Hacking Closed Networks

SECURE
MENTEM

Ira Winkler, CISSP
ira@securementem.com
+1-443-603-0200

Impossible to Hack

- The network is closed
- It’s just a bunch of hype

HOLD MY ~~BEER~~

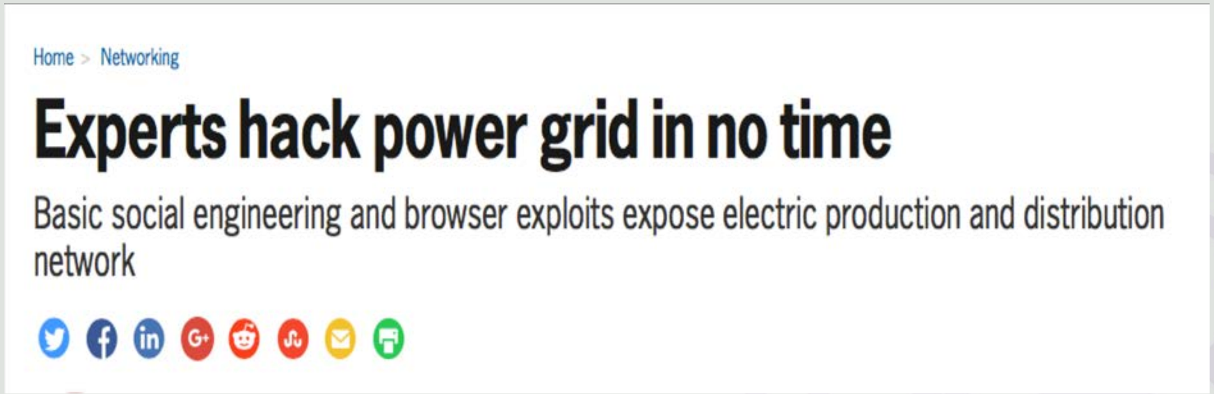
diet
Mtn
Dew

Ignorance is Dangerous, NOT Bliss

- When you don’t realize something is a threat, you don’t protect against it
- The risk profile must be well understood
- Generally networks are closed, because of the perceived risk

If it’s valuable enough to close a network, with all of the costs, it’s valuable enough for an attacker to try to find a way in

