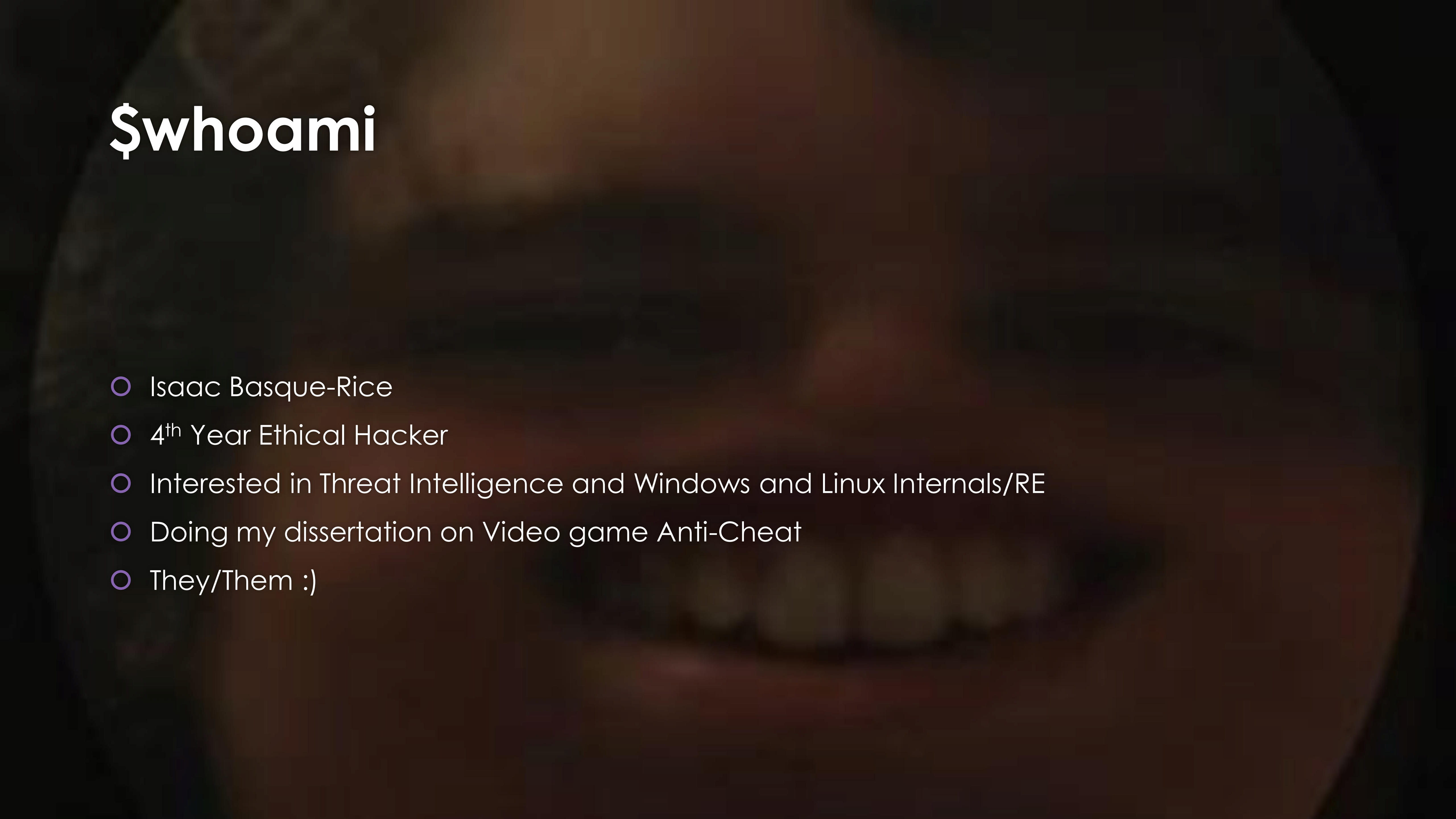
The Syscall Is Coming From Inside The House!

An introduction to APT Groups

By Isaac Basque-Rice

Support Your Lecturers!!



$whoami

- Isaac Basque-Rice
- 4th Year Ethical Hacker
- Interested in Threat Intelligence and Windows and Linux Internals/RE
- Doing my dissertation on Video game Anti-Cheat
- They/Them :)

Why APTs?

- Coolest shit ever
- My gateway drug
  - US Election Tampering
  - WannaCry
  - Stuxnet
- Have you ever wondered who did it?

