Current Cyber Threats & the Impact of SolarWinds

Brad Rhodes

Colossal Colorado Virtual Industry Event 2021

Outline

- WHOIS
- The Cyberspace Frame
- Attacker “Families”
- Defender “Families”
- Tools of the Trade
- Attack Surfaces & Vectors
  - Web
  - Network Systems
  - Endpoints
  - Internet of Things
  - People
- Live Attack Demo
- Current Cyber Threats
  - Phishing & Social Engineering
  - Business Email Compromise
  - Clouds & Third Parties
  - Ransomware
  - Disinformation
- The Impact of SolarWinds
  - Do you know your supply chain?
- 2021 Strikes Back
  - Microsoft Exchange
  - CNA Ransomware
  - Ubiquiti
- Protecting You and Your Business

WHOIS

WHOIS: Brad Rhodes

TLDR:

- Head of Cybersecurity at zvelo
- LTC, Cyber (17A) Colorado Army National Guard & Cyber Shield OIC
- Military Cyber Professionals Association, HammerCon Co-Lead
- Speaker, Author, Professor, Instructor, Coach
- #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, PMP, CEH, GMON, GCIH, RHCSA, CCNA Cyber Ops, CySA+

zvelo
We categorize the Web

ARMY NATIONAL GUARD COLORADO

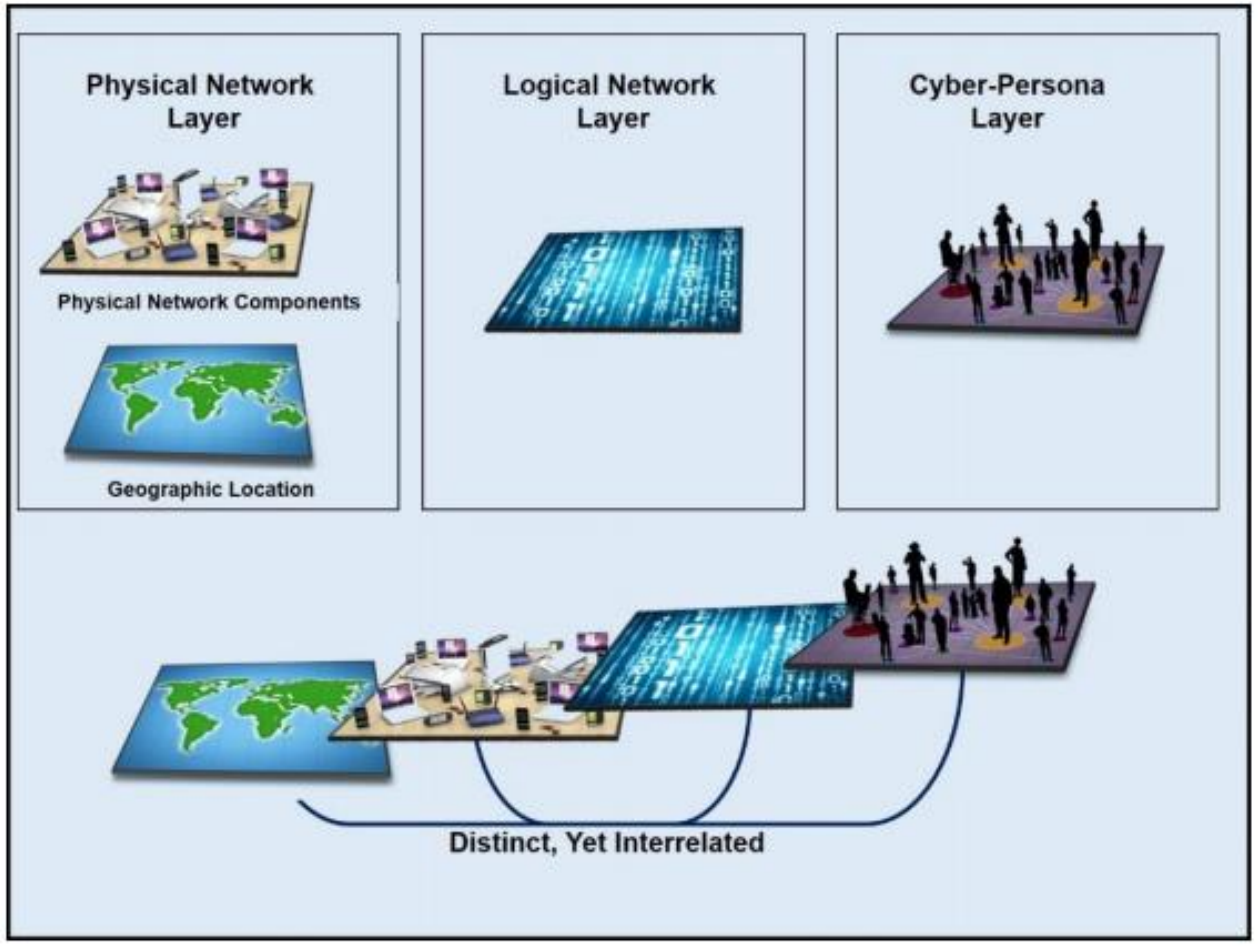
CYBER SHIELD 2021 DEFEND · ATTACK · EXPLOIT

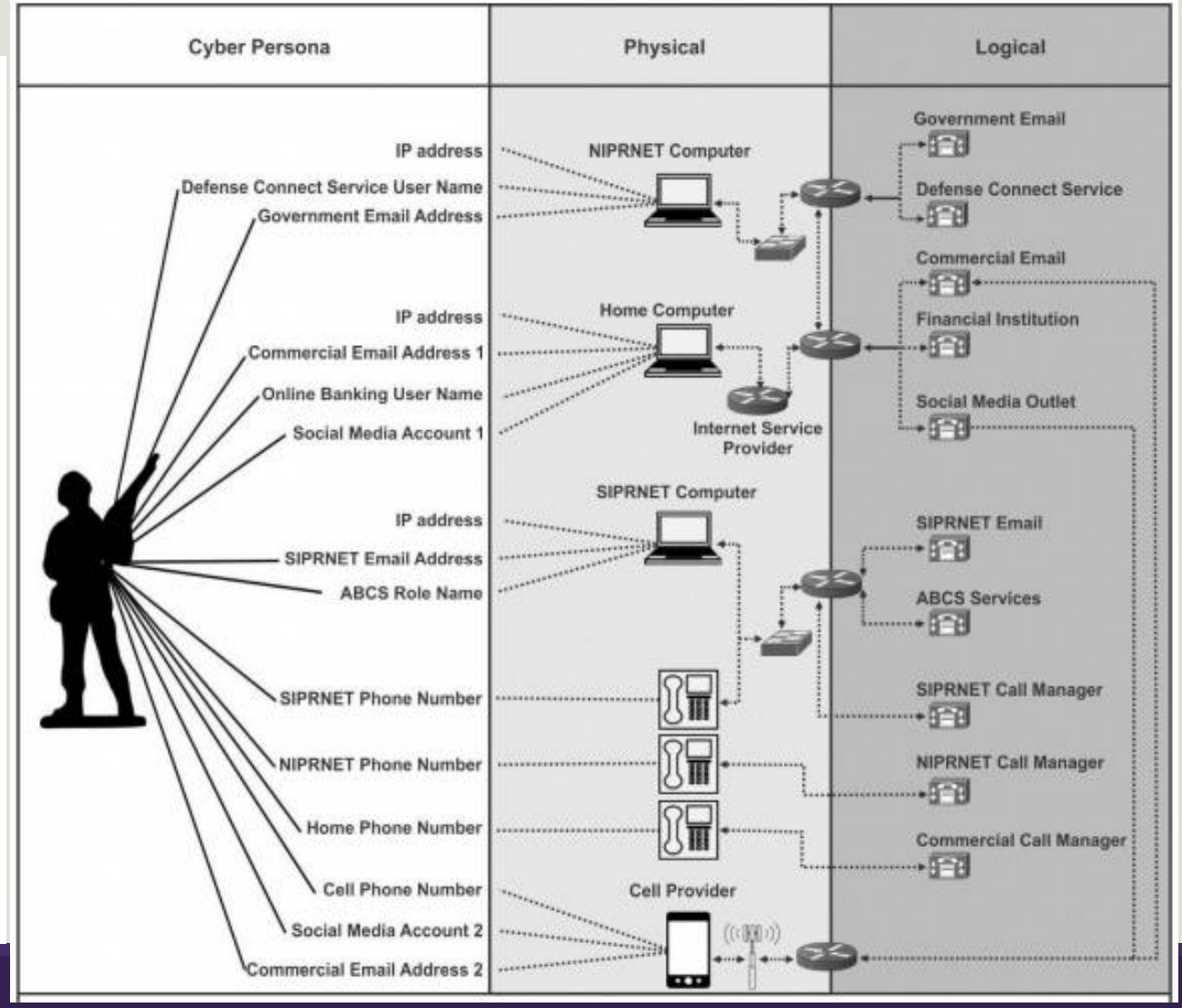
UNIVERSITAS REGISIANA SOCIETATIS JESU 1877 IHS MEN AND WOMEN IN SERVICE OF OTHERS

GU

CYBRARY

COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021



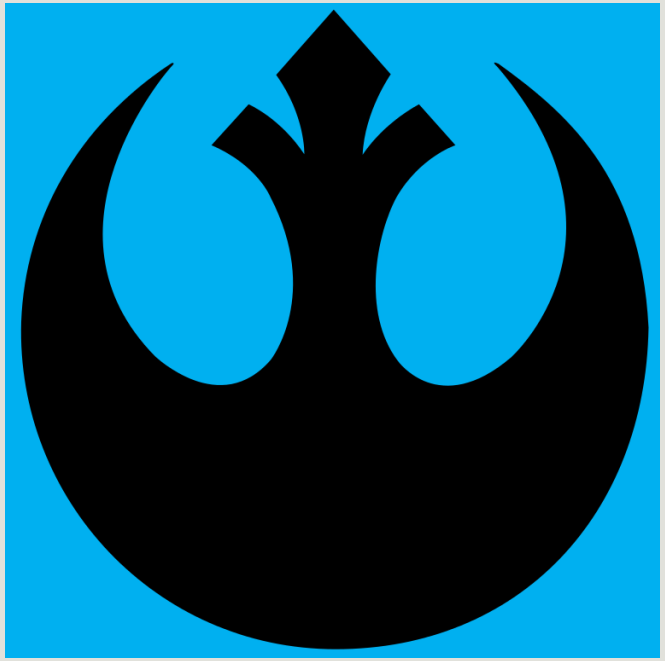


The Cyberspace Frame (1 of 2): Layers

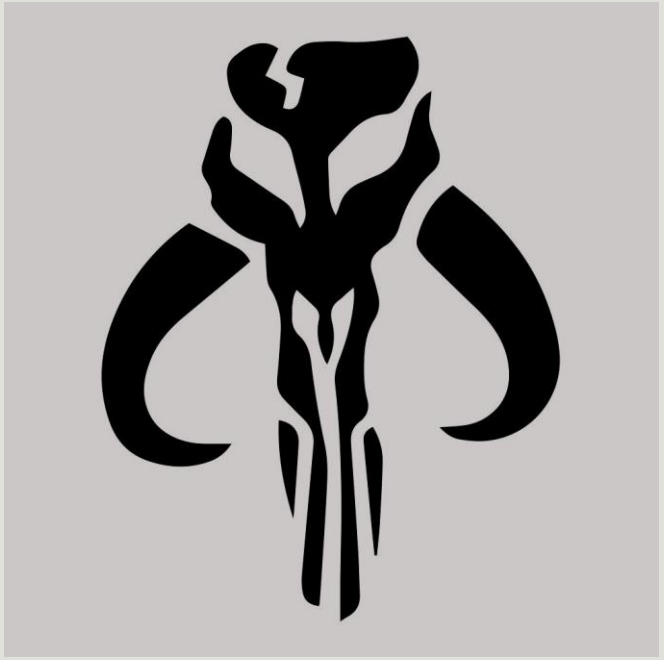
Ref: https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf

