Ransomware Incident and Response

or

What actually happened in the trenches…

A “mostly” true set of stories

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Overview

- About me…
- Current environment
- A tale of two incidents…
- Open discussion

About me…

- Andrew (Andy) Green, Ph.D.
  - Assistant Professor of Information Security and Assurance
  - Longtime Infosec practitioner before joining academia
  - Research interests in security, privacy, public policy
    - Responsible for alerting KSU about Election Center data leakage of all Georgia voter registration data
    - Helped raise attention to SB 315 which was vetoed by Gov. Deal
    - Frequent media contributor on infosec-related topics
  - Troublemaker, but with (mostly) good intent…
  - Like to say "Roll Tide"… a lot

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

How to find me

- Email – andy.green@kennesaw.edu
- Twitter - @AndyGreenPhD
- Website – https://AndyGreenPhD.com (slides will be posted here)
- LinkedIn - https://www.linkedin.com/in/andygreenphd

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Disclaimer

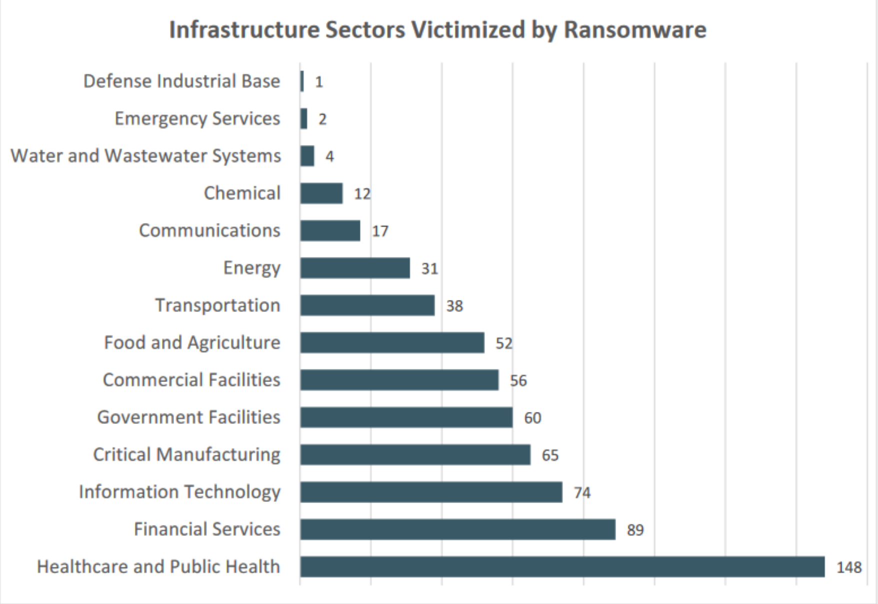
- Thoughts and ideas presented here are mine (or cited authors)
- I am not speaking for KSU or the USG today

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Current environment

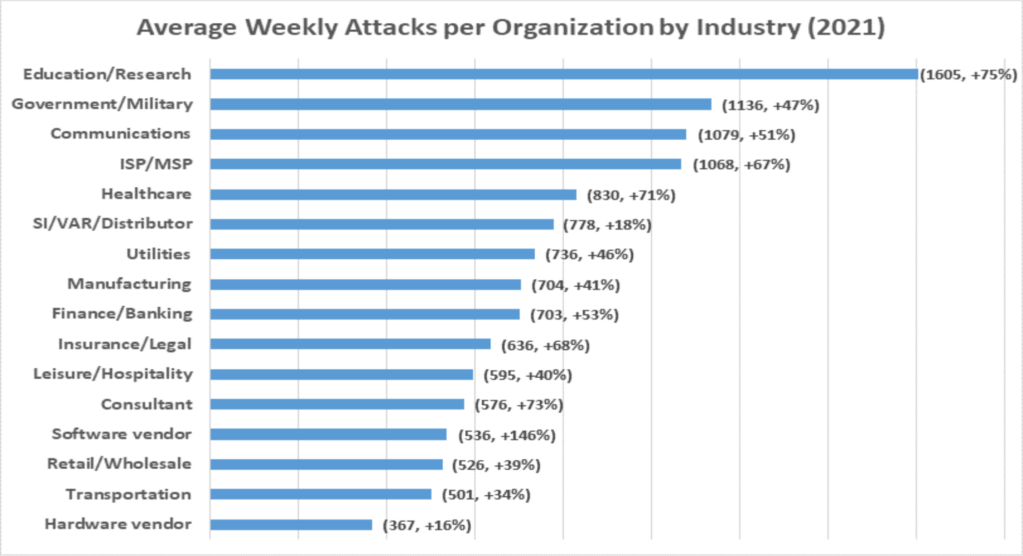
Current environment

- 2021 FBI IC3 report data (excludes lost business, time, wages, files, equipment or third-party remediation services)
  - 2021 - $49,207,908
  - 2020 – $29,157,405
  - 2019 - $8,965,847