It *IS* APTs

Who are they?

Advanced

Persistent

Threat

Who are they? (cont.)

- (Almost) always state actors
  - Often military or security services
- Fifth domain of warfare
- "APT" is an American Invention
  - Convenient, eh?
- How do we know about them???

MITRE ATT&CK

What is MITRE ATT&CK?

- Adversarial Tactics, Techniques, & Common Knowledge
- Framework developed by MITRE
- Categorised list of TTPs
- Previously only available to professionals and spooks
- Designed to fit into orgs’ threat models

MITRE
ATT&CK™

Tactics, techniques, and Procedures

Pre-Attack

- Recon
    - Information gathering for future operations
    - Example: Active Scanning
- Resource Development
    - Creation, purchasing, theft of resources
    - Example: Develop Capabilities

Getting In And Staying In

- Initial Access
  - Getting in lol
  - Example: Phishing
- Execution
  - AKA RCE, results in attackers’ code running on target machine
  - Example: Command and Scripting Interpreter
- Persistence
  - Maintaining a foothold
  - Example: Boot or Logon AutoStart Execution

Working Their Way Up Undetected

- Privilege Escalation
  - Gaining higher level permissions
  - Example: Access Token Manipulation
- Defense Evasion
  - Avoiding being detected
  - Example: Process Injection
- Credential Access
  - Stealing account names, passwords, etc.
  - Example: Grabbing from Password Stores

Having A Look Around

- Discovery
  - Figuring out the Environment
  - Example: Account Discovery
- Lateral Movement
  - Moving Through an Environment
  - Example: Remote Services
- Collection
  - Gathering Information of Interest
  - Example: Clipboard Data

Staying In Control and Getting Out

- Command and Control
  - Communicating with Compromised Systems to control them
  - Example: Application Later Protocols
- Exfiltration
  - Getting data out, stealing it from a target
  - Example: Automated Exfiltration
- Impact
  - Attempting to manipulate, interrupt, or delete systems and data
  - Example: Data Destruction

Case Studies

ALLEGED!!!!!

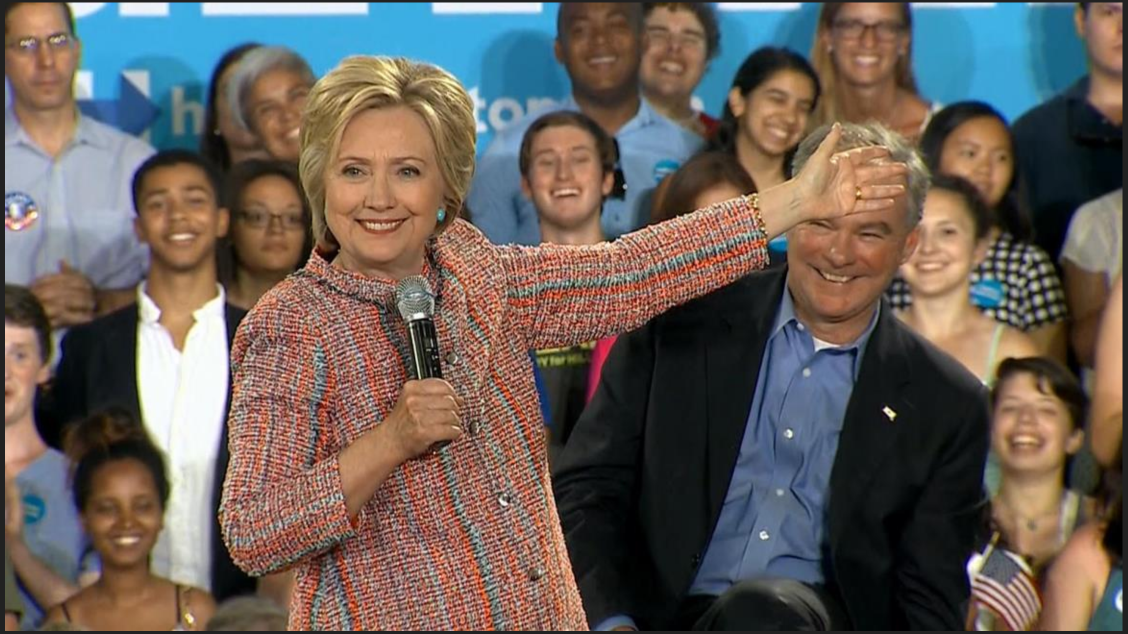
APT28

Who Are They?

