CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY, SECURE TOMORROW

COVID-19 Communication Products

Last Updated May 7, 2020

Joint Alerts

[CISA Current Activity: FBI Releases Guidance on Defending Against VTC Hijacking and Zoom-bombing]

- On April 2, the FBI released an article on defending against video-teleconferencing (VTC) hijacking (referred to as "Zoom-bombing" when attacks are to the Zoom VTC platform). The FBI released this guidance in response to an increase in reports of VTC hijacking.

[UK and US Security Agencies Issue COVID-19 Cyber Threat Update]

- On April 8, CISA, in partnership with the UK's National Cyber Security Centre (NCSC), released a joint advisory on the growing number of cyber criminals and other online malicious groups exploiting the COVID-19 outbreak. In addition to alerting people to the threat, the advisory directs them to resources available to counter it.

[CISA Alert AA20-099A: COVID-19 Exploited by Malicious Cyber Actors]

- On April 8, CISA and the UK's NCSC issued a joint alert which provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups during the COVID-19 pandemic.

[Joint Bulletin: Physical Security Considerations for the Healthcare Industry During COVID-19 Response]

- On April 24, CISA, Health and Human Services, and the Federal Bureau of Investigation, jointly released a bulletin regarding potential threats to the healthcare industry and resources on how to mitigate these threats.

[Cyber Warning Issued for Key Healthcare Organizations in UK and USA]

- On May 5, CISA and the UK's NCSC released a joint advisory to address the large-scale "password spraying" campaigns against healthcare bodies and medical research organizations.

[Joint CISA and UK Tip on COVID-19 Cyber Threat Exploitation]

- On May 5, CISA and the UK's NCSC released a joint advisory to address an increase in malicious activity with themes related to COVID-19. Malicious cyber actors are targeting individuals, small and medium enterprises, and large organizations worldwide through COVID-19-related scams and phishing campaigns. At the same time, the surge in teleworking has increased the use of potentially vulnerable services.

Cyber Alerts

[Defending Against COVID-19 Cyber Scams Alert]

- On March 6, CISA released this alert warning individuals to remain vigilant for scams related to COVID-19.

Enterprise VPN Security Alert

- On March 13, CISA released this alert to provide information on VPN security as more organizations implement remote work options—or telework—which require an enterprise virtual private network (VPN) solution to connect employees to an organization's information technology (IT) network.

The United States Issues an Advisory on North Korean Cyber Threats

- On April 15, the U.S. Departments of State, Homeland Security, and Treasury, and the Federal Bureau of Investigation issued an advisory to raise the awareness of the cyber threat posed by North Korea. The advisory highlights North Korea's malicious cyber activities around the world, identifies U.S. government resources that provide technical and threat information, and includes recommended measures to counter the cyber threat.

CISA: AA20-107A: Continued Threat Actor Exploitation Post Pulse Secure VPN Patching

- On April 16, CISA released this alert to update to alert administrators that threat actors who successfully exploited CVE-2019-11510 and stole an organization's credentials will still be able to access—and move laterally through— the organization's network after it has patched this vulnerability if the organization did not change those stolen credentials.

Infrastructure Security

Letters to Faith-Based Communities

- On April 8, CISA issued letters to members of faith-based communities about the need to remain vigilant, and expressed its commitment to supporting their efforts in maintaining safe and secure houses of worship and related facilities during a time when stressors caused by the pandemic may contribute to an individual's decision to commit an attack or influence their target of choice.

Emergency Communications

Priority Telecommunications Services

- As of May 6, CISA provided Priority Telecommunications Services to approximately 70,000 additional users, increasing connectivity for essential critical workers access to Government Emergency Telecommunications Service (GETS), Wireless Priority Services (WPS), and Telecommunications Service Priority (TSP).

Election Security

COVID-19 Elections Working Group

- In March, CISA, in partnership with the U.S. Election Assistance Committee, created a COVID-19 working group within its election sector coordinating councils. This working group is a joint effort between the private sector and the government to identify information needed by election officials to support the expansion of vote-by-mail that many states are looking to implement as well as improve the safety of polling places in a COVID-19 environment.