They Will Fight and Lie to Hide the Vulnerability



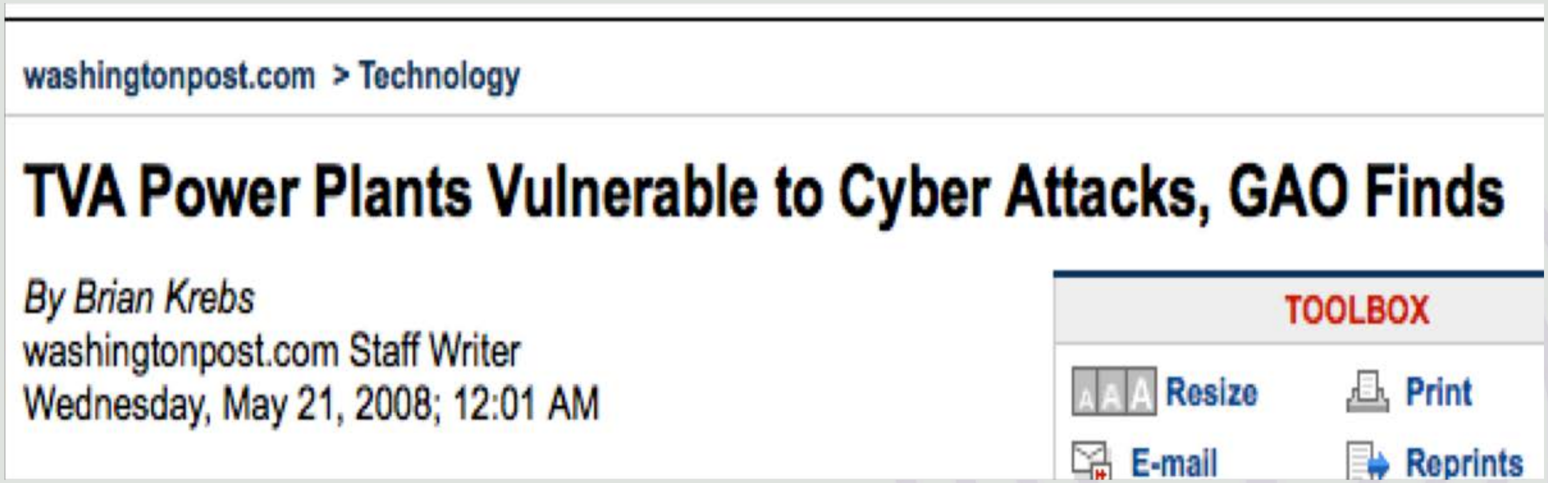
Home > Networking

Experts hack power grid in no time

Basic social engineering and browser exploits expose electric production and distribution network

- 2008 RSA presentation about hacking the power grid
- 5 federal agents contacted me
  - 2 unannounced
- Lobbying group said they wanted to talk
  - “It’s not like we want to discredit you, or anything like that”
- Brian Krebs called saying the NRC wanted to brief him on why what I described was impossible
  - So he knew I was right

Two Months Later



washingtonpost.com > Technology

TVA Power Plants Vulnerable to Cyber Attacks, GAO Finds

By Brian Krebs
washingtonpost.com Staff Writer
Wednesday, May 21, 2008; 12:01 AM

The Ways Are Almost Infinite

- Limited by creativity
- Many versions of the different scenarios
- Networks aren’t really “closed”
- Access points uncontrolled
- Diagnostic equipment
- Insider abuse
- Compromise developers

Targeting “Closed” Networks

- CERT TA18-074A
  - Russia targeting ICS through multi-stage campaigns
- Watering Hole Attacks
- Phishing
  - Credentials
  - Malware
- Open source information

Closed Networks Usually Aren’t

- Might have started out closed
- Functionality added periodically
- Don’t want expense of multiple networks
- Put in “limited” connections that really aren’t
- Bridges are added

