

Current Cyber Threats & the Impact of SolarWinds

Brad Rhodes

Colossal Colorado Virtual
Industry Event 2021

Outline

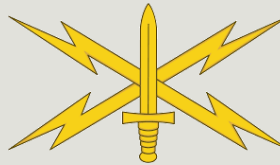
- WHOIS
- The Cyberspace Frame
- Attacker “Families”
- Defender “Families”
- Tools of the Trade
- Attack Surfaces & Vectors
 - Web
 - Network Systems
 - Endpoints
 - Internet of Things
 - People
- Live Attack Demo
- Current Cyber Threats
 - Phishing & Social Engineering
 - Business Email Compromise
 - 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

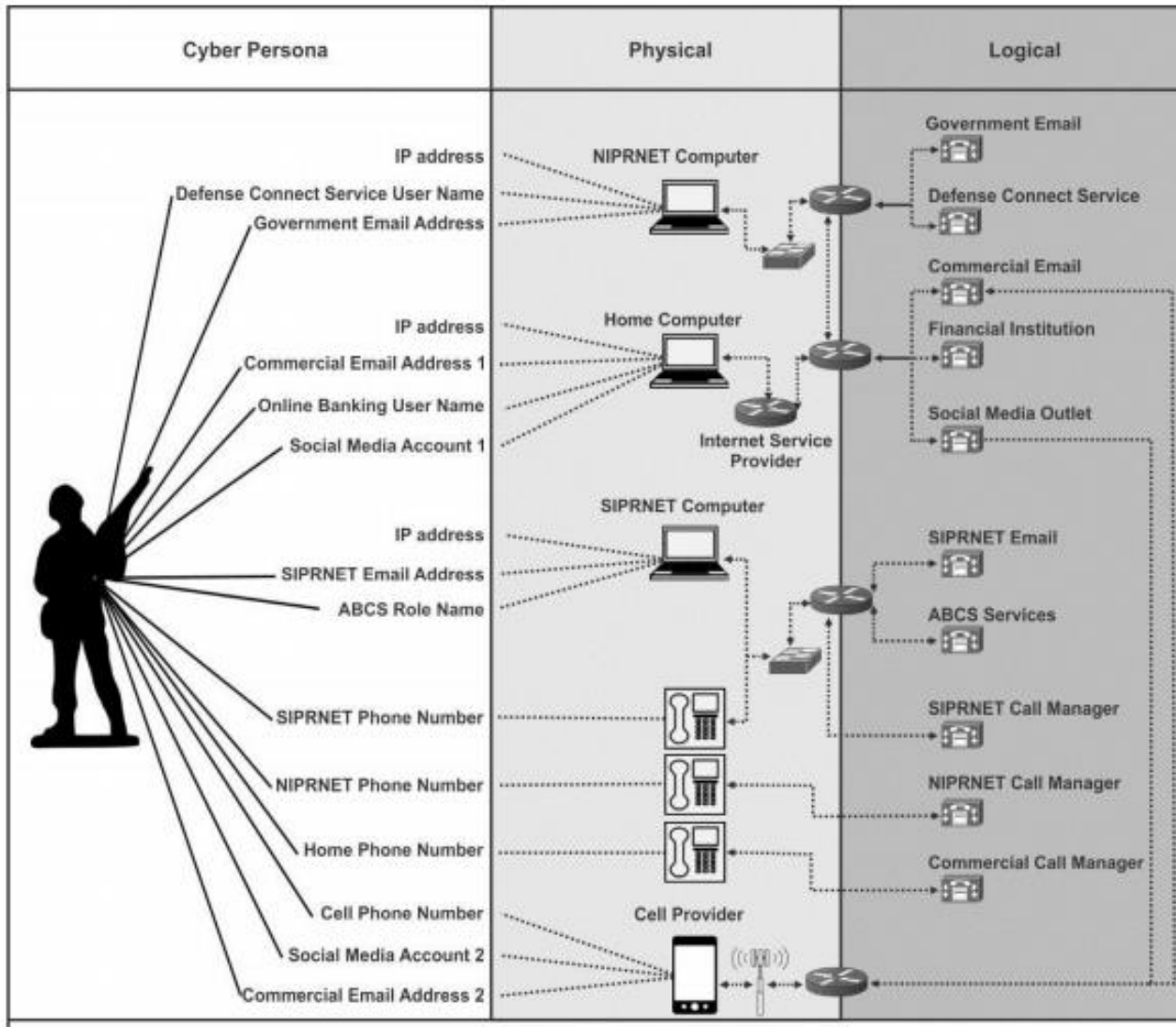
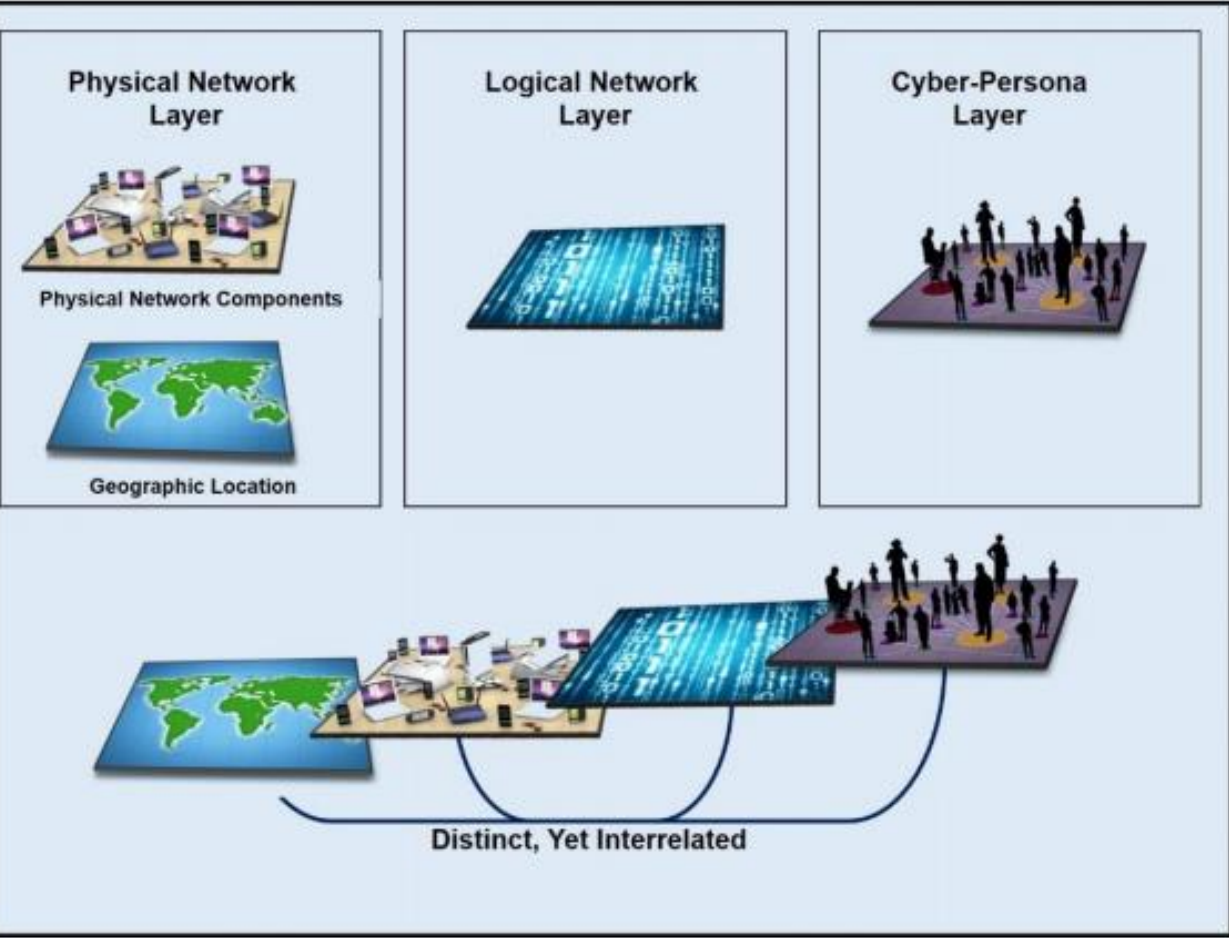
WHOIS

