Executive Order (EO) on Improving the Nation's Cybersecurity

The Executive Order (EO) on Improving the Nation's Cybersecurity was signed in May and is now in the process of being implemented. The EO is broad ranging in scope, focusing on key areas of vulnerability, including:

- Removing barriers to threat information sharing between government and the private sector
- Modernizing and implementing stronger cybersecurity standards in the federal government
- Improving software supply chain security
- Establishing a cybersecurity safety review board
- Creating a standard playbook for responding to cyber incidents
- Improving detection of cybersecurity incidents on federal government networks
- Improving investigative and remediation capabilities

The principal aim of the EO is to enhance the cybersecurity of government departments and supply chains. However, expect this to have a trickle-down impact on all types of businesses within the private sector, both big and small.

Therefore, small businesses should make themselves aware of the requirements of the EO and determine if they are required to make any changes to remain in compliance, specifically with regards to their vendor relationships.

AN OFFERING IN THE BLUE CYBER SERIES:

The Importance of DIB Small Business Cybersecurity

Presented by
Ms. Krystal Covey, Director
The DoD DIB Collaborative Information Sharing Environment (DCISE)

1 Mar 2022

#21 in the Blue Cyber Education Series

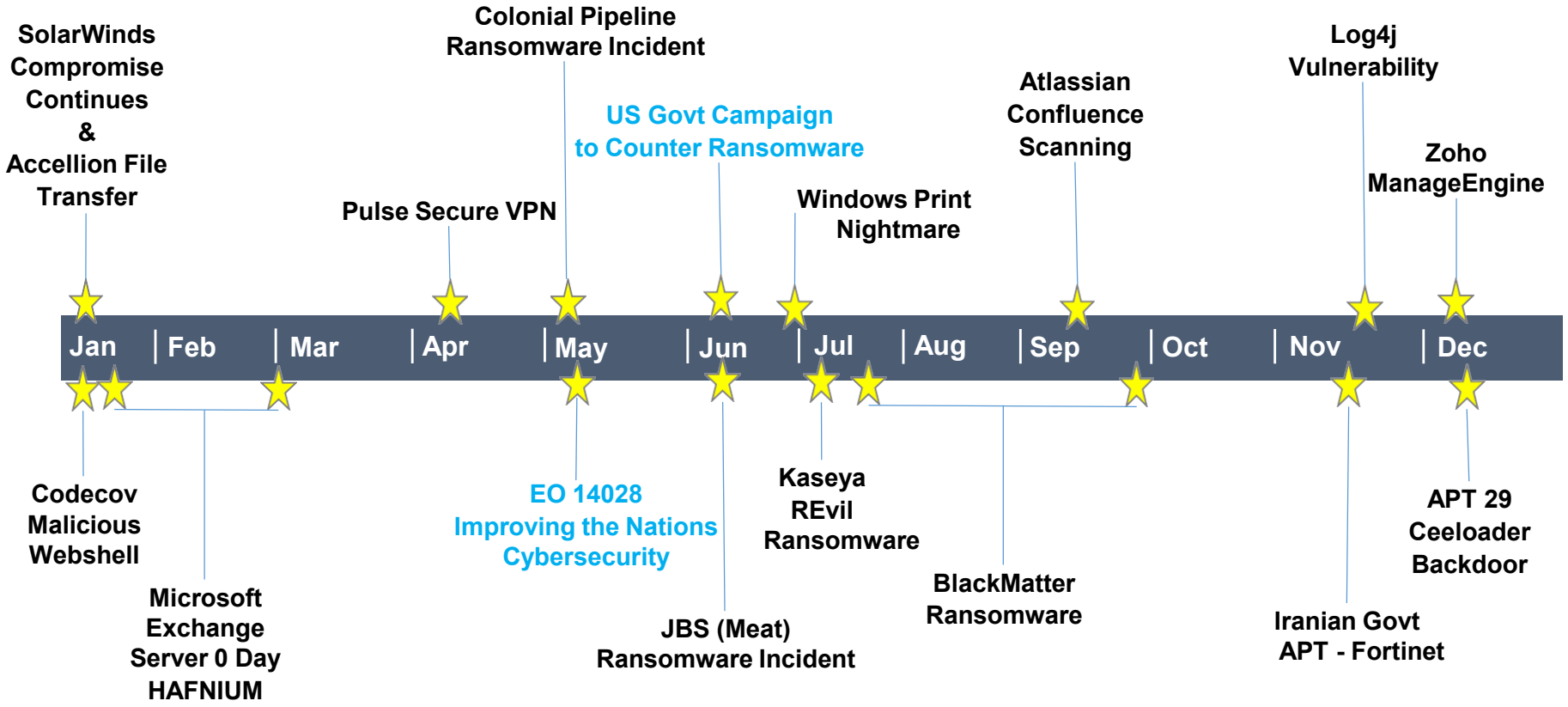
The Importance of DIB Small Business Cybersecurity

