February 28, 2024

What if the "Wicked Witch of the West" Had a Laptop

33rd Annual Trust Advisors Forum

Steve Wujek

Network Architect & Security Engineer

Stars of the Show

Steve Wujek

- ✓ Network Architect & Security Engineer
- ✓ Cybersecurity Speaker & Consultant
- ✓ Expert Legal Witness

"Wicked Witch"

- ✓ Chief Infiltration Officer
- ✓ Flying Monkey Phisher
- ✓ Broomstick Collector

Same Old, Same Old, what you hear:

"Don't…":

- Click on emails
- Download files
- Install unknown software
- Reuse passwords
- Use public Wi-Fi

"Beware of…":

- Phishing emails
- Ransomware
- Supply chain attacks
- Malicious insiders
- Misconfigurations / errors

IT says: "*Because the bad guys will encrypt / steal / delete your data, blah blah blah….*"

But What Did the “Wicked Witch” Actually Do with That Stolen Data?

The Villains

The Villians

Nation State: person or group employed by a nation, who hacks under the direction and guidance of their nation to obtain information.

Private Hacker: person or group who hack for personal or group objectives.
AKA – Black hats, Cyberterrorists, Script kiddie, Hacktivist, Whistleblower, Cryptojackers

The Villians

Nation State Hackers Want:

- Espionage
- Spread Political Misinformation
- General Chaos

Targets:

- Governments
- People in Power
- Major Corporations

Who?

- Russia, China, North Korea, Iran, United States

The Villians

Private Hackers Goal:

- Financial gain
- Fight/Spread Political & Social Injustice
- Ego

Target: Varies; Easy Targets

Who are they?

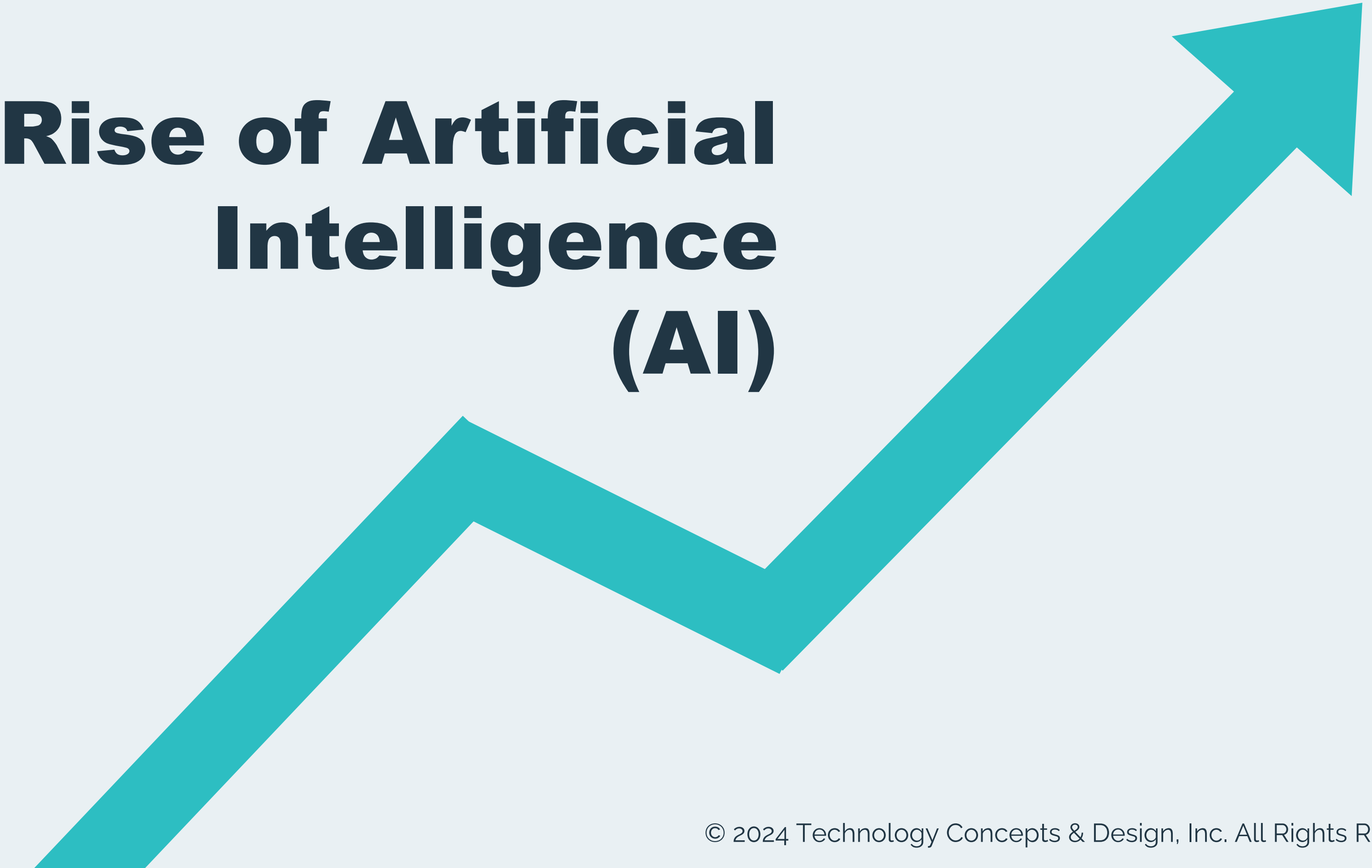
- Hacktivists
- Your neighbor?
- AI (via incorrect use)
- Anonymous – famous group