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+



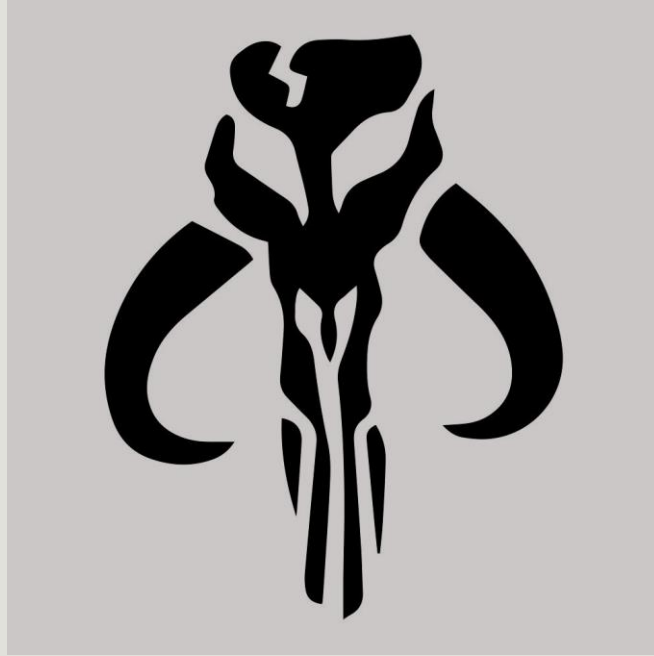


The Cyberspace Frame (1 of 2): Layers

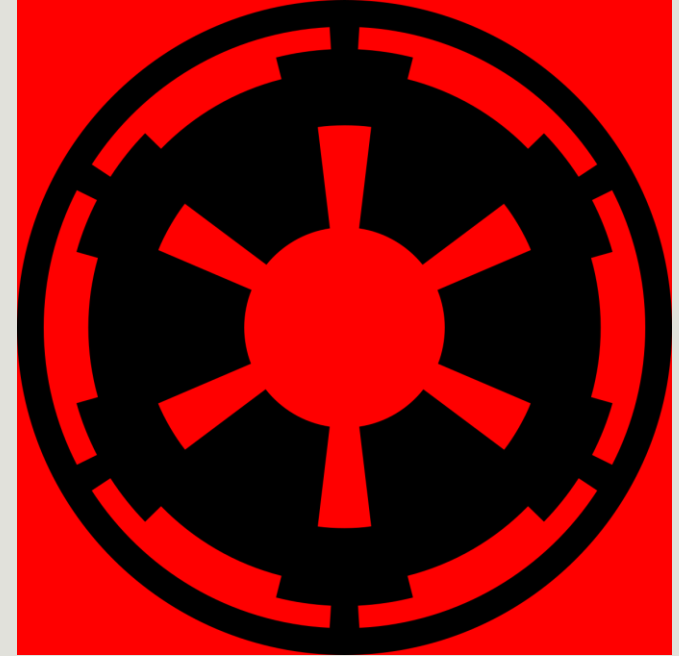
Blue Space (Good)



Gray Space (Internet)

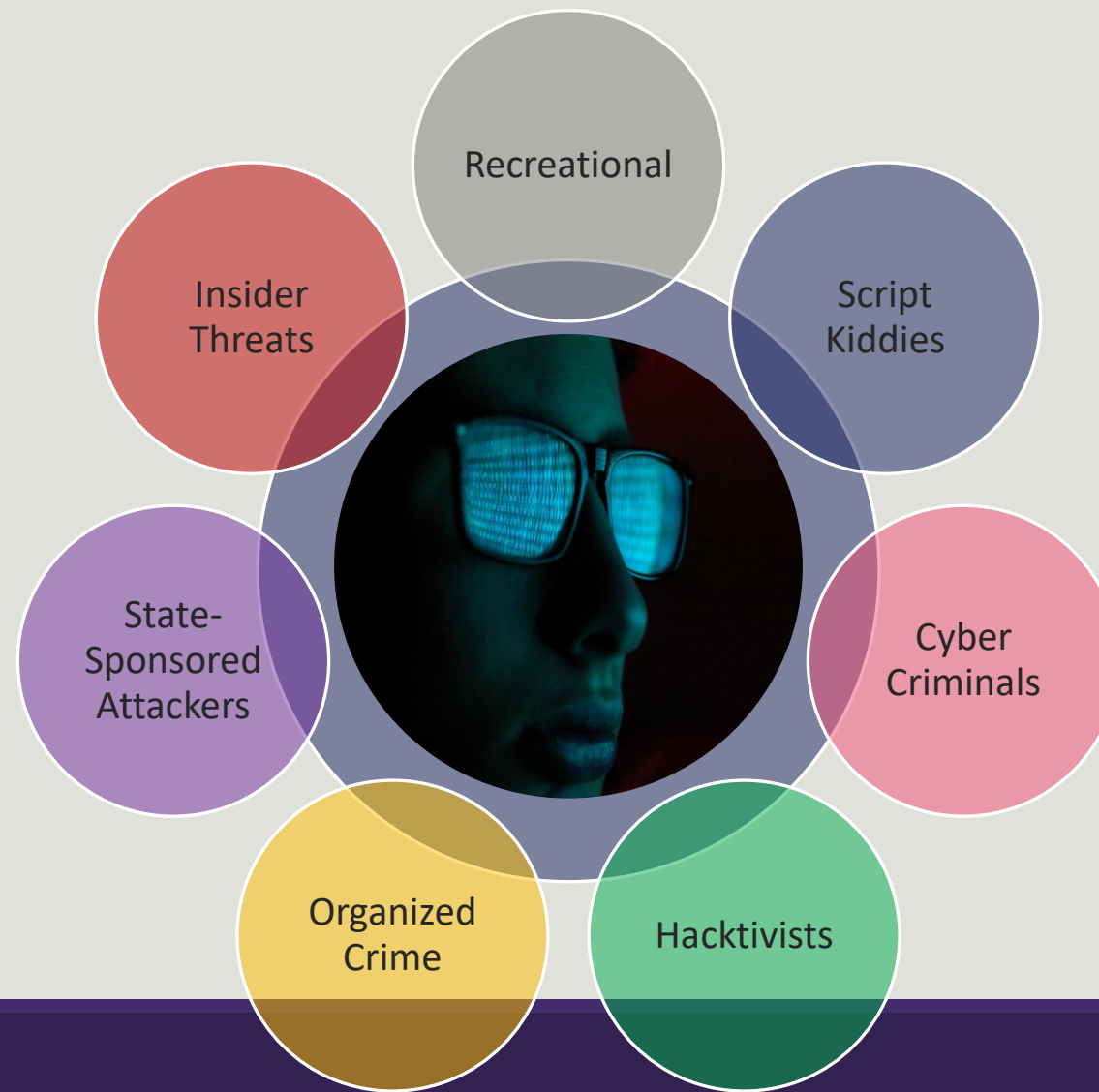


Red Space (Bad)

