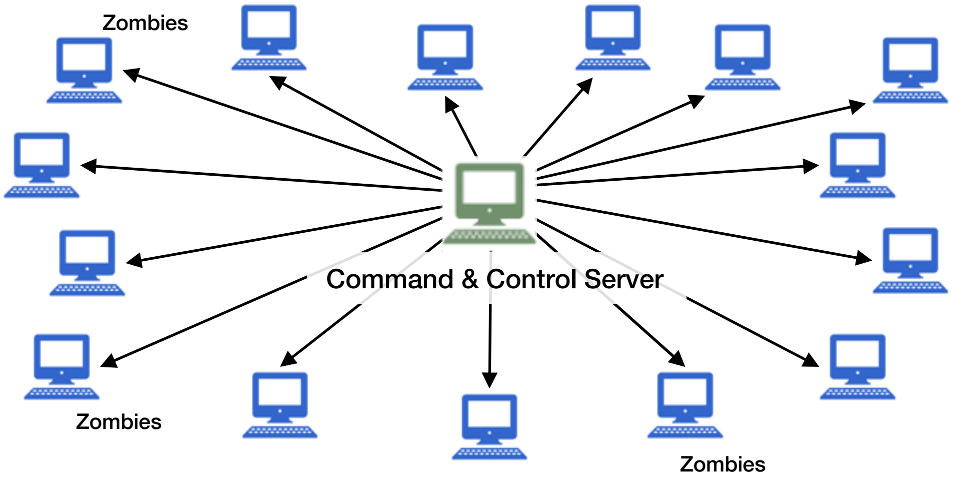
Botnets

Botnet: collection of computers owned by innocent people but infected with malicious software

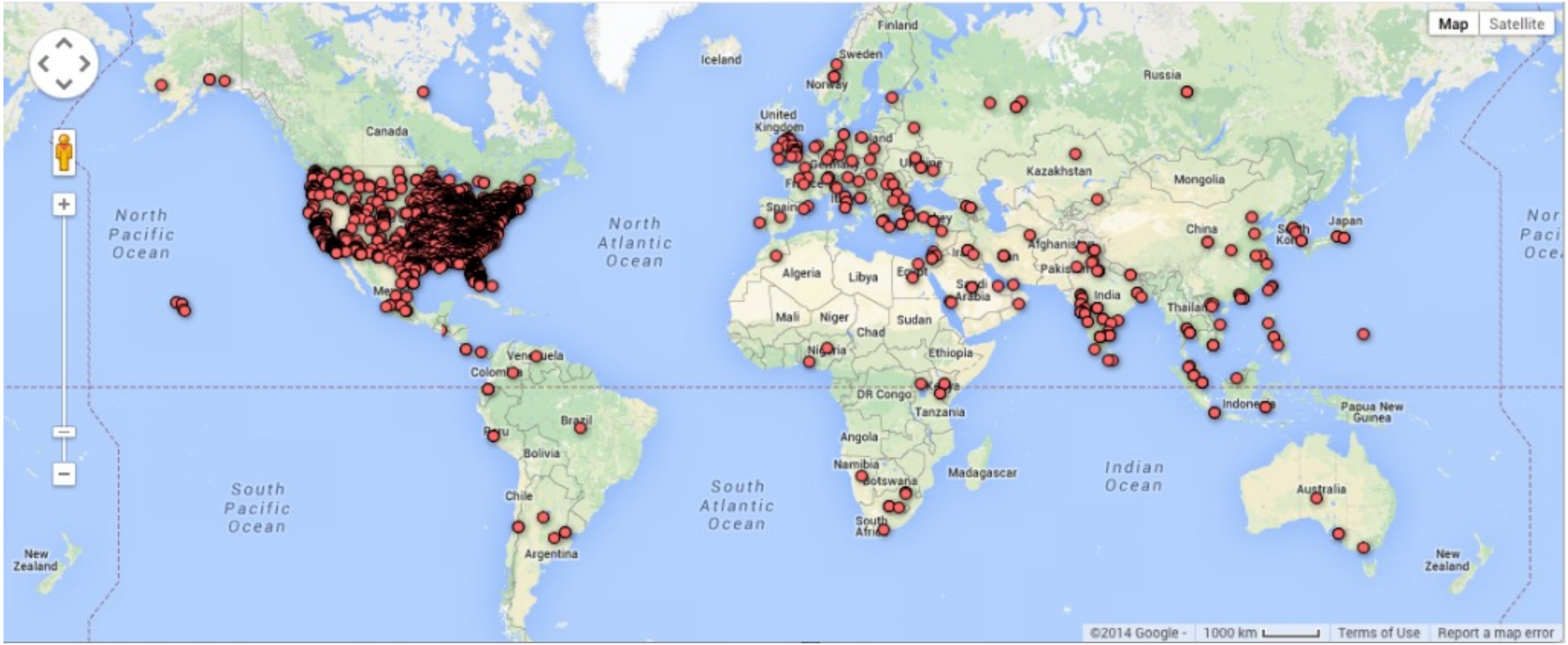
- Botnet software periodically contacts a command & control server for directions on what additional software to download and what to run and whom to attack