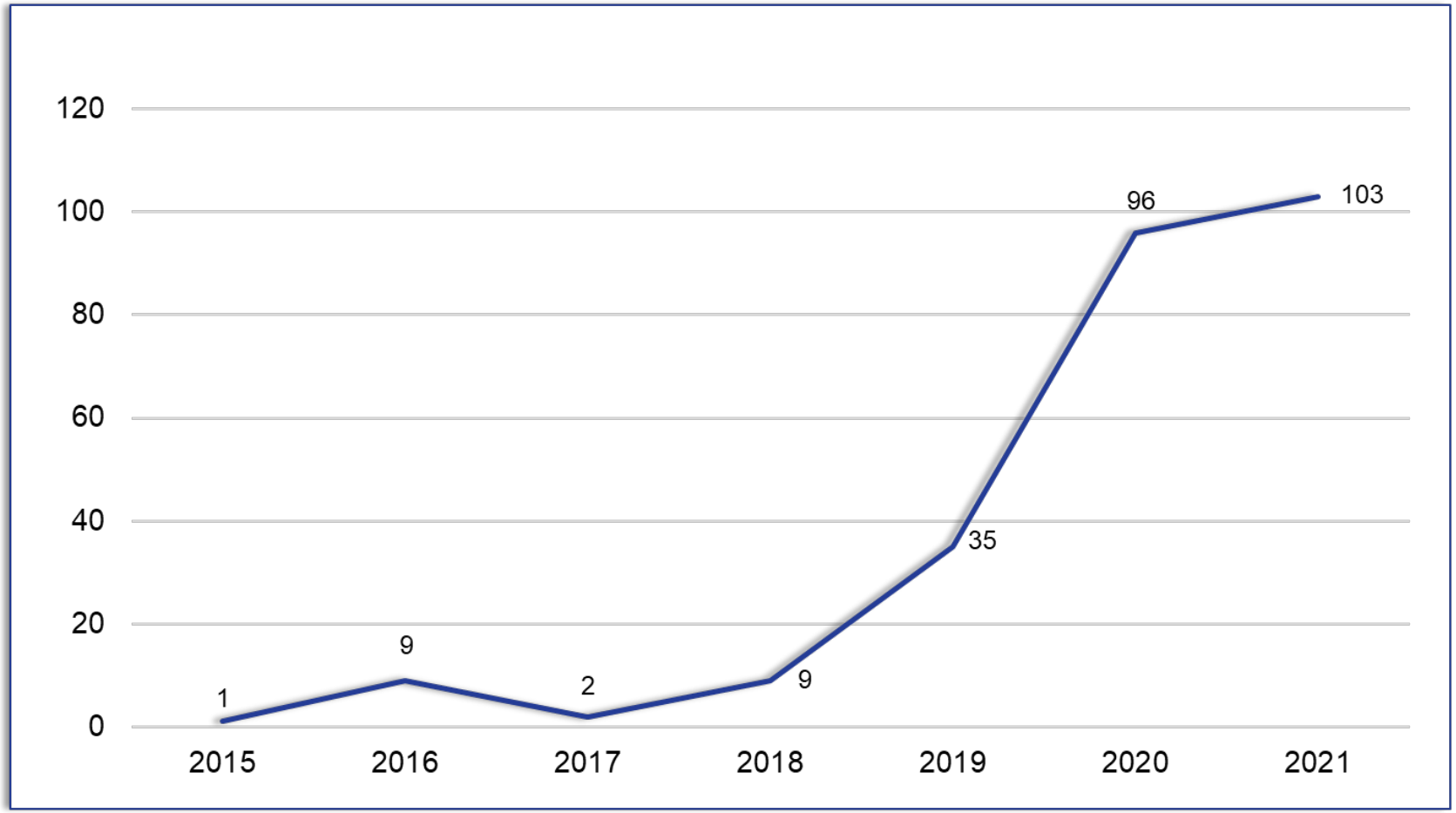
Krystal Covey
Director, DCISE
2 Mar 22

- Value of Small Businesses
- The threat is real
  - Highlights
  - Ransomware
  - Nation states
- So what? (Impacts)
- How compromises happen
- What does prevention look like? What should you do?
- DCISE's role
- Resources

