SolarWinds (Supply Chain), Microsoft Exchange (Zero Days), and Colonial Pipeline (Ransomware) - Oh My: Why Should You Care About These Events...

BE Rhodes

Roles: Industry/Military/Academia

October 2021

Outline

- WHOIS
- Where to begin?
- Solar Winds Orion (Supply Chain)
- Microsoft Exchange (Zero Days)
- Colonial Pipeline (Ransomware)
- Predicting What's Next
- What can <u>you</u> do?

WHOIS: Brad Rhodes

- WHOIS: Brad Rhodes
- TLDR:
  - ✔ Head of Cybersecurity at zvelo
  - ✔ COL, Cyber (17A), 76th Operational Response Command G6/CIO
  - ✔ Military Cyber Professionals Association, HammerCon Co-Lead
  - ✔ Speaker, Author, Professor, Coach
  - ✔ #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+

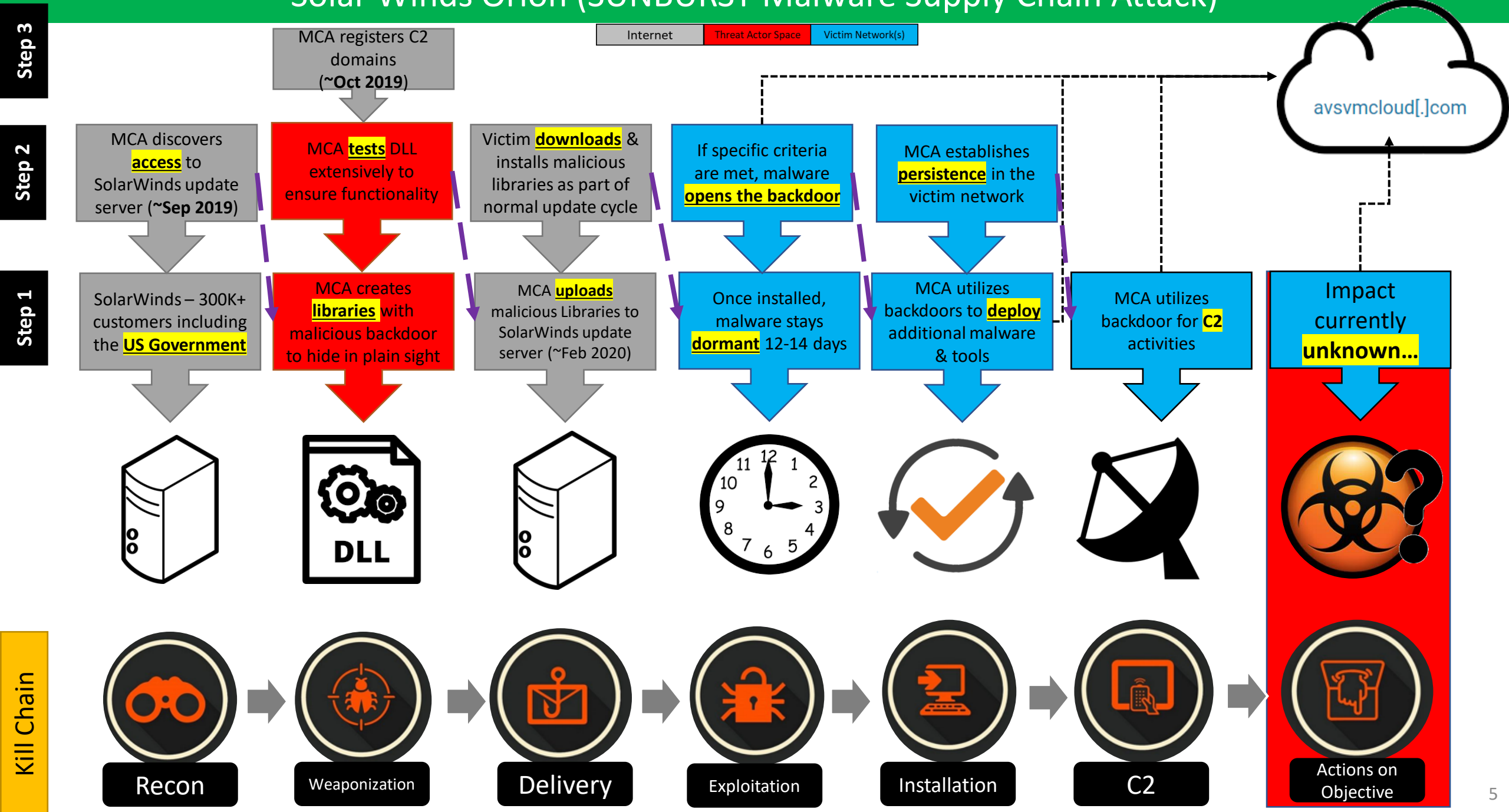
Feel to view/listen/grab my previous presentation/articles here:
https://github.com/cyberguy514