Ref: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf

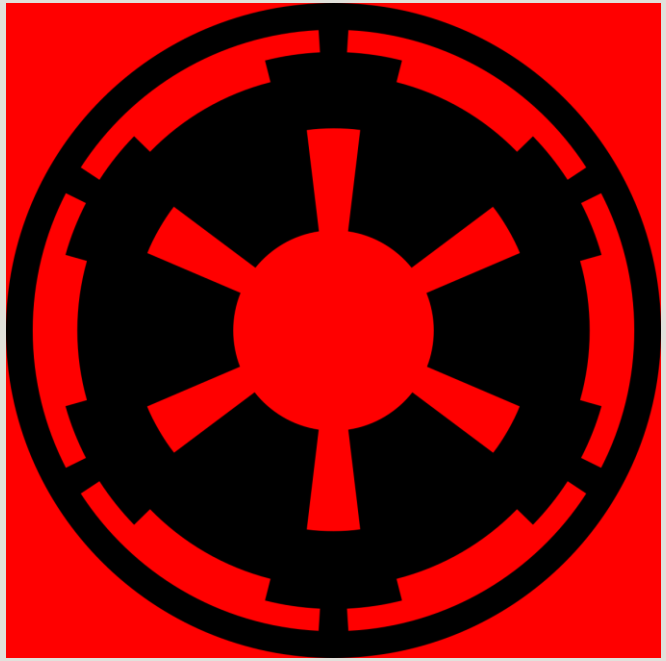
Blue Space (Good)



Gray Space (Internet)

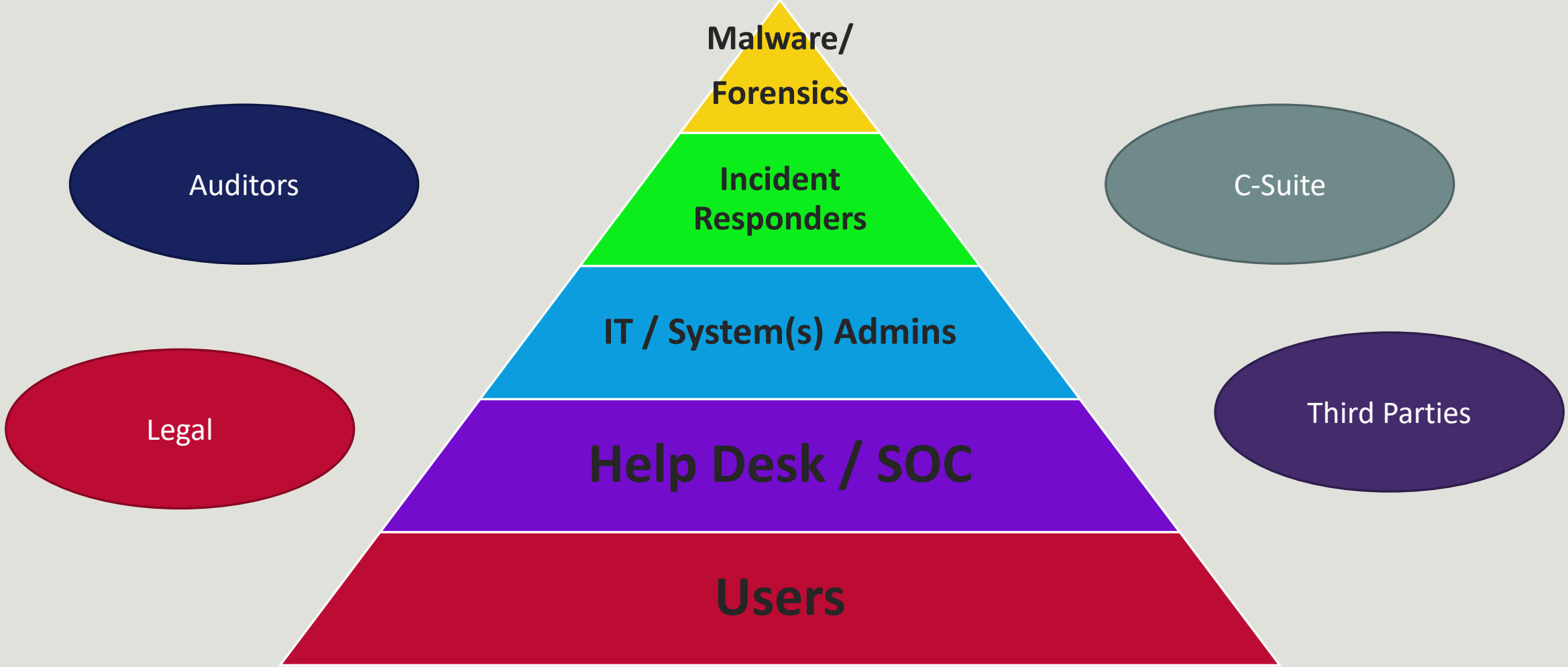


Red Space (Bad)



The Cyberspace Frame (2 of 2): A Different View

Attacker “Families”



Defender “Families”

80% of the Threat Actors work is here!

All this work happens in your network & systems!

Recon	Weaponization	Delivery	Exploitation	Installation	C2	Actions on Objective
Weeks-Years	Days-Years	Minutes-Hours	Minutes-Hours	Seconds-Minutes	Minutes-Years	Minutes-Years
Free	Free	Free < $10	Free	Free	Free < $10	Free < $10

Per IBM, the global average for breach detection in 2019 was 206 days!!

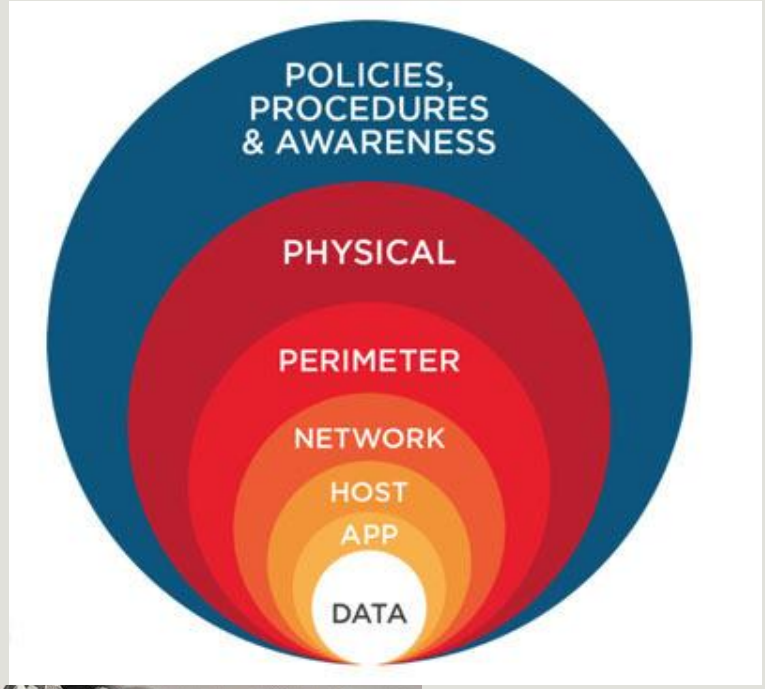
Recon	Weaponization	Delivery	Exploitation	Installation	C2	Actions on Obj
- Google (P) - Spyse (P) - Wireshark (P) - Shodan (P) - Nmap (A) - OpenVAS (A) - Nikto (A) - Metasploit (A)	- Commodities - Custom Code - Infrastructure - Personas	- Phishing - Pharming - Watering Holes - Drive-Bys - Brute Force	- Metasploit - Cobalt Strike - Live off the Land	- Live off the land - Persistence	- Beacons - Call backs - Back Doors	- Data exfiltration - Data mod. - Sabotage - Destruction

Tools of the Trade (1 of 2): Attackers

Ref: https://www.kali.org/

Ref: https://opensource.org/

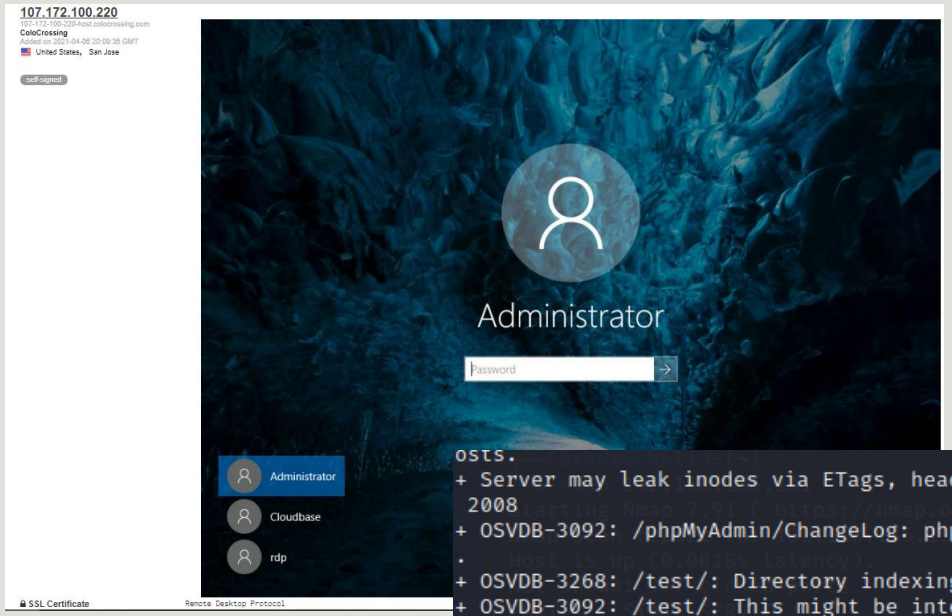
Defense Area	Tools
Policies, Procedures, & Awareness	Acceptable Use Policy, Multi-Factor Policy, Password Policy, Business Continuity Plan, Disaster Recovery Plan, Training, etc…
Physical	Bollards, Fences, Guard, Locks, Key Cards, System Logs
Perimeter	Firewalls, Intrusion Detection/Prevention Systems, Device Logs
Network	Netflow, Device Logs
Host	Endpoint Detection & Response (EDR), Mobile Device Management (MDM), Host Logs
Application	Whitelisting, Application Logs
Data	Data Loss Prevention (DLP), Database Logs



