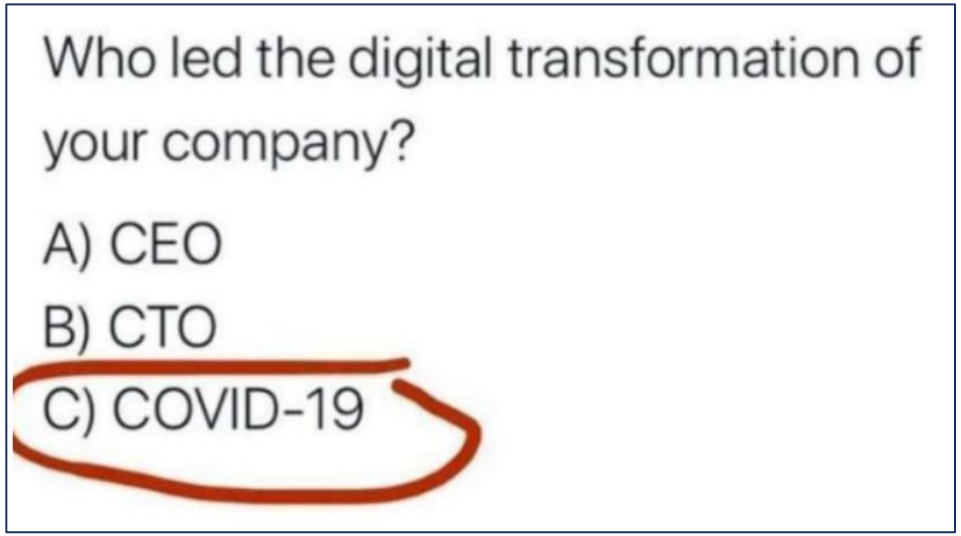
WHY CYBERSECURITY

A PRESENTATION FOR THE SOCIETY OF AMERICAN MILITARY ENGINEERS, DENVER POST, AUGUST 20TH, 2020

BE RHODES

OUTLINE

- WHOIS
- Standards
- Cyber Threats
- Cyber Kill Chain
- Cyber is “the” Big Data Challenge
- Live Attack Demo
- Why Cybersecurity



WHOIS

- **Brad Rhodes**
- TLDR:
  - Head of Cybersecurity at zvelo
  - LTC, Cyber (17A) Colorado Army National Guard & Cyber Shield Planner
  - 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+

Recent Podcast Appearance (Colorado = Security, Episode 159):
https://www.colorado-security.com/podcast

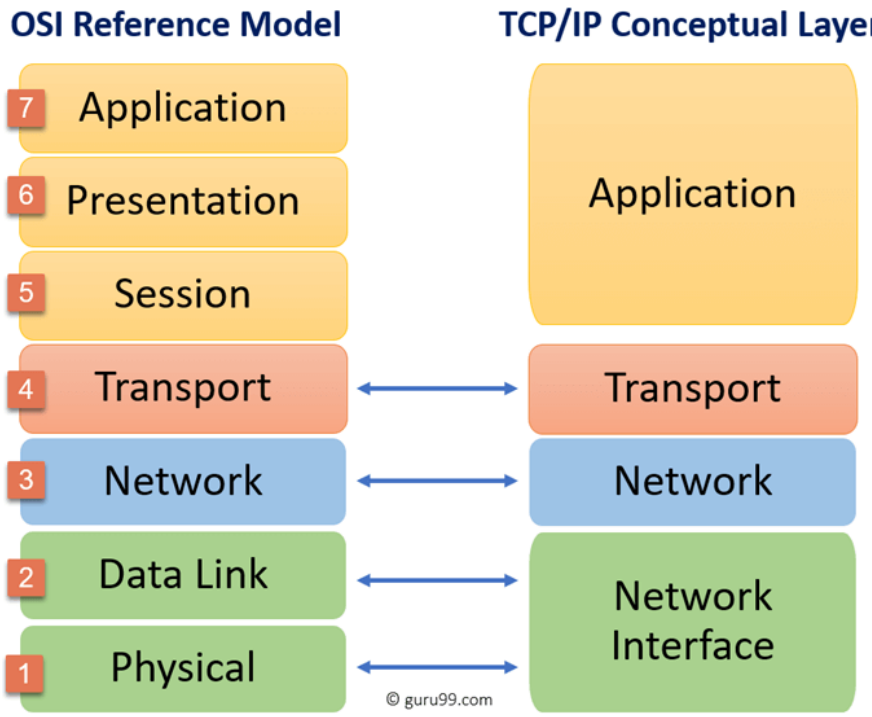
Cyber & Big Data presentation for ISSA/ISACA:
https://www.youtube.com/watch?v=dI8jxLbjWiA

