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 you do?

#### **WHOIS: Brad Rhodes**

- WHOIS: Brad Rhodes
- TLDR:
  - ✓ Head of Cybersecurity at zvelo
  - ✓ COL, Cyber (17A), 76<sup>th</sup> 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



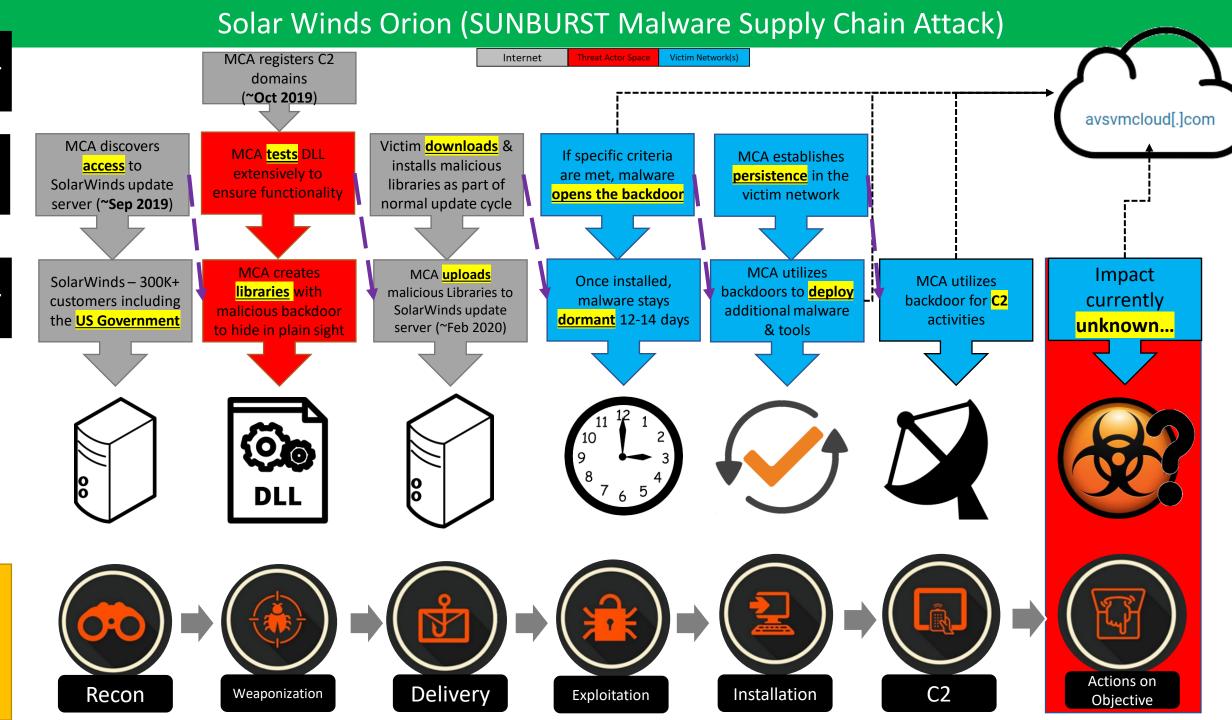






# Where to begin?

- 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



#### 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



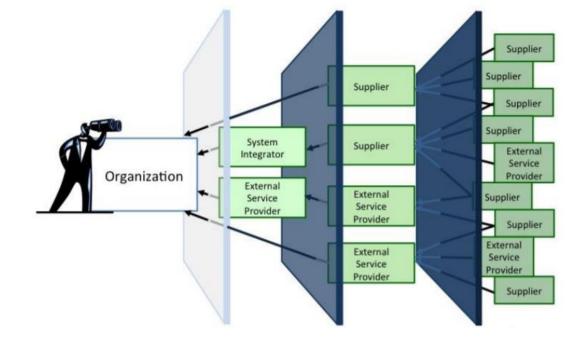
Ref: https://www.cobaltstrike.com/



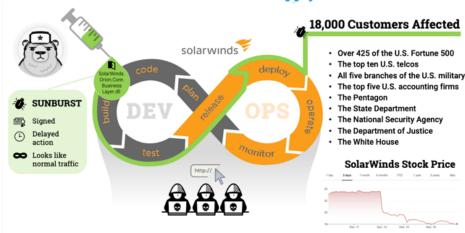
Ref: https://portswigger.net/

### (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...



#### **Protect Your Software Supply Chain**



#### Microsoft Exchange (Zero Days) Diamond Model



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

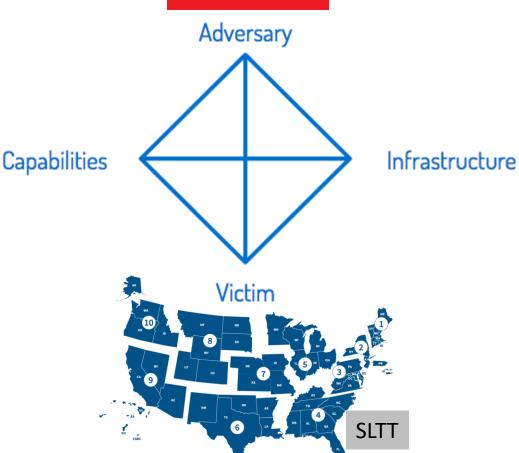




Image: https://www.atlantic.net/vps-hosting/

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

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

#### Microsoft Exchange #cyberrealtalk

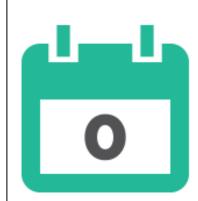
"Research" tools make it easy for the MCAs