- DIB Small Business Ecosystem
- Oct 21: SECDEF Memo- DoD Small Business Contracting
  - Critically important to DoD mission success
  - Dynamic, innovative, & resilient small business industrial base
- Jan 22: SECAF Memo
  - Critical resource for national defense; high priority focus
  - Accelerated tech, innovation, adaptability, agility, affordability

- Threats to Small Businesses
  - DIB & supply chain networks provide access and insight
- What can happen to your networks/data?
  - Compromise → escalated permissions → unautho access (PII/PHI/CUI) → IP theft → foothold to compromise other key players in supply chain → e
- Why are SB targets?
  - Easier; compromise and leverage to exploit larger companies
  - Less mature in CS
  - Therefore cheaper for the adversary
- Being a target & getting compromised should not be taboo
  - 2 types of companies
  - Emphasis is on Cyber Resilience: ability to recover

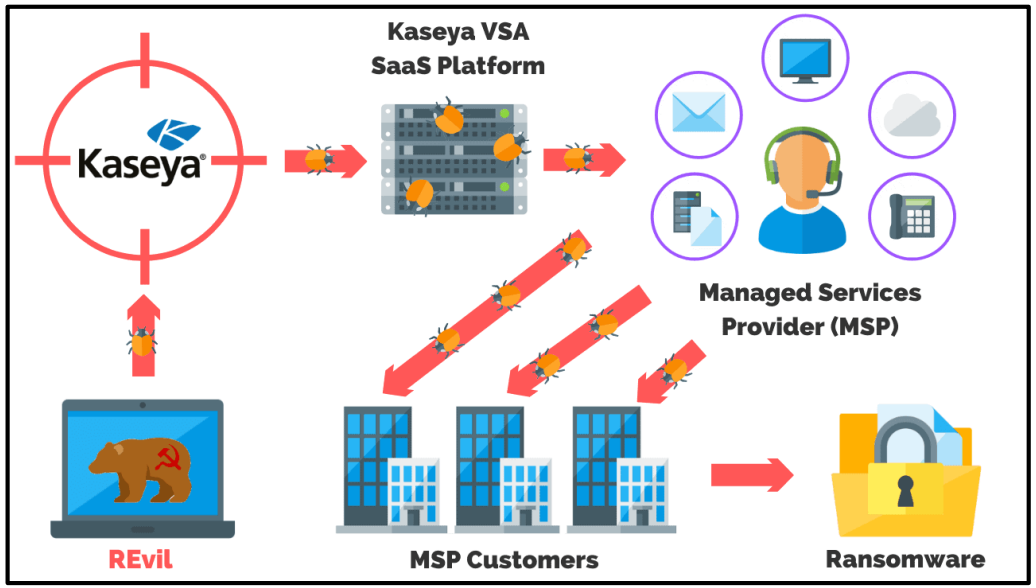

SolarWinds Compromise Continues & Accellion File Transfer
Colonial Pipeline Ransomware Incident
US Govt Campaign to Counter Ransomware
Pulse Secure VPN
Windows Print Nightmare
Atlassian Confluence Scanning
Log4j Vulnerability
Zoho ManageEngine
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Codecov Malicious Webshell
Microsoft Exchange Server 0 Day HAFNIUM
EO 14028 Improving the Nations Cybersecurity
JBS (Meat) Ransomware Incident
Kaseya REvil Ransomware
BlackMatter Ransomware
Iranian Govt APT - Fortinet
APT 29 Ceeloader Backdoor



https://www.cisa.gov/stopransomware

- **2 Jul 21 - Supply chain ransomware attack discovered**
  - Vulnerability in Virtual System Administrator (VSA) software as a service
  - Over 50 managed services providers (MSPs) impacted
    - 800 - 1500 downstream businesses impacted