ISO

DoD/DARPA

IEEE

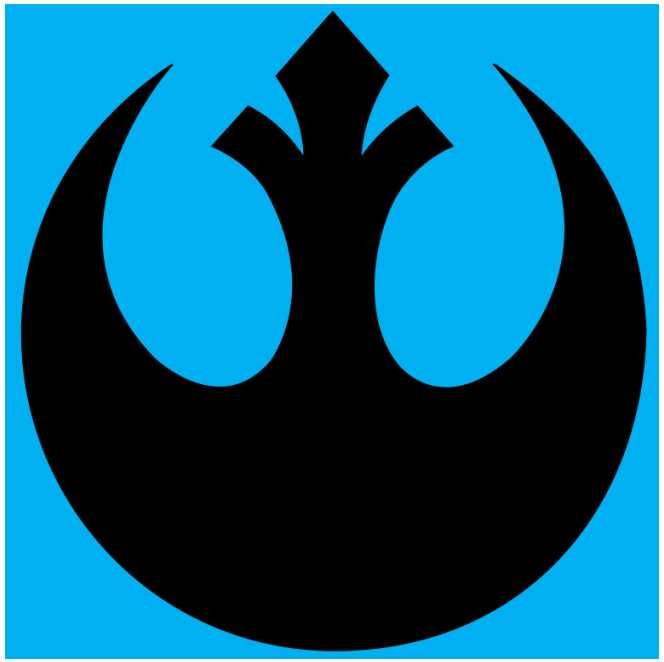
NIST

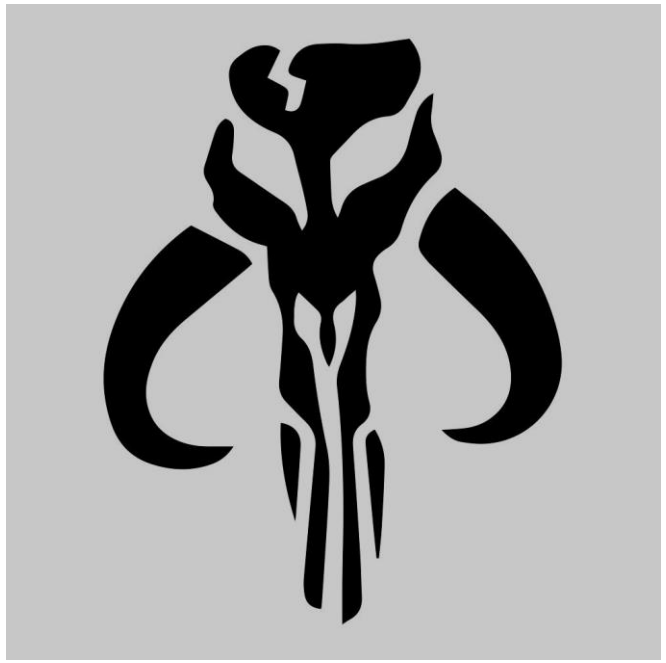


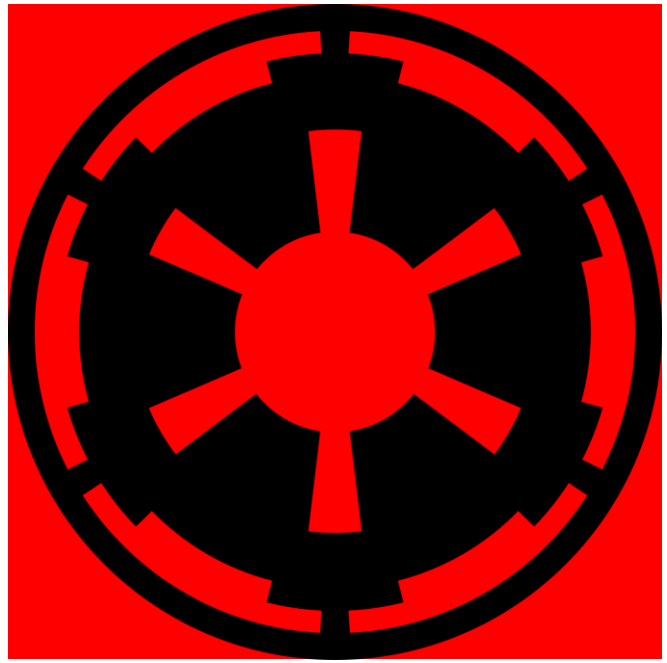
IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	late 2019 (expected)	60 GHz	100 Gbps	300-500 m.
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