Three common uses are:

1. Distributed Denial of Service (DDoS) attacks
   - One company has only so many servers
   - Send too much traffic to the servers and the server gets overloaded
   - Now nobody can get through – even legitimate traffic
   - Data is not destroyed but service is disrupted
   - Attacks come from the network of zombies
2. Spamming/phishing
   - Send tens of millions of malicious emails or texts
3. Cryptocurrency mining
   - Use the computing power of the zombies



Zeus Botnet



https://news.softpedia.com/news/New-Gameover-Zeus-Botnet-Forming-the-US-Sees-Most-Infections-455112.shtml

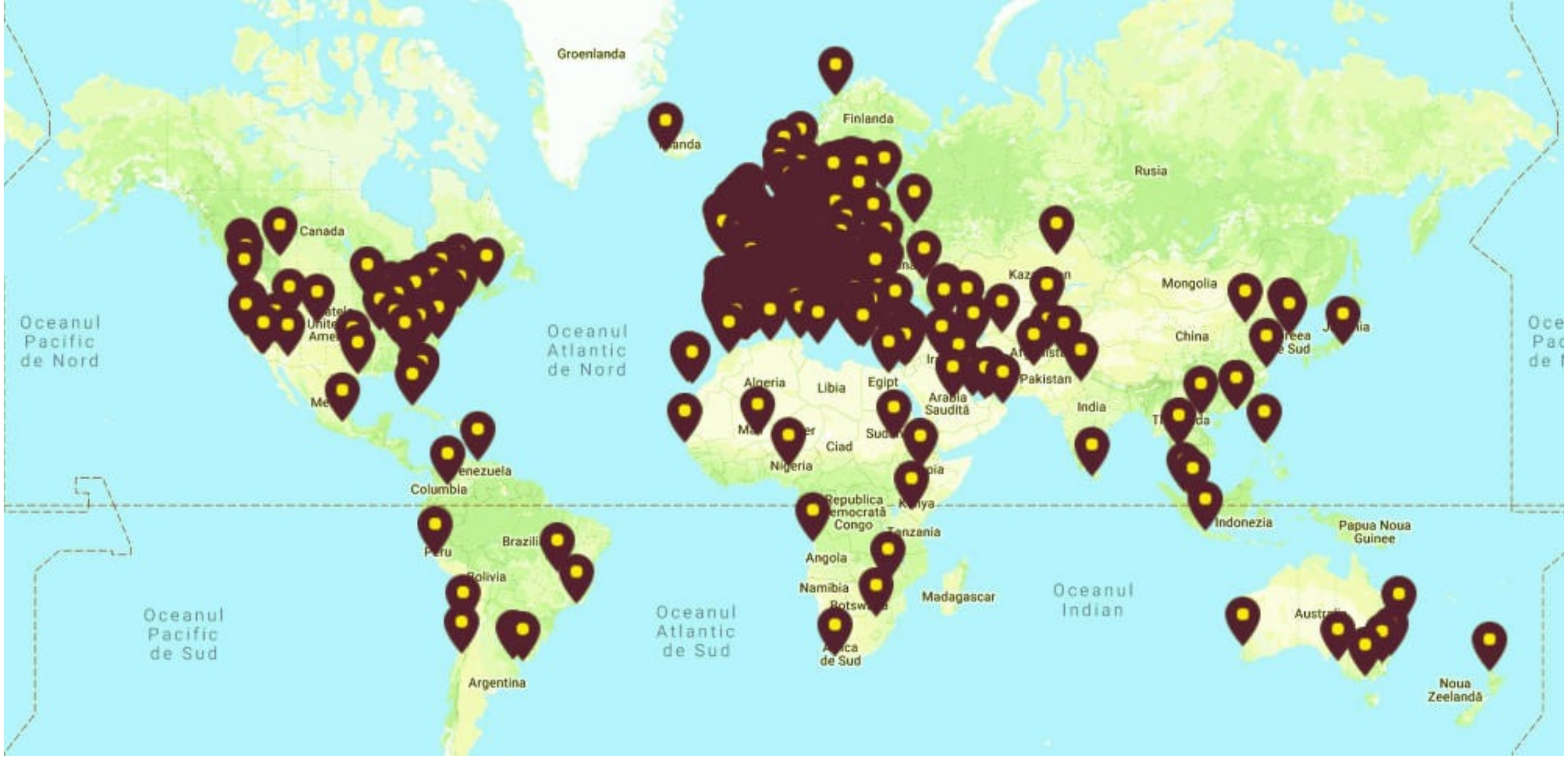
Mēris Botnet – 2021 - present

- Exploited a 2018 bug in routers from Latvian vendor MikroTik
  - Winbox, a management component and a Windows GUI application for MikroTik's RouterOS
  - Allowed attackers to write files in the router, reconfiguring it for remote access
  - Only 30% of routers were had a patch applied
- Estimated 250,000 MikroTik routers were hacked
- The Meris botnet broke the record for the largest volumetric DDoS attack twice in 2021
- Attacks
  - Targets 50 different websites every single day with a daily average of 104 unique DDoS attacks
  - Top targets are banking, financial services, and insurance companies
  - 21.8 million RPS (requests per second) attack at a Russian bank hosting infrastructure on Yandex servers
  - 33%+ of attack traffic targeted China-based sites

https://blog.cloudflare.com/meris-botnet

https://cybernews.com/security/weve-seen-just-the-tip-of-the-meris-botnet-iceberg/