Other Tools (to put all the "pieces" together):
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)
- Threat Hunting Platforms
- Cyber Threat Intelligence (CTI) feeds

Tools of the Trade (2 of 2): Defenders

Ref: https://www.gotyoursixcyber.com/portfolio-item/defense-in-depth/




```
osts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 405
 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected
.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This give
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be p
zed hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or
+ 8726 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2021-04-06 14:47:59 (GMT-6) (51 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

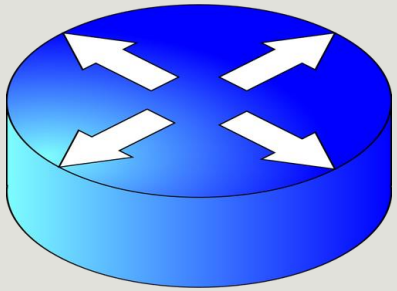
SHODAN

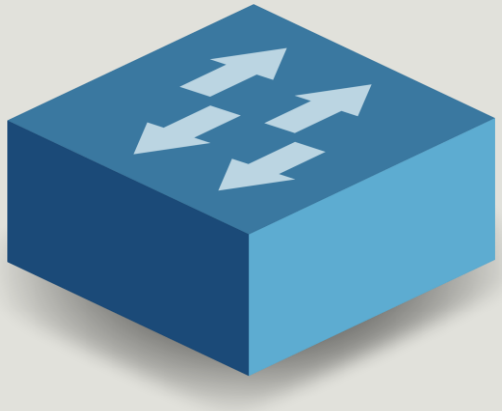
TM

Microsoft IIS

Images: Copyright Microsoft, Apache, WordPress, shodan.io

Attack Surfaces: Web



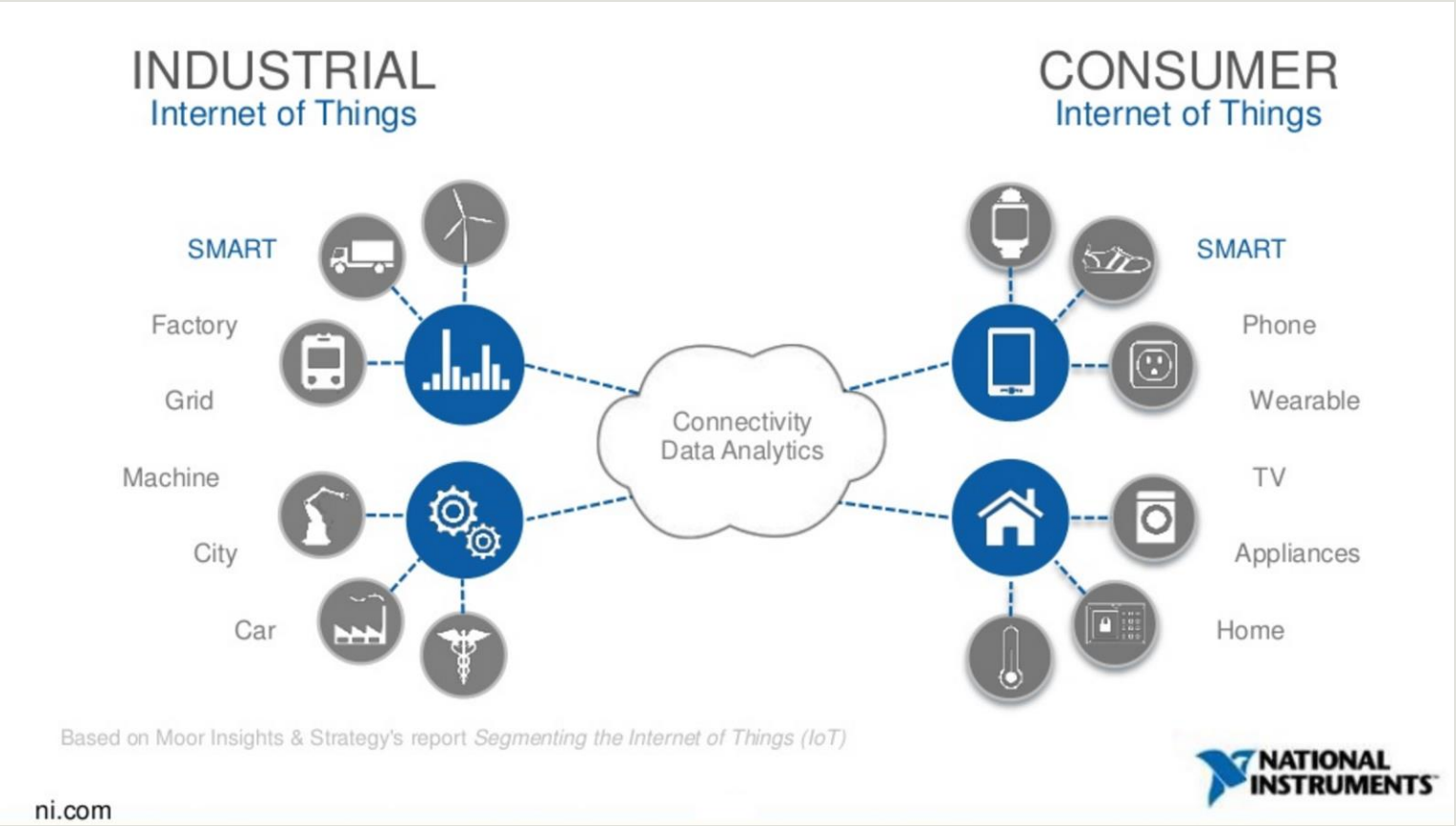


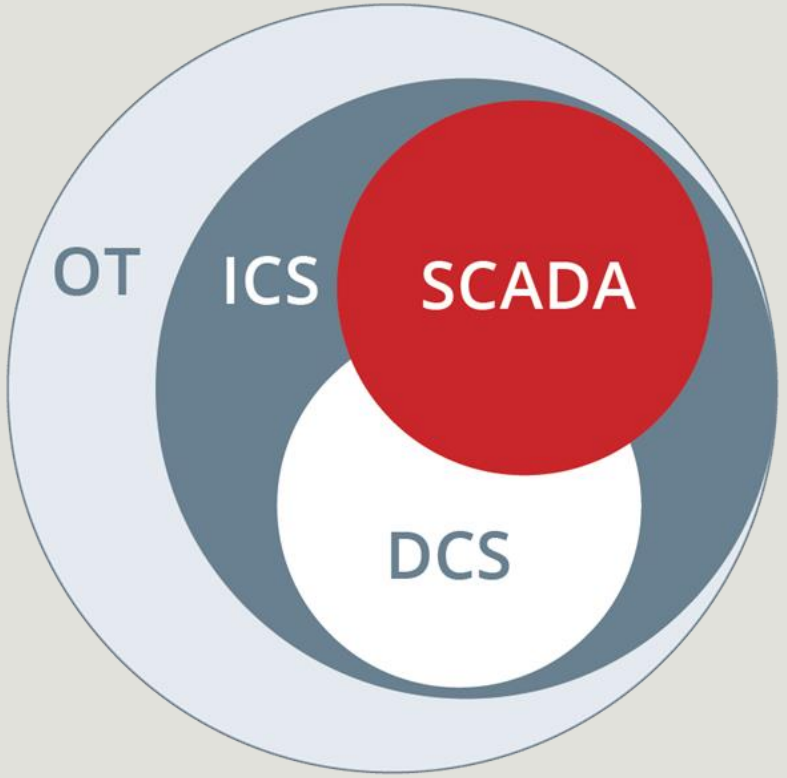
Attack Surfaces: Network Systems