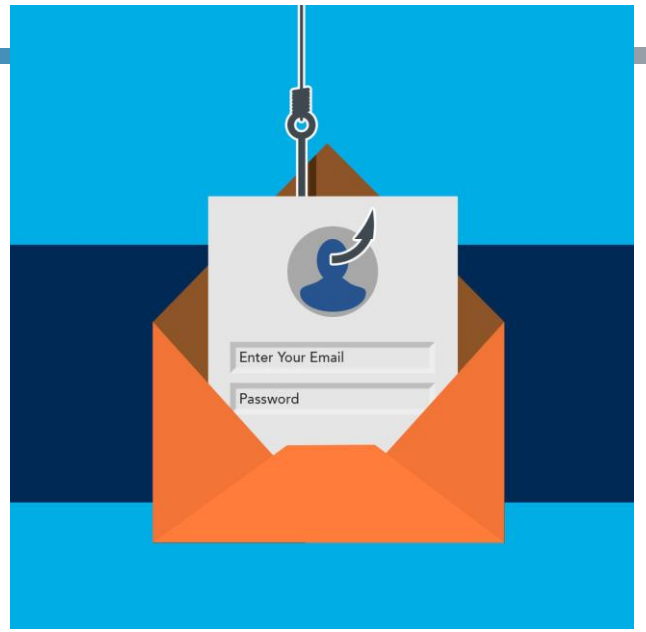
STANDARDS

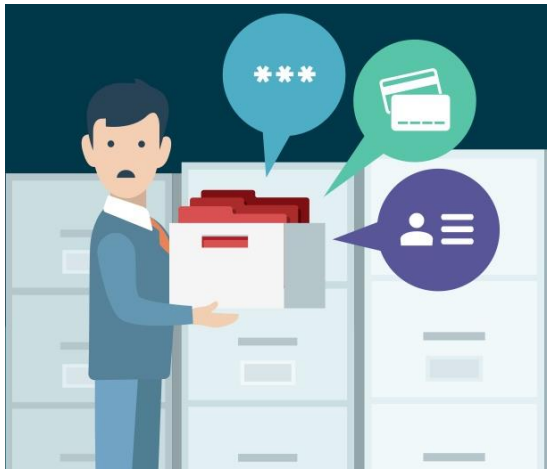




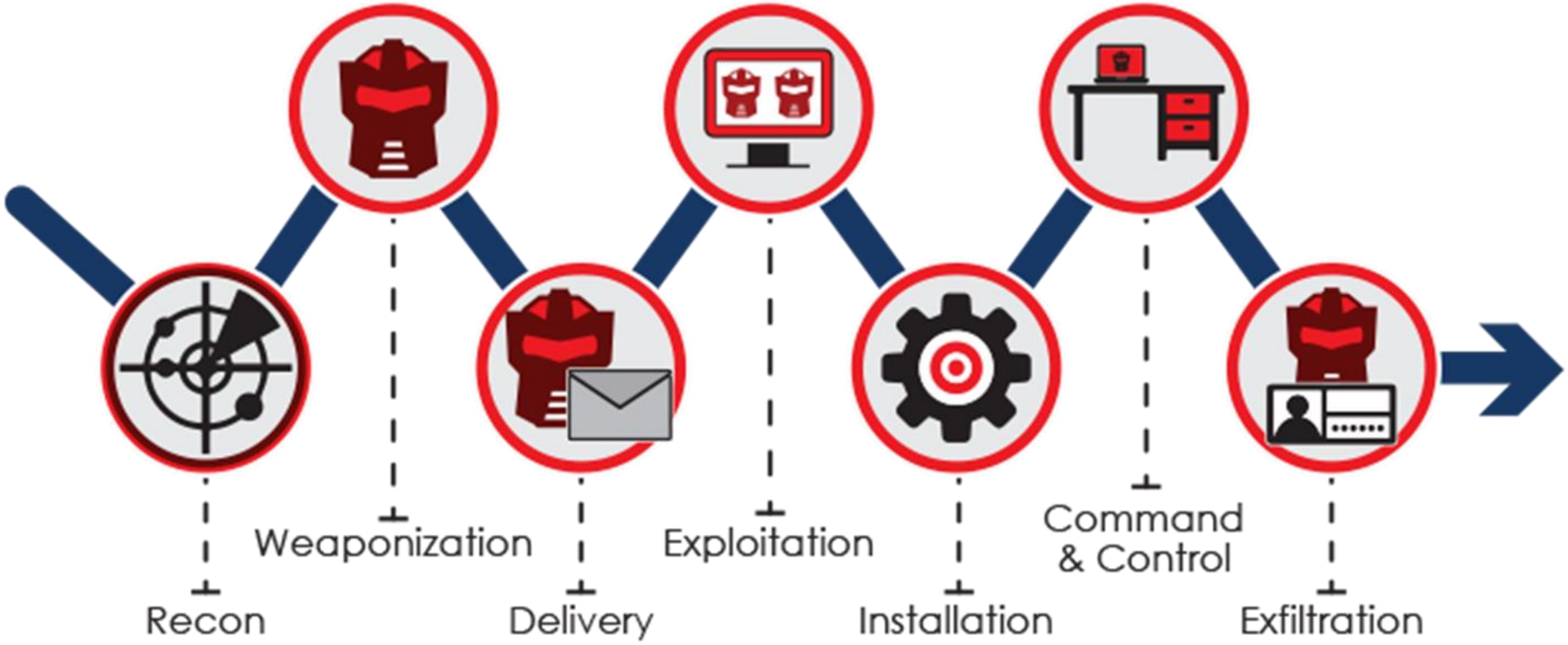


STANDARDS & TOOLS – SAME ONES USED BY BLUE, GRAY, & RED



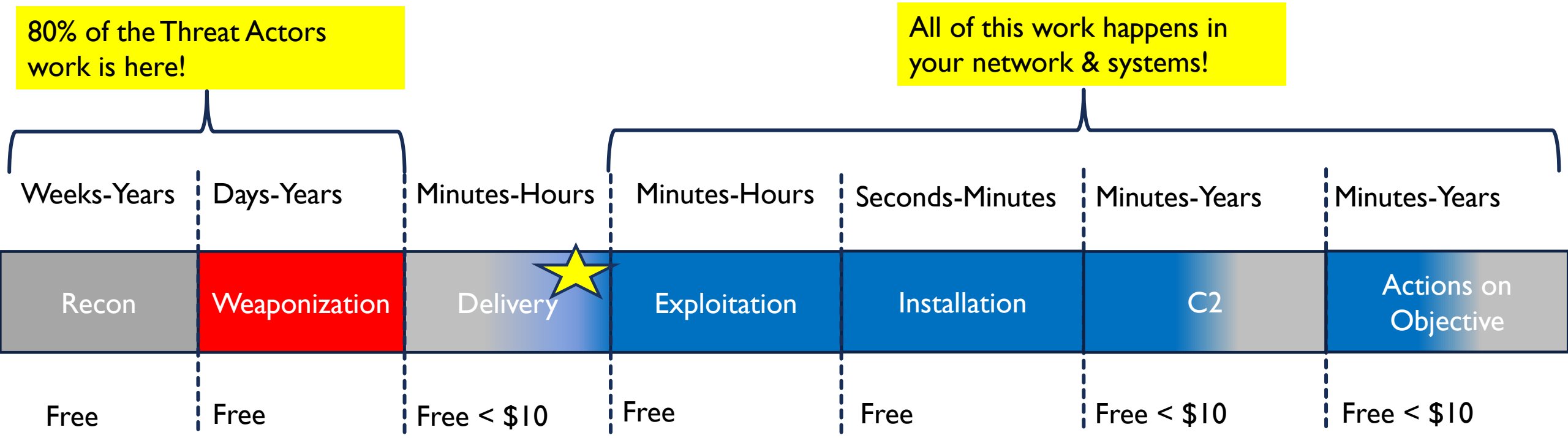