zvelo

Where to begin?

- The last 18+ months have been nuts!
  - A global pandemic
  - Lockdowns & restrictions
  - Massive shift to work from home / remote work
  - Emboldened malicious cyber actors (MCA)
  - Medicine and vaccine scams
  - Misinformation on just about everything
  - US Presidential election
  - US Capitol attack
  - Afghanistan withdrawal

Solar Winds Orion (SUNBURST Malware Supply Chain Attack)



SolarWinds Orion #cyberrealtalk

- Launched around the initial lockdowns in 2020
- Long MCA persistence (9+ months)
- Command and Control (C2) domains were registered in the United States
- MCA used Cobalt Strike droppers
- APT29 Cozy Bear is the prime suspect

avsvmcloud[.]com

databasegalore[.]com

deftsecurity[.]com

freescanonline[.]com

highdatabase[.]com

incomeupdate[.]com

panhardware[.]com

thedoccloud[.]com

websitetheme[.]com

zupertech[.]com

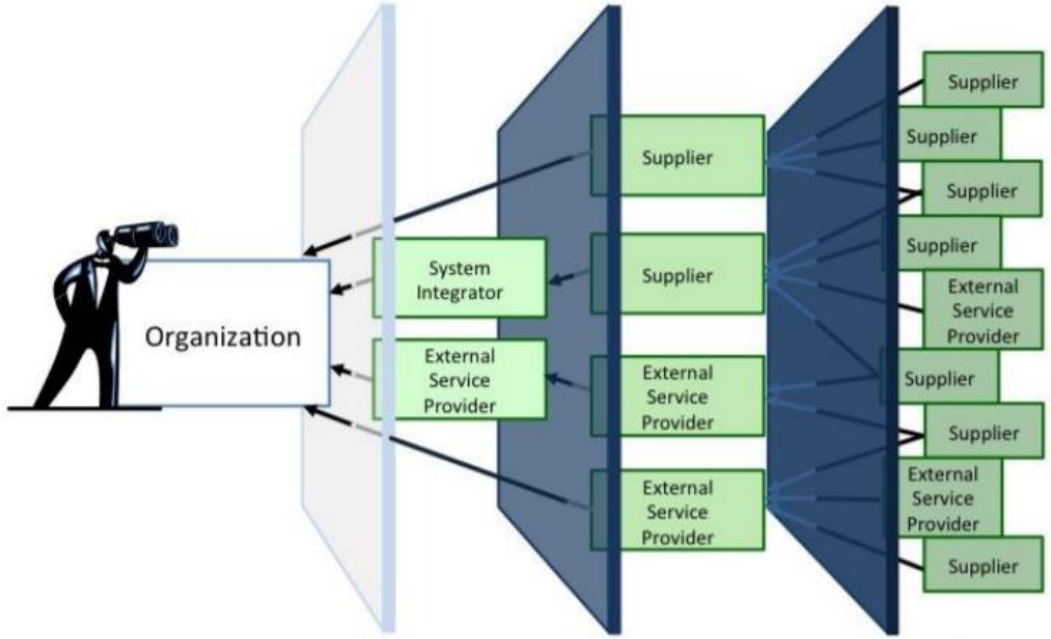
Ref: https://zvelo.com

Ref: https://www.cobaltstrike.com/

Ref: https://portswigger.net/

(Cyber) Supply Chains – Why should you care?