Attack Surfaces: End Points

COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021





Operational Technology (OT)
Industrial Control Systems (ICS)
Distributed Control Systems (DCS)
Supervisory Control And Data Acquisition (SCADA)

Attack Surfaces: Internet of Things

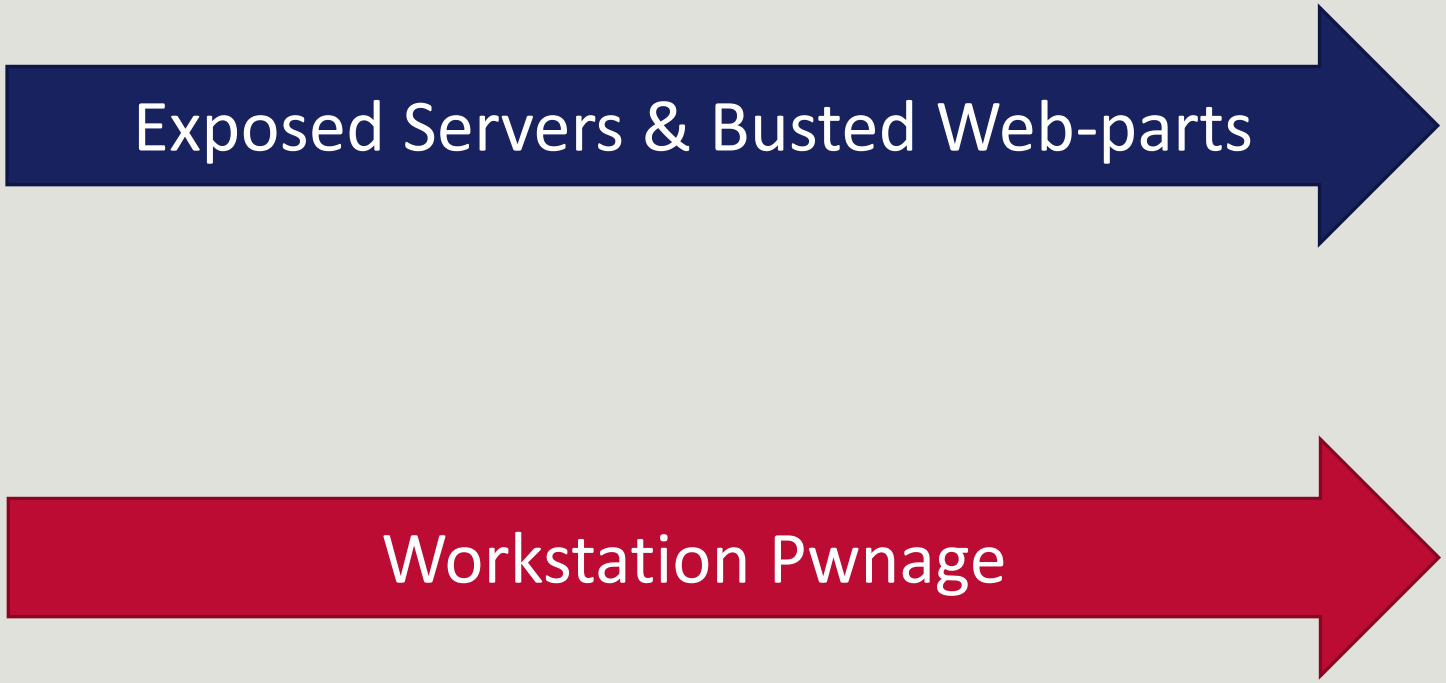
Ref: https://blogs.grammatech.com/tackling-the-software-development-challenges-of-the-industrial-internet-of-things

Ref: https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/

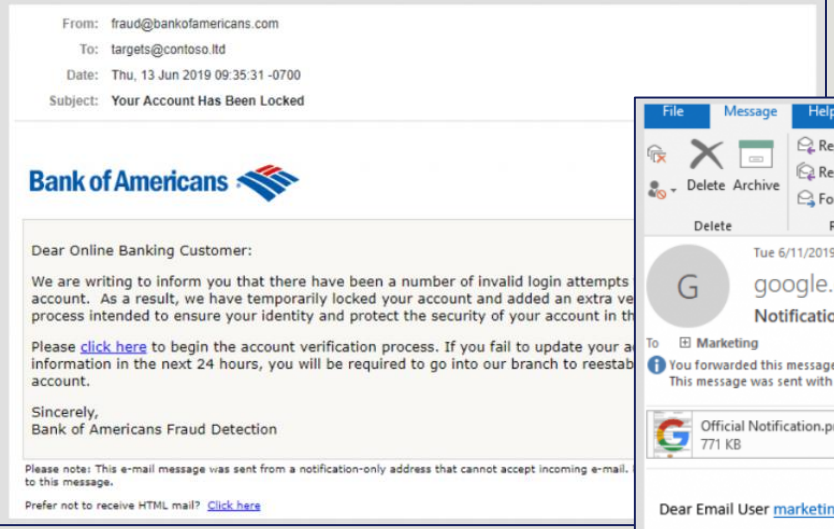
- C-Suite/Executives
- Support Staff
- Users

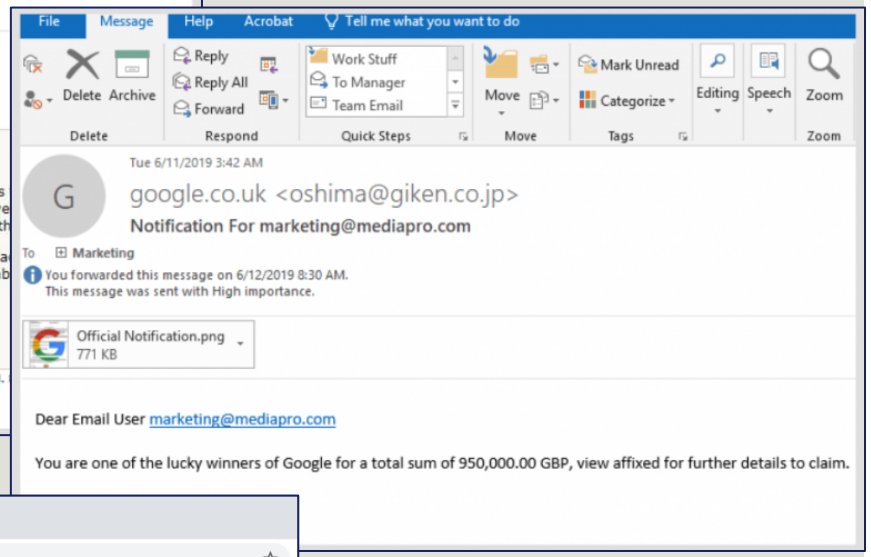
Attack Surfaces: People

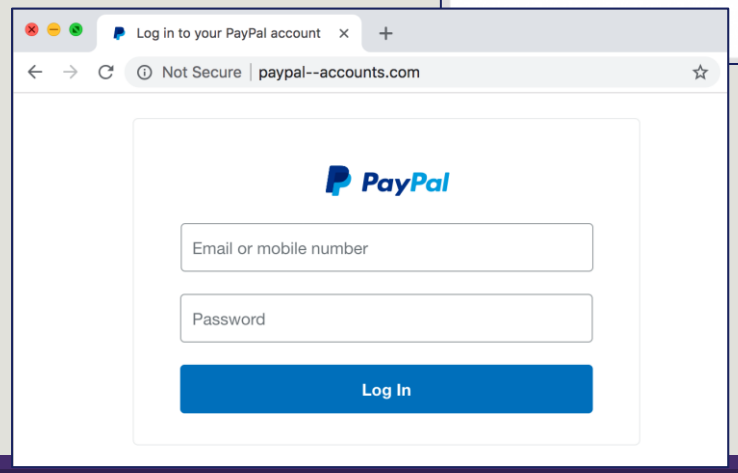
Live Attack Demo



COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021







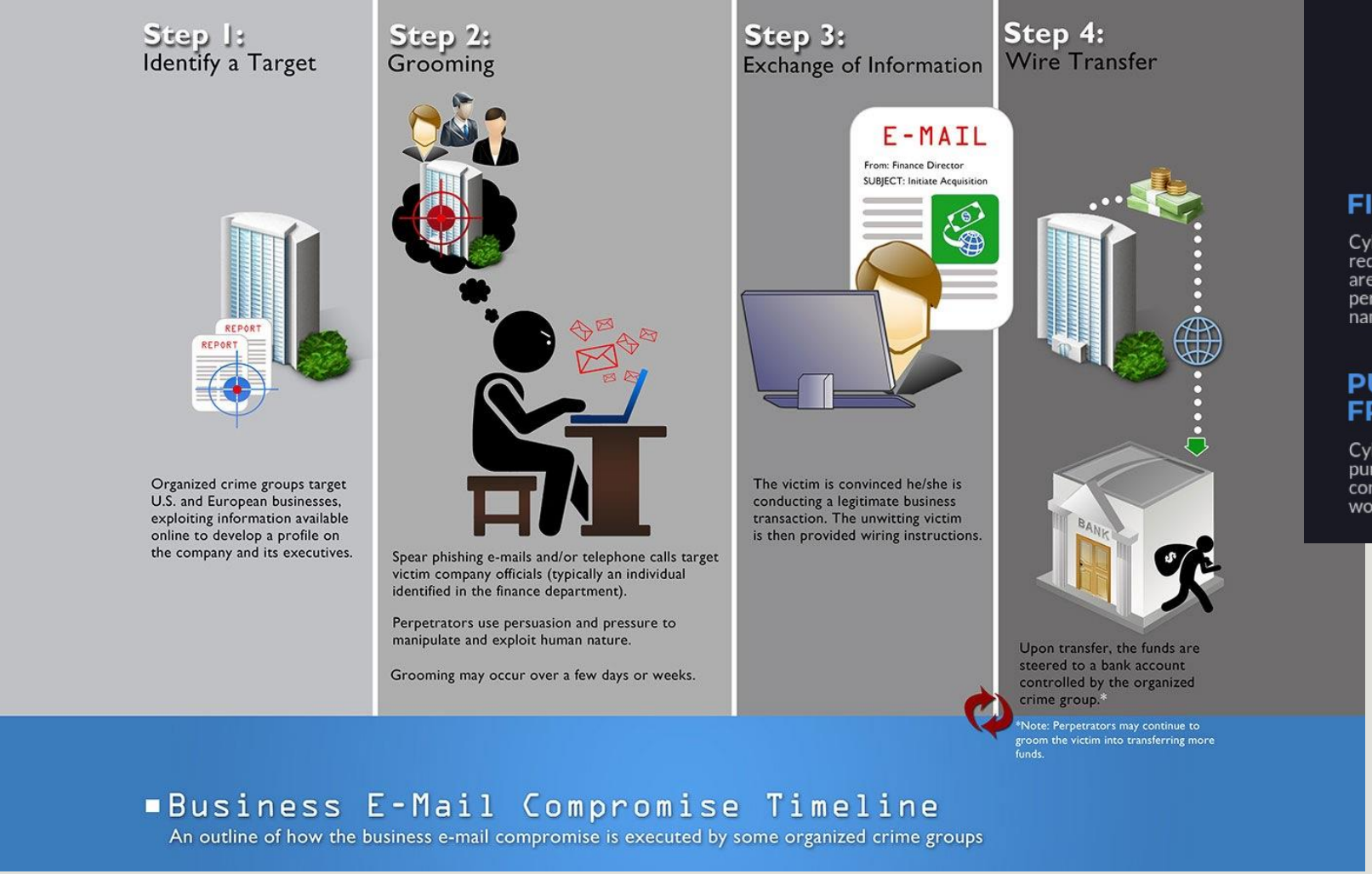
Current Cyber Threats: Phishing & Social Engineering

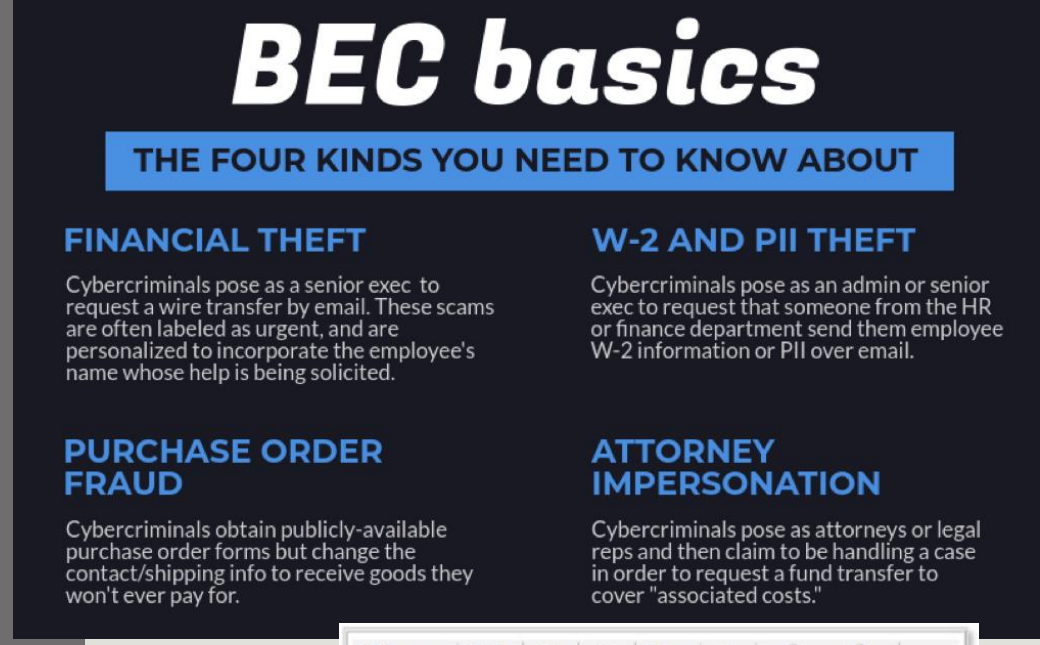
Ref: https://www.mediapro.com/what-is-phishing/

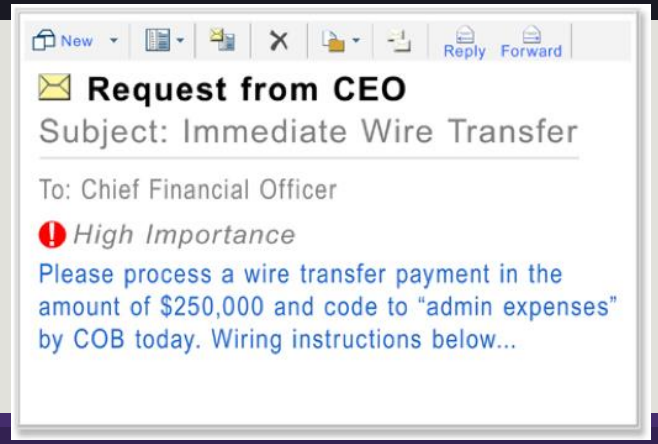
Ref: https://www.mdpi.com/1999-5903/11/4/89/htm