- Fancy Bear
- Russian Federation
- Spear-Phishing and Zero-Days
- Their aims have been suspiciously closely linked with Russia’s

What Have They Done?

- US Election Interference (maybe Brexit too? Idk)
- Fucktons of data stolen
- CrowdStrike determined it was them
  - Unsure exactly *how*
  - But…



What Have They Done? (cont.)

- Attacks on journalists
- Parliament of Germany
- Ministries in the Netherlands
- The International Olympic Committee
- The Ecumenical Patriarchate
- UKRAINE!!!

How Do They Operate?

- Mostly Email Phishing > MalDoc/MalLink > Creds entered >Malware > Compromise
- Domains registered that look like legitimate news sites
- Use compromised orgs as proxies
- EXTREMELY up to date malware

APT38

Who Are They?

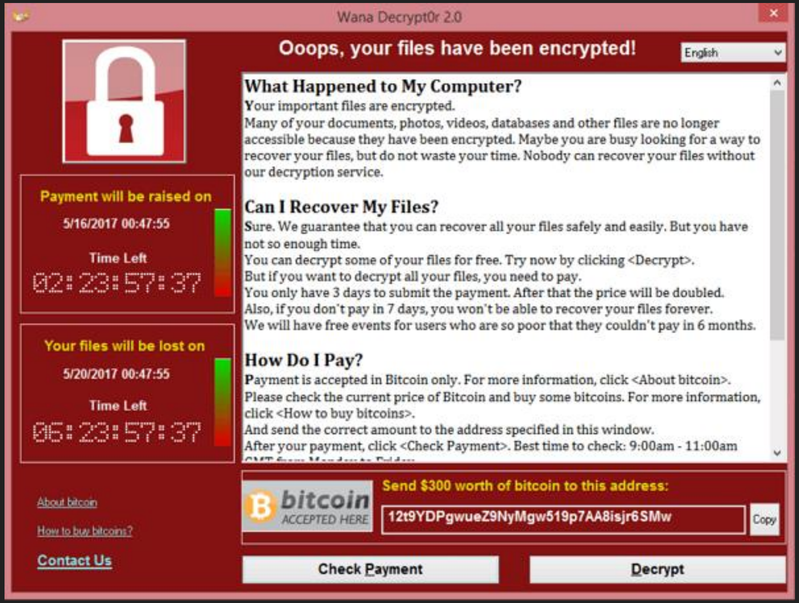
- Lazarus
- Democratic People's Republic of Korea
- LOTS of Ransomware and Financial Crimes
- Likely a huge chunk of the DPRK's income

Financial Crimes

- Theft of SWIFT credentials
  - Done to raise funds for the North Korean state
- Bangladesh Central Bank Heist
  - Also Banco Del Austro, Philippines Bank, Vietnam Tien Phong Bank, and an unnamed bank in Poland

WannaCry? WannaPissAndShit?

- You probably remember this
- NHS was massively affected
  - So was Telefónica, Chinese universities, German railway, loads of state-run stuff in Russia
- Consistent with the theory that they are raising money
- How were they caught?
  - Code similarities
  - Machine translation in specific cases
  - Rest is secret



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

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:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Other Attacks

- 2014 Sony pictures breach
- Astra-Zeneca and other pharma companies

VON DEN KAPITALISTENSCHWEINEN,
DIE AUCH BAD NEIGHBORS GEMACHT HABEN
JAMES FRANCO
SETH ROGEN
IHR TRIP NACH NORDKOREA LIEF NICHT NACH PLAN.
THE INTERVIEW
www.TheInterview.de