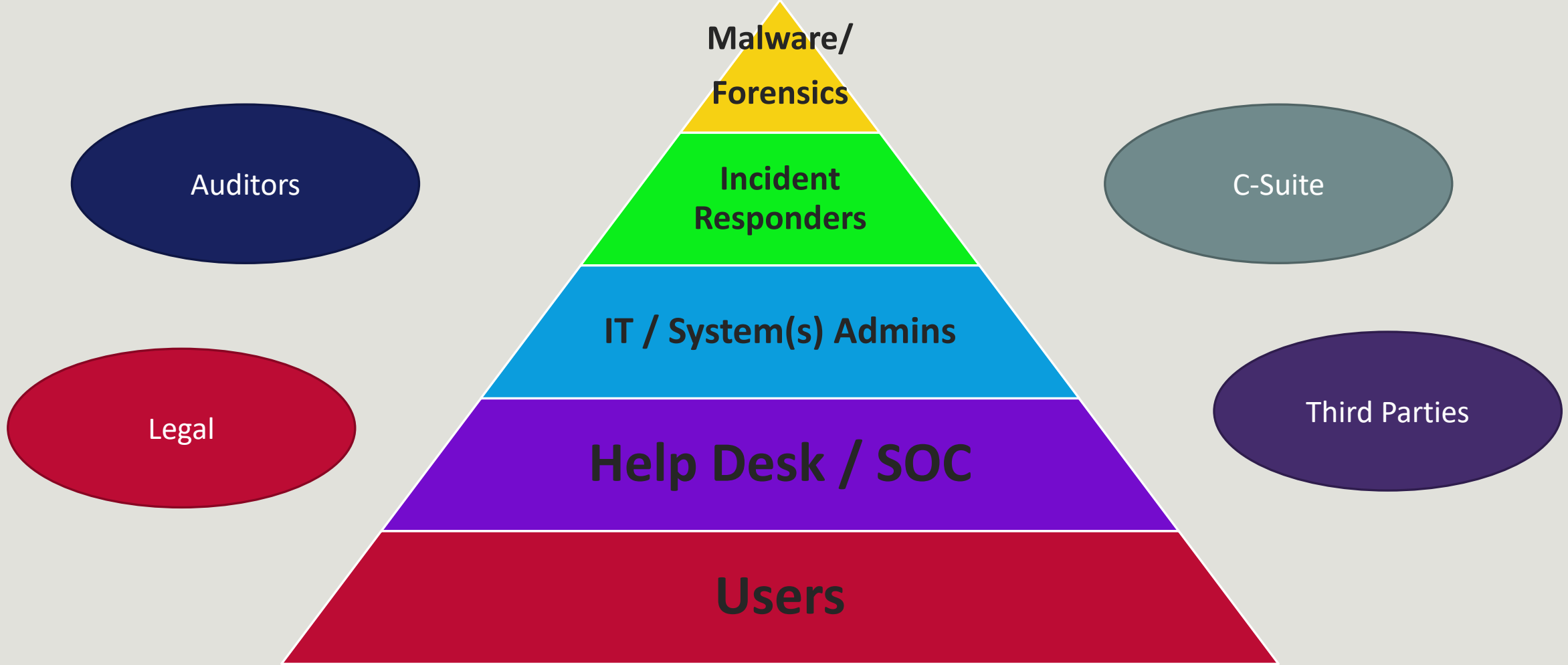


Images: Copyright Disney/Lucasfilm

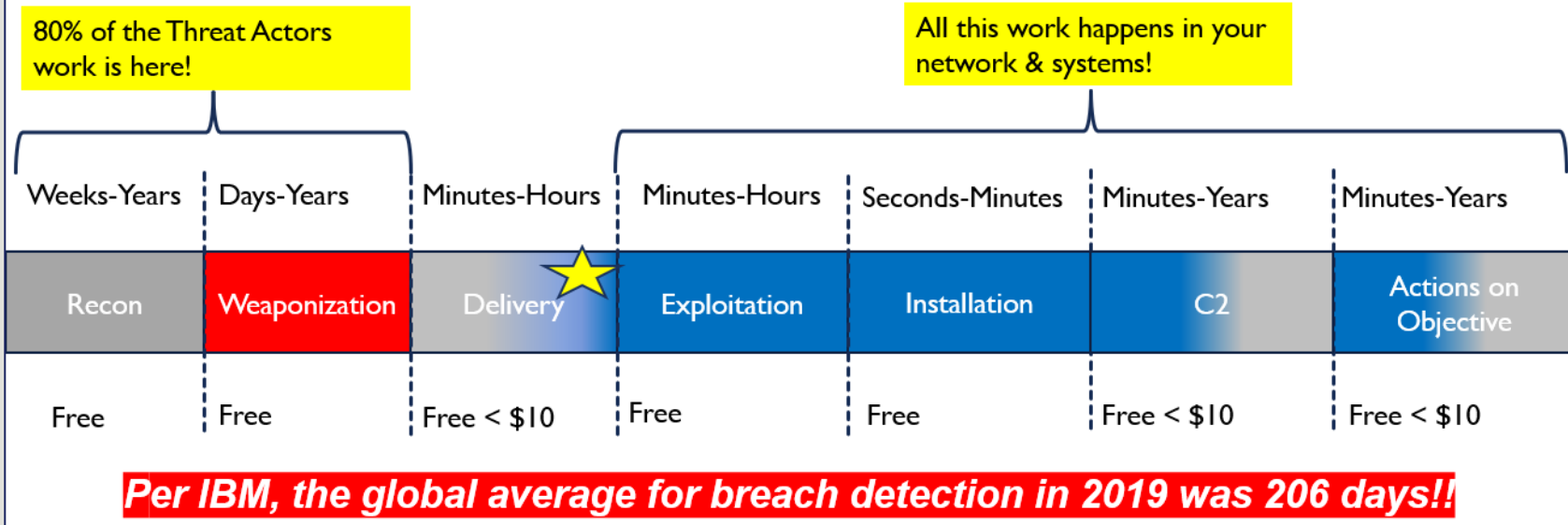
The Cyberspace Frame (2 of 2): A Different View



Attacker “Families”



Defender “Families”



<u>Recon</u> <ul style="list-style-type: none">- Google (P)- Spyse (P)- Wireshark (P)- Shodan (P)- Nmap (A)- OpenVAS (A)- Nikto (A)- Metasploit (A)	<u>Weaponization</u> <ul style="list-style-type: none">- Commodities- Custom Code- Infrastructure- Personas	<u>Delivery</u> <ul style="list-style-type: none">- Phishing- Pharming- Watering Holes- Drive-Bys- Brute Force	<u>Exploitation</u> <ul style="list-style-type: none">- Metasploit- Cobalt Strike- Live off the Land	<u>Installation</u> <ul style="list-style-type: none">- Live off the land- Persistence	<u>C2</u> <ul style="list-style-type: none">- Beacons- Call backs- Back Doors	<u>Actions on Obj</u> <ul style="list-style-type: none">- Data exfiltration- Data mod.- Sabotage- Destruction
--	--	--	--	---	---	--

Tools of the Trade (1 of 2): Attackers

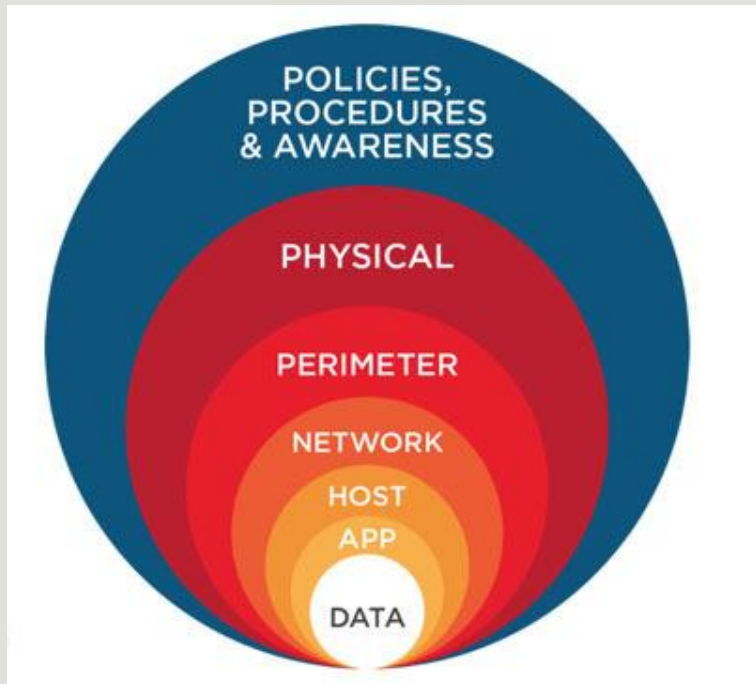


Ref: <https://www.kali.org/>

Ref: <https://opensource.org/>

APRIL 5- APRIL 30, 2021

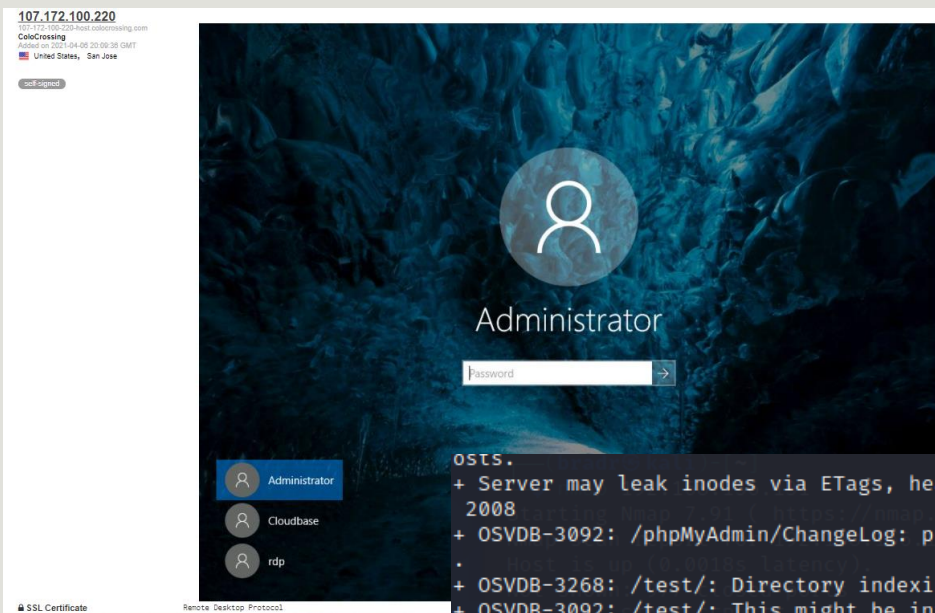
Defense Area	Tools
Policies, Procedures, & Awareness	Acceptable Use Policy, Multi-Factor Policy, Password Policy, Business Continuity Plan, Disaster Recovery Plan, Training, etc...
Physical	Bollards, Fences, Guard, Locks, Key Cards, System Logs
Perimeter	Firewalls, Intrusion Detection/Prevention Systems, 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



```
OSTS.  
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 4052008  
+ 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 gives  
+ 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 protected on  
+ 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
```