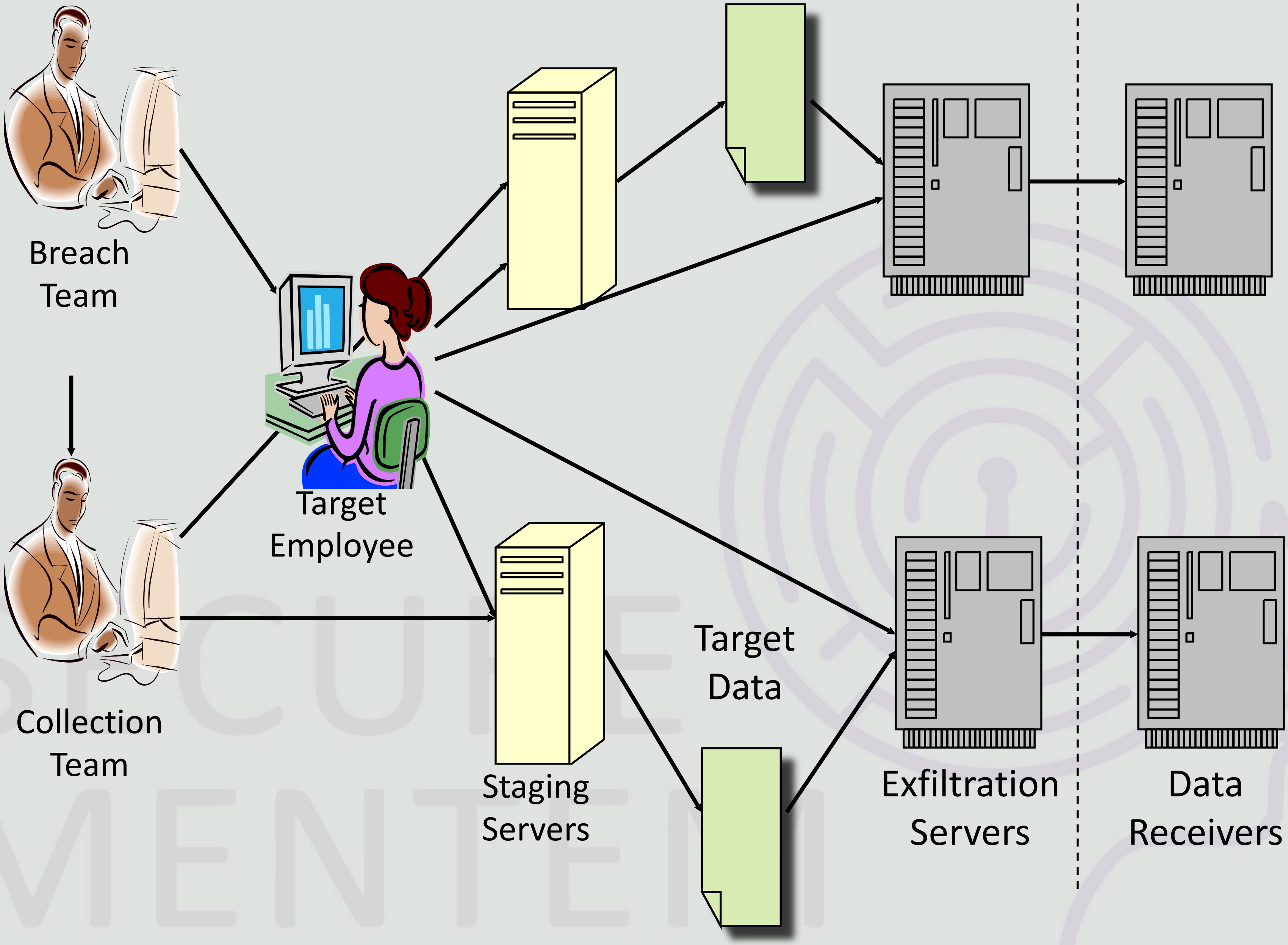
Even Worse

- Doesn’t include:
  - Wireless
  - Rogue IT
  - Subcontract connections
  - Etc.

Once In

- Systems are frequently not patched
  - Wannacry for example
- Outdated systems
- Insecure configurations