We Aren’t in Kansas Anymore!

What’s changed?

We Aren’t in Kansas Anymore

The Rise of Artificial Intelligence (AI)



But What Would the "Wicked Witch" Actually Do with THAT Stolen Data…

…now that she has access to AI?

tcdi

Famous Cyber Attacks

Let’s revisit the stolen data…

‘The Villians’ stole the data in these attacks…

Let’s take that data and apply AI

White House, Democratic National Committee

When: 2014 - 2016

Impact: White House, State Dept. and DNC Email

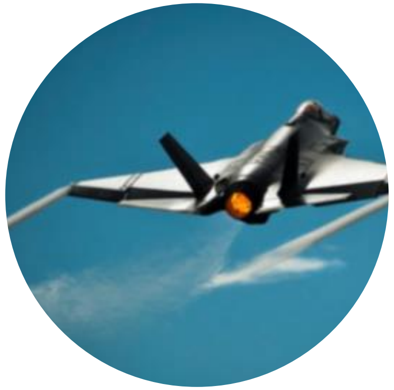
- Attacks attributed to two Russian hacker groups: Cozy Bear and Fancy Bear

How: Theft of Credentials

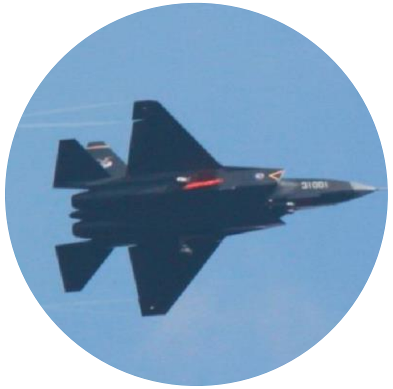
- Obtained the same credentials, separately
- Deployed several variants of malware over time

https://en.wikipedia.org/wiki/Democratic_National_Committee_cyber_attacks

Lockheed Martin's F-35 Fighter



Which one is the Chinese J-31/J-35 clone: Top or bottom?