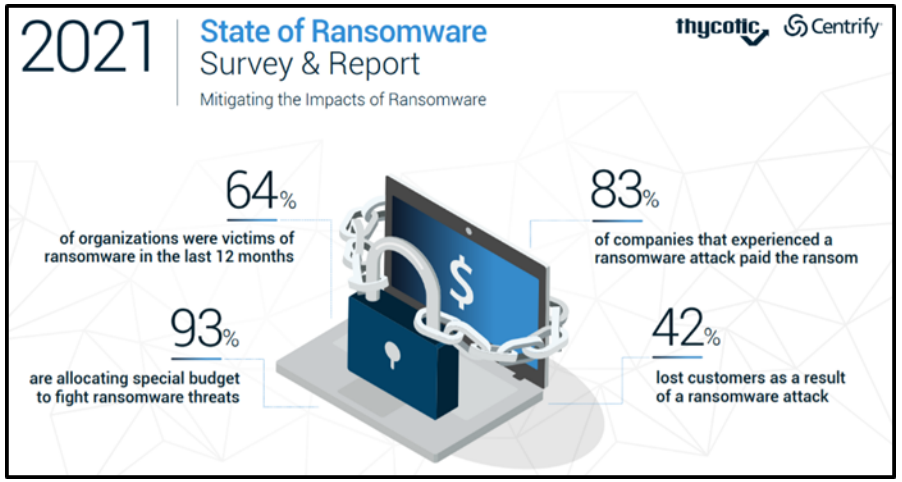
- **13 Jul 21 - Sodinokibi website went offline**
- **22 Jul 21 - Kaseya acquired universal decryption key**
- **DCISE pushed this info to Partners before it made it into media cycles**



https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

Prevention and Mitigation

- CISA MS-ISAC Guide
  - Maintain offline backups of data
  - Develop incident response plans
  - Institute cybersecurity training
  - Regularly update anti-virus and anti-malware software
  - Employ authentication protocols
- 21 Sep 21 - US Treasury Department's Office of Foreign Assets Control issued updated advisory
  - Emphasis on cooperation with law enforcement as a significant mitigating factor



1 Nov 21 - FBI Private Industry Notification

"The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities."

https://www.cisa.gov/uscert/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa


BAD NEIGHBOUR
BAD NEIGHBOUR
BAD NEIGHBOUR
BAD NEIGHBOUR
BAD NEIGHBOUR

CY21 DoJ Indictments

- **North Korea:** Three Military Hackers Indicted in Sony & WannaCry Incidents (17 Feb 21)
- **Latvia:** National Charged for Alleged Role in Transnational Cybercrime Organization "Trickbot" (4 Jun 21)
- **Ukraine:** Arrested and Charged with Ransomware Attack on Kaseya (REvil) (8 Nov 21)
- **Iran:** Two Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election (18 Nov 21)

- Why does it matter that the adversary is targeting you?
- What do the adversaries do with the data that they access on your networks?
- “My company is so small, there is no way that we are a target.”
- A small business survey from CNBC and Momentive shows majority (56%) of America’s small business owners are not worried about being the victim of a cyberattack

https://www.cnbc.com/2021/08/10/main-street-overconfidence-small-businesses-dont-worry-about-hacking.html

- “60% of Small Companies close within 6 months of being hacked”
  - **Recovery costs can be anywhere from thousands to millions, depending upon the scope/scale of incident**
- Emphasis on Cyber Resilience, not being impenetrable
  - **Achievable goals**

https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

STATS:

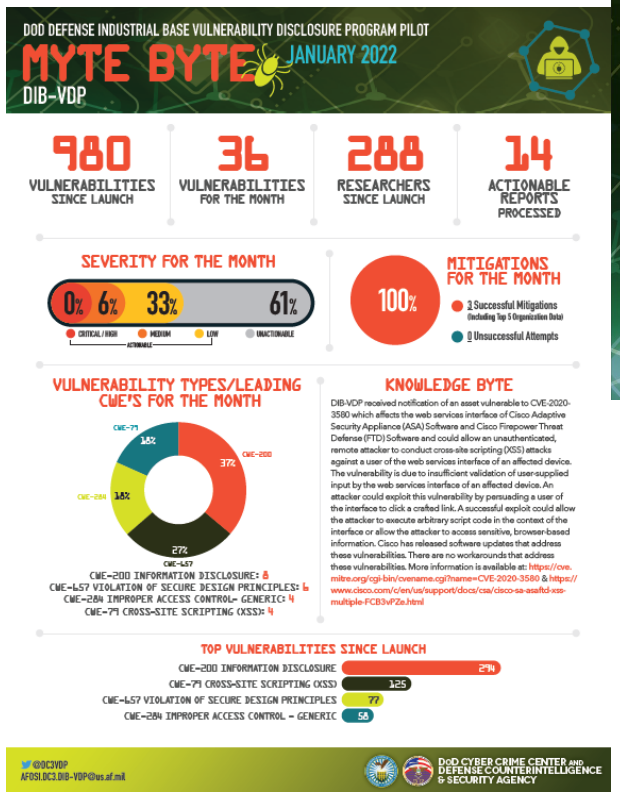
1003 All Time Reports

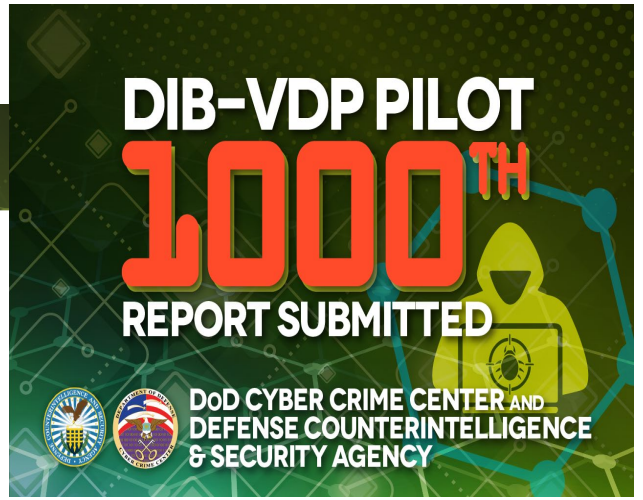
288 Researchers

439 Actionable Reports Processed

40 DIBCO Participants

347 assets in scope since launch





To join, send an email to: DIB-VDP@dc3.mil

$500 Billion

The estimated annual losses from intellectual property theft cases associated with the People's Republic of China perpetrated in the United States.

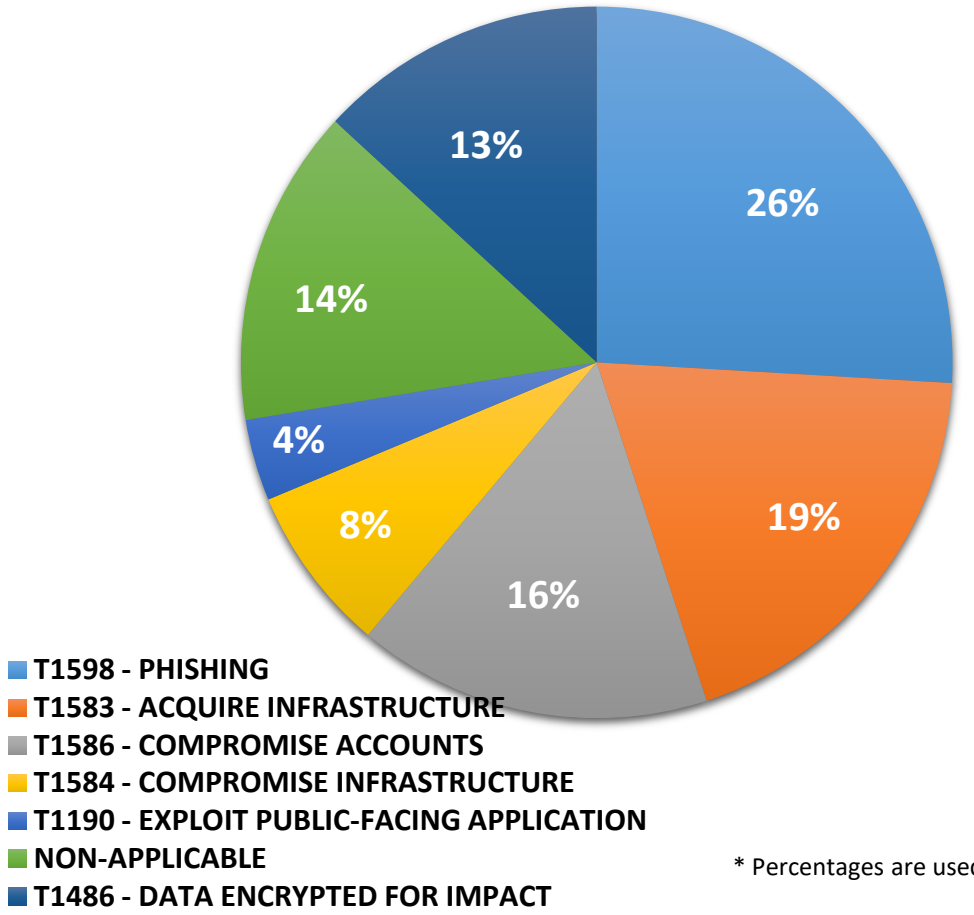
F-35	Specifications	**Shenyang J-31**
51.4 ft (15.7 m)	**Length**	56 ft 9 in
35 ft	**Wingspan**	37 ft 9 in
14.4 ft	**Height**	15 ft 9 in
69.9K lbs	**Max takeoff weight**	61.7K lbs
1200 Mph	**Max cruise speed**	1242 Mph
1726 Miles	**Range**	2485 Miles
19.9K lbs	**Max payload**	17.6K lbs

- Adversaries gain access to systems in many different ways
  - Example: through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.
  - Example: Adversaries can use compromised email accounts to further their operations, such as leveraging them to conduct Phishing for Information or Phishing
    - Utilizing an existing persona with a compromised email account may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona. Compromised email accounts can also be used in the acquisition of infrastructure (ex: Domains)
- They can purchase domains used during targeting
  - Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free.