COLOSSAL COLORADO VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021



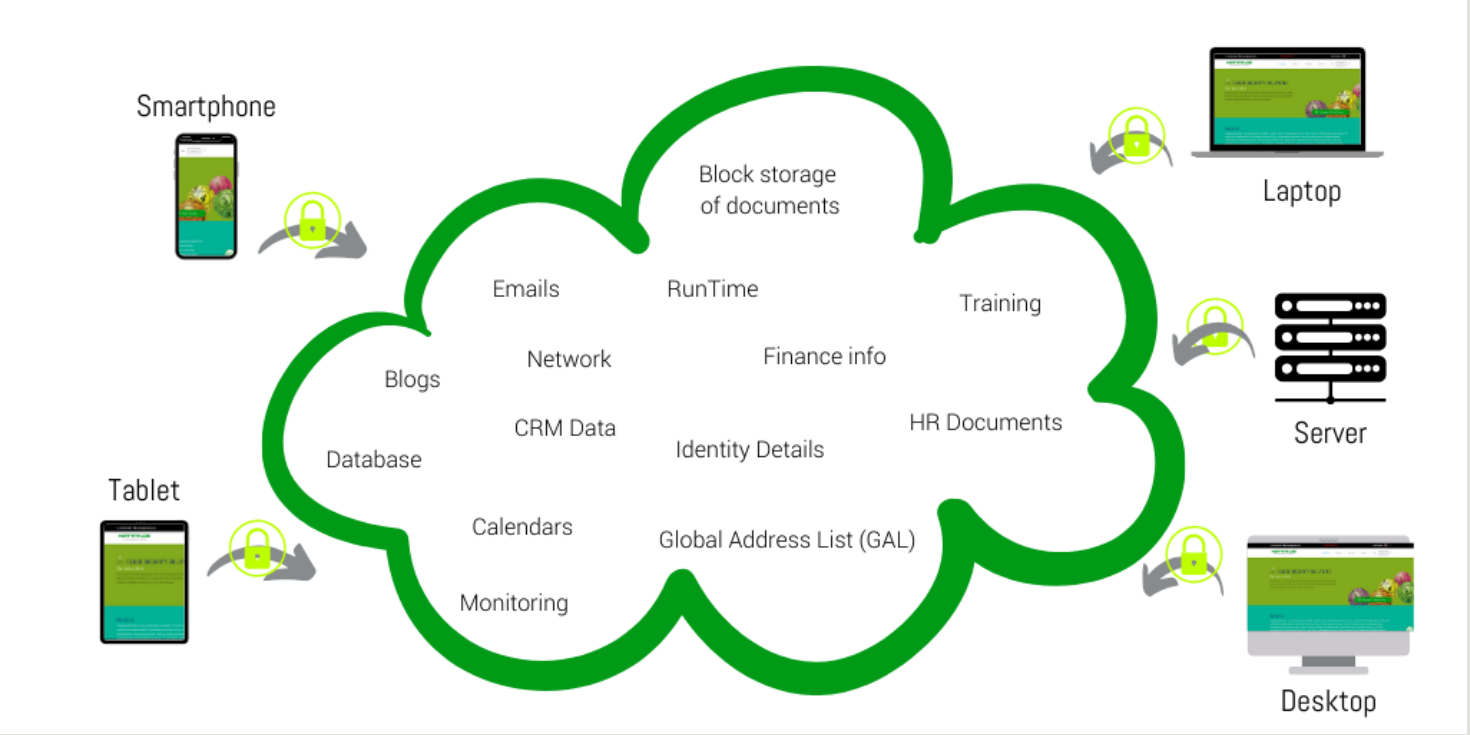


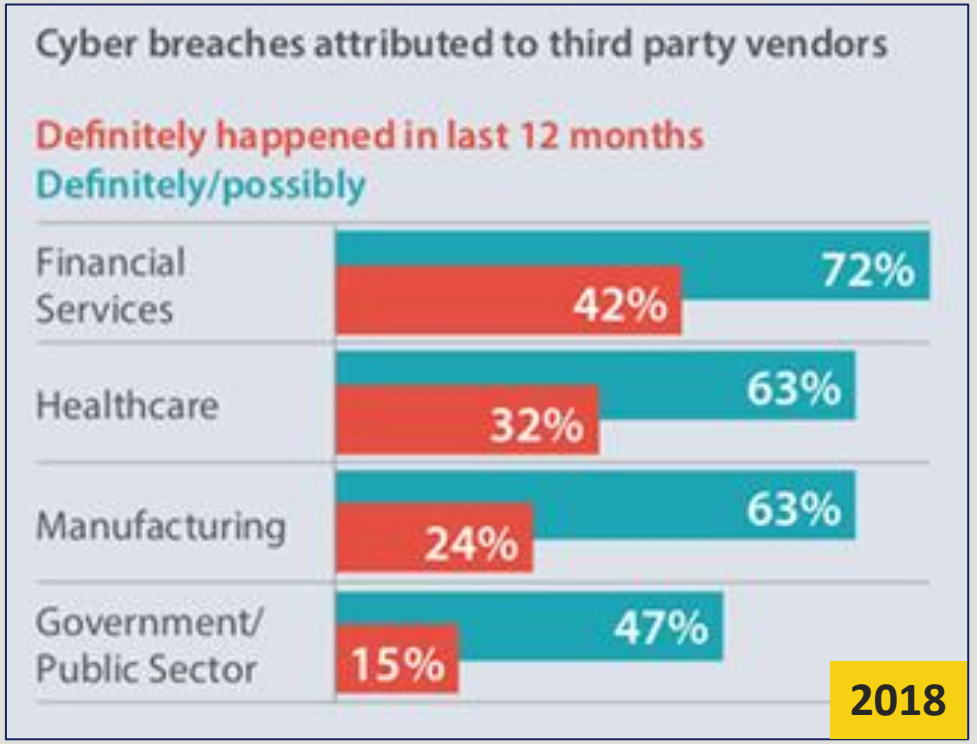


Current Cyber Threats: Business Email Compromise

Ref: https://www.cisecurity.org/press-release/cis-offers-new-guidance-to-public-private-businesses-on-email-related-scams-in-december-5-manhattan-workshop/

Ref: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise





Everyone has Cloud(s) & Third Parties!

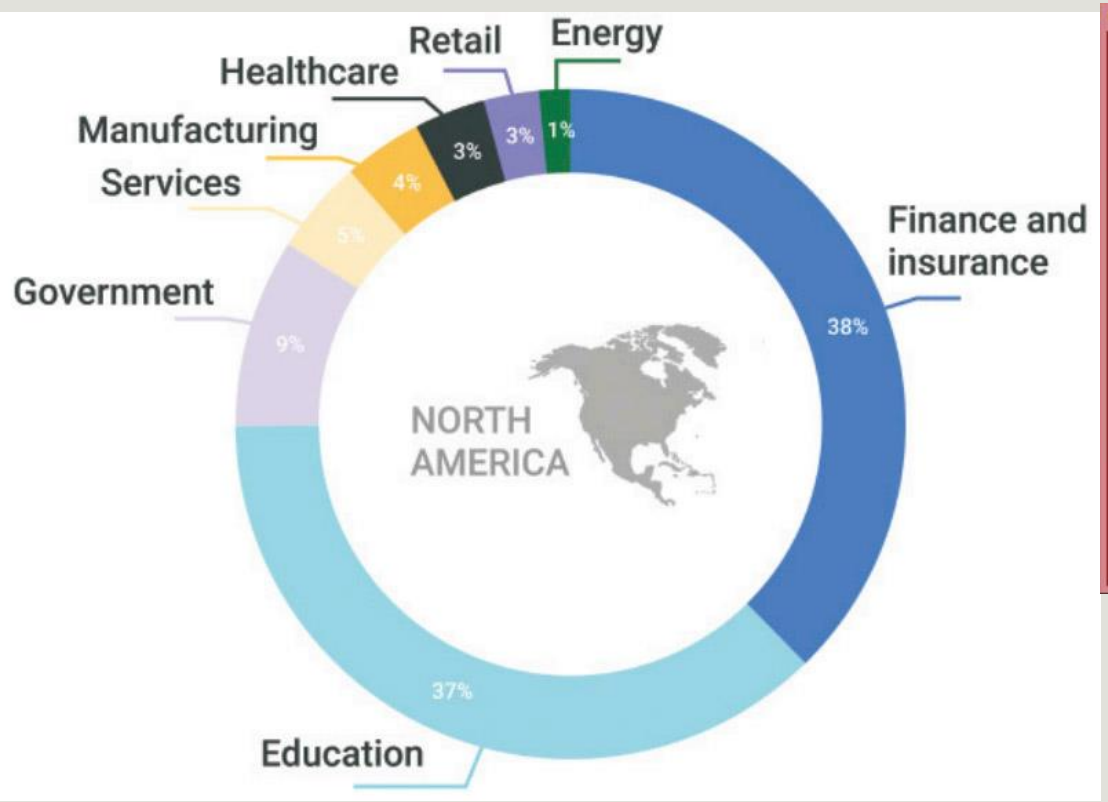
Current Cyber Threats: Clouds & Third Parties

Ref: https://www.helpnetsecurity.com/2018/04/16/privileged-access-threat/

Ref: https://blog.nettitude.com/the-top-4-security-threats-in-cloud-computing-2020-nettitude

COLOSSAL COLORADO VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021



January-June 2019

2020 projection: $1 Trillion in losses due to Ransomware!!

Current Cyber Threats: Ransomware

Ref: https://www.helpnetsecurity.com/2019/08/07/weapon-ransomware-attack/

Ref: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