COVID-19 Elections Web page

- On April 9, CISA launched the COVID-19 Elections web page on CISA.gov. The website contains a number of election security resources for state and local election officials including the following resources developed by the Election Infrastructure Subsector's Government Coordinating Council (GCC) and Sector Coordinating Council (SCC):
    - Ballot Drop Box
    - Election Education & Outreach for Increased Absentee or Mail Voting
    - Electronic Ballot Delivery and Marking
    - Helping Voters to Request a Mail-In Ballot
    - Importance of Accurate Voter Data When Expanding Absentee or Mail Ballot Voting
    - Inbound Ballot Process
    - Managing an Increase in Outbound Ballots
    - Signature Verification & Cure Process
    - Vote by Mail Project Timeline
- The website is updated frequently as the COVID-19 Elections Working group, and CISA and other election partners continue to provide additional content.

Supply Chain

Building Collective Resilience for the ICT Supply Chain

- On May 5, CISA released a blog to provide information on how individual companies and organizations can build and implementing an effective ICT supply chain risk management program to improve their overall security posture during COVID-19.

CISA and INL Release Commercial Routing Assistance App

- On May 6, CISA and the Idaho National Laboratory (INL) launched a new "Commercial Routing Assistance (CRA) tool "for truckers and other commercial drivers in the United States. The free app incorporates coordinated data streams and plots multiple routing options so commercial operators can plan and manage vehicle movements across multiple states quickly in times of disasters or other restrictions. CISA and INL also released a Commercial Routing Assistance Fact Sheet.

Tools and Resources

Coronavirus Web page

- On Feb. 28, CISA launched its Coronavirus web page to ensure that the public and private sectors have the information they need to ensure America's cyber and infrastructure security during the COVID-19 pandemic.

CISA Insights Risk Management for Novel Coronavirus (COVID-19)

- On March 18, CISA released a new CISA Insights to help executives think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19.

Guidance on Essential Critical Infrastructure Workers During COVID-19

- On March 19, CISA released guidance to help state and local jurisdictions and the private sector identify and manage their essential workforce while responding to COVID-19. Subsequent versions were introduced to include additional services and industries that were deemed essential after receiving feedback and suggestions from its partners. The latest version was published on April 17.

Implementing Safety Practices for Critical Infrastructure Workers Who May Have Had Exposure to a Person with Suspected or Confirmed COVID-19

- In April, CISA and the CDC released interim guidance to aid critical infrastructure workers in 16 different sectors of work to provide information on what they should do if they have been exposed to COVID-19.

Trusted Internet Connections (TIC) 3.0 Interim Telework Guidance

- On April 8, CISA released interim Trusted Internet Connections (TIC) guidance to aid agencies in securing their network and cloud environments. The "TIC 3.0 Interim Telework Guidance" supports the current surge in teleworking and use of collaboration tools amongst the federal workforce.

Critical Infrastructure Operations Centers and Control Rooms Guide for Pandemic Response

- On April 23, CISA released guidance geared toward all 16 critical infrastructure sectors identified by the federal government. The guide provides considerations and mitigation measures for operation centers and control rooms but can be applied further to any critical node that is required to continue functioning in a pandemic environment.

Telework Guidance and Resources

- On April 24, CISA launched telework guidance and resources on its website to help agencies and organizations that have implemented more telework in response to COVID-19. In addition to the "TIC 3.0 Interim Telework Guidance," the web page also includes information on:
  - Telework Best Practices from DHS and the National Security Agency
  - Video Conferencing Tips
  - Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing
  - Cybersecurity Recommendations for Federal Agencies Using Video Conferencing
  - Guidance for Securing Video Conferencing

COVID-19 Action Team

- CISA.CAT@CISA.DHS.GOV

FEMA Mission Assignment

- CISA has been activated as part of ESF-2 (Communications) and ESF-14 (Cross Sector Business and Infrastructure) to provide 24/7 support at FEMA's National Response Coordination Center (NRCC) and in the 10 CISA regions.