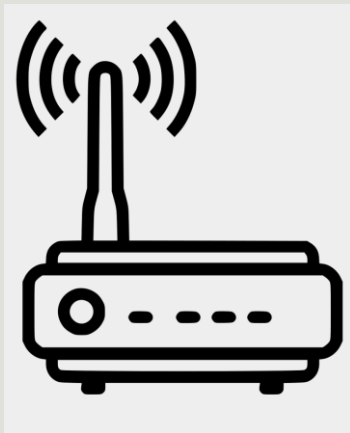
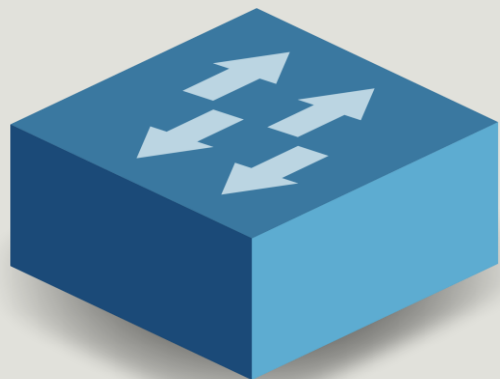
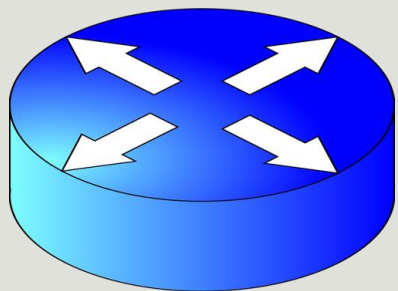


Images: Copyright Microsoft, Apache, WordPress, shodan.io

Attack Surfaces: Web



APRIL 5- APRIL 30, 2021



Images: Copyright Microsoft, Google, AWS

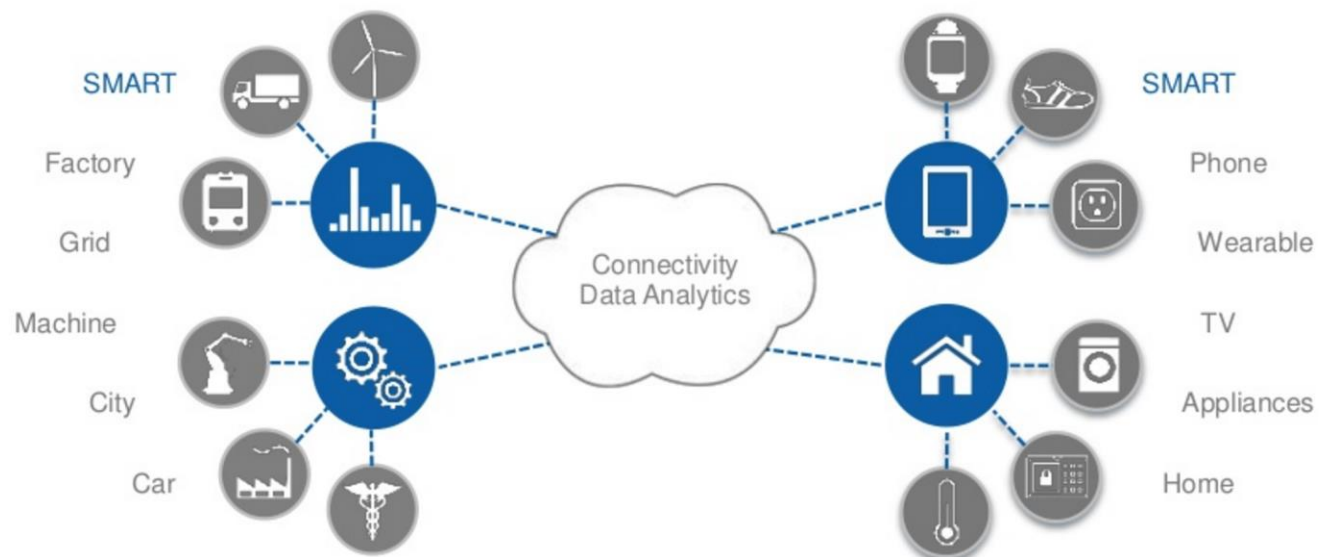
Attack Surfaces: Network Systems



Attack Surfaces: End Points

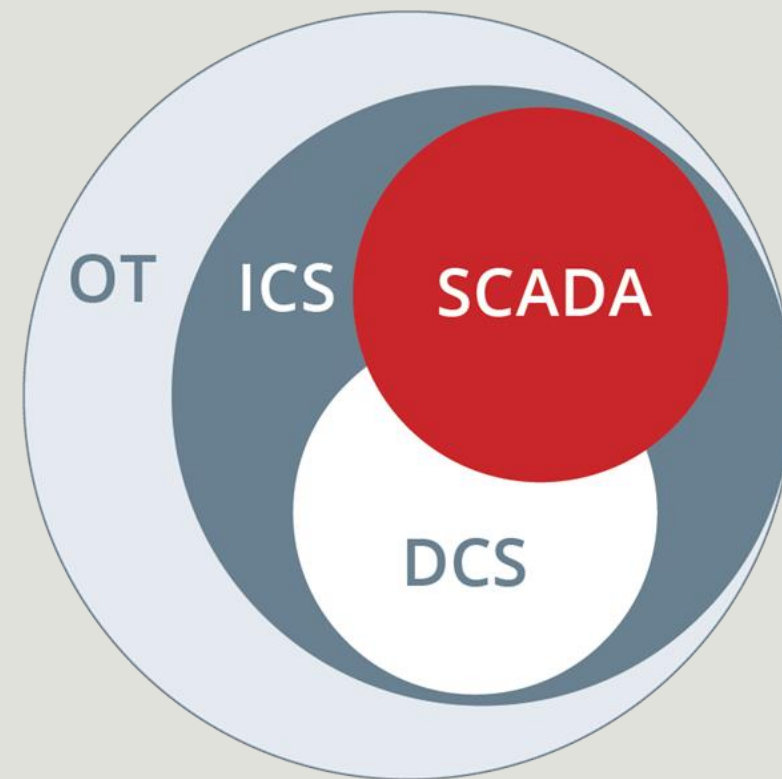
INDUSTRIAL Internet of Things

CONSUMER Internet of Things



Based on Moor Insights & Strategy's report *Segmenting the Internet of Things (IoT)*

ni.com



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/>

APRIL 5- APRIL 30, 2021



C-Suite/Executives



Support Staff



Users

Attack Surfaces: People

Live Attack Demo

Exposed Servers & Busted Web-parts

Workstation Pwnage

From: fraud@bankofamericans.com

To: targets@contoso.ltd

Date: Thu, 13 Jun 2019 09:35:31 -0700

Subject: Your Account Has Been Locked

Dear Online Banking Customer:

We are writing to inform you that there have been a number of invalid login attempts account. As a result, we have temporarily locked your account and added an extra verification process intended to ensure your identity and protect the security of your account in the future.

Please [click here](#) to begin the account verification process. If you fail to update your account information in the next 24 hours, you will be required to go into our branch to reestablish your account.

Sincerely,
Bank of Americans Fraud Detection

Please note: This e-mail message was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Prefer not to receive HTML mail? [Click here](#)

File Message Help Acrobat Tell me what you want to do

Delete Archive Reply Reply All Forward Quick Steps Move Tags Editing Speech Zoom

Tue 6/11/2019 3:42 AM

google.co.uk <oshima@giken.co.jp>

Notification For marketing@mediapro.com

To Marketing

You forwarded this message on 6/12/2019 8:30 AM. This message was sent with High importance.