CYBER THREATS: RANSOMWARE, PHISHING, HACKING, MISCONFIGURATIONS, INSIDER THREAT, AND APTS



CYBER KILL CHAIN

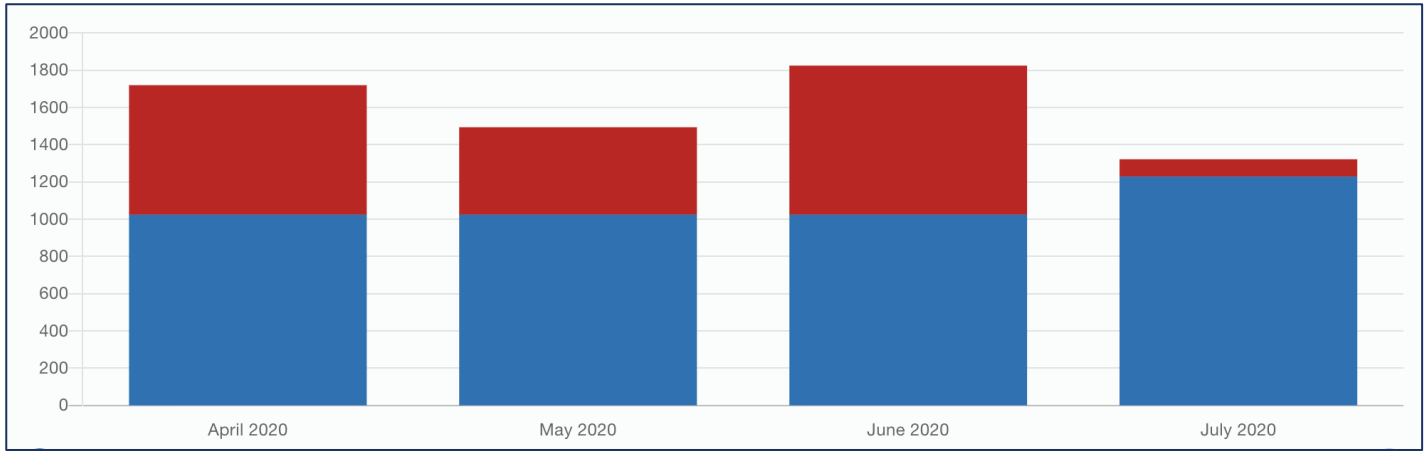
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html