How much have US taxpayers spent on the F-35?

https://securityaffairs.com/32437/intelligence/china-stole-plans-f-35-aircraft.html
https://www.industrialcybersecuritypulse.com/networks/throwback-attack-chinese-hackers-steal-plans-for-the-f-35-fighter-in-a-supply-chain-heist/
https://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/
https://www.eglin.af.mil/ Samuel King Jr
Chinese Internet

Mearsk Shipping, Merck, FedEx

When: June 2017

Impact: 1/5 World’s Shipping in Standstill

- NonPetya ransomware corrupts and deletes data
- All companies suffered significant financial losses, not including reputational damage:
  - Maersk: $750 million
  - Merck: $1.4 billion
  - FedEx: $1 billion

How: Unpatched System

- Did not patch against EternalBlue vulnerability

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Equifax, Experian

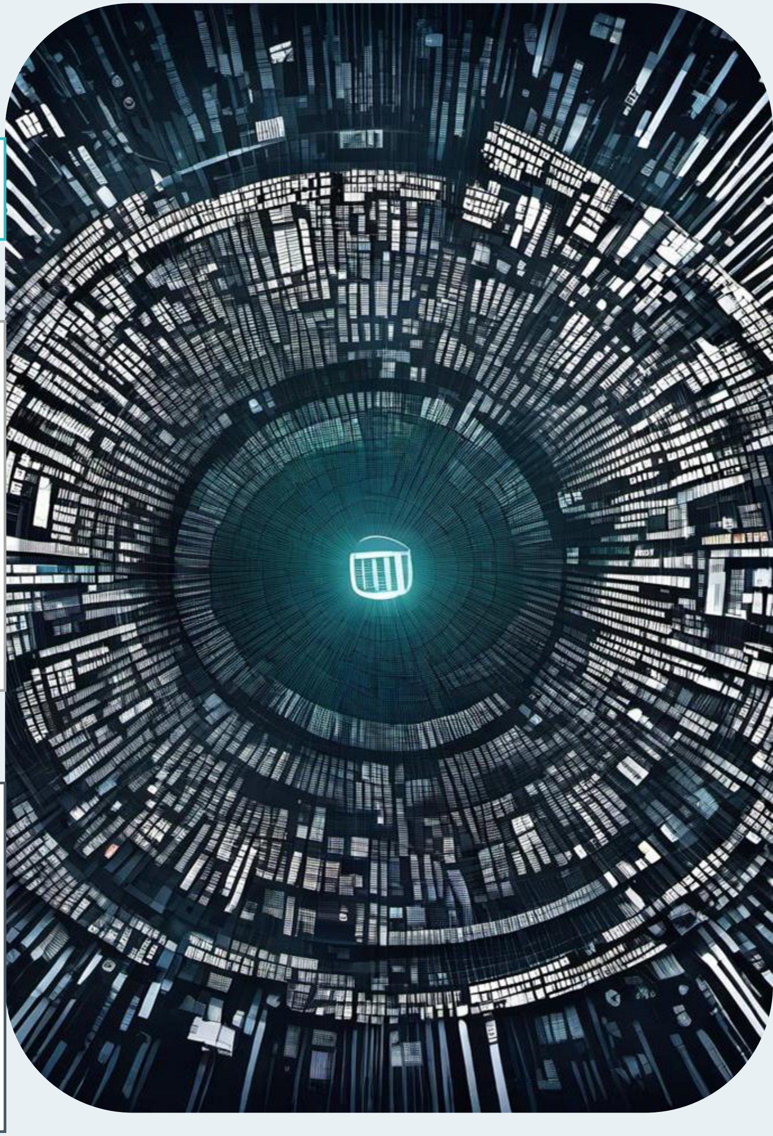
When: Equifax - 2017, Experian – 2020

Impact: Equifax - 162+ million customers, Experian – 24 million customers

- Equifax – 40% of American population
- 147 million Americans, 15.2 million British citizens, and 19,000 Canadian citizens were compromised
- They know what car/house/boat you bought, what credit cards you have, your bank accounts, your dog's name, etc…

How: Terrible Cybersecurity Hygiene

- Equifax - Failed to patch a 'Critical' vulnerability for 6 months
- Passwords in plain text, left at defaults "password123"
- Social Engineering – pretended to be an Experian employee



https://www.upguard.com/blog/biggest-data-breaches-financial-services tcdi

Capital One; The First American Corporation

When: March 2019; May 2019

Impact: Credit Card Applications

- Capital One - 100 million credit card applications;
- The First American - 885 million credit card applications