Official Notification.png 771 KB

Dear Email User marketing@mediapro.com

You are one of the lucky winners of Google for a total sum of 950,000.00 GBP, view affixed for further details to claim.

Log in to your PayPal account

Not Secure | paypal--accounts.com

Email or mobile number

Password

Log In



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>

APRIL 5- APRIL 30, 2021

Step 1: Identify a Target



Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2: Grooming



Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information



The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer



Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

BEC basics

THE FOUR KINDS YOU NEED TO KNOW ABOUT

FINANCIAL THEFT

Cybercriminals pose as a senior exec to request a wire transfer by email. These scams are often labeled as urgent, and are personalized to incorporate the employee's name whose help is being solicited.

W-2 AND PII THEFT

Cybercriminals pose as an admin or senior exec to request that someone from the HR or finance department send them employee W-2 information or PII over email.

PURCHASE ORDER FRAUD

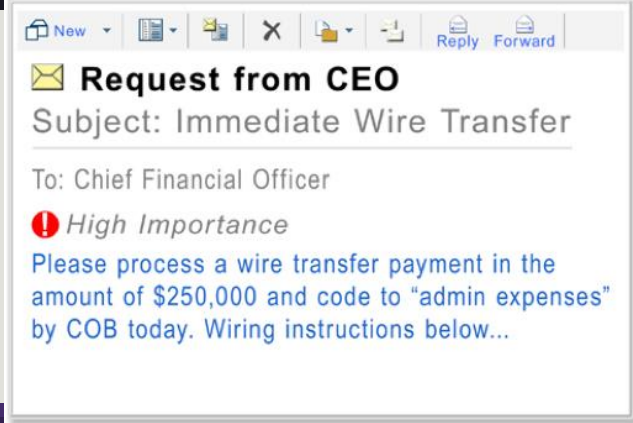
Cybercriminals obtain publicly-available purchase order forms but change the contact/shipping info to receive goods they won't ever pay for.

ATTORNEY IMPERSONATION

Cybercriminals pose as attorneys or legal reps and then claim to be handling a case in order to request a fund transfer to cover "associated costs."

Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

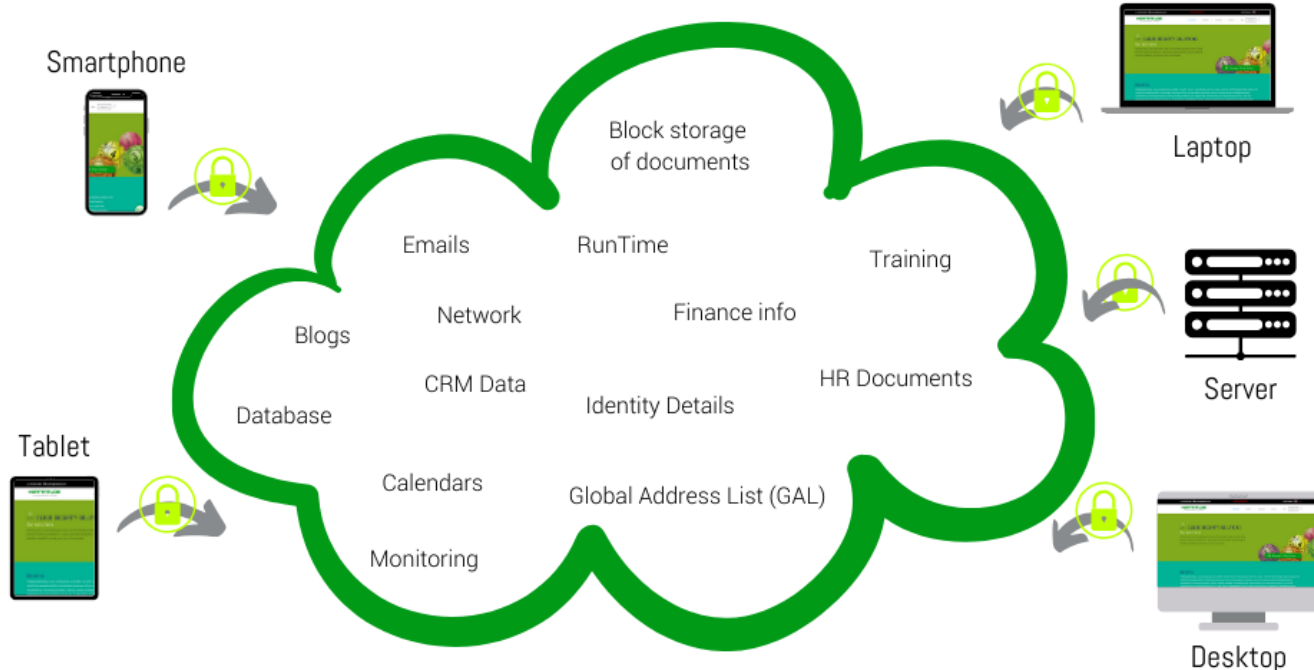


Current Cyber Threats: Business Email Compromise

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

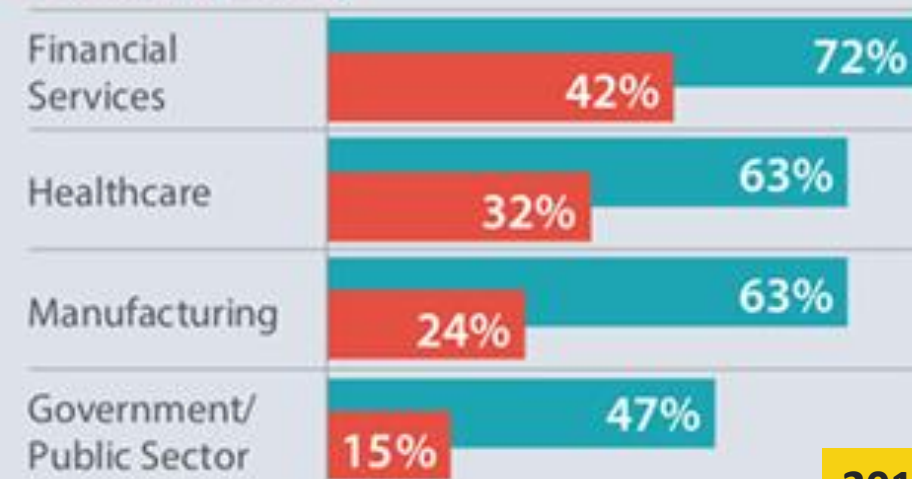
Ref: <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise>

APRIL 5- APRIL 30, 2021



Cyber breaches attributed to third party vendors

Definitely happened in last 12 months
Definitely/possibly



2018

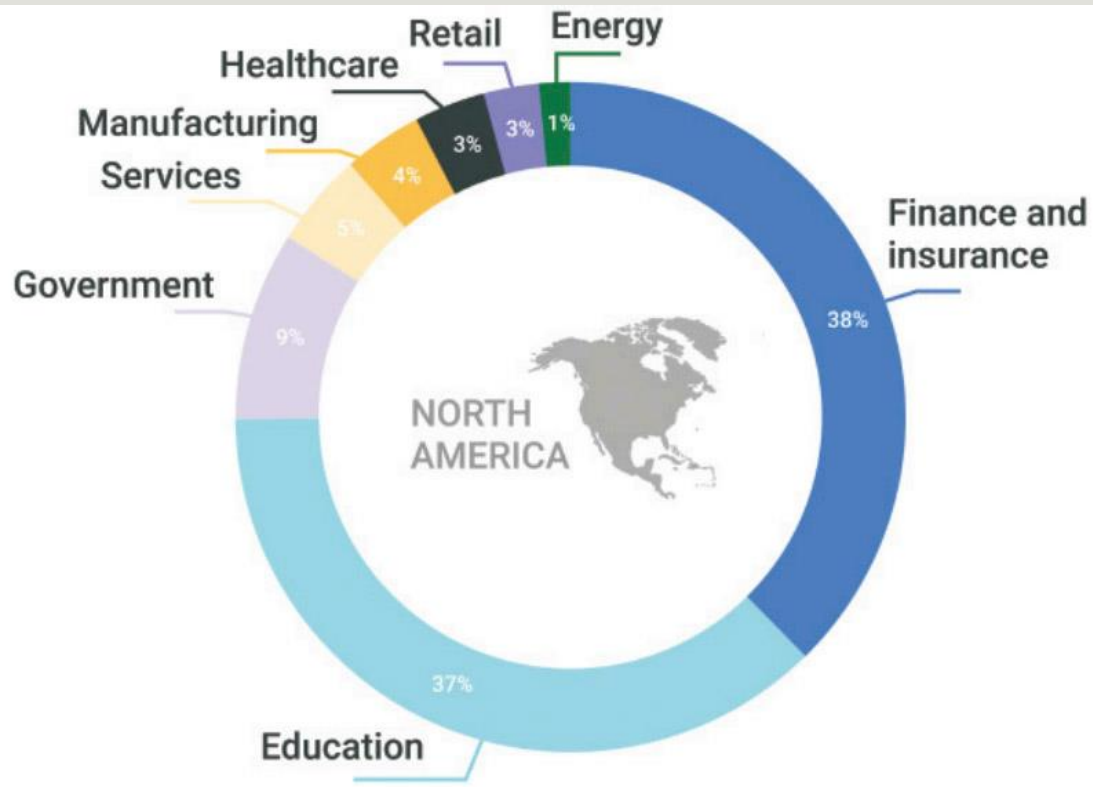
Everyone has Cloud(s) & Third Parties!