APT Compromise Methodology



Breach Team

Target Employee

Collection Team

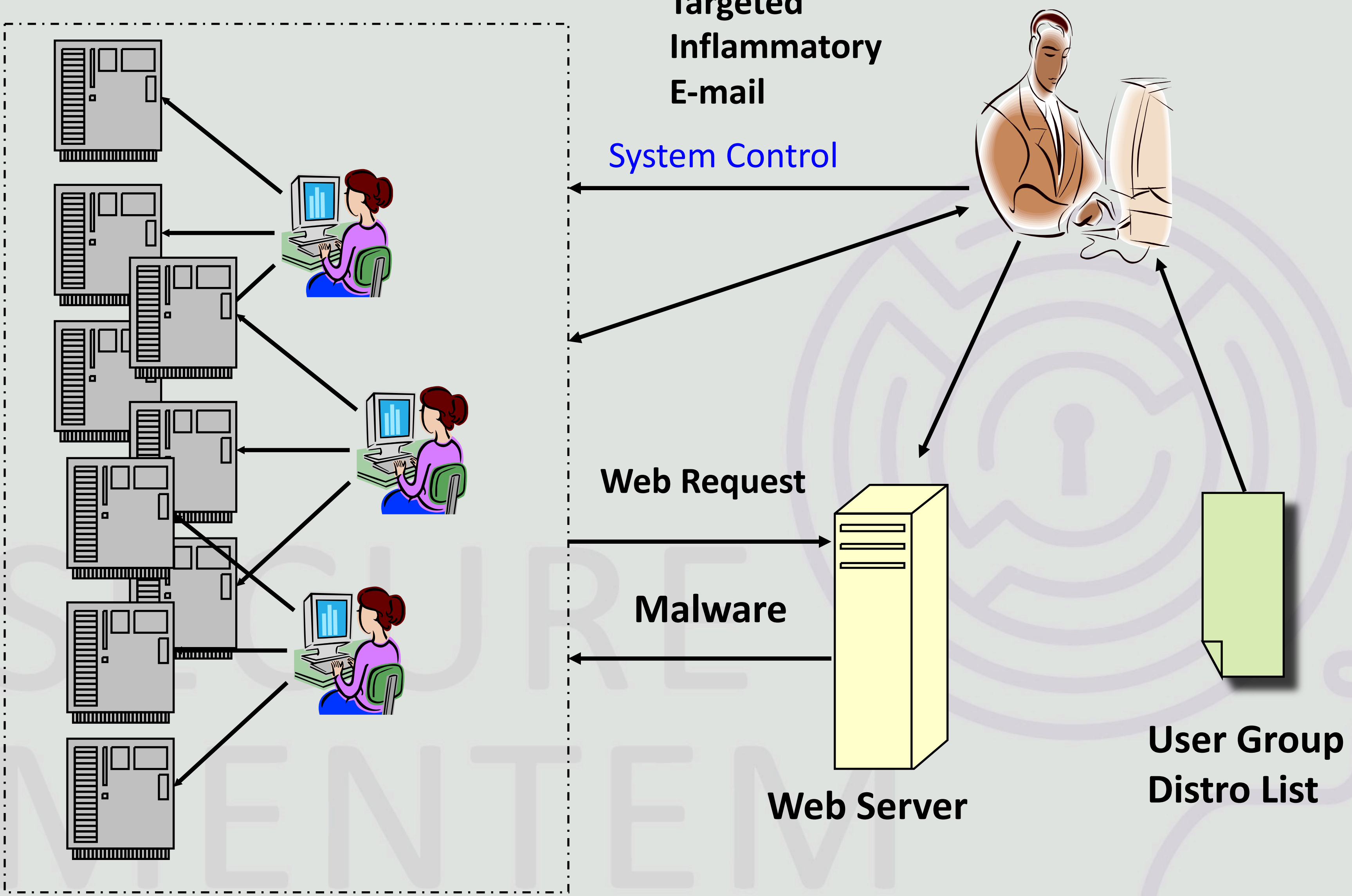
Staging Servers

Target Data

Exfiltration Servers

Data Receivers

Power Grid Example



Targeted
Inflammatory
E-mail

System Control

Web Request

Malware

Web Server

User Group
Distro List

General Note

- My case study in 2008
- Siobhon Gorman reported Russia and China hacking US power grid in 2009
- Wired reported it as new on September 6, 2017
- New round of stories on March 15, 2018
- New round of stories in another 6 months
- BTW: Russia hacked Ukraine power grid in June 2017

Uncontrolled Access Points

- Closed networks frequently have many access points
- Power grid has many points where diagnostic equipment can plug in
- Critical infrastructures are distributed and have many access points
  - Consider the Air Traffic Control System – radar, transmitters, airport operations, etc.
  - Water systems have controls throughout hundreds of miles
  - Telecom systems have access points all over

Maroochy Incident

- Vitek Boden worked for a contractor that installed radio controlled SCADA equipment
- Left under bad circumstances
- Stole radio equipment and drove around finding open access points to sewage system
- Released hundred of thousands of gallons of sewage

Diagnostic Equipment

- Can be specialized equipment
- Can be a PC
- Can be a USB device to put in updates
- Plugged into critical systems to perform diagnostics
- Connected to equipment through USB or other connectors

Worldwide Issue

- With naval vessels, they can be at all ports around the world
- Think about the thousands of people who have access to a naval base
  - Local contractors
  - Naval personnel
  - Defense contractors
- Not everyone is cleared
- Diagnostic equipment may not be treated as sensitive

Some Hacks Require Detailed Research

- Might need to know system configuration
  - Such as Stuxnet
- Might require hacking of contractors development facilities
- Might get from insiders
- Might get from documents available to maintenance personnel or elsewhere
- Some information might be available from open sources