- Adversaries may encrypt data on target systems or large numbers of systems in a network to interrupt availability to system and network resources
  - They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key
    - This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted. In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.
- Adversaries may hijack domains and/or subdomains that can be used during targeting
  - Domain registration hijacking is the act of changing the registration of a domain name without the permission of the original registrant
    - An adversary may gain access to an email account for the person listed as the owner of the domain. The adversary can then claim that they forgot their password in order to make changes to the domain registration. Other possibilities include social engineering a domain registration help desk to gain access to an account or taking advantage of renewal process gaps.

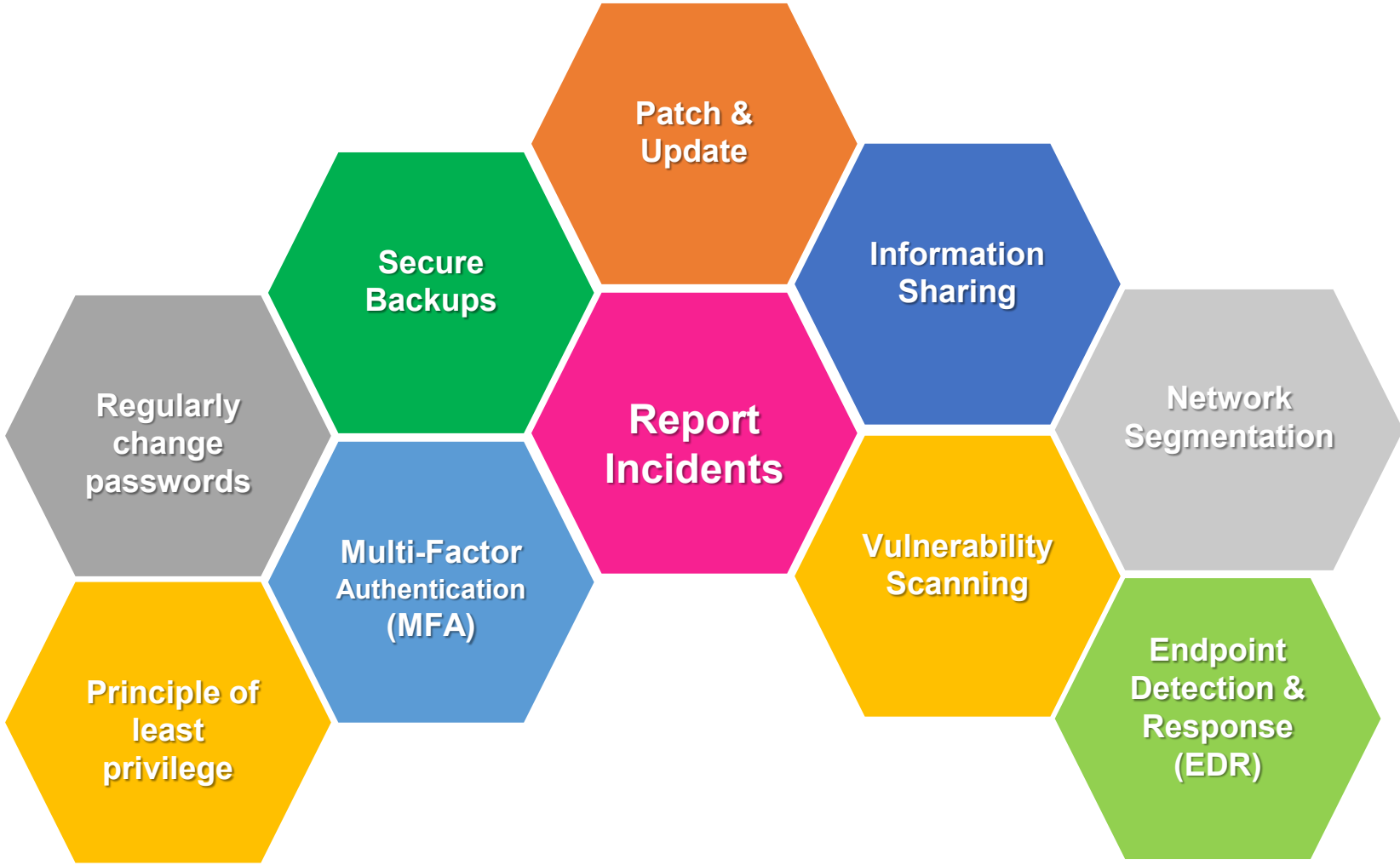
- On 1 Oct 21, DCISE began officially using the MITRE ATT&CK Framework to denote reported event/incident TTPs to meet a growing awareness and use throughout the DIB and US Govt organizations