- **Everyone** has one!
  - Laptops/Desktops
  - Mobile Phones
  - Amazon
- The longer your supply chain, the less you "see"!
- Supply chains include:
  - Hardware
  - Software
  - Services
  - Cloud
  - And more…



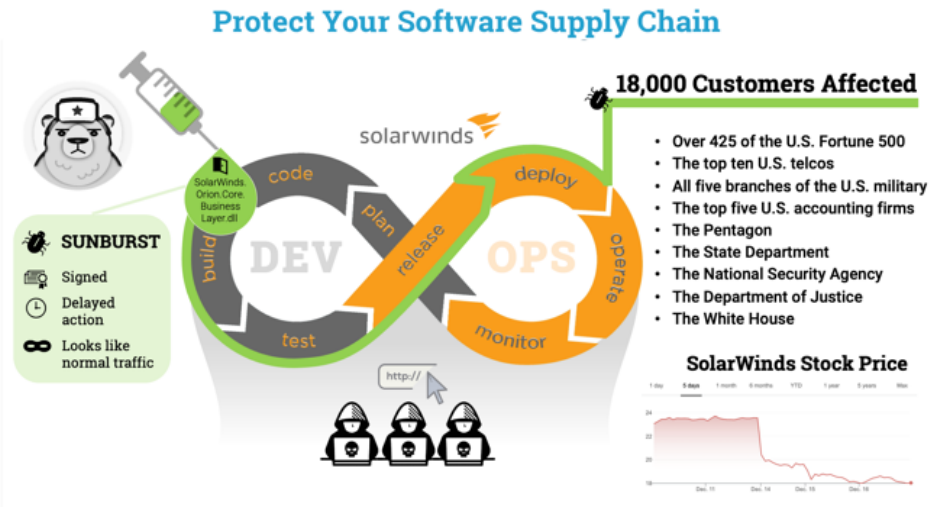
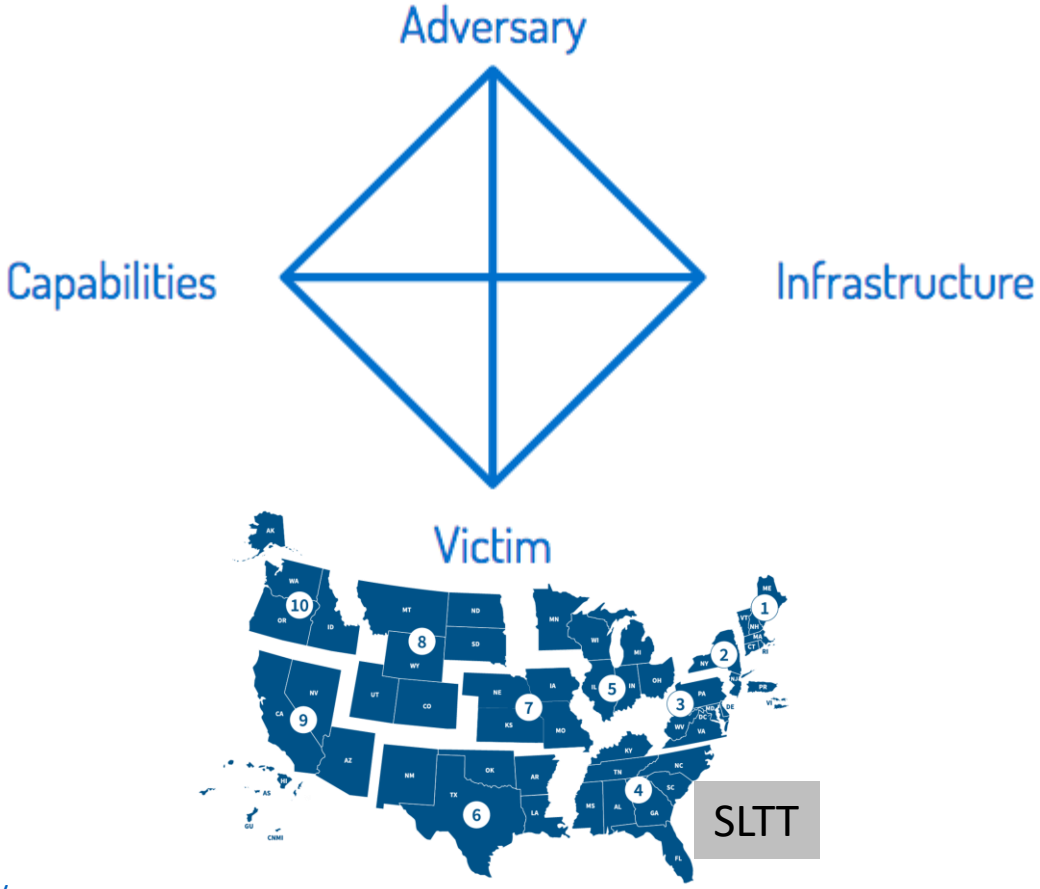