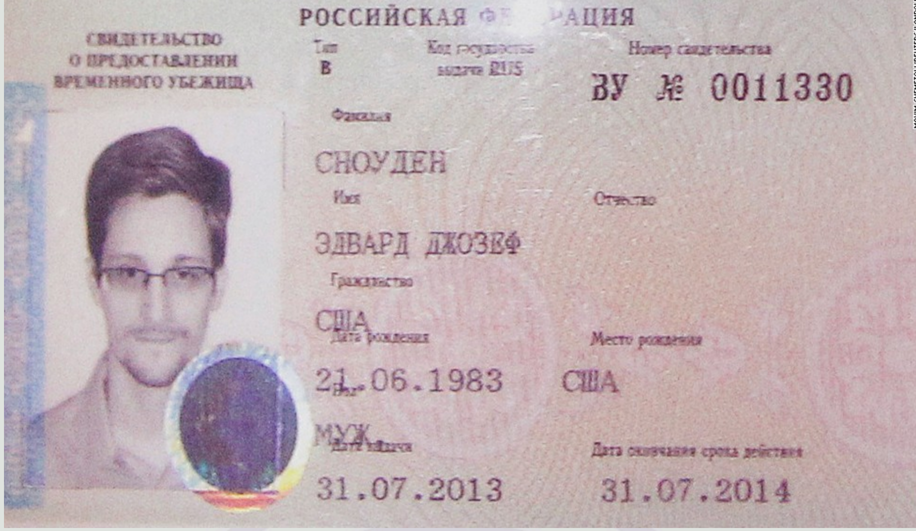
Hacking the Developers

- With naval vessels, I mean defense contractors
- Su Bin group hacked 50 TB from 2008-2014
  - Included details of onboard computer systems
- BAE Systems hacked in 2009
- Lockheed Martin hacked in 2011
- Australian contractor reported hacked in 2017
  - F-35, C-130, and P-8 data hacked, along with 30GB of data about smart bombs and naval vessels
- If you can hack it out, you can put it in

Compromise the Supply Chain

- Intercept equipment to plant malware/proactively sabotage recipient
- Equation Group supposedly doing it since early 2000s
- China accused of doing this
- Stuxnet likely delivered via equipment compromised prior to delivery
- Can be for initial delivery or periodic updates

Insiders



РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО
О ПРЕДОСТАВЛЕНИИ
ВРЕМЕННОГО УБЕЖИЩА

Тип
В

Код государства выдачи RUS

Номер свидетельства
ВУ № 0011330

Фамилия
СНОУДЕН

Имя
ЭДВАРД ДЖОЗЕФ

Отчество

Гражданство
США

Дата рождения
21.06.1983

Место рождения
США

Пол
МУЖ.

Дата выдачи
31.07.2013

Дата окончания срока действия
31.07.2014

- Many potential insiders
- Insiders at developers
- Insiders on ships
- Insiders at repair facilities
- Insiders have planted time bombs and sabotaged operations elsewhere
- They’ve taken things out; little stops them from putting things in

Black Bag Operations

- Outsiders infiltrate an organization
- Can be through pretexts
- Assumed identities
- Get jobs inside targeted organizations
  - Frequently through contractors
- When you don’t have or trust insiders
  - Usually a last resort

Making Closed Networks Open

- A simple patch cable between network equipment
  - If equipment is co-located
  - Ships at sea now provide Internet for morale and other purposes
- Attaching routers to the network
  - Wireless or connected to a cellular/satellite device
  - A more permanent Maroochy
  - There are tools that look for rogue WiFi, so don't laugh
- Modems
  - Yes they still exist

Stuxnet Basics

- In theory, US and Israeli assets determined internal architecture
- Identified software in use
- Developed hack
- Created malware laden USB drives, or
- Compromised supply chain and delivered pre-infected equipment to contractor
- Dropped or delivered drives near developers
- Malware worked autonomously as designed
- Able to consistently upgrade attacks

So, Can You Hack a Naval Vessel?

- Yep, but admittedly complicated
- Stuxnet-like attack strategy
  - Probably autonomous attack
- Determine architecture
- Determine attack vectors
- Plant malware through supply chain, maintenance, or hacking
- Or, placing taps or inside sabotage

Disclaimer

- Of course, this attack is theoretical
- Similar attacks have been accomplished
- It is more complicated than described, but still possible
  - If anyone said you’re going to regularly get malware in an underground Iranian facility, they would have been derided, probably like I will be
- To my terrorist followers, there’s not enough here to launch the attacks

Hacking Open Networks Can Use Similar Techniques

- Supply chain, insiders, outsiders, network taps, etc. are still similar threats
- The attack vectors are the same, with a wider attack surface