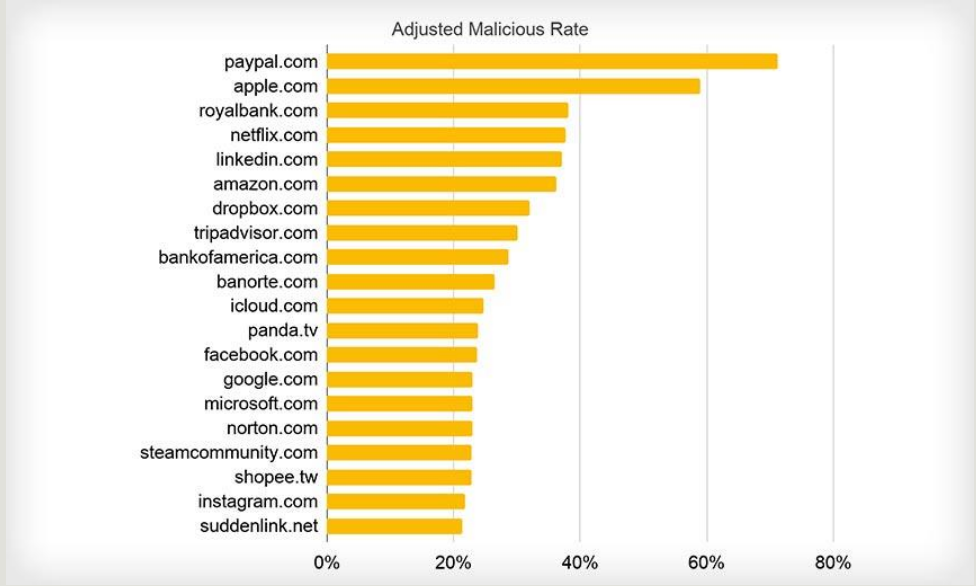
Ref: https://zvelo.com/raas-ransomware-as-a-service/

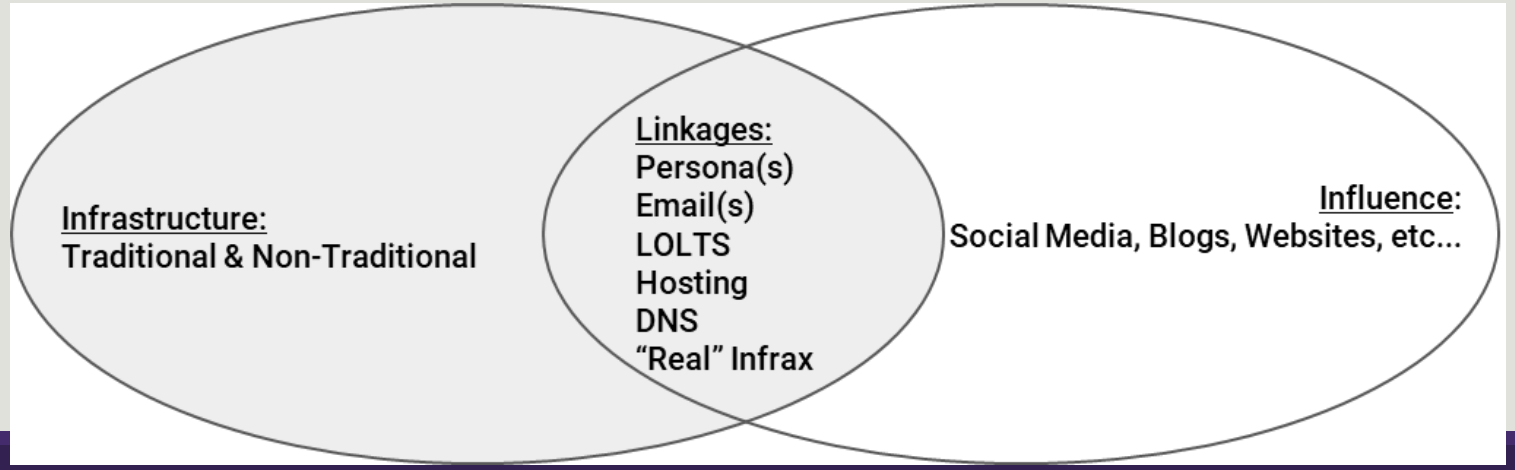
COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021

Disinformation - so easy, anyone can do it!

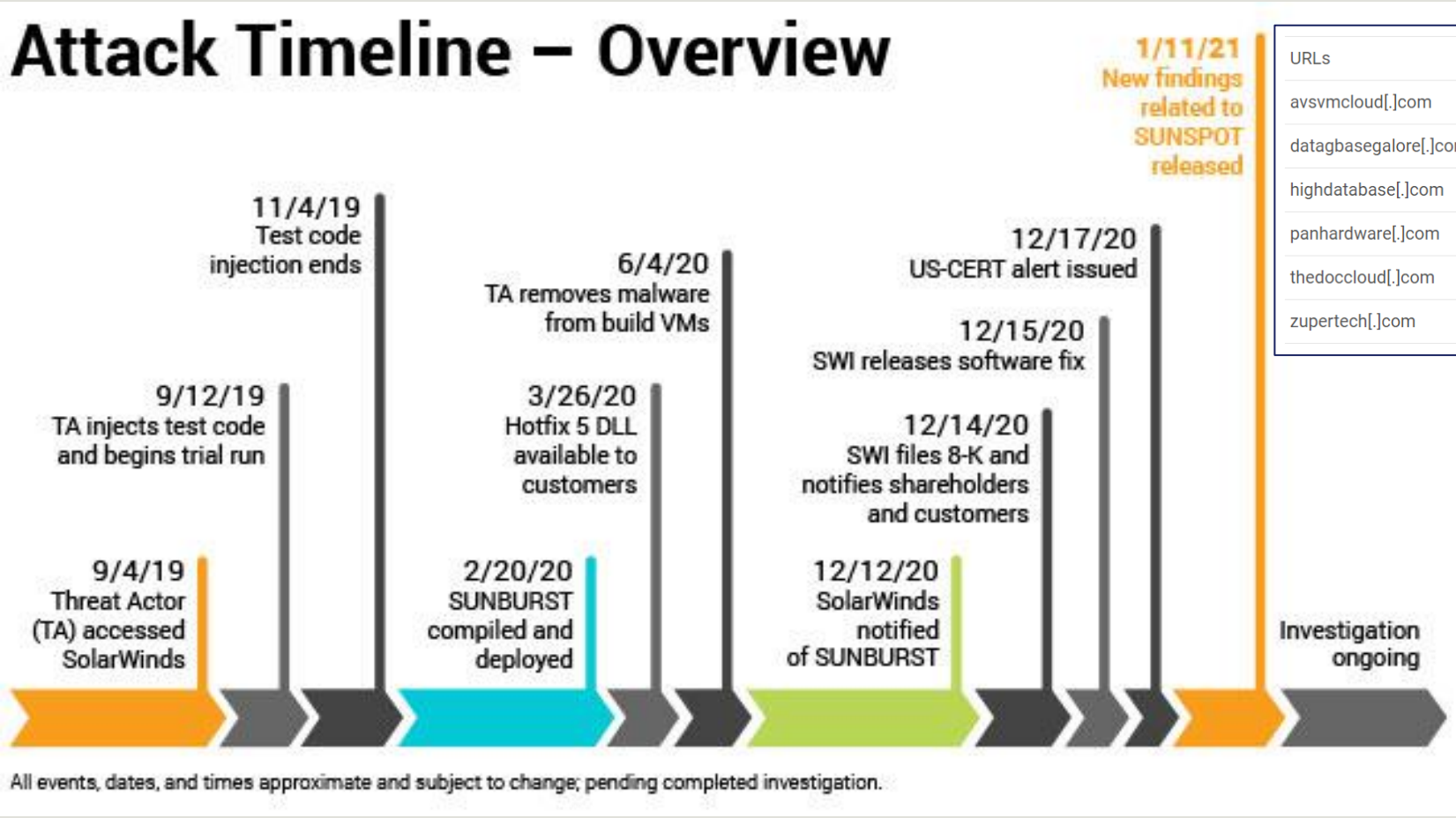
- Social Media Platforms
  - ✔ Facebook
  - ✔ Twitter
  - ✔ LinkedIn
  - ✔ Instagram
  - ✔ Blogger
  - ✔ YouTube
  - ✔ Overseas platforms (e.g. WeChat - China, Telegram - Russia)
- Foreign State use of social media
- Foreign State-sponsored media
- Terrorist propaganda
- Homegrown conspiracy theorists (2017, example: https://www.youtube.com/watch?v=xifWTiThf5A&t=5s)
- Really, anyone...





Current Cyber Threats: Disinformation

Ref: https://www.bankinfosecurity.com/tracking-targets-cybersquatting-attacks-a-14951



URLs	Notes	Date Range
avsvmcloud[.]com	12 hits including some exact matches of the identified subdomains	Dec 12 -15
datagbasegalore[.]com	1 hit	Dec 14
highdatabase[.]com	1 hit	Dec 13
panhardware[.]com	1 hit	Dec 14
thedoccloud[.]com	1 hit	Dec 15
zupertech[.]com	1 hit	Dec 15