Image: https://blog.adolus.com/blog/three-things-the-solarwinds-supply-chain-attack-can-teach-us

Microsoft Exchange (Zero Days) Diamond Model

- CVE-2021-26855 is a server-side request forgery (SSRF) vulnerability in Exchange.
- CVE-2021-26857 is an insecure deserialization vulnerability in the Unified Messaging service.
- CVE-2021-26858 is a post-authentication arbitrary file write vulnerability in Exchange.
- CVE-2021-27065 is a post-authentication arbitrary file write vulnerability in Exchange.
- **Plus: ASPXSpy, China Chopper, PsExec**



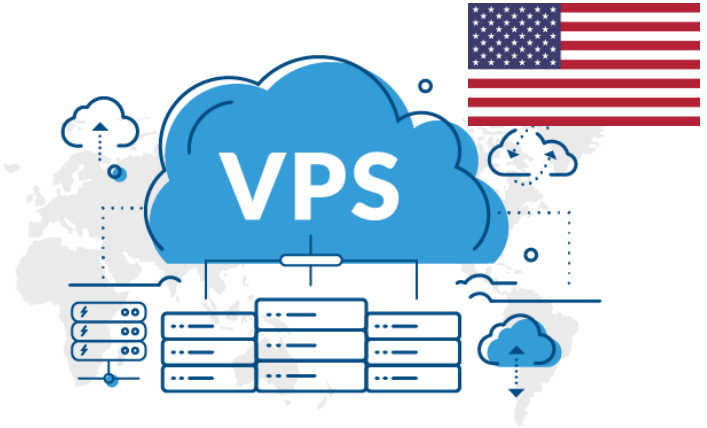


Image: https://www.atlantic.net/vps-hosting/

Ref: https://attack.mitre.org/groups/G0125/

Ref: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Microsoft Exchange #cyberrealtalk

"Research" tools make it easy for the MCAs

Widespread usage of local Microsoft Exchange / **Outlook Web Access** across State / Local / Tribal / Territorial government entities

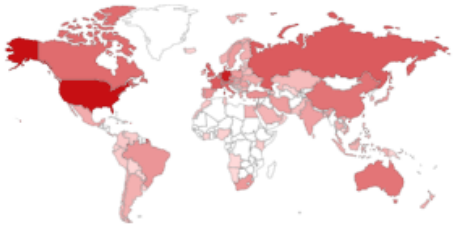
Different than SolarWinds Orion, but worse – affecting smaller organization without response capabilities or $$$

Prevented by patching

TOTAL RESULTS

365,427

TOP COUNTRIES



United States	84,708
Germany	63,916
France	17,774
United Kingdom	17,739
Russian Federation	17,214

Outlook Web App

[redacted]

United States, Buffalo

SSL Certificate

Issued By:

|- Common Name:

DigiCert SHA2 Secure Server CA

|- Organization:

DigiCert Inc

Issued To:

|- Common Name:

[redacted]

|- Organization:

[redacted]

Supported SSL Versions:

SSLv3, TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.5
request-id: 916dcb8a-990d-481f-a8c9-68c2614694c3
Set-Cookie: ClientId=IFEAAVWM0IDYYOQIDUCG; expires=Sat, 20-Aug-2022 16:27:23 GMT; path=/; HttpOnl...
```

Ref: https://www.shodan.io/

Zero Days – Why should you care?

- **Everyone** has them!
- You own products today with zero day vulnerabilities in them
- If you write your own code, you own the zero days vulnerabilities (and the MCAs will own you)
- Weaponization of zero days can be very <u>fast</u> (days to weeks)
- Are zero day scary? Yes! Are they the norm? **No!**

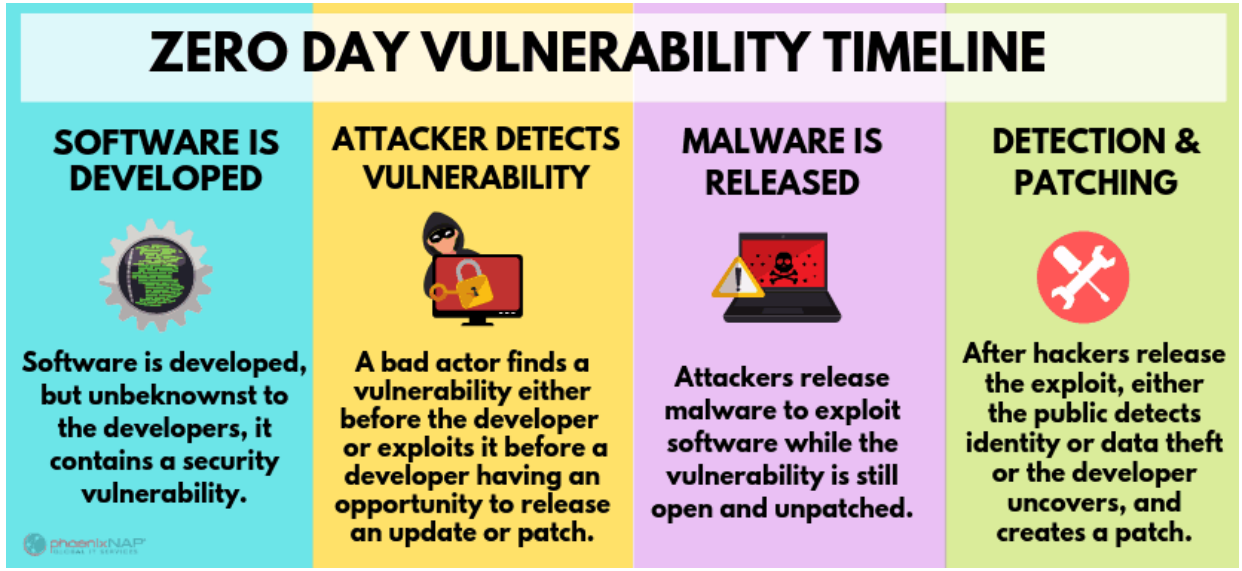
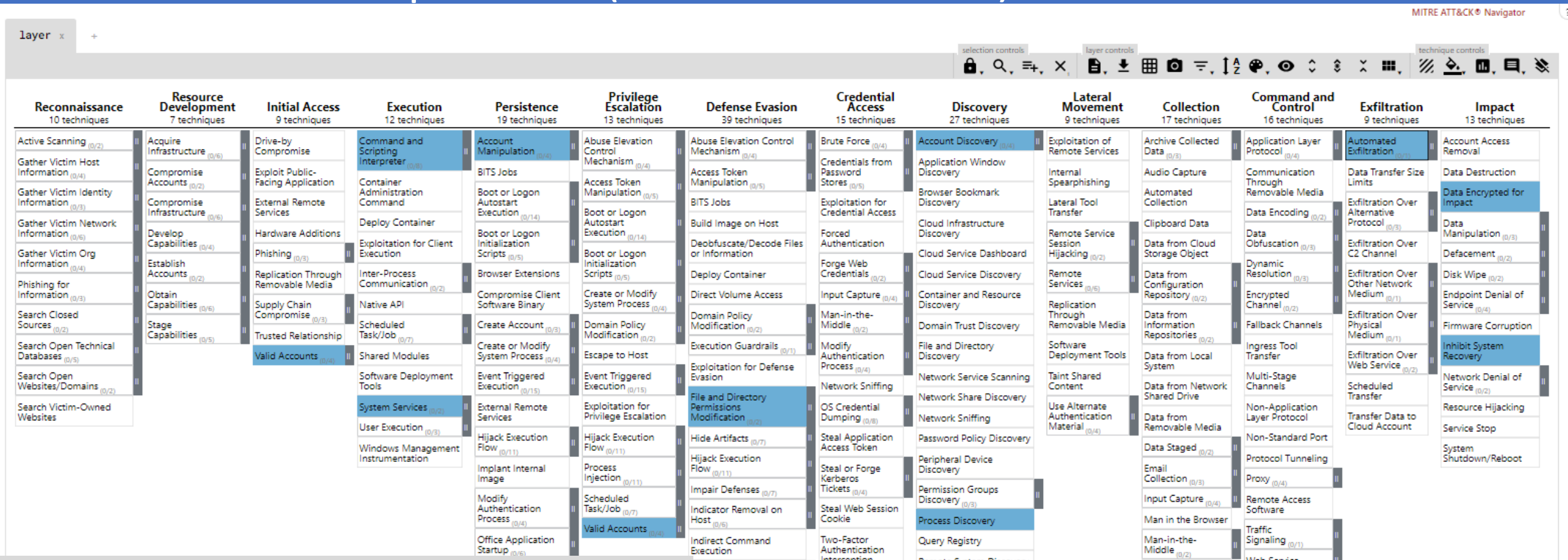


Image: https://phoenixnap.com/blog/what-is-a-zero-day-exploit

Image: https://www.varonis.com/blog/zero-day-vulnerability/

Colonial Pipeline (Ransomware) MITRE ATT&CK



- System Information Discovery (https://attack.mitre.org/techniques/T1082/)
- Process Discovery (https://attack.mitre.org/techniques/T1057/)