Necurs Botnet



2008 Cyberattack on the U.S. Military

- **Significant compromise of classified military computer networks**
- **Started with an infected USB flash drive inserted into a U.S. military laptop at a base in the Middle East**
- **Malicious code uploaded to a network run by U.S. Central Command**
  - Spread onto other systems, allowing data to be transferred under foreign control via a remote **command and control** server
- **Served as an important wake-up call for the U.S. Department of Defense**
- **Author unknown – suspected Russian hackers because of common code from previous attacks**

http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html

2021 Colonial Pipeline Attack

- **Attackers**
  - DarkSide, a cybercriminal group believed to originate from Eastern Europe, possibly Russia
- **Method**
  - Ransomware; exploited a compromised password for a VPN account
- **Impact**
  - Colonial Pipeline was forced to shut down ~5,500 miles of pipeline
  - Affected fuel supply on the U.S. East coast
  - Triggered fuel shortages and panic buying
- **Ransom**
  - Colonial Pipeline paid a ransom of approximately $4.4 million in cryptocurrency

2023 China/Russia access U.S. govt emails/networks

China

- Chinese-backed hackers accessed email of U.S. State Department officials and Commerce Secretary Gina Raimondo
- Exploited a vulnerability in Microsoft email systems
- Microsoft investigators identified the infiltrators as Storm-0558, a group that targets government agencies in Western Europe