Current Cyber Threats: Clouds & Third Parties

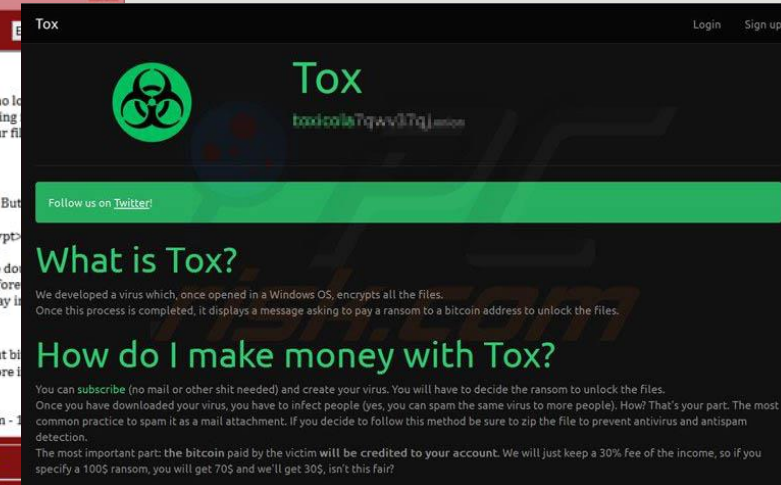
Ref: <https://www.helpnetsecurity.com/2018/04/16/privileged-access-threat/>

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

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/>

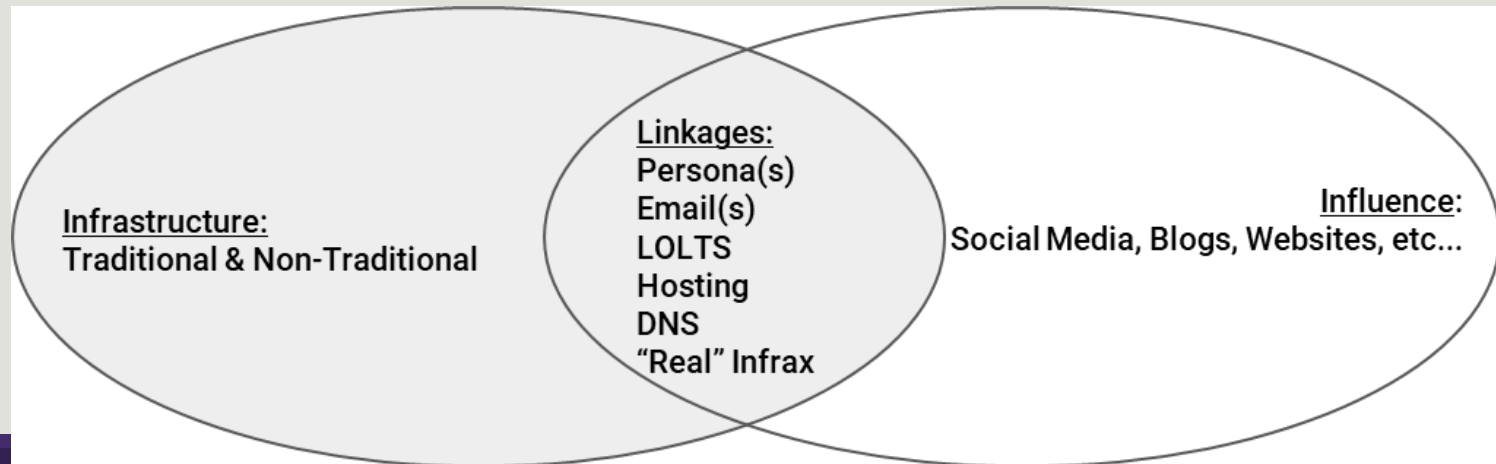
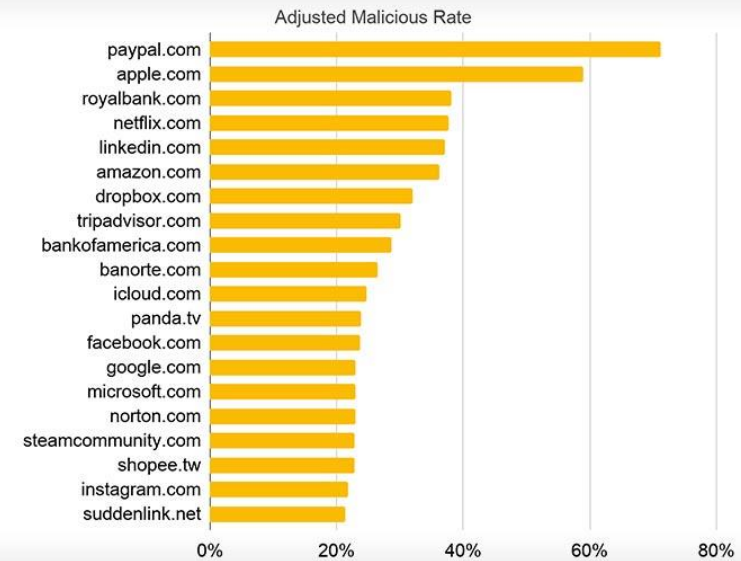
Ref: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

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

APRIL 5- APRIL 30, 2021

Disinformation - so easy, anyone can do it!

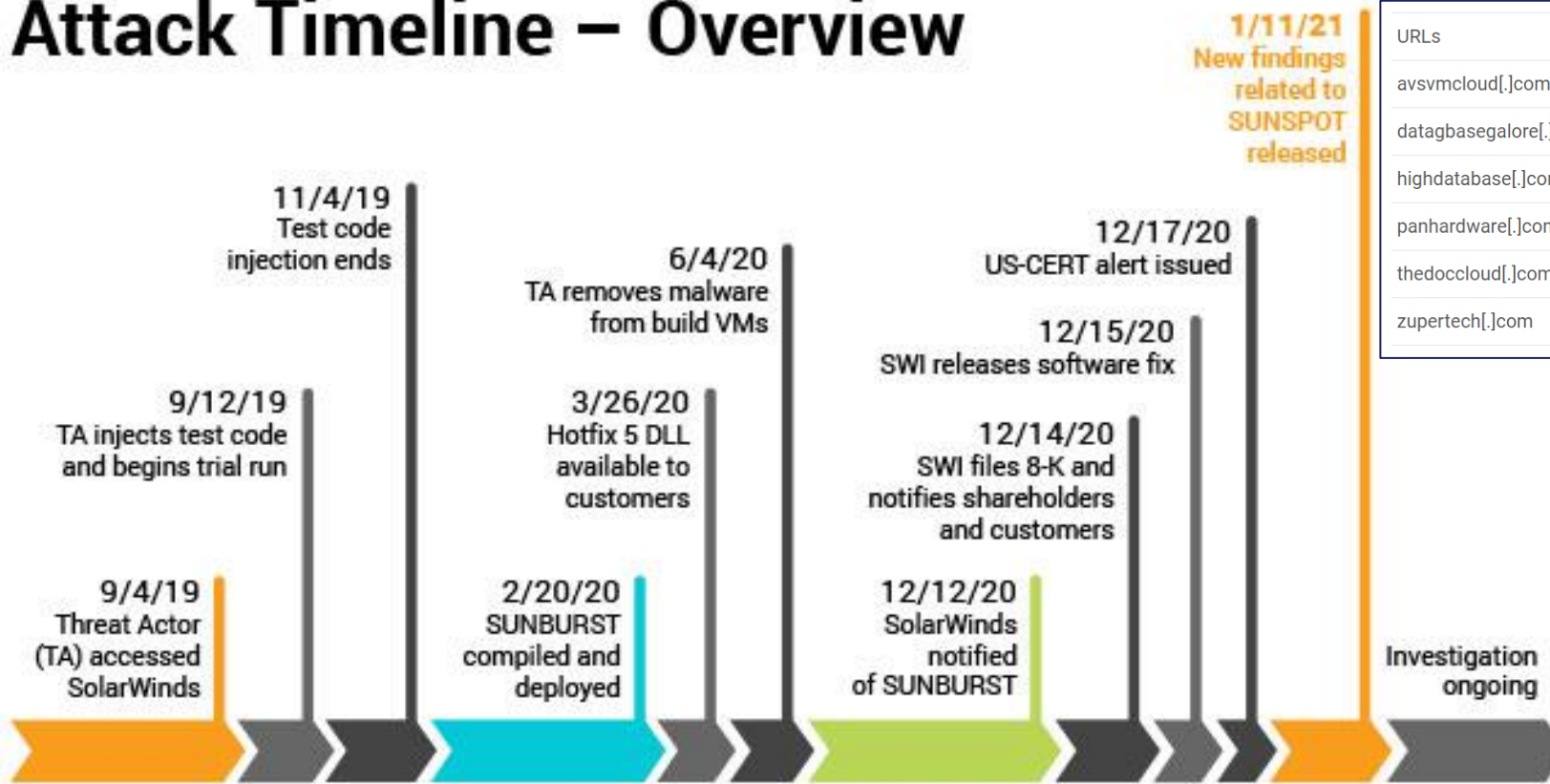
- Social Media Platforms
 - ✓ Facebook
 - ✓ Twitter
 - ✓ LinkedIn
 - ✓ Instagram
 - ✓ Blogger
 - ✓ YouTube
 - ✓ Overseas platforms (e.g. WeChat - China, Telegram - Russia)
- Foreign State use of social media
- Foreign State-sponsored media
- Terrorist propaganda
- Homegrown conspiracy theorists (2017, 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>