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







#### 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!

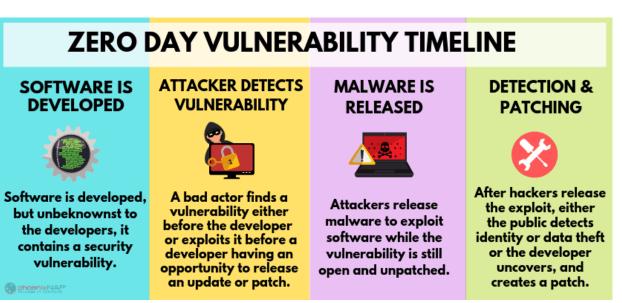


Image: https://phoenixnap.com/blog/what-is-a-zero-day-exploit



#### Colonial Pipeline (Ransomware) MITRE ATT&CK

MITRE ATT&CK® Navigator layer Privilege Escalation Credential Command and Resource Lateral Initial Access Defense Evasion Collection Exfiltration Reconnaissance Development Execution Persistence Access Discovery Movement Control Impact 39 techniques 10 techniques 7 techniques 9 techniques 12 techniques 19 techniques 13 techniques 15 techniques 27 techniques 9 techniques 17 techniques 16 techniques 9 techniques 13 techniques Abuse Elevation Control Drive-by ommand and Abuse Elevation Brute Force Account Discovery Exploitation of Archive Collected Application Layer utomated Account Access Active Scanning Acquire nfrastructure Compromise cripting Manipulation Control Mechanism Remote Services Data, rotocol xfiltration Removal Mechanism Gather Victim Host nterpreter Credentials from Application Window Exploit Public-Information ..... Compromise BITS Jobs Access Token Password Discovery Internal Audio Capture Communication Data Transfer Size Data Destruction Access Token Accounts max Facing Application Container Manipulation Stores m/s Spearphishing Through Gather Victim Identity Boot or Logon Browser Bookmark Automated Removable Media Data Encrypted for Administration Manipulation, External Remote BITS Jobs Exploitation for Lateral Tool Exfiltration Over Information Compromise Command Autostart Discovery Collection Infrastructure Services Execution Boot or Logon Credential Access Transfer Data Encoding Alternative Deploy Container Autostart Build Image on Host Cloud Infrastructure Clipboard Data Protocol Data Gather Victim Network Information. Develop Hardware Additions Boot or Logon Execution, Forced Discovery Remote Service Data Manipulation ... Exploitation for Client Deobfuscate/Decode Files Data from Cloud Obfuscation, Exfiltration Over Capabilities, nitialization Authentication Session Phishing Cloud Service Dashboard Storage Object C2 Channel Defacement ,, Gather Victim Ord Execution Scripts, Boot or Logon or Information Hijacking. Information Establish nitialization Forge Web Dynamic Browser Extensions Exfiltration Over Inter-Process Remote Accounts Replication Through Scripts ... Deploy Container Credentials Cloud Service Discovery Data from Resolution Disk Wipe " Phishing for Communication Services Other Network Removable Media Configuration Create or Modify Information Obtain Compromise Client Direct Volume Access Input Capture, Container and Resource Repository (n/ Encrypted Medium Endpoint Denial of Capabilities . Native API Software Binary System Process Discovery Replication Supply Chain Channel ... Service Exfiltration Over Search Closed Compromise Domain Policy Man-in-the-Through Data from Sources Stage Create Account Domain Policy Modification, Middle Domain Trust Discovery Removable Media Information Fallback Channels Physical Firmware Corruption Capabilities Modification, Repositories Medium, Trusted Relationship Task/Job Software ngress Tool Search Open Technical Create or Modify Execution Guardrails Modify File and Directory Inhibit System Escape to Host Deployment Tools Exfiltration Over Databases, Valid Accounts Shared Modules System Process Authentication Discovery Data from Local Transfer Recovery Web Service Process in /a Exploitation for Defense Software Deployment Event Triggered Event Triggered Taint Shared Multi-Stage Search Open Network Denial of Evasion Network Service Scanning Websites/Domains Execution in Network Sniffing Data from Network Channels Scheduled Service, Shared Drive Transfer ile and Directory Network Share Discovery Search Victim-Owned External Remote Exploitation for OS Credential Use Alternate Non-Application Resource Hijacking Privilege Escalation lodification Authentication Transfer Data to Websites Services Dumping (n/8) Network Sniffing Data from Layer Protocol Material Cloud Account Removable Media Service Stop Hijack Execution Hijack Execution Steal Application Non-Standard Port Hide Artifacts ,, Password Policy Discovery Windows Management Access Token Data Staged System Shutdown/Reboot Hijack Execution Protocol Tunneling Instrumentation Peripheral Device Process Implant Internal Steal or Forge Discovery Injection Kerberos Collection In/3 Proxy .... Image mpair Defenses .... Tickets... Permission Groups Modify Scheduled Input Capture, Remote Access Discovery , Steal Web Session Authentication Task/Job Indicator Removal on Software Process Cookie Man in the Browser Process Discovery Valid Accounts Traffic Office Application Indirect Command Two-Factor Query Registry Man-in-the-Signaling Authentication Middle, Interception Remote System Discovery Web Service . System Information Discovery (https://attack.mitre.org/techniques/T1082/) Masquerading Screen Capture Unsecured Software Discovery Process Discovery (https://attack.mitre.org/techniques/T1057/) Credentials Video Capture Modify Authentication stem Information Process my Valid Accounts (https://attack.mitre.org/techniques/T1078/) Modify Cloud Compute nfrastructure System Location Account Manipulation (https://attack.mitre.org/techniques/T1098/) Discovery Modify Registry Command and Scripting Interpreter (https://attack.mitre.org/techniques/T1059/) System Network Modify System Image Configuration System Services (https://attack.mitre.org/techniques/T1569/) Discovery ,, Network Boundary Account Discovery (https://attack.mitre.org/techniques/T1087/) Bridging System Network File and Directory Permissions Modification (https://attack.mitre.org/techniques/T1222/) **Dbfuscated Files or** 