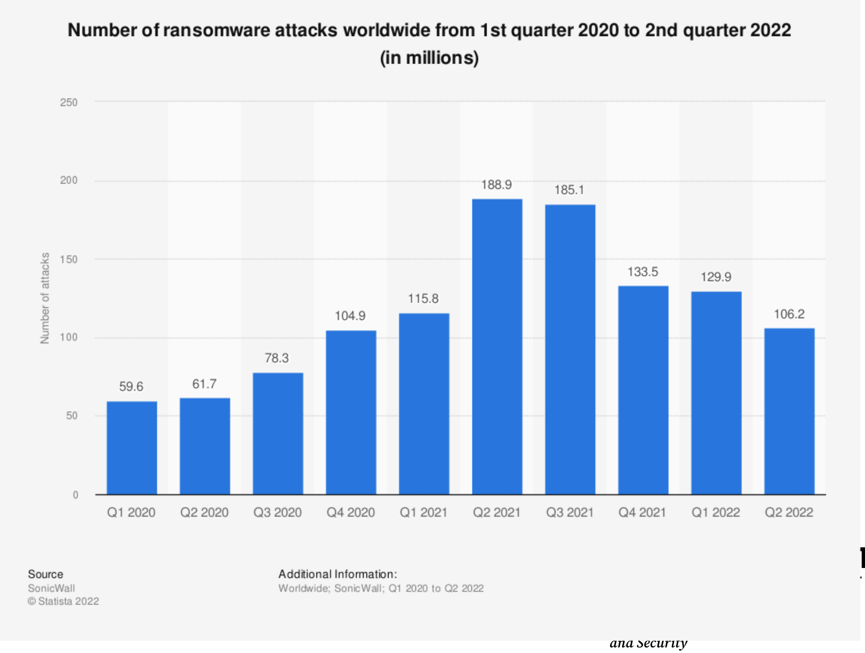
Current environment

- 2021 Report from Checkpoint on overall attacks per firm by industry



Current environment

- Maybe there is some hope?



Number of ransomware attacks worldwide from 1st quarter 2020 to 2nd quarter 2022 (in millions)

Source
SonicWall
© Statista 2022

Additional Information:
Worldwide; SonicWall; Q1 2020 to Q2 2022

Current environment

A tale of two incidents

Colonial Pipeline (2021)
Saudi Aramco (2012)

A tale of two incidents

- <Insert CYA academic disclaimer here>
  - Frequently done to avoid responsibility and blame for speculation or failed attempts to be humorous
  - Definite “Roll Tide” situation…

Colonial Pipeline

- Provides 45% of the region’s fuel (TX, LA, MS, TN, AL, GA, SC, NC, VA, MD, PA, DE, NJ)
  - Serves ~ 50 million Americans
- Suffered ransomware attack in 2021

Colonial Pipeline

- Timeline (left of “bang”)
  - February 2014
    - Department of Energy and TSA release “Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) version 1.1
  - March 2018
    - TSA releases “Pipeline Security Guidelines” document
  - February 18, 2020
    - CISA releases an alert titled “Ransomware Impacting Pipeline Operations” in response to natural gas compression facility compromise

Colonial Pipeline

- Timeline (“bang”)
    - May 7, 2021
        - ~5:00 am – First observed ransom note. Note claimed data had been exfiled (later discovered to be 100GB) from a shared internal drive and asked for $5 million (US) ransom paid via Bitcoin
        - ~5:55 am – Pipeline shutdown process initiated
        - ~6:10 am – Pipeline shutdown confirmed (~5,500 miles of pipeline)
        - FBI contacted within hours of attack onset, exact time unclear
        - Mandiant called in to investigate and respond

Colonial Pipeline

- Why shut down the pipeline?
  - Safety?
  - Security?
  - Public welfare?

Colonial Pipeline

Colonial Pipeline

Shutdown decision based on “the imperative to isolate and contain the attack to help ensure the malware did not spread to the Operational Technology network, which controls our pipeline operations, if it had not already.”

Colonial Pipeline

TRANSLATION

Pipeline operational technology (OT) was NOT impacted by ransomware.

Traditional IT systems were. Billing and accounting was impacted, so firm was unable to bill customers for oil sent out.

Colonial Pipeline

Colonial Pipeline

- Timeline (right of “bang”)
  - May 8, 2021
    - Colonial pays ransom of 75 bitcoin (~$4.4 million US)
    - CEO stated entity paid was not on the Office of Foreign Asset Control sanctions list at the time
    - Colonial Pipeline IT staff discover the decryption key is inefficient and time-intensive to use.

Colonial Pipeline

- Timeline (right of “bang”)
  - May 9, 2021
    - Colonial Pipeline announces their operation team is developing a system restart plan.
    - Main lines are still offline (1,2,3,4), but some lateral lines between terminals and delivery points are operational.
    - Biden administration declares a regional emergency for 17 states and Washington D.C.