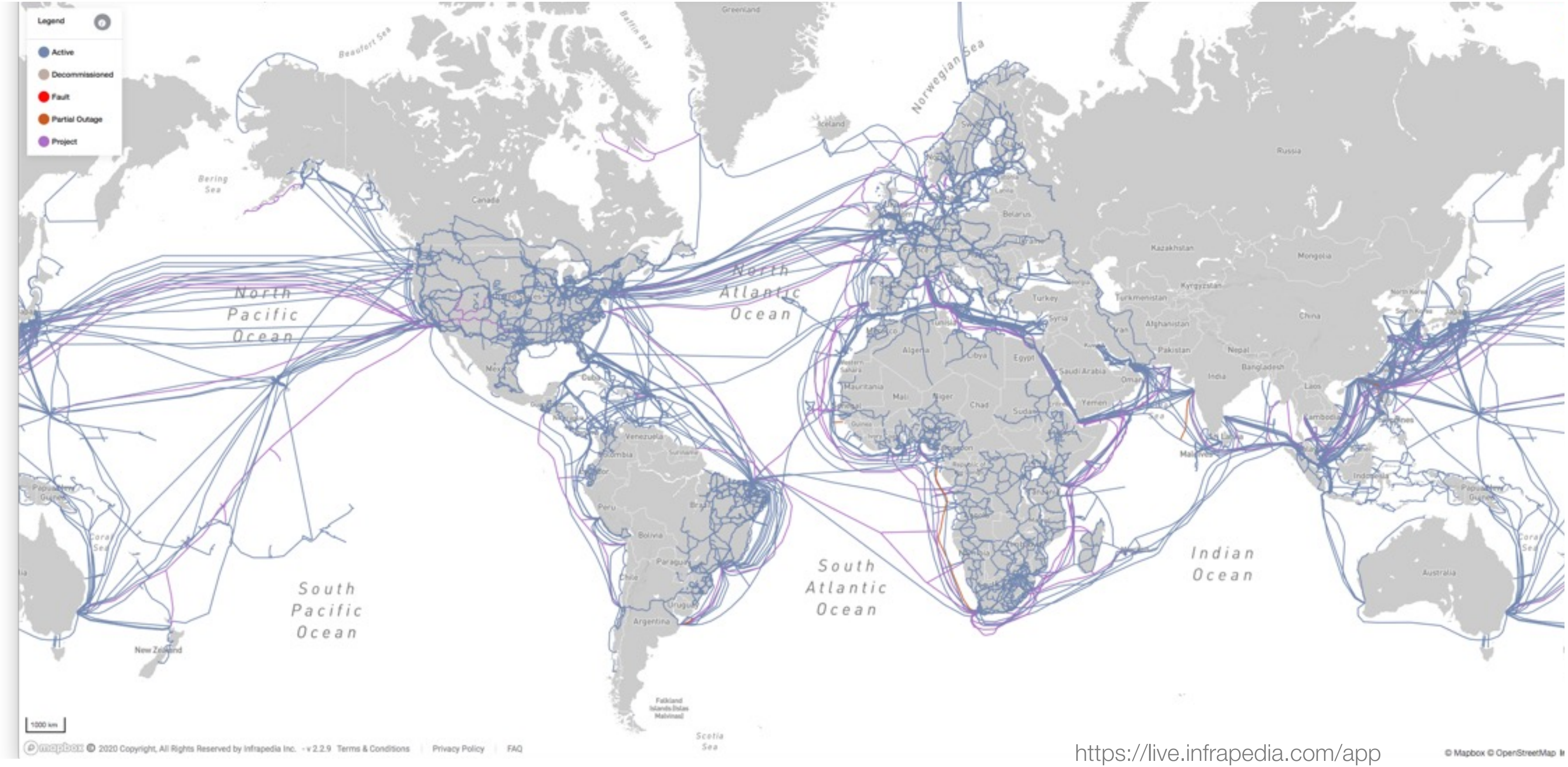
- **Russia**
  - Russia-linked cybercriminal group CLoP breached networks at various U.S. agencies
  - Exploited a vulnerability in the MOVEit file transfer program
  - CLoP began stealing files Sept 2022 and gave agencies to June 2023 to respond to its ransom demands

https://www.politico.com/news/2023/07/12/chinese-hackers-government-emails-microsoft-breach-00105879
https://www.politico.com/news/2023/06/15/multiple-federal-agencies-hit-by-hack-00102229