Attack Timeline – Overview



All events, dates, and times approximate and subject to change; pending completed investigation.

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

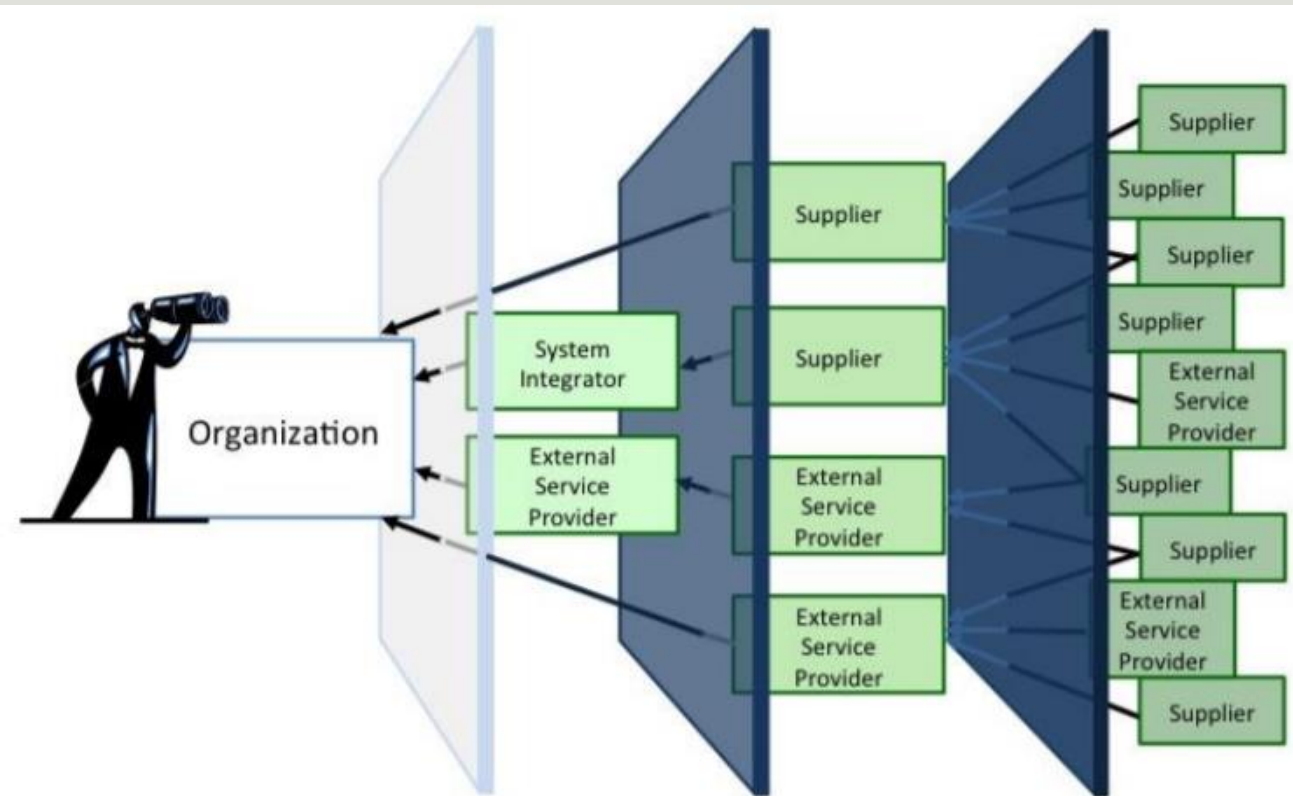
```
public static void Initialize()
{
    try
    {
        if (OrionImprovementBusinessLayer.GetHash(» Process.GetCurrentProcess().ProcessName.ToLower()) != 1729180623)
            return;
        OrionImprovementBusinessLayer.Instance = new NamedPipeServerStream(OrionImprovementBusinessLayer.appId);
        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.IsNullOrEmptyIn
            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

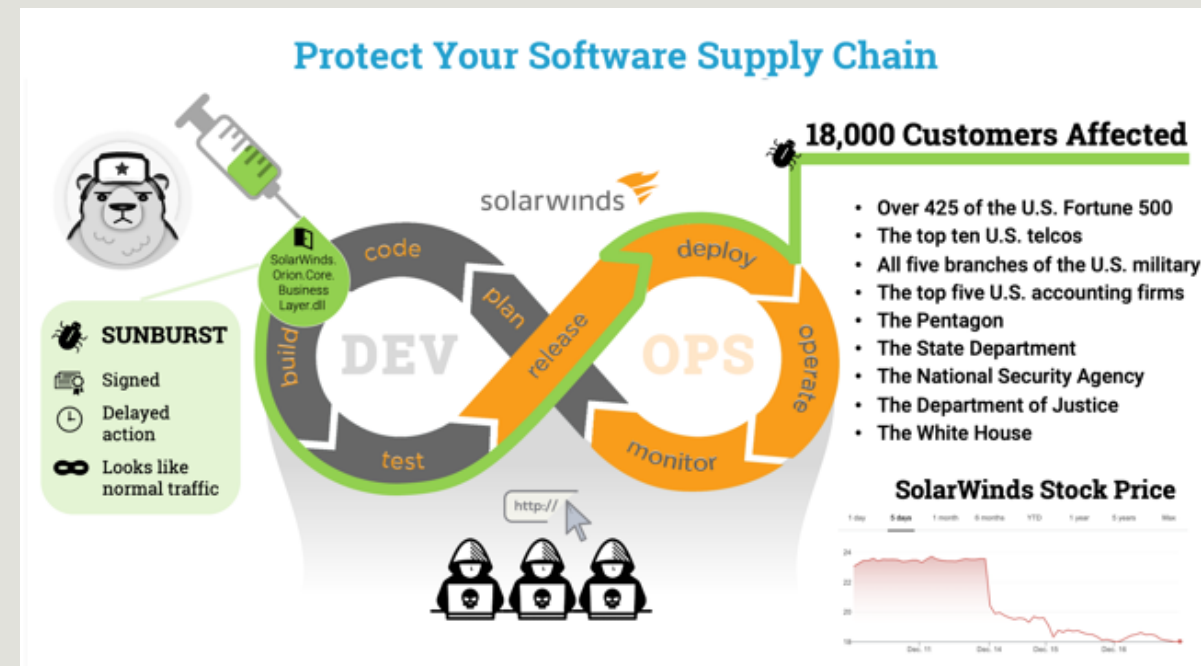
Ref: <https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/>

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

APRIL 5- APRIL 30, 2021



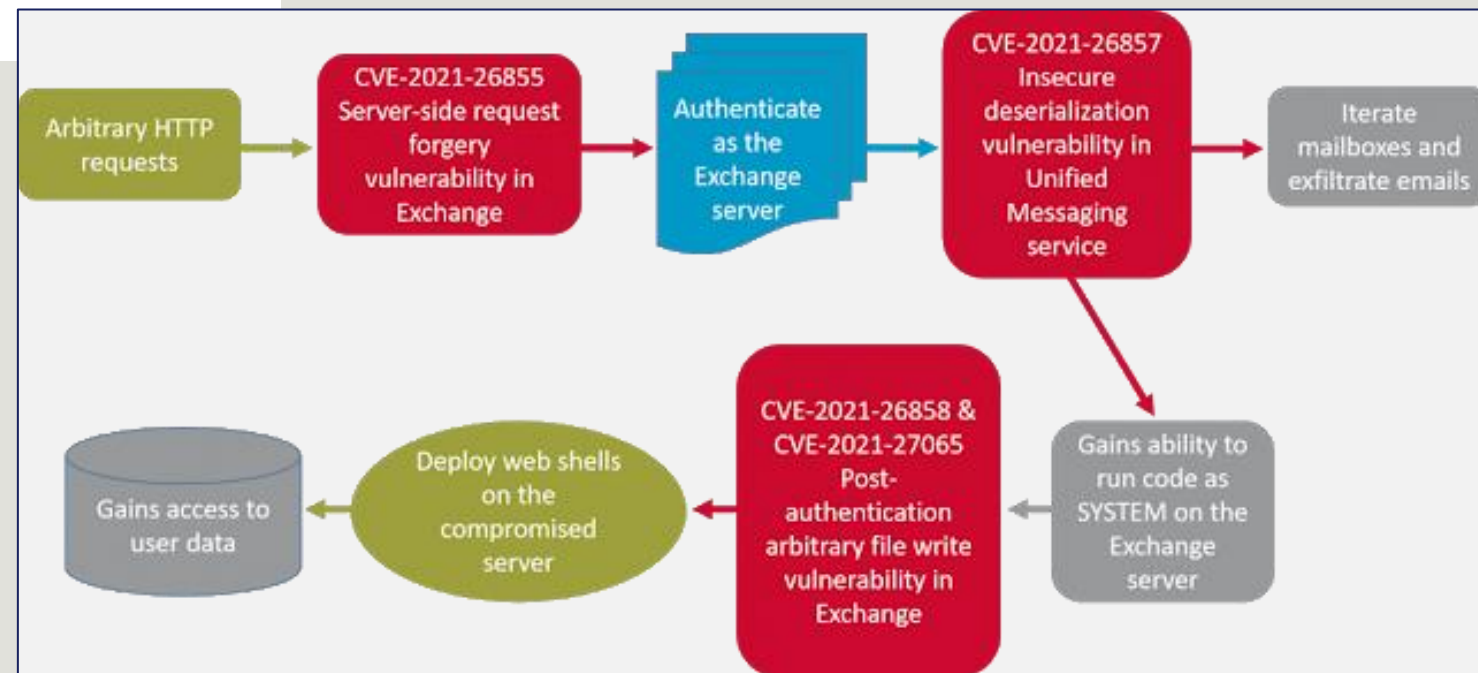
The LONGER your supply chain, the LESS visibility you have!



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



At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software



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>

APRIL 5- APRIL 30, 2021