How: Disgruntled Employee; Website Design Error

- Former AWS software engineer illegally accessed an AWS server storing Capital One’s data
- Website had no Authentication to verify user access (accident)

https://www.upguard.com/blog/biggest-data-breaches-financial-services

SolarWinds

When: Late 2019 – Early 2020

- Access to systems for up to 18 months prior to discovery
- Russians first, followed by the Chinese

Impact: 60% publicly traded companies

- Affected most government entities through a sophisticated supply-chain attack

How: Supply Chain Attack

- Delivered backdoor malware during a software update

https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Kaseya

When: July 2021

Impact: 1,500 Managed Service Providers (MSP)

- Network monitoring and management system for MSPs
- MSPs - design, configure and monitor multiple businesses
- 1,500 MSPs x (how many businesses per MSP) = ‘X’ number of businesses
- (‘X’ number of businesses) x (‘Y’ number of databases/business) = ‘Z’ databases

How: Supply Chain Attack

- Delivered ransomware during a software update

https://www.forbes.com/sites/forbestechcouncil/2022/01/25/the2021-kaseyaattack-highlighted-the-seven-deadly-sins-of-future-ransomware-attacks/?sh=500b19fc5f75

Hospitals and Medical Records

When: 2022 - 2024

Impact: Medical Records

- Medibank - 9.7 million medical records
- Integris – 2.4 million medical records
- Singing River Hospitals – 225,000 medical records
- Hundreds more across the globe!
- Extortion … *already happening!*
- Blackmail … *already happening!*

How: Ransomware, Social Engineering

https://www.upguard.com/blog/what-caused-the-medibank-data-breach
https://www.bleepingcomputer.com/news/security/integris-health-says-data-breach-impacts-24-million-patients/