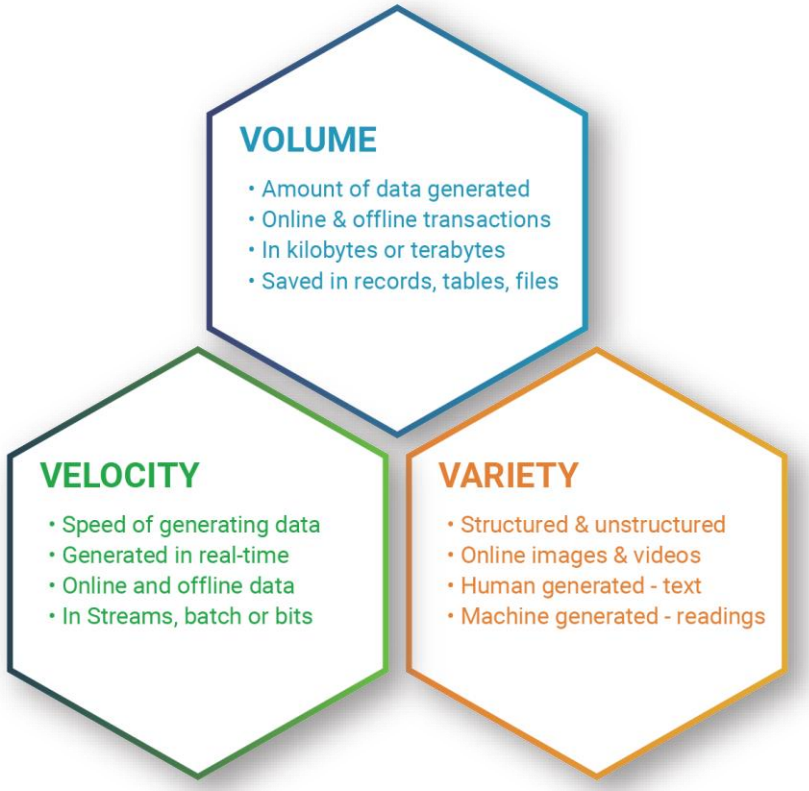
Per IBM, the global average for breach detection in 2019 was 206 days!!

CYBER KILL CHAIN – TIMES & COST (THREAT ACTOR)

- **VOLUME:** Zettabytes (~1 Billion Terrabytes) of data on the internet (source: Cisco)
- **VOLUME *and* VARIETY:** 5G — support for 1,000,000 devices per km^2 (source: Rogers Communications)
- **VARIETY:** 500 Billion '*things*' on the internet by 2030 (source: Cisco)
- **VOLUME *and* VARIETY:** Small Home Network has 40-50 devices and millions of data points daily
- **VELOCITY:** 1Gbps typical network speeds



THE 3VS OF BIG DATA



CYBER IS "THE" BIG DATA CHALLENGE

Chemical Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Communications Sector

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. The Department of Homeland Security is the Sector-Specific Agency for the Communications Sector.

Dams Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Emergency Services Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.

Commercial Facilities Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

Critical Manufacturing Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Defense Industrial Base Sector

The U.S. Department of Defense is the Sector-Specific Agency for the Defense Industrial Base Sector. The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.

Energy Sector

The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector-Specific Agency for the Energy Sector.

Financial Services Sector

The Department of the Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Government Facilities Sector

The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Information Technology Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Food and Agriculture Sector

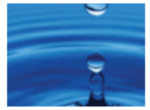
The Department of Agriculture and the Department of Health and Human Services are designated as the co-Sector-Specific Agencies for the Food and Agriculture Sector.

