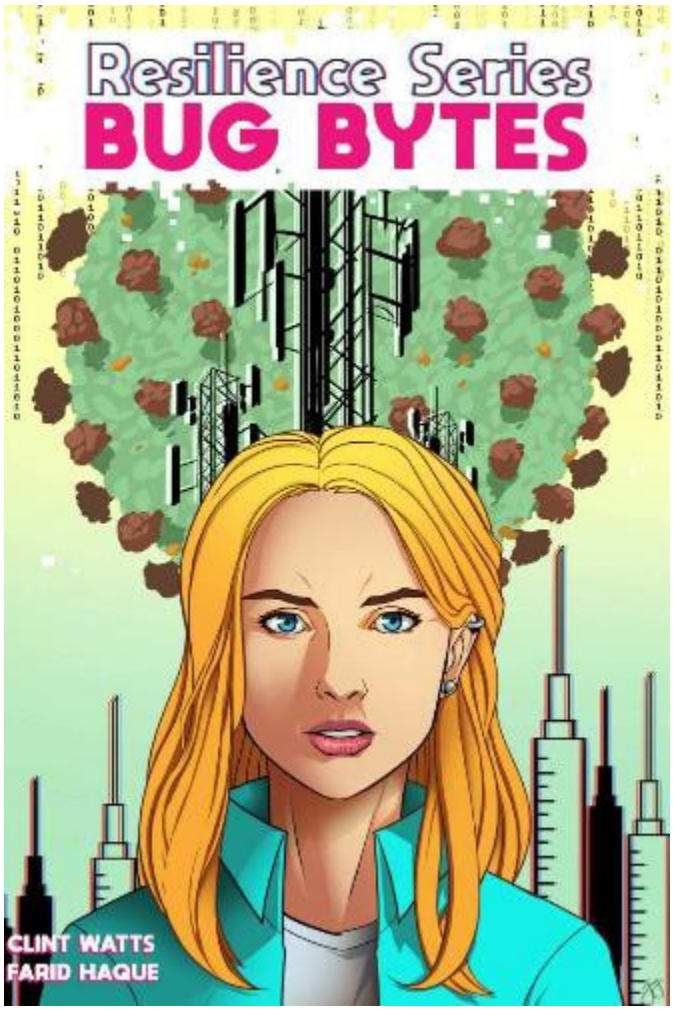
DEFEND TODAY, SECURE TOMORROW

CISA Community Bulletin - June 16, 2021



CISA Releases Second Graphic Novel in Resilience Series

The Cybersecurity and Infrastructure Security Agency (CISA) released Bug Bytes, the second graphic novel in CISA's Resilience Series. This publication communicates the dangers and risks associated with threat actors using social media and other communication platforms to spread mis-, dis-, and malinformation (MDM) for the sole purpose of planting doubt in the minds of targeted audiences to steer their opinion.

Readers follow protagonist Ava who uses her wits and journalism skills to uncover a disinformation campaign set to damage 5G critical communications infrastructure in the United States.

CISA's first graphic novel, Real Fake, was released in October 2020 and demonstrates how threat actors capitalize on political and social issues (especially around election cycles) to undermine public confidence by causing chaos, confusion, and division.

Learn More About the Resilience Series Here

Alerts & Announcements

CISA Releases Best Practice Guidance to Help Organizations Map Adversary Behavior to MITRE ATT&CK Framework

In partnership with Homeland Security Systems Engineering and Development Institute (HSSEDI), which worked with the MITRE ATT&CK team, this framework is an example of a successful collaboration by committed partners with a shared mission.

The guide provides analysts with a detailed step-by-step instruction to best map adversary behavior to the MITRE ATT&CK framework. MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. ATT&CK is freely available to any person or organization in the hopes of bringing communities together to develop more effective cybersecurity.

The MITRE ATT&CK framework can be used to align resources and exchange information across the public and private sectors. It provides improved cyber threat intelligence (CTI) analysis through better, more informed use of the MITRE ATT&CK framework—a robust knowledge base of adversary tactics and techniques based on real-world observations. To that end, the guide includes a recent Joint Cybersecurity Advisory from CISA and the Federal Bureau of Investigation (FBI) as an example of how this framework can be used in practice.

Learn More About Best Practices for MITRE ATT&CK Mapping Here

CISA Holds Virtual Meeting for Priority Telecommunications Services Users

On May 19, CISA held its biannual User Council webinar, bringing together CISA's Priority Telecommunications Services (PTS) subscriber organizations and others within the

communications community for updates on the current state of PTS as well as a glimpse of what the future holds for these vital services.

The webinar focused on the priority services that cover wireline (Government Emergency Telecommunications Service), wireless voice communications (Wireless Priority Service), and priority repair and installation of critical voice and data circuits (Telecommunications Service Priority). Over 700 participants heard presentations from PTS representatives on program highlights (including the high call completion rates during the Capitol riots, presidential inauguration, and Texas power outage); the efforts of the Priority Area Representatives (PARs) and PTS Production Team to spread awareness of the services; and the evolution of Next Generation Networks (NGN) Priority Services (PS) to include data, video, and information services (DVIS) capabilities.