Colonial Pipeline

- Timeline (right of "bang")
  - May 10, 2021
    - Colonial Pipeline announces execution of a plan that involves incremental turnup in a phased approach. Goal is to substantially restore operational service by end of week
    - Georgia Governor Brian Kemp declared a state of emergency and temporarily waived collection of state taxes on motor fuels.
    - North Carolina Governor Roy Cooper declared a state of emergency and temporarily suspended some fuel regulations

Colonial Pipeline

- Timeline (right of “bang”)
  - May 10, 2021 (continued)
    - Darkside ransomware group apologizes for the “social consequences” of the attack, says they’ll do better in the future
    - Colonial Pipeline announces manual operation of main line #4 for a limited time

Colonial Pipeline

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Colonial Pipeline

- Timeline (right of “bang”)
  - May 11, 2021
    - Florida Governor Ron DeSantis declared a state of emergency, suspended enforcement of various state laws, and activated the National Guard.
    - Virginia Governor Ralph Northam declared a state of emergency
    - South Carolina Attorney General Alan Wilson declared “…an abnormal disruption in the market” and activated price gouging laws
    - Colonial Pipeline announced additional lateral lines opened up, and delivery of ~41 million gallons of gas to GA, NC, MD, and NJ

Colonial Pipeline

- Timeline (right of “bang”)
  - May 12, 2021
    - Colonial Pipeline restarted pipeline operations
  - May 13, 2021
    - Colonial Pipeline announced entire pipeline has been restarted and product is being delivered

Colonial Pipeline

- Timeline (right of “bang”)
  - May 15, 2021
    - Colonial back to regular operations
  - June 7, 2021
    - Department of Justice recovers 63.7 bitcoin (~$2.3 million US)

Colonial Pipeline

- Suspected cause of breach
  - Leaked VPN creds and no MFA

Saudi Aramco

- Worth ~$781bn
- World’s largest daily production of oil, annual output of ~8bn barrels
- 2012 attack was “wiper” attack, not ransomware
- Attack put 10% of the world’s oil supply at risk
- US officials attributed attack to Iran

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Saudi Aramco

- August 15, 2012 (“bang”)
  - Ramadan, major religious holiday
  - Most IT staff not in office
  - Computers start to shut down, files disappear, screens flicker
  - “Cutting Sword of Justice” claims responsibility, cites firm’s support of the Al Saud royal family’s authoritarian regime

Saudi Aramco

- August 15, 2012 (“bang”)
  - IT staff begins unplugging servers in all global data centers. Every office physically unplugged from the Internet
  - OT systems and networks are unaffected, only IT systems
  - ~35K systems wiped during the attack
  - MBR wiped on Windows systems, essentially “bricking” them

Saudi Aramco

- “Right of bang” actions – timeline unclear
  - Company stopped selling oil for 17 days
  - Eventually gave it away to keep it flowing within Saudi Arabia
  - Aramco sent representatives directly to computer factory floors in Southeast Asia, paying higher prices to cut in line ahead of other clients to buy new hard drives

Saudi Aramco

- “Right of bang” actions – timeline unclear
  - In one purchase alone, 50,000 hard drives were bought.
  - This incident caused a global shortage in hard drives due to existing supply chain issues resulting from flooding in Thailand.

Saudi Aramco

- August 29, 2012
  - Saudi Aramco announces main network services are back online and damaged systems are back online
- January 2013
  - Paid consultant says this is when Aramco brought systems back online

Saudi Aramco

- Suspected cause of breach
  - Employee hooked a “phish”

Open discussion

- What do you think about these incidents?
- What questions do you have for me?

References

- Background
  - https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
  - https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/
  - https://www.statista.com/statistics/1315826/ransomware-attacks-worldwide/

References

- Colonial Pipeline
  - https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html
  - https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
  - https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html
  - https://www.cnn.com/us/live-news/us-gas-demand-hack-05-11-21/index.html
  - https://www.vice.com/en/article/bvzzez/colonial-pipeline-hackers-statement-darkside
  - https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption
  - https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/
  - https://www.cisa.gov/uscert/ncas/alerts/aa20-049a
  - https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf
  - https://www.energy.gov/sites/prod/files/2014/03/f13/ONG-C2M2-v1-1_cor.pdf

References

- Saudi Aramco
  - https://money.cnn.com/2015/08/05/technology/aramco-hack/
  - https://pastebin.com/HqAgaQRj
  - https://money.cnn.com/2011/11/01/technology/thailand_flood_supply_chain/?iid=EL
  - https://www.cfr.org/cyber-operations/compromise-saudi-aramco-and-rasgas
  - https://www.cnbc.com/2021/07/22/saudi-aramco-facing-50m-cyber-extortion-over-leaked-data.html
  - https://www.theregister.com/2012/08/29/saudi_aramco_malware_attack_analysis/

Thank you!

- Email – andy.green@kennesaw.edu
- Twitter - @AndyGreenPhD
- Website – https://AndyGreenPhD.com (slides will be posted here)
- LinkedIn - https://www.linkedin.com/in/andygreenphd

KENNESAW STATE
UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security