Healthcare and Public Health Sector

The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Nuclear Reactors, Materials, and Waste Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

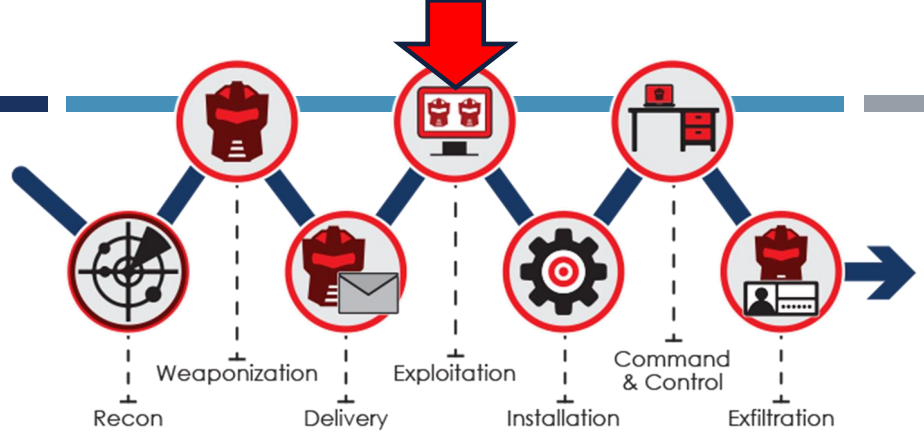


Water and Wastewater Systems Sector

The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

CYBER IS "THE" BIG DATA CHALLENGE – SPANS **ALL** VERTICALS!

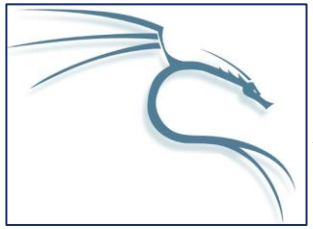
https://www.cisa.gov/critical-infrastructure-sectors



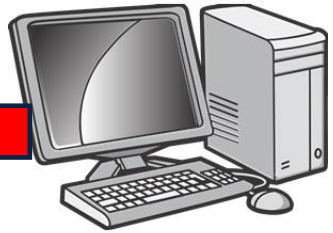
Attack #1:

Web-based

Attack #2:



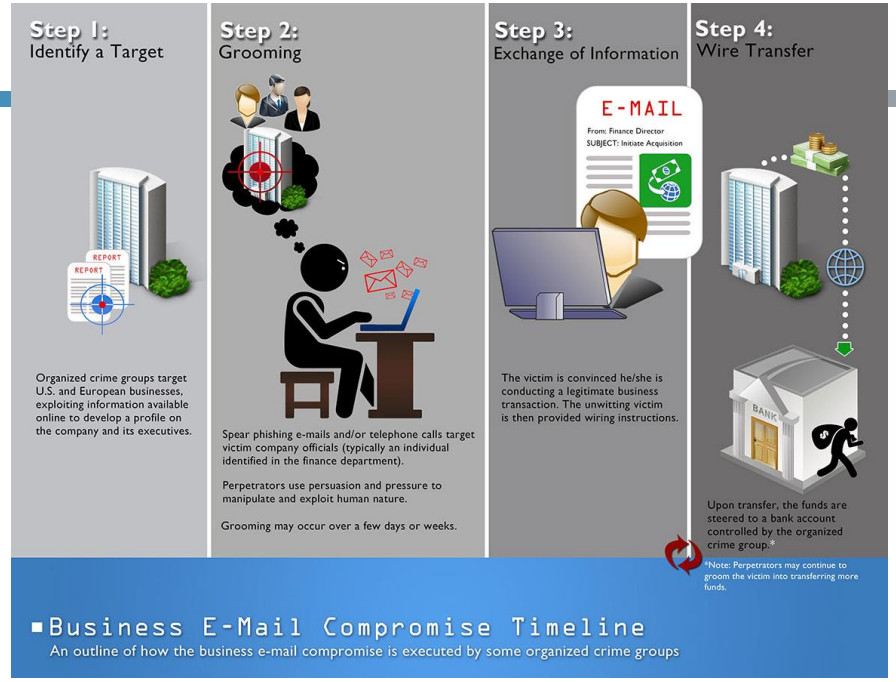
Phishing



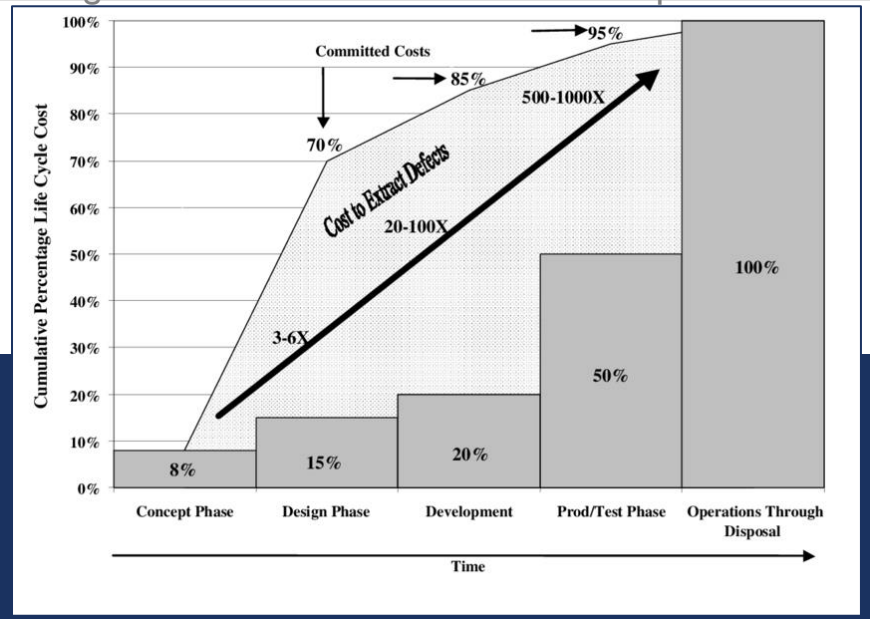
LIVE ATTACK DEMO

WHY CYBERSECURITY

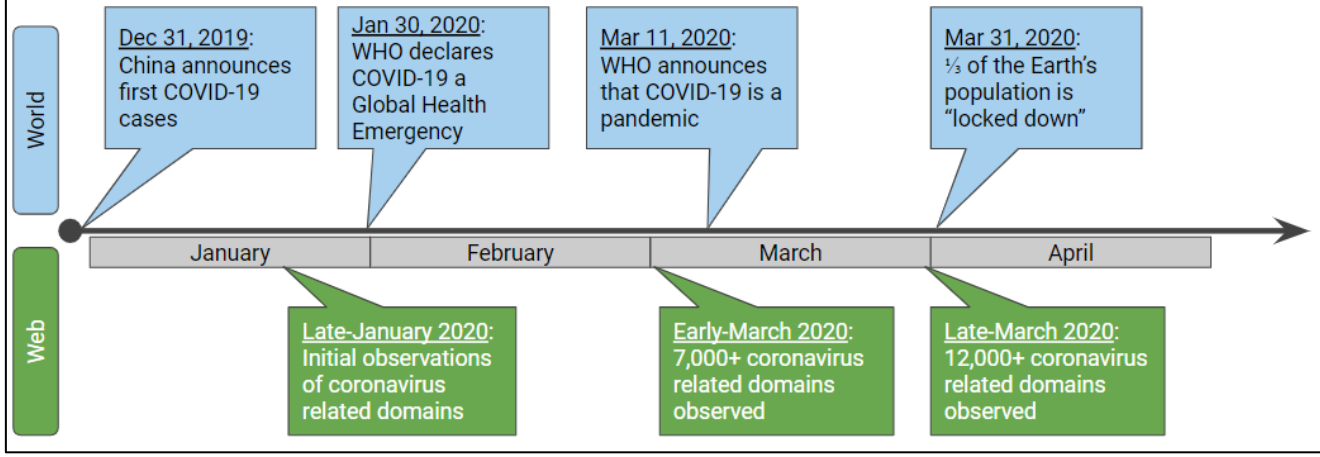
- Loss of funds (Business Email Compromise (BEC))
- Loss of Intellectual Property
- Loss of Reputation
- Legal/Regulatory Requirements (& fines)
  - HIPAA, GDPR, CCPA, SOX/GBLA, COPPA, Privacy Act, etc…
- Cost of Recovery
- **Cybersecurity Maturity Model Certification (required when doing business with the Federal Government: https://www.acq.osd.mil/cmmc/)**



https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise



Coronavirus Domains Timeline

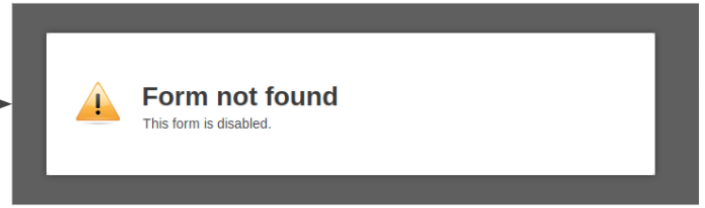


beirutblast[.]org
helpbeirut[.]org
helpforbeirut[.]org
savebeirut[.]org

Trends Observed

#2 Redirection to Potential Malicious Content (2 of 2) - Example

curecoronavirus[.]life: redirects to a popular "forms" site likely built to harvest personal information.