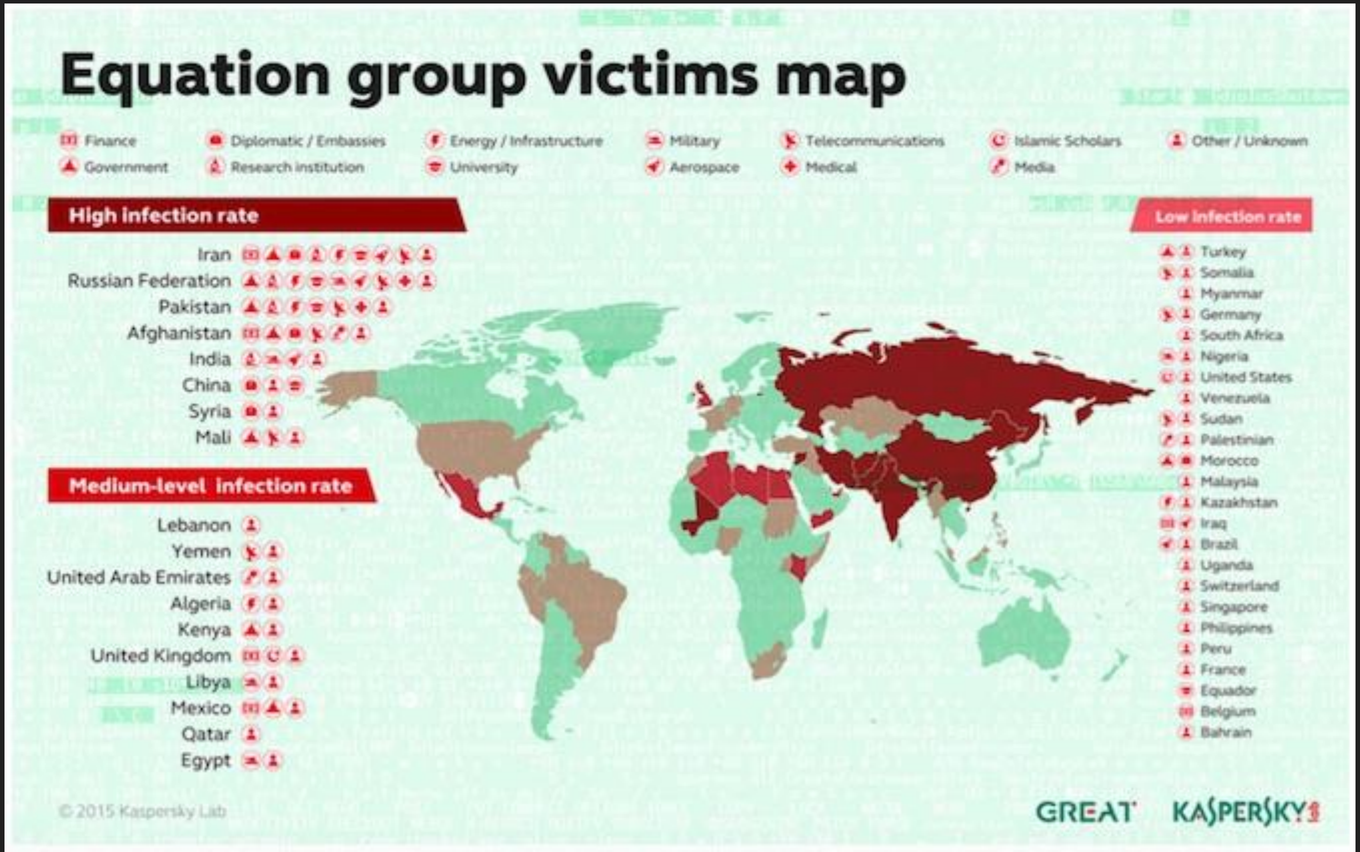
Equation Group

Who Are They?

- USA! USA! USA! USA!
- The most efficient, dangerous, complex, and potentially destructive APT out there
- Stuxnet, Flame, DOGROUND, FannyWorm (lol), super complex
  - Can Bridge Air-gapped systems
  - (At least in theory… well… you know)

Modus Operandi

- Attacking Critical Infrastructure
  - Telecommunications
  - Energy Production
  - Transportation
  - Military and Nuclear Research
  - Financial companies
  - Cryptographic companies
  - Aerospace companies
- Islamic Activists and Scholars



Stuxnet

- Equation/Israeli attack on Iran Nuclear Plant
- Targeted Siemens SCADA systems
- Used 4 zero days in one
- Got into an airgapped facility
- Feedback seemingly legit data
- “The best malware ever”

Shadow Brokers and Other Leaks

- Five leaks of EquationGroup malware, tools, and exploits
- Leak number 5 contained EternalBlue
  - Used by loads of other APTs, other mal actors, and Skids
- WikiLeaks leaked Ghidra
  - Ghidra my beloved <3

Conclusions

Conclusions

- Massive threat to everyone
- Important to learn from them
- Their TTPs and tools trickle down

Questions?

Socials

- Twitter: https://twitter.com/IBRice101
- Mastodon: https://infosec.exchange/@IBRice101
- LinkedIn: https://www.linkedin.com/in/izbr/
- Website: https://ibrice101.github.io/ ← Past Talks (And This One) Are Here