Learn More About Priority Telecommunications Services Here

CISA Protects Critical Infrastructure Information Through PCII Program

CISA's Protected Critical Infrastructure Information (PCII) Program protects private sector and State, local, tribal, and territorial infrastructure information voluntarily shared with the government for the purposes of homeland security from disclosure under the Freedom of Information Act, state and local disclosure laws, civil action, and regulatory proceedings.

Despite the challenges of the COVID-19 pandemic, CISA's PCII Program Office not only continued operations with stakeholders, but also increased its tempo through remote work, thus proving its flexibility to support major events such as the 2020 election and the National Football League's Super Bowl.

Since 2004, the PCII Program Office has validated and protected more than 127,000 submissions. with over 4,400-plus PCII Authorized Users accessing the information on a need-to-know basis, the flexibilities built into information collection, protection, and sharing ensure the PCII Program is a value-added tool for stakeholders.

Learn More About the PCII Program Here

Potential Threat Vectors to 5G Infrastructure

The deployment of 5G has begun, and with it, a wealth of benefits that has the potential to impact every aspect of our lives and work. With faster connectivity, ultra-low latency, greater network capacity, 5G will redefine the operations of critical infrastructure activities from the plant floor to the cloud. To secure the full scope of 5G use cases, it is critical that strong cybersecurity practices are incorporated within the design and development of 5G technology.

CISA, the National Security Agency, and the Office of the Director of National Intelligence, as part of the Enduring Security Framework (ESF)—a cross-sector, public-private working

group—initiated an assessment of the cybersecurity and vulnerabilities to 5G infrastructure. The ESF 5G Threat Model Working Panel, a subgroup within the ESF, developed this paper, "Potential Threat Vectors to 5G Infrastructure", to enhance understanding of the threats posed to 5G adoption. The Working Panel examined three major threat vectors in 5G—standards, the supply chain, and threats to systems architecture—to develop a summary and technical review of types of threats posed by 5G adoption in the United States and sample scenarios of 5G risks.

Learn More About Securing 5G Infrastructure Here

Upcoming HSIN Training

As many readers may be aware, CISA uses the Homeland Security Information Network (HSIN) to provide a secure, web-based, collaborative system to share sensitive cyber-related information and news with select cybersecurity partners.

On June 25, the HSIN Team will officially launch the Inviter, Requester, Approver (IRA) process, an upgrade from the current Nominator/Validator (Nom/Val) tools and functionalities.

To best prepare for the new IRA process, HSIN Mission Integration & Outreach (MIO) will be offering training sessions from **Monday, June 21 through Friday, June 25**. Training sessions will take place twice a day at both **10 a.m.** and **3 p.m. Eastern Time**. For each of these sessions, HSIN Mission Advocates will provide a presentation outlining the IRA process followed by a brief Q&A session.

All current HSIN Community Nominators and Validators are encouraged to participate in one of these training sessions to become familiar with the new IRA process.

Access these sessions using the link and dial-in information below:
URL: https://dhsconnect.connectsolutions.com/hsinirapt
Dial-In: 800-735-5968

The HSIN Training Team has also provided all HSIN users access to IRA quick reference guides (QRGs) on the HSIN Access Management curriculum page. Prior to joining IRA training sessions, it's highly recommended that users review these documents to gain a better understanding of the process and so that they can come prepared with any questions.

Users may contact HSIN@hq.dhs.gov with any questions or reach out to their HSIN Mission Advocate for assistance.

Learn More About HSIN Here

Chemical Security Seminars Save-the Date

Save the date! CISA will be hosting the virtual 2021 Chemical Security Seminars on December 1, 8, and 15, 2021, from 11:00 a.m. to 3:00 p.m. ET (8:00 a.m. to noon PT).

These seminars, held in lieu of the Chemical Security Summit, will be the signature industry event for chemical representatives across the chemical and interconnected sectors—including energy, communications, transportation, and water—to learn, share perspectives, and engage in dialogue regarding chemical security.

Registration and a provisional agenda will be available in the coming weeks. For more information, please email ChemicalSummitReg@hq.dhs.gov.

Events

Partner Webinar: Safety and Security for an Online World

Join the National Initiative for Cybersecurity Education (NICE) for a webinar that will explore the importance of evaluating online information and resources for reliability and validity.

Date: June 16, 2021

Time: 2:00 p.m. EST

Learn More Here

Partner Webinar: How to Pass the Cyber Attacks Testing K-12 Schools

Join the National Cyber Security Alliance (NCSA) and CrowdStrike for a webinar on the evolving cybersecurity threats affecting K-12 schools observed in the past year.