Data Encrypted for Impact (<a href="https://attack.mitre.org/techniques/T1486/">https://attack.mitre.org/techniques/T1486/</a>)
 Inhibit System Recovery (<a href="https://attack.mitre.org/techniques/T1490/">https://attack.mitre.org/techniques/T1486/</a>)

• Exfiltration (https://attack.mitre.org/tactics/TA0010/)

#### 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

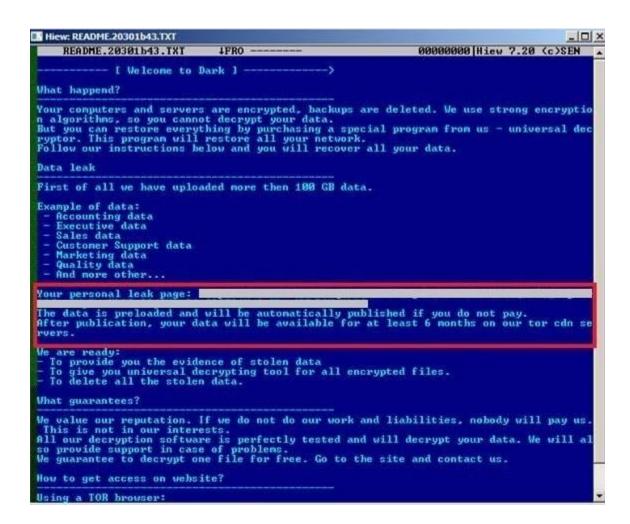


Image: <a href="https://www.trendmicro.com/en\_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html">https://www.trendmicro.com/en\_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html</a>

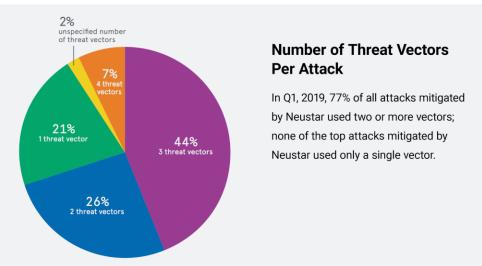
# Predicting what's next...







Image: <a href="https://arconnet.com/">https://arconnet.com/</a>



#### 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: <a href="https://www.cisecurity.org/controls/cis-controls-list/">https://www.cisecurity.org/controls/cis-controls-list/</a>
  - Australian Signals Directorate (ASD) Top 8: <a href="https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-explained">https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-explained</a>
- Allocate budget for training!
- Trust your gut if something feels wrong, it probably is!

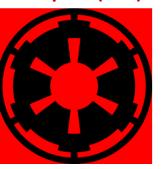
**Blue Space (Good)** 



**Gray Space (Internet)** 



Red Space (Bad)



# Thank you, US Department of Transportation!

For the honor and privilege of this speaking opportunity!



Presentation(s) on GitHub:
<a href="https://github.com/cyberguy5">https://github.com/cyberguy5</a>
14/presentations

### Questions?

#### **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