2021 DCISE Identified ATT&CK TTPs*



* Percentages are used due to classification constraints

- Is it about prevention? Or about resilience?
- Good cybersecurity hygiene contributing to resilience
  - CIO Top 10 from Town Halls
  - DFARS 252.204-7012
    - NIST SP 800.171
  - CMMC


Patch & Update
Secure Backups
Information Sharing
Regularly change passwords
Report Incidents
Network Segmentation
Multi-Factor Authentication (MFA)
Vulnerability Scanning
Principle of least privilege
Endpoint Detection & Response (EDR)

- Ensuring a company can defend itself against cyberattacks starts by implementing essential cybersecurity practices

  1) Keep up-to-date architecture diagrams with inventories of all hardware and software to be able to respond to threats quickly.

  2) Patch and configure security settings on all devices and software.

  3) Employ active defenses for known attack vectors and stay ahead of attackers with the latest intelligence and response actions.

  4) Monitor network and device activity logs and look for anomalous behaviors.

  5) Employ multi-factor authentication because username and passwords are easily hacked.

  6) Employ email and browser defenses and prevention for two of the most prevalent attack vectors.

  7) Employ malware protection on the networks.

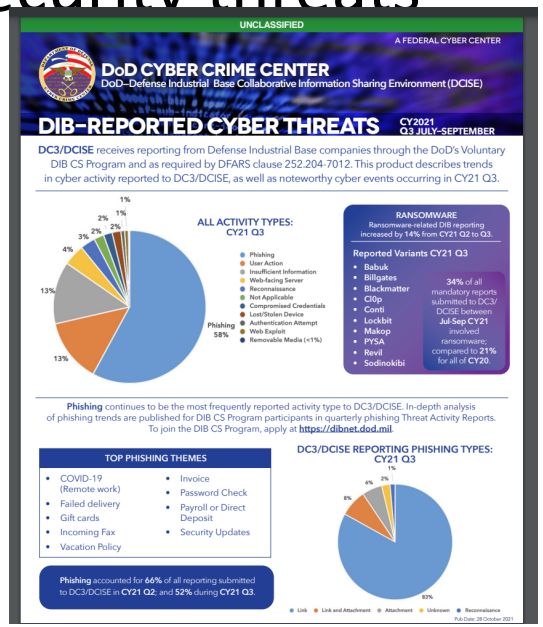
  8) Encrypt data at rest and in transit.

  9) Train staff to avoid and respond to suspicious events.

  10) Have contingency plans and exercise them. Employ backup and recovery, alternative services, emergency response/notification and other similar processes to ensure the organization can successfully respond to a cyber event.

https://www.defense.gov/News/News-Stories/Article/Article/2926539/dod-focused-on-protecting-the-defense-industrial-base-from-cyber-threats/

- DCISE promotes collaborative information sharing and delivers DIB-focused Cybersecurity services and resources. DCISE is the DoD conduit for DIB cyber incidents, leveraging 14+ years of subject matter expertise to inform the USG of Cybersecurity threats and trends impacting the DIB.
  - Cyber Threat Round-Up (CTR)
  - Slicksheets
  - 32 CFR part 236 expansion (Future state)
  - DIBNET splash page


UNCLASSIFIED

A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER
DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DIB–REPORTED CYBER THREATS CY2021 Q3 JULY–SEPTEMBER

DC3/DCISE receives reporting from Defense Industrial Base companies through the DoD's Voluntary DIB CS Program and as required by DFARS clause 252.204-7012. This product describes trends in cyber activity reported to DC3/DCISE, as well as noteworthy cyber events occurring in CY21 Q3.