```
public static void Initialize()
{
  try
  {
    if (OrionImprovementBusinessLayer.GetHash(Process.GetCurrentProcess().ProcessName.ToLower()) != 1729180623
      return;
    OrionImprovementBusinessLayer.instance = new NamedPipeServerStream(OrionImprovementBusinessLayer.appId);
    OrionImprovementBusinessLayer.ConfigManager.ReadReportStatus(out OrionImprovementBusinessLayer.status);
    if (OrionImprovementBusinessLayer.status == OrionImprovementBusinessLayer.ReportStatus.Truncate)
      return;
    OrionImprovementBusinessLayer.DelayMin(0, 0);
    OrionImprovementBusinessLayer.domain4 = IPGlobalProperties.GetIPGlobalProperties().DomainName;
    if (string.IsNullOrEmpty(OrionImprovementBusinessLayer.domain4) || OrionImprovementBusinessLayer.IsNullOrInv
      return;
    OrionImprovementBusinessLayer.DelayMin(0, 0);
    if (!OrionImprovementBusinessLayer.GetOrCreateUserID(out OrionImprovementBusinessLayer.userId))
      return;
    OrionImprovementBusinessLayer.DelayMin(0, 0);
    OrionImprovementBusinessLayer.ConfigManager.ReadServiceStatus(_readonly:false);
    OrionImprovementBusinessLayer.Update();
    OrionImprovementBusinessLayer.instance.Close();
  }
  catch (Exception ex)
  {
  }
}
```

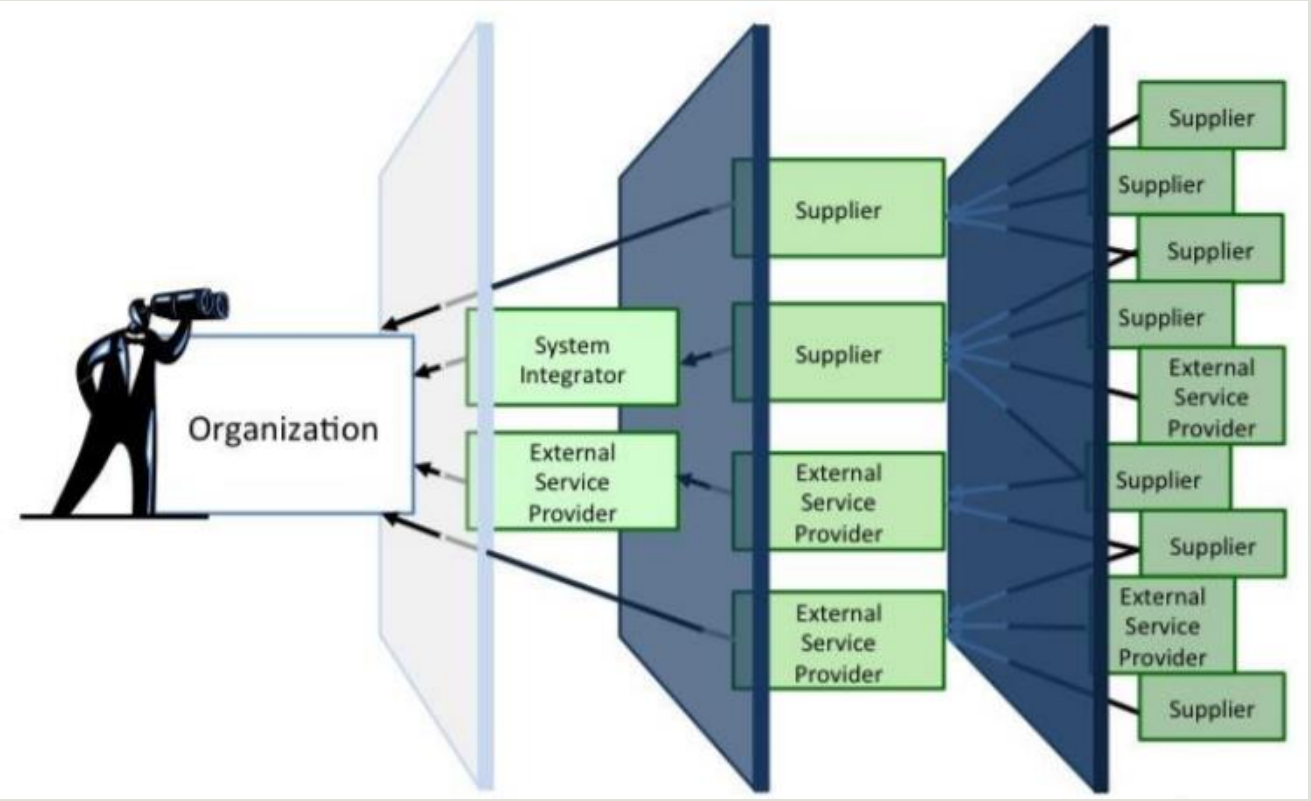
The Impact of Solar Winds: Timeline

Ref: https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

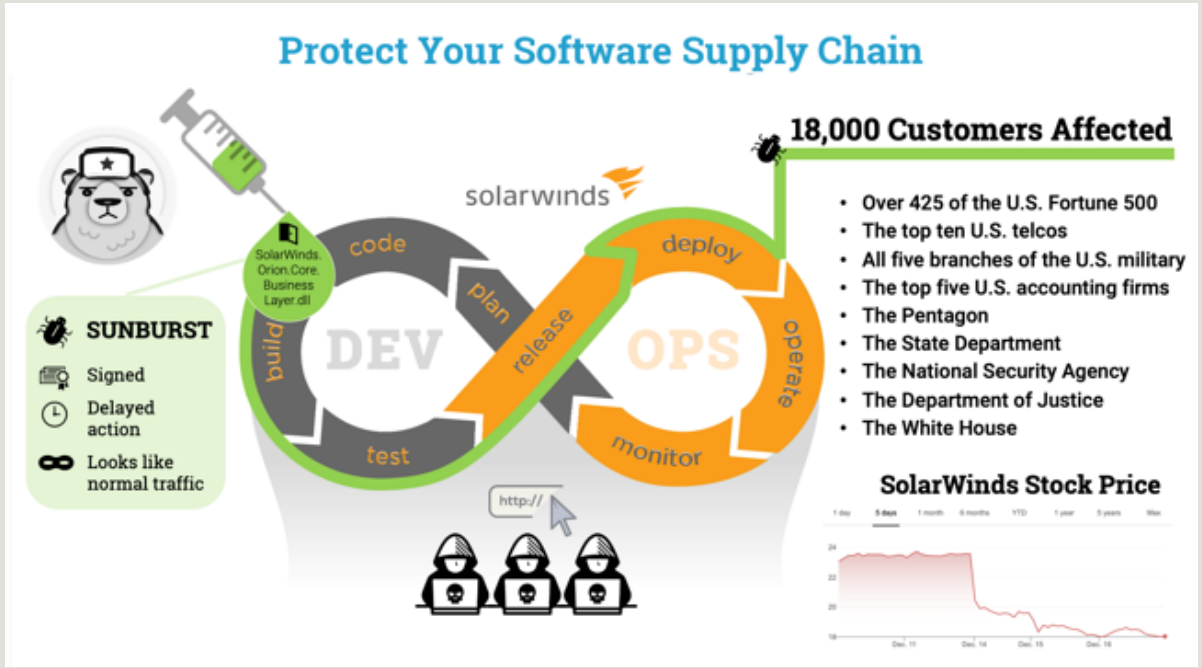
Ref: https://zvelo.com/zvelo-early-response-to-solarwinds-attack-protects-massive-partner-network/

COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021



The LONGER your supply chain, the LESS visibility you have!

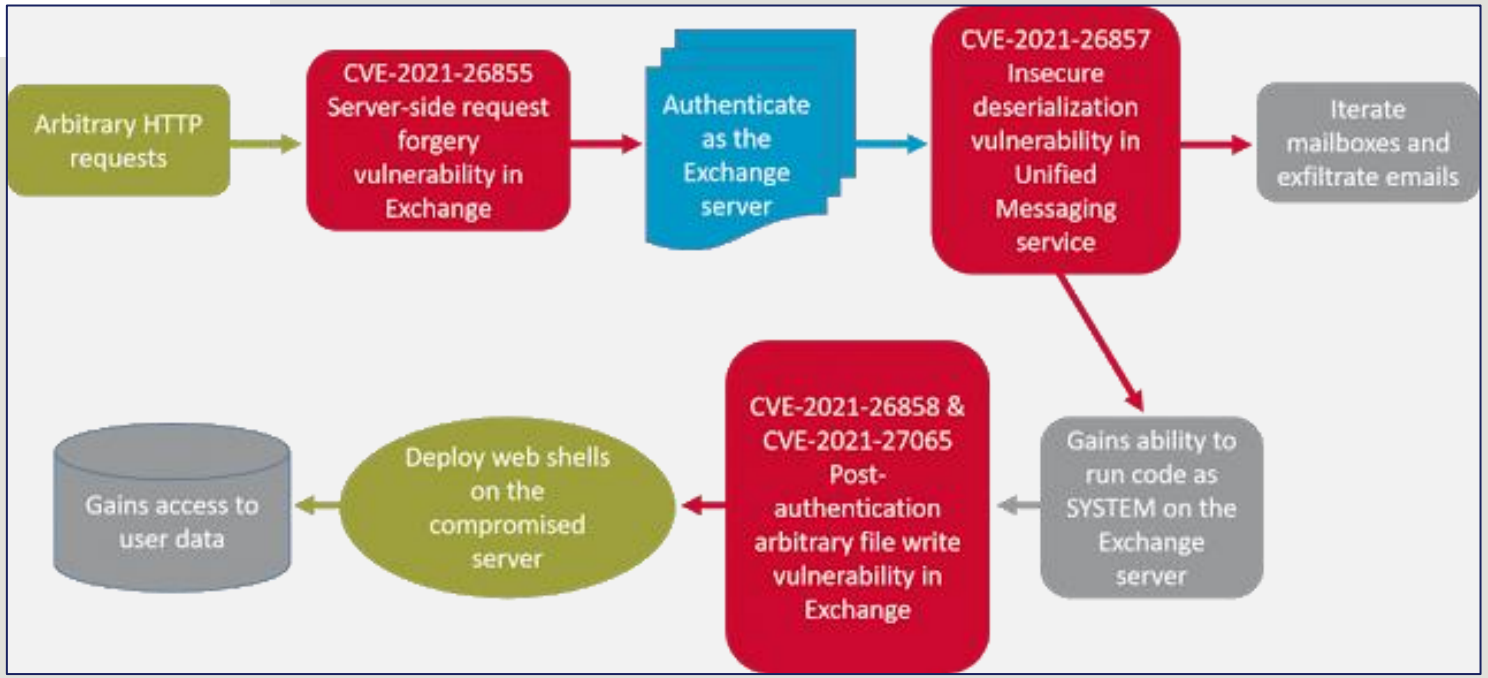


The Impact of Solar Winds: Do you know your supply chain?

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

COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021



2021 Strike Back: Microsoft Exchange

Ref: https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/

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

Hot off the press!!

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of TEXAS

HOME | ABOUT | NEWS | U.S. ATTORNEY | DIVISIONS | PROGRAMS | E

U.S. Attorneys » Southern District of Texas » News

Department of Justice

U.S. Attorney's Office

Southern District of Texas

SHARE

FOR IMMEDIATE RELEASE — Tuesday, April 13, 2021

Justice Department announces court-authorized effort to disrupt exploitation of Microsoft Exchange Server vulnerabilities

Action copied and removed web shells that provided backdoor access to servers, b additional steps may be required to patch Exchange Server software and expel hackers from victim networks.

HOUSTON – Authorities have executed a court-authorized operation to copy and remove malicious wel shells from hundreds of vulnerable computers in the United States. They were running on-premises versions of Microsoft Exchange Server software used to provide enterprise-level email service.

Through January and February 2021, certain hacking groups exploited zero-day vulnerabilities in Microsoft Exchange Server software to access email accounts and place web shells for continued access