- Valid Accounts (https://attack.mitre.org/techniques/T1078/)
- Account Manipulation (https://attack.mitre.org/techniques/T1098/)
- Command and Scripting Interpreter (https://attack.mitre.org/techniques/T1059/)
- System Services (https://attack.mitre.org/techniques/T1569/)
- Account Discovery (https://attack.mitre.org/techniques/T1087/)
- File and Directory Permissions Modification (https://attack.mitre.org/techniques/T1222/)
- Data Encrypted for Impact (https://attack.mitre.org/techniques/T1486/)
- Inhibit System Recovery (https://attack.mitre.org/techniques/T1490/)
- Exfiltration (https://attack.mitre.org/tactics/TA0010/)

Built with: https://mitre-attack.github.io/attack-navigator/

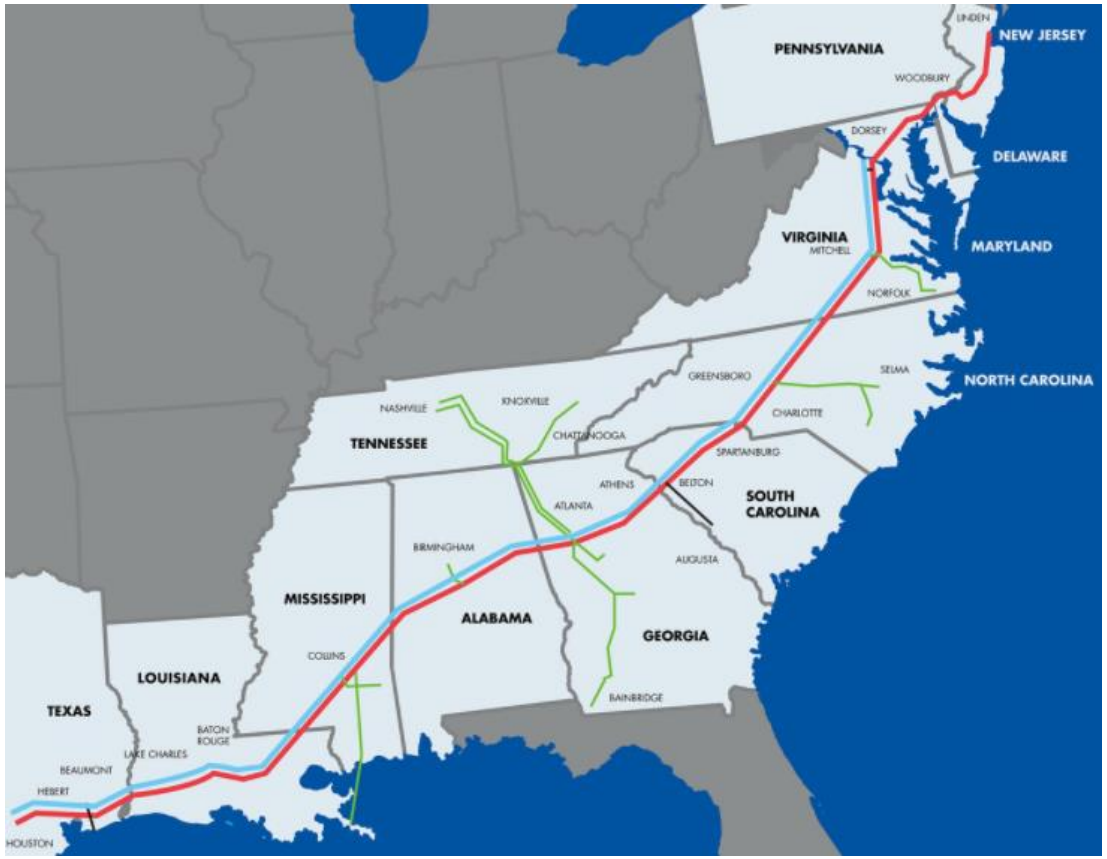
Colonial Pipeline **#cyberrealtalk**

Target of opportunity

DarkSide threat actors threatened to release data unless the ransom was paid

Paid the ransom (yes, the FBI got some of it back)

Gave the bad guys a “playbook” for causing a panic in the United States