ALL ACTIVITY TYPES: CY21 Q3

Phishing 58%
13%
13%
4%
3%
2%
2%
2%
1%
1%

Phishing
User Action
Insufficient Information
Web-facing Server
Reconnaissance
Not Applicable
Compromised Credentials
Lost/Stolen Device
Authentication Attempt
Web Exploit
Removable Media (<1%)

RANSOMWARE
Ransomware-related DIB reporting increased by 14% from CY21 Q2 to Q3.

Reported Variants CY21 Q3
- Babuk
- Bilgates
- Blackmatter
- CiOp
- Conti
- Lockbit
- Makop
- PYSA
- Revil
- Sodinokibi

34% of all mandatory reports submitted to DC3/DCISE between Jul-Sep CY21 involved ransomware, compared to 21% for all of CY20.

Phishing continues to be the most frequently reported activity type to DC3/DCISE. In-depth analysis of phishing trends are published for DIB CS Program participants in quarterly phishing Threat Activity Reports. To join the DIB CS Program, apply at https://dibnet.dod.mil.

TOP PHISHING THEMES
- COVID-19 (Remote work)
- Failed delivery
- Gift cards
- Incoming Fax
- Vacation Policy
- Invoice
- Password Check
- Payroll or Direct Deposit
- Security Updates

Phishing accounted for 66% of all reporting submitted to DC3/DCISE in CY21 Q2; and 52% during CY21 Q3.

DC3/DCISE REPORTING PHISHING TYPES: CY21 Q3

83%
8%
4%
3%
1%

Link
Link and Attachment
Attachment
Unknown
Reconnaissance

Pub Date: 28 October 2021

Welcome to the DIBNet Portal

DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program.

Cyber Reports

Report a Cyber Incident

A Medium Assurance Certificate is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report.

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS 252.239-7010 Cloud Computing Services

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Need Assistance?
Contact DoD Cyber Crime Center (DC3)
DC3.DCISE@us.af.mil
Hotline: (410) 981-0104
Toll Free: (877) 838-2174

DoD's DIB Cybersecurity (CS) Program

Apply Now!

The DIB CS Program is a voluntary public-private cybersecurity partnership in which DoD and participants share cyber threat information, mitigation and remediation strategies, and more.

DIB CS Participant Login | Voluntary Report

Cyber Threat Roundup

The Cyber Threat Roundup is a weekly collection of recent open-source articles of interest for the Defense Industrial Base. For the latest edition of the Cyber Threat Roundup, please click here.

For more information about other products, please apply to the DIB CS Program.

Need Assistance?
Contact the DIB CS Program Office
OSD.DIBCSIA@mail.mil
Hotline: (703) 604-3167
Toll Free: (855) DoD-IACS
Fax: (571) 372-5434

- What tools/resources exist?
  - DHS CISA list of free resources
    - https://www.cisa.gov/free-cybersecurity-services-and-tools
  - NSA pDNS service
  - DC3 EMS/AMR?
  - DC3/DCSA DIB VDP Pilot
  - DCISE Hotline (add 877 #) /Inbox (DC3/DCISE@us.af.mil)
  - Project Spectrum
  - FBI NDCA
  - FBI Infragard

- DAF Cyber Blue Team is your friend!!
- Kelley Kiernan is standing by to assist you and hosts sessions every Tuesday
- If you are interested in a particular topic, ask

- You are a target! (But that’s okay if you are resilient!)
- You can get ahead of the adversary and take steps to defend your data
- Ask for help
- Leverage resources- there are many!

Questions?

DC3.DCISE@us.af.mil
Hotline: 410-981-0104
Web: www.dc3.mil

References

- DOD Cyber Crime Center www.dc3.mil
- To join the VDP Pilot: To join, send an email to: DIB-VDP@dc3.mil
- The DoD Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) HTTPS://WWW.DC3.MIL/ORGANIZATIONS/DIB-CYBERSECURITY/DIB-CYBERSECURITY-DCISE/
- DIBNET Cyber Incident Reports https://dibnet.dod.mil/portal/intranet/
- DOD CMMC Website https://www.acq.osd.mil/cmmc/
- Very solid guide to getting started from NIST: https://www.nist.gov/publications/getting-started-nist-cybersecurity-framework-quick-start-guide
- Another NIST guide to understanding the WHY of cybersecurity: https://svtc-va.org/wp-content/uploads/2018/01/JMU_Oct_30_15.pdf
- Connect to local support through the SBA at https://www.sbir.gov/local-assistance
- CISA Cyber Essentials to get started today: https://www.cisa.gov/publication/cisa-cyber-essentials