Anonymity

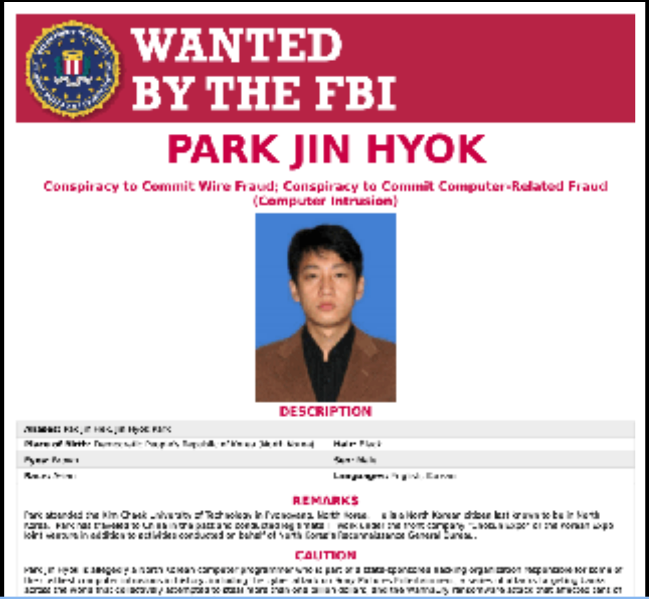
- **Internet protocols don’t require identification**
- **We often can’t identify the attacker**
  - Nobody knows who ran some of the biggest botnets or cyber-attacks
  - Identifying a source can be difficult
  - *Attack with impunity. We won't know who fired the missile.*
- **Make guesses**
  - Reverse engineer the code, compare to other known malware and attacks
  - Identify the location of the command & control server & who is accessing it
  - Trace packets & propagation paths
- **Sometimes we will never know**
- **Trust becomes a challenge**
  - How do you know you are really communicating with your bank? How does the bank know it's you?

Lack of Borders & Checkpoints



https://live.infrapedia.com/app

We expect you to show up in court…



WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park

Place of Birth: Democratic People's Republic of Korea (North Korea) Hair: Black

Eyes: Brown Sex: Male

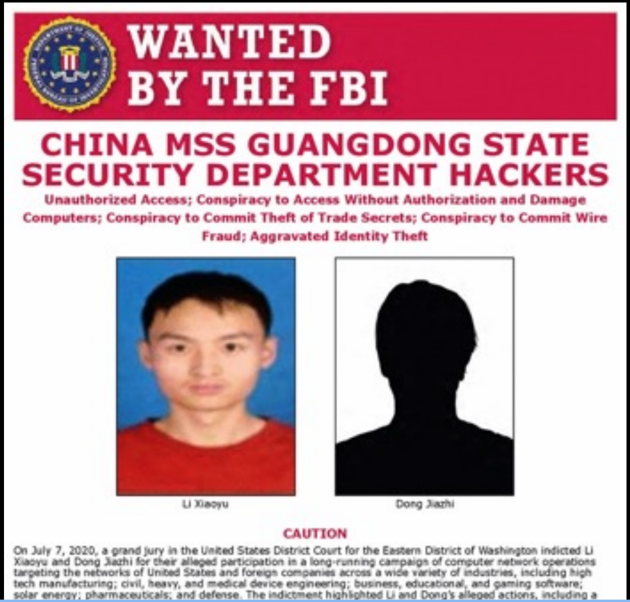
Race: Asian Languages: English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. [illegible] is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted hacking [illegible] work under the front company Chosun Expo [illegible] Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including [illegible] Sony Pictures Entertainment, [illegible] across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected parts of



WANTED BY THE FBI

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

Li Xiaoyu

Dong Jiazhi

CAUTION

On July 7, 2020, a grand jury in the United States District Court for the Eastern District of Washington indicted Li Xiaoyu and Dong Jiazhi for their alleged participation in a long-running campaign of computer network operations targeting the networks of United States and foreign companies across a wide variety of industries, including high tech manufacturing; civil, heavy, and medical device engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. The indictment highlighted Li and Dong's alleged actions, including a

Allegedly part of hacking team responsible for WannaCry ransomware, attack on Sony Pictures, and others

Allegedly responsible for stealing terabytes of data, including coronavirus research, from western companies in 11 nations

Lack of Distinction in Data

- **All bits look the same**
- **How can you tell which data is malicious?**

Networked Computer vs. Real-World Risks

- **Physical world risks are low (for most of us)**
  - Most people are not attacked
  - Most people are not victims of espionage
- **Same threats in cyberspace as real-world threats:**
  - Theft, vandalism, extortion, fraud, coercion, con games
- **Same motivation by criminals**
  - But the mechanisms, risks, and access are different

The End