23andMe

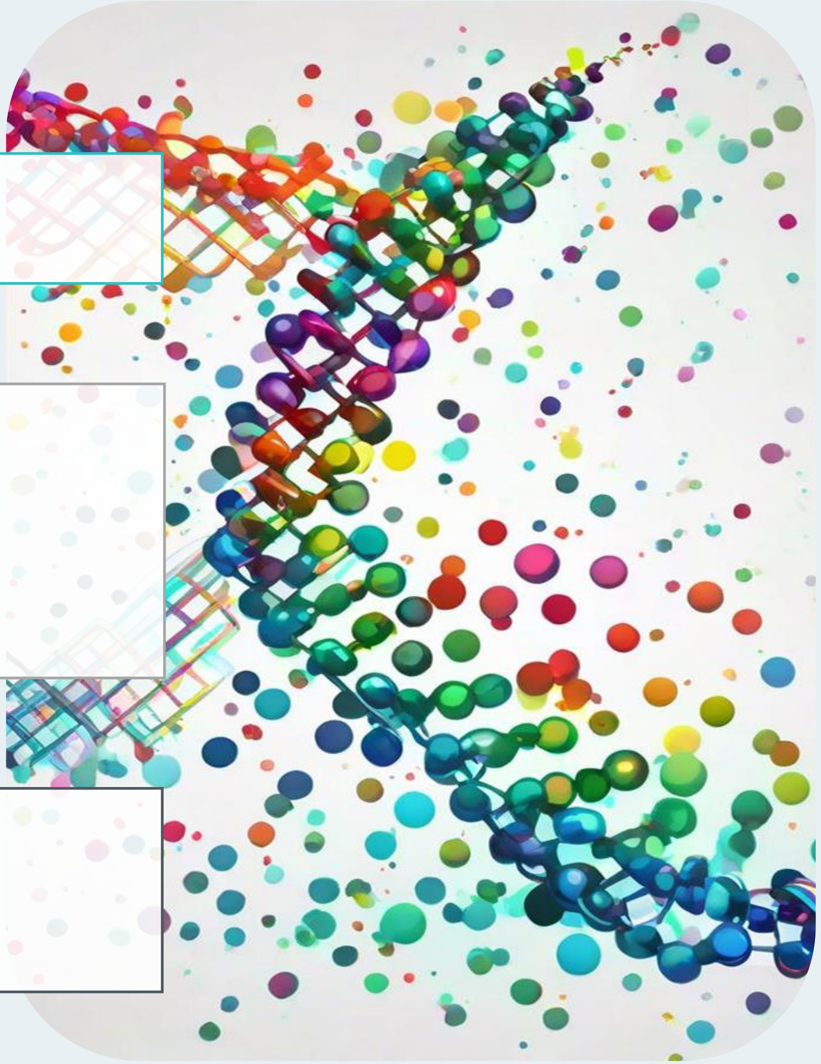
When: April – September 2023

Impact: 14,000 accounts & 6.9 million people

- Biological/genetic/blood markers, cancer screening pulled from mail-to-home kits using the individual’s own blood.

How: Reused Passwords

- Brute force attacks – ‘*Kindergarten hacking*’



https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/

Office of Personnel Management (OPM)

When: April 2015

- Chinese NS hack, believed to have gained access in 2013 but stole data as far back as 2000

Impact: 5 million fingerprints & background checks

- US Government employees (includes US Military branches)
- Contractor’s Security Clearance applications going back to 2000
- *This one could be a real ‘sleeper’ of a hack!*

How: Poor Cybersecurity Decisions

- Not implementing basic level security best practices

https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

How the “Wicked Witch” is Using AI right now…

- Deepfake Technology
- Malware Detection and Evasion
- ‘*Turbocharging*’: Automated Attacks, Password Cracking, Data Mining, Crypto mining/hacking
- Phishing and Social Engineering

https://cyberseniors.org/uncategorized/how-hackers-and-scammers-use-ai-artificial-intelligence/#:~:text=Deepfake%20Technology%3A%20AI%2Dgenerated%20deep,security%20measures%2C%20evading%20detection%20systems.

Deepfakes – The proverbial "shot across the bow"

Already well under way, Feb 2024:

- Hong Kong Financial Officer tricked into releasing $25 million to hackers on a videocall, AI used for their voices, faces and mannerisms.
- President Biden's 'Baby Shark' video
- Taylor Swift photos
- NJ Junior High boys creating photos to bully girls

https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/?mod=djemCIO
https://www.nbcnews.com/tech/tech-news/deepfake-law-ai-new-jersey-high-school-teen-image-porn-rcna133706

What Will Slow AI Down?

- Misleading Information
- Data Privacy
- Biased Data Feeding
- Legal & Ethical Concerns
- Needing the “Human Touch”
- **Copyright** and Confidentiality Concerns

What’s next: The Good?

- Cure for Cancer
- Spinal Cord Injuries
- Limb regeneration
- Financial
- Medicines
- Fusion Energy

More Good: How Finance is Using AI

- Chatbots
- Fraud Detection & Prevention
- Customer Relationship Management (CRM)
- Predictive Analytics
- Credit Risk Management

Goal: Drive Efficiencies and Customer Experience

https://www.deloitte.com/content/dam/assets-zone1/ng/en/docs/services/risk-advisory/2023/ng-how-artificial-Intelligence-is-Transforming-the-Financial-Services-Industry.pdf

The Path to Securing your Network for AI

The Real Secret to Defeating the "Wicked Witch"

- **Cyber does NOT have a bucket of water for the Wicked Witch**
- **Businesses need to change their Cyber mindset from '*Weeks & Days*' to '*Minutes & Seconds*'**

There's No "Magic Fix" for AI Security

- You can't click your heels 3x and get better network security…
- AI security is out of scope for this presentation
- Layered Security, lots and lots of layers
- Training
- Lock it down?

Your Companions down the Yellow Brick Road are…

The Brains

- **Cyber/Risk Assessment**
- Identify Security Gaps
- You Don’t Know What You Don’t Know

The Heart

- **Penetration Test (Pen Test)**
- Involve the “Human Element”
- “Can’t fix what you don’t know is broken”

The Courage

- **Incident Response Plan (IR Plan)**
- Practice Regularly

Questions?

Steve Wujek

s_wujek@tcdi.com

Greg Michalek

Senior Director, Business Development, TCDI
1-888-823-2880
g_michalek@tcdi.com

Wicked Witch

She’ll be contacting you!