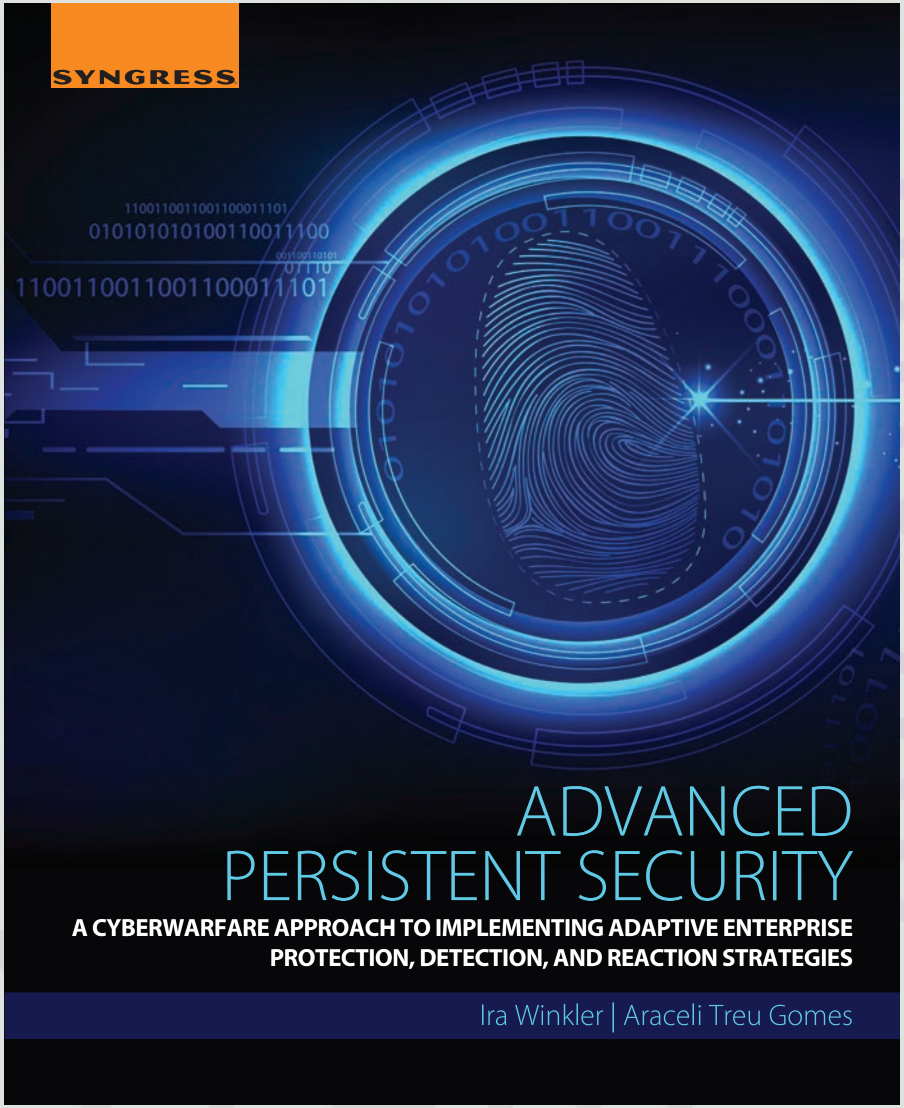
Stopping These Things

- Ignorance of the risk is the greatest threat
- Acknowledge the threat
  - Again, if it is valuable enough to cause the network to be closed, it is valuable enough for an outsider to target you
  - Everything is on the table
- Supply chain security
- Protection needs to be as tight as the most valuable open network
- Detection needs to be constant and pervasive
  - Assume technical and physical compromise

The Big Takeaway

- This can be done
- This has been done
- Saying such an attack is impossible is the greatest threat

The Book, The Myth, The Legend



SYNGRESS

ADVANCED PERSISTENT SECURITY

A CYBERWARFARE APPROACH TO IMPLEMENTING ADAPTIVE ENTERPRISE PROTECTION, DETECTION, AND REACTION STRATEGIES

Ira Winkler | Araceli Treu Gomes

For More Information

ira@securementem.com

+1-443-603-0200

@irawinkler

www.securementem.com

www.linkedin.com/in/irawinkler

Facebook.com/irawinkler