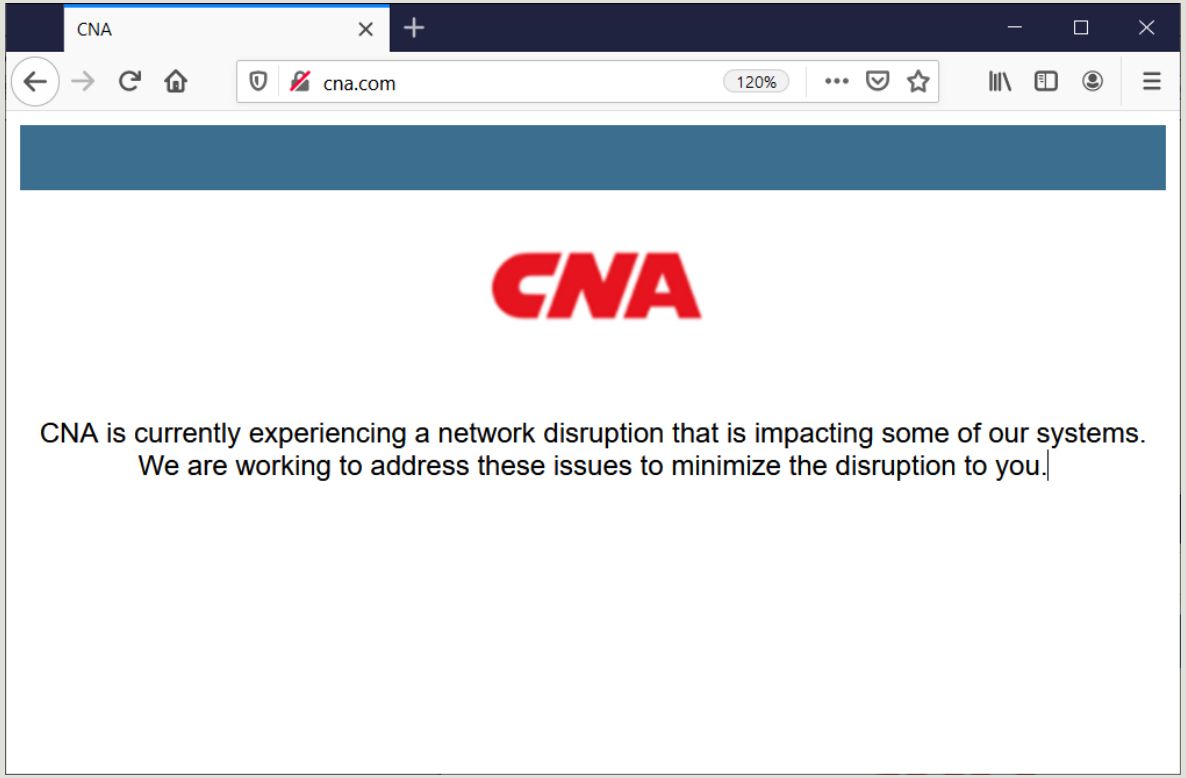
2021 Strike Back: Microsoft Exchange

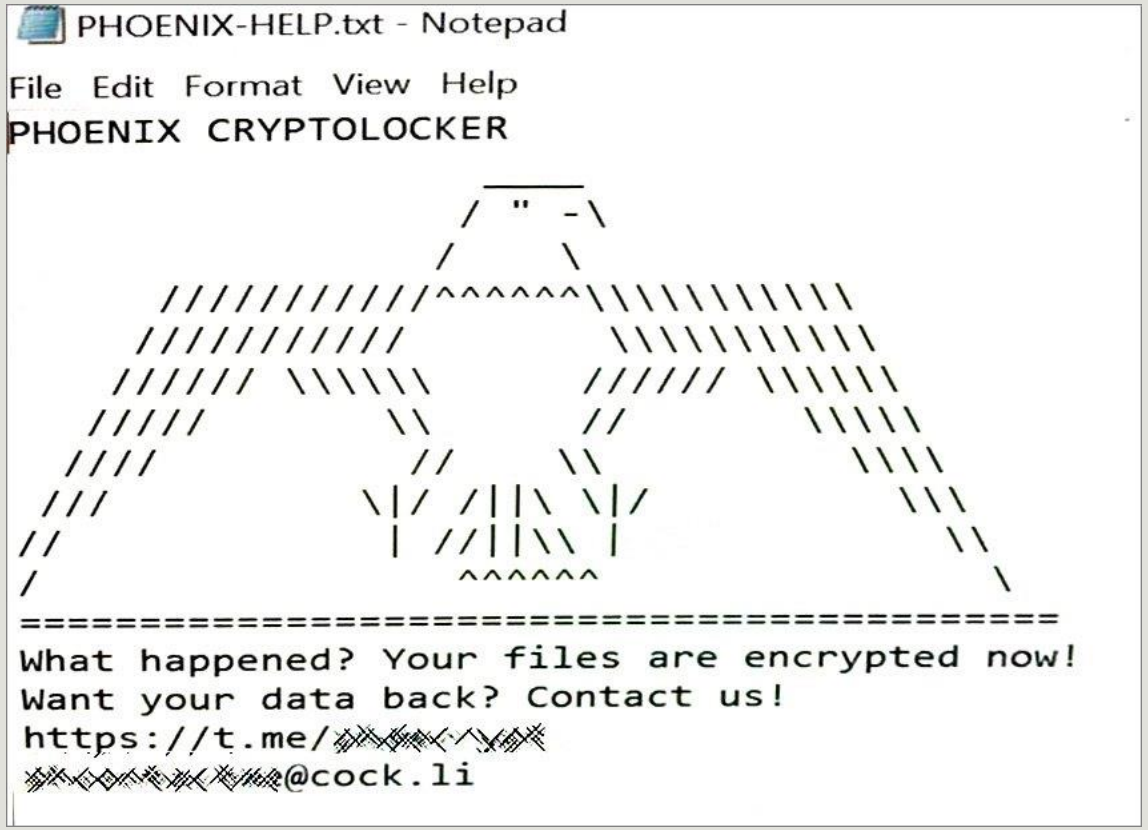
Ref: https://www.justice.gov/usao-sdtx/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft

Ref: https://thehackernews.com/2021/04/nsa-discovers-new-vulnerabilities.html

COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021





2021 Strike Back: CNA Ransomware

Ref: https://www.bleepingcomputer.com/news/security/insurance-giant-cna-hit-by-new-phoenix-cryptolocker-ransomware/

COLOSSAL COLORADO VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021

Dear Customer,

We recently became aware of unauthorized access to certain of our information technology systems hosted by a third party cloud provider. We have no indication that there has been unauthorized activity with respect to any user's account.

We are not currently aware of evidence of access to any databases that host user data, but we cannot be certain that user data has not been exposed. This data may include your name, email address, and the one-way encrypted password to your account (in technical terms, the passwords are hashed and salted). The data may also include your address and phone number if you have provided that to us.

As a precaution, we encourage you to change your password. We recommend that you also change your password on any website where you use the same user ID or password. Finally, we recommend that you enable two-factor authentication on your Ubiquiti accounts if you have not already done so.

Change Password Enable Two-Factor Authentication

We apologize for, and deeply regret, any inconvenience this may cause you. We take the security of your information very seriously and appreciate your continued trust.

Thank you,
Ubiquiti Team

2021 Strike Back: Ubiquiti

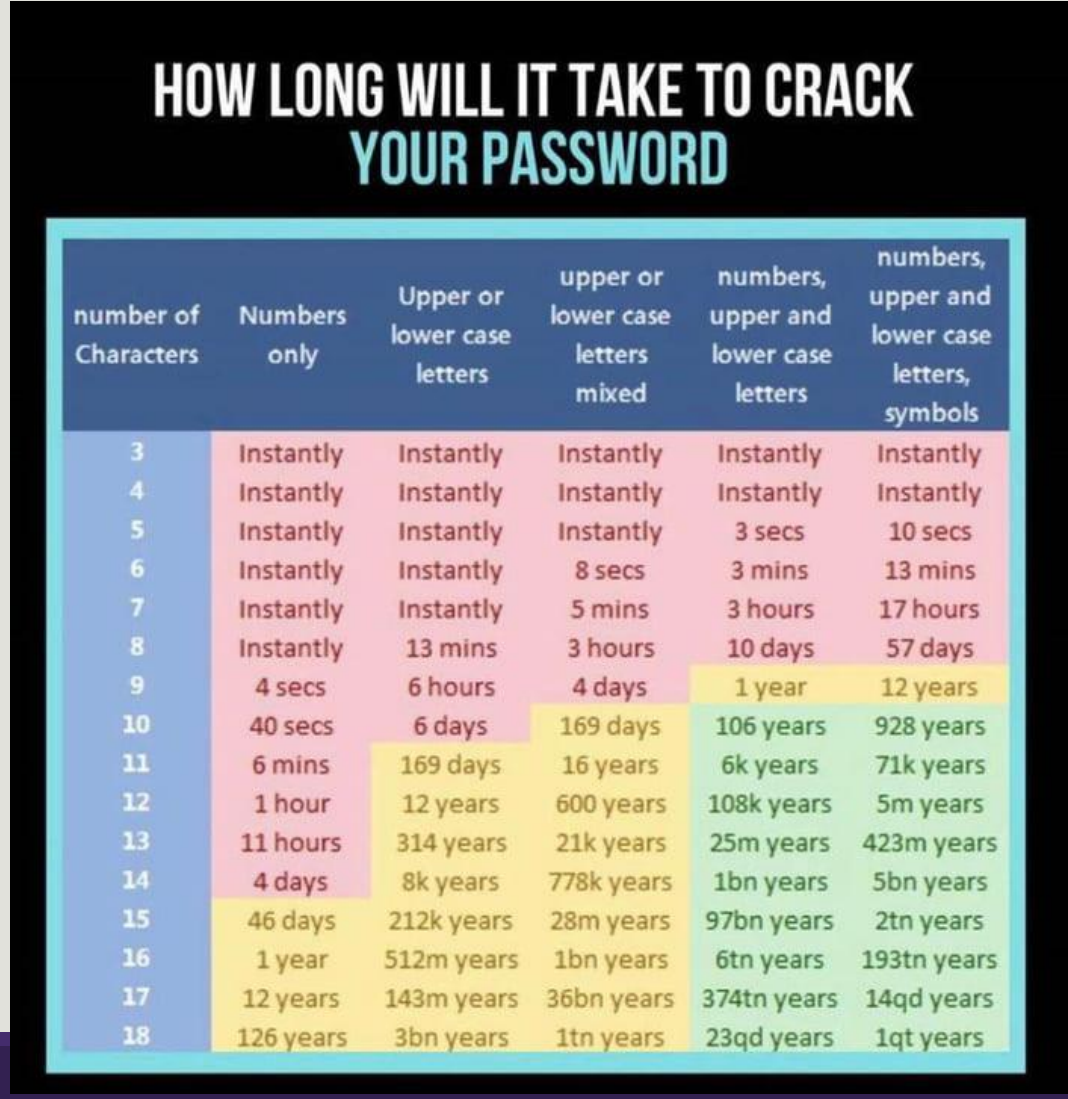
Ref: https://www.bleepingcomputer.com/news/security/networking-giant-ubiquiti-alerts-customers-of-potential-data-breach/

Ref: https://krebsonsecurity.com/2021/03/whistleblower-ubiquiti-breach-catastrophic/

COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021

- **The Basics – stop 80% of attacks!**
  - Complex Passwords (don't share them, use a password manager)
  - Multifactor Authentication (MFA)
  - Patch your systems
  - Use a Virtual Private Network (VPN)
  - Don't click on untrusted links
  - Don't bypass security solutions
  - Use a Browser Add Blocker (e.g. https://privacybadger.org/)
  - Beware Universal Serial Bus (USB) sticks in parking lots
  - 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!**



number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Protecting You and Your Business

COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021

APRIL 5- APRIL 30, 2021

Contact Information

Email:
brhodes@zvelo.com
brad.e.rhodes.mil@mail.mil
brad.rhodes@milcyber.org

Social Media:
https://www.linkedin.com/in/brad-rhodes-1951ba7/
https://github.com/cyberguy514
@cyber514 (Twitter)

Thank you!!

Questions & Conversation

COLOSSAL COLORADO
VIRTUAL INDUSTRY EVENT 2021