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, but 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 web 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.



Exchange Server is running one of the following supported CUs:

- Exchange Server 2013 CU23
- Exchange Server 2016 CU19 or CU20
- Exchange Server 2019 CU8 or CU9

Install April 2021 Security Updates

Exchange is up to date

Updated for all known security vulnerabilities including April 2021

Exchange Server is **NOT** running any of the above supported CUs.

Install supported CU
<https://aka.ms/ExchangeUpdateWizard>

Install April 2021 Security Updates

Exchange is up to date

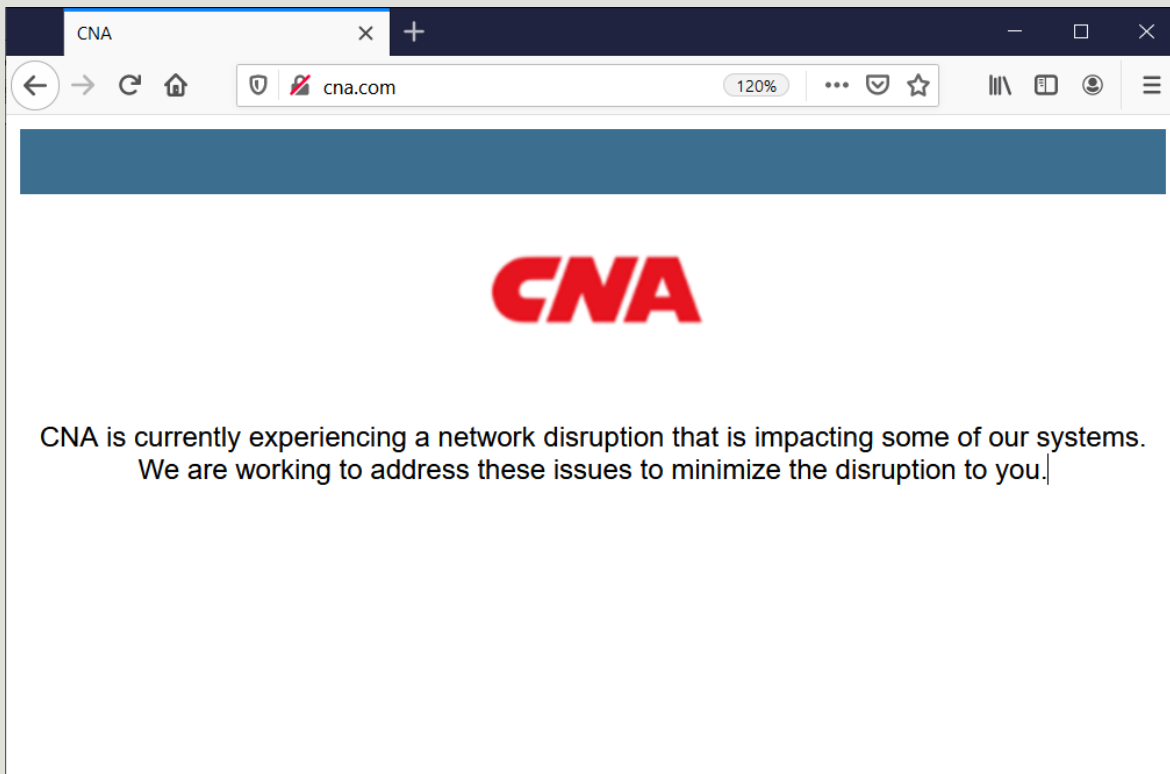
Updated for all known security vulnerabilities including April 2021

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>

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/>

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/>

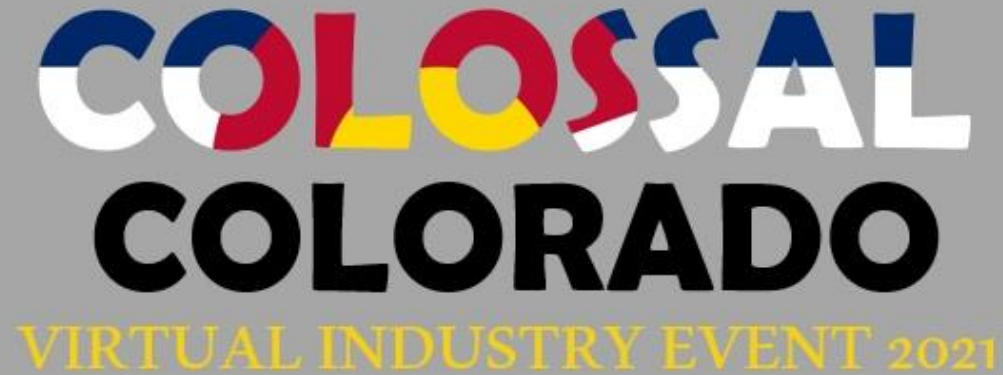
APRIL 5- APRIL 30, 2021

- **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!**

HOW LONG WILL IT TAKE TO CRACK YOUR PASSWORD

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



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!!



APRIL 5- APRIL 30, 2021

Questions & Conversation