https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/

Ransomware – Why should you care?

- **Everyone** is a potential victim!
- Ransomware is designed to move very FAST!
- Ransomware-as-a-Service (RaaS) is proliferating
- Ransomware developers excel at “living off the land” (using Powershell, psexec, even GPO)
- MCAs leveraging ransomware do their homework on you

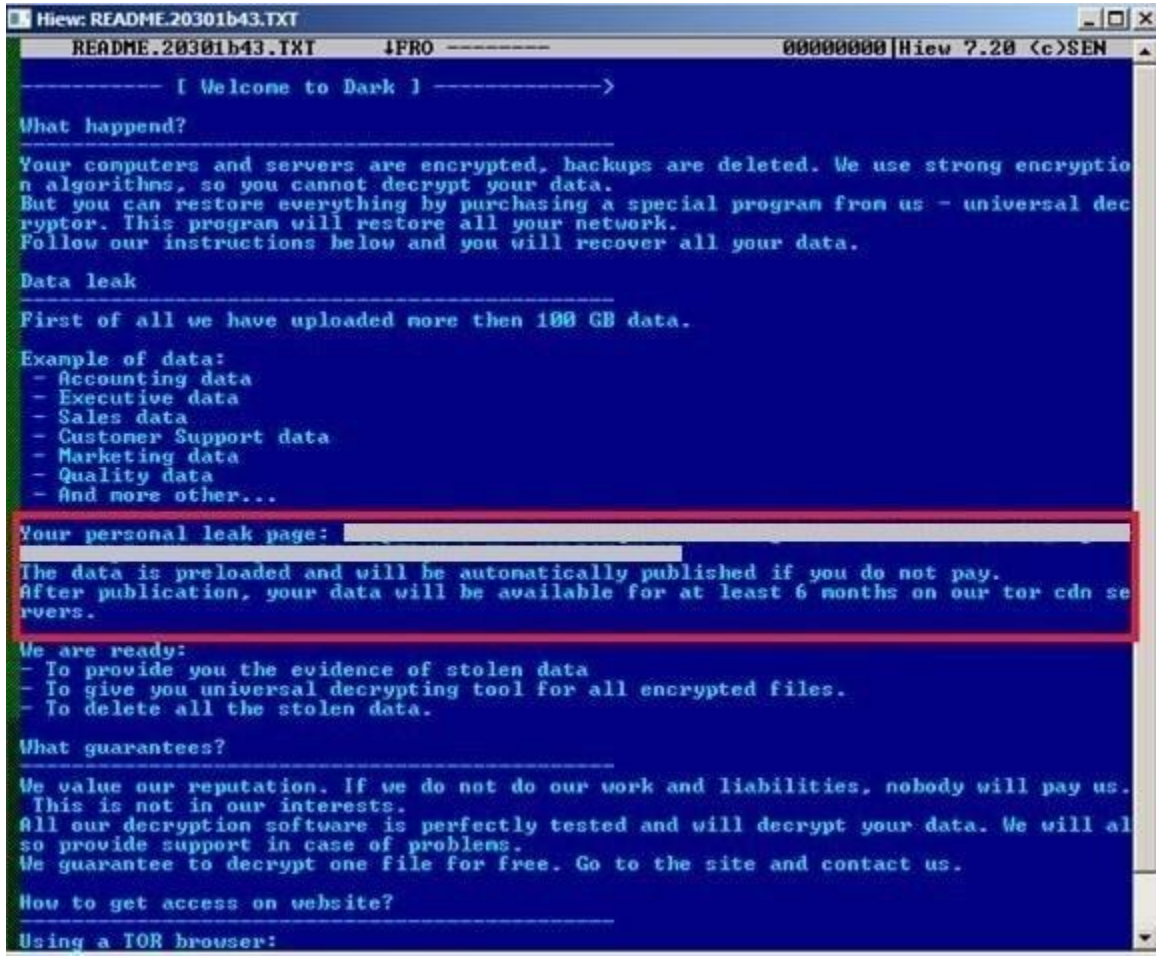


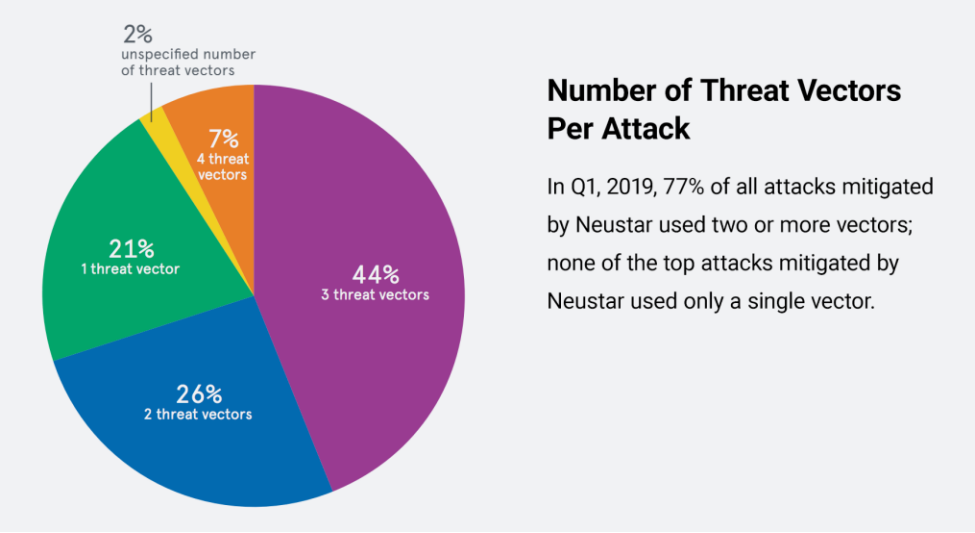
Image: https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

Resource: https://www.cisa.gov/stopransomware/resources

Predicting what’s next…

Image: https://www.vadesecure.com/en/

Image: https://arconnet.com/



Ref: https://circleid.com/posts/20190428_large_attacks_growing_as_multi_vector_exploits_increase

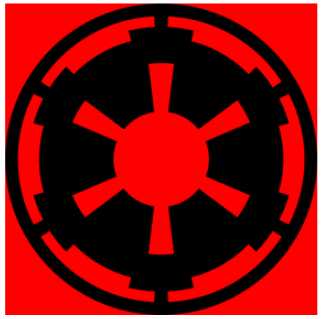
What can you do?

- Learn your **supply chains**!
- Understand what you have **exposed on the web** – it is being targeted right now!
- Code reviews and involve your cybersecurity teams at the **beginning** of development, not the end.
- **Don't pay ransoms**! Please don't pay ransoms – don't be afraid to get law enforcement involved.
- Be willing to **share** (anonymized) Indicators of Compromise (IOC)!
- Follow **standards**:
  - Center for Internet Security (CIS) Top 20: https://www.cisecurity.org/controls/cis-controls-list/
  - Australian Signals Directorate (ASD) Top 8: https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-explained
- *Allocate budget for **training**!*
- **Trust your gut – if something feels wrong, it probably is!**

Blue Space (Good)

Gray Space (Internet)

Red Space (Bad)



Thank you, US Department of Transportation!

For the honor and privilege of this speaking opportunity!

Questions?

Presentation(s) on GitHub:
https://github.com/cyberguy514/presentations

Contact Details:

Civilian: brhodes@zvelo.com

Military: brad.e.rhodes.mil@mail.mil

MCPA: brad.rhodes@milcyber.org

LinkedIn: https://www.linkedin.com/in/brad-rhodes-1951ba7/

Twitter: @cyber514