Date: June 22, 2021

Time: 2:00 p.m. ET

Learn More Here

Partner Webinar: Cybersecurity: Identify Your Gaps & Protect Your Business

Join the Small Business Administration (SBA) for a webinar to learn how to protect your business – and your customers – from a cyberattack.

Date: June 22, 2021

Time: 12:00 p.m. ET

Learn More Here

Featured Programs and Resources

CISA and NIST: Defending Against Software Supply Chain Attacks

A software supply chain attack occurs when a cyber threat actor infiltrates a software vendor's network and stealthily employs malicious code to compromise the software before the vendor sends it to their customers. The reality is, supply chain attacks can be difficult to detect and protect against because there are many ways threat actors can attack networks, and because vulnerabilities may be introduced during any phase of a product's life cycle.

To help software vendors and customers defend against these attacks, CISA and the National Institute of Standards and Technology (NIST) jointly released a new resource: Defending Against Software Supply Chain Attacks. This interagency resource provides an overview of software supply chain risks, recommendations, and guidance on using NIST's Cyber Supply Chain Risk Management (C SCRM) framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate risks.

Download this resource to learn more: www.cisa.gov/publication/software supply chain attacks.

CISA's New *TRIPwire* Annual Report Underscores Diverse IED Threats

In 2020, there were 2,061 total bomb threat, suspicious package and device related incidents. A confluence of factors, including civil unrest, the COVID 19 pandemic, the re emergence of conspiracy theories about government actions in domestic violent extremism (DVE) circles, and a surge in anti government sentiment, led to a substantial increase in DVE attacks, plots, and messaging.

Those are just two of the main findings from CISA Office for Bombing Prevention (OBP)'s *TRIPwire* 2020 Domestic Open Source Intelligence (OSINT) Improvised Explosive Device (IED) Report.

The annual report provides data insights about each of the 10 Federal Regions during 2020 related to explosive, bomb making material, IED incidents, and notable tactics, techniques, and procedures. The report's analysis supports intelligence and law enforcement partners, public safety officers, and many other security and emergency services professionals across the Federal, State, local, and tribal government sectors of the United States.

Some of the report's other key findings include:

- The COVID 19 pandemic spurred a substantial decline in the number of reported bomb threats and suspicious packages, likely driving the 48.9% decline from 2019.
- There were 974 device related incidents in 2020, a 23.9% increase compared to 2019. An “incident” refers to a device that functioned, was emplaced or discovered, and to bomb making material that was found.
- The number of reported suspicious packages declined 48.8% in 2020 from 2019.
- Compared to prior years, 2020 saw a rise in attempted and successful attacks on law enforcement personnel and property.

For the report, OBP derived its data from open source reporting by news outlets, social media, and other multimedia channels related to explosive activity. To learn more, visit https://tripwire.dhs.gov/

CISA Releases New Insights on Critical Infrastructure Doxing

Last month, CISA published the *CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure*. CISA developed this product to bring awareness to the impacts of doxing to critical infrastructure and to share guidance and resources with critical infrastructure owners and operators, security professionals, and the general public.

Organizations are using online spaces now more than ever to conduct business operations. While critical, the increased use of online spaces also heightens concerns over the risk of doxing the act of gathering an individual’s personally identifiable information (PII), or an organization’s sensitive information, from open source material and publishing it online for malicious purposes. Threat actors may target critical infrastructure organizations and personnel with doxing attacks as a result of grievances related to organizational activities or policies. Incidents of doxing that target personnel and facilities often serve to harass, intimidate, or inflict financial damages, and can potentially escalate to physical violence.

CISA encourages individuals and organizations to take an active role in protecting themselves by controlling the information that is shared and stored online and implementing a series of best practices. For more information and to access the product, visit cisa.gov/insights. For questions, please email central@cisa.gov.

CISA Launches School Safety Series

To address new and emerging threats facing the K 12 academic community, CISA recently launched the *2021 School Safety Webinar Series*. Hosted in coordination with the Federal School Safety Clearinghouse, the monthly program covers school safety topics ranging from targeted violence and cybersecurity best practices to funding and grant opportunities for states, districts, and school communities.

Each session features leaders and subject matter experts from across the Federal government who share insights and information on critical school security threats and risks, and the resources available to combat them. Webinars are open to all members of the academic community and there is no cost to attend.

For more information on upcoming school safety webinars, please visit https://www.schoolsafety.gov/opportunities, or email SchoolSafety@hq.dhs.gov.

Social Media

Help CISA spread the word about upcoming events and new resources by sharing the following posts via your social media channels. Thank you for your support!

- Check out the new guidance from @CISAgov on protecting information from doxing: https://www.cisa.gov/publication/mitigating-impacts-doxing-critical-infrastructure
- Want to learn more about securing 5G infrastructure from cybersecurity risks? @CISAgov has the resources you need: www.cisa.gov/5G
- Save the date! @CISAgov will be hosting the virtual 2021 Chemical Security Seminars on December 1, 8, and 15, 2021, from 11 am to 3 pm ET (8 am to noon PT).