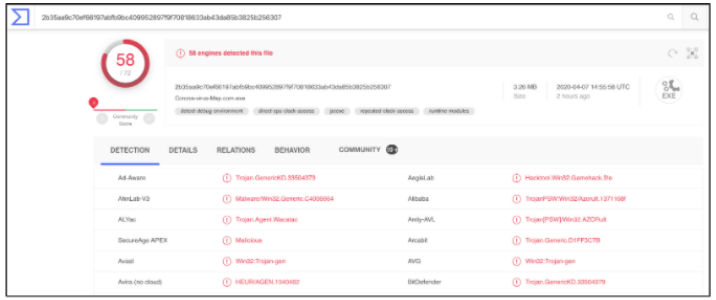


Good news: This form is no longer active! Bad news: This form was probably successful in collecting information from an unknown number of victims.

Trends Observed

#4 Malicious Traffic via Third Parties

Strange redirect to a legitimate site pulling a third party source that had been compromised delivering known malware: corona-virus-map.com.exe (AZORult information stealer).



https://www.virustotal.com/gui/file/2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307/detection

WHY CYBERSECURITY - PANDEMIC

- The Basics – stop 80% of attacks
  - Complex Passwords (don't share them, use a password manager)
  - Multifactor Authentication
  - 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
  - **Trust your gut – if something feels wrong, it probably is!**

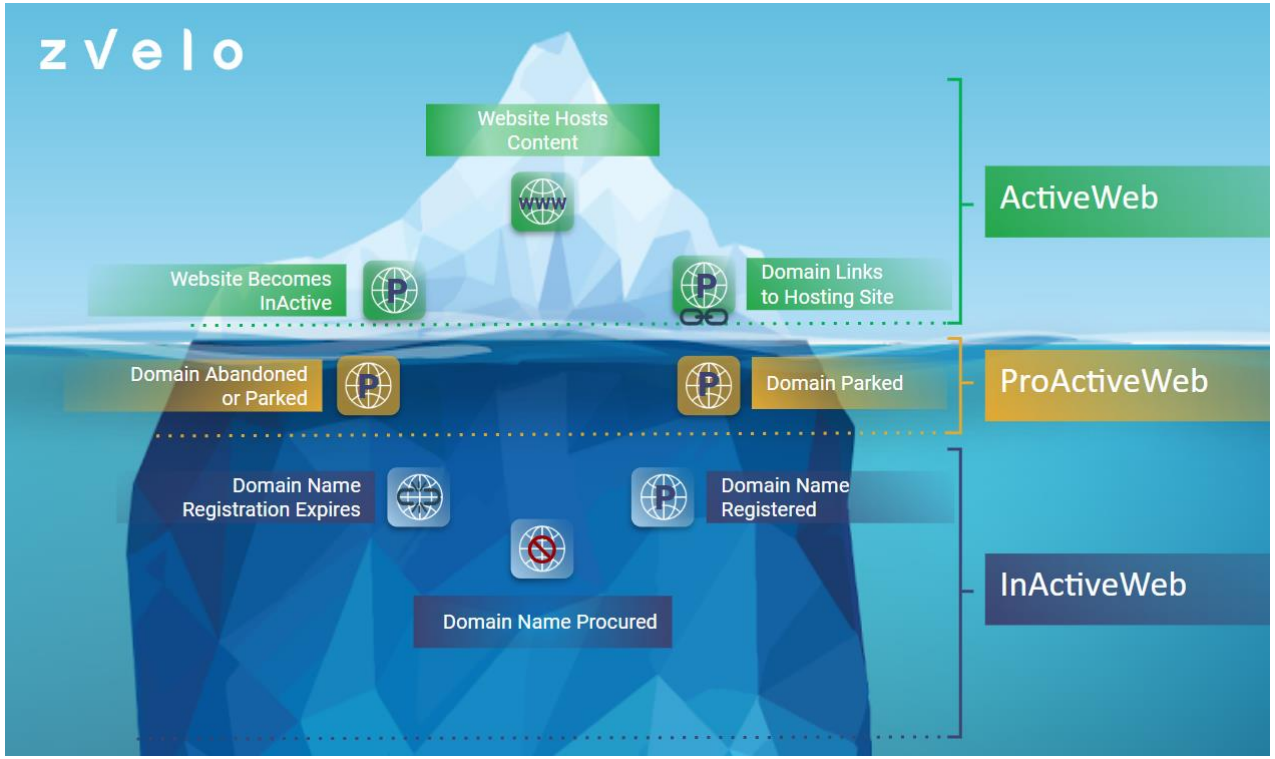
number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	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

WHAT CAN YOU DO RIGHT NOW?

FUTURE SESSIONS

- October – Cyber Panel (Elections)
- Winter – Cyber Exercises/CTF
- Spring – Cyber Panel (Vulnerabilities & Risks)

zvelo



- To learn more, visit us at: https://zvelo.com & Tech Blog: https://zvelo.com/blog/

THANK YOU & QUESTIONS

BRHODES@ZVELO.COM

BRAD.E.RHODES.MIL@MAIL.MIL

BRAD.RHODES@MILCYBER.ORG