Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 19 — Issue 15 | May 9, 2019

Recognizing Arson With a Nexus to Terrorism

The alleged shooter in the Poway, California, synagogue shooting last month has also been charged with arson in connection to a fire set at an Escondido mosque in March. The arsonist left graffiti referencing the recent New Zealand mosque shootings that killed 50 people.

Terrorists remain interested in arson to conduct attacks, as its use requires little to no specialized skills or training. Precursors are inexpensive, legal and readily available.

The First Responder's Toolbox "Recognizing Arson With a Nexus To Terrorism" (PDF, 424 KB), originally published in 2017 by the Joint Counterterrorism Center (JCAT), has been downgraded from For Official Use Only (FOUO) to Unclassified (U) to provide situational awareness to a broader audience.

First responders and other governmental authorities who may be involved with mitigating arson incidents can benefit from the response and investigative considerations the JCAT provides in this bulletin.

The toolbox is also publicly available at nctc.gov, as well as on the JCAT page on the Emergency Services (ES) and Intelligence Communities of Interest on the Homeland Security Information Network (HSIN), and the Special Interest Group (SIG) on FBI's Law Enforcement Enterprise Portal (LEEP).

(Source: JCAT)

Fire and police departments using paper and pencil after Ryuk attack

The Stuart, Florida, police and fire departments were offline and operating with paper and pencil for at least a week following a Ryuk ransomware attack. The city was hit on April 13, 2019, when Ryuk infected its computers and servers. It's likely a city employee fell for a phishing email.

Ransomware encrypts files on computers and networks. Cybercriminals then demand a payment, usually paid in bitcoin, in exchange for the decryption program. The FBI does not recommend paying the ransom because it does not guarantee files will be decrypted despite the promises that they will. Ultimately that decision is left to those affected

"All the data behind both the police department and the fire department's servers still exist," the chief of police said. "We were back up on the internet for a short time today...so we are moving forward, probably I would say another week or week and a half we should be back in service."

Officials would not disclose the dollar amount hackers demanded, to be paid in bitcoin. City officials refused to negotiate and the FBI is investigating. This is just the latest in a recent rash of ransomware attacks against municipalities across the country.

A key part of surviving a ransomware attack is regularly backing up all systems and data and then storing the backup off of the network. Your systems can be restored from backed-up data, with minimal data loss, if you back up regularly.

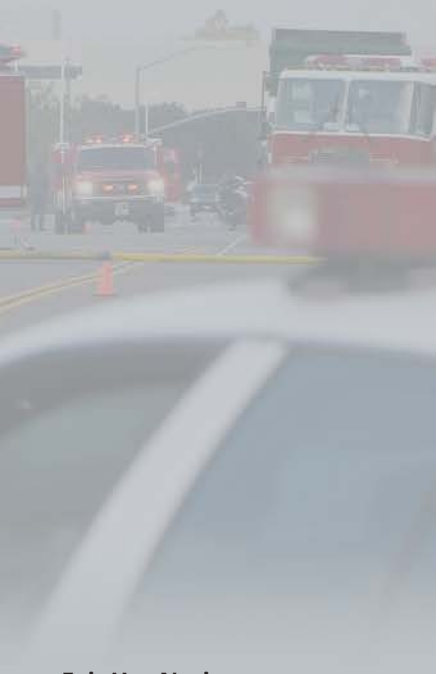
Highlights

U.S. Fire Administration

The U.S. Fire Administration operates the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC).

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.

Subscribe here



See this short article for more information on Ryuk ransomware and indicators that your systems may be infected.

(Source: CSOonline)

FEMA releases Senior Leader Toolkit

The Federal Emergency Management Agency (FEMA) National Integration Center today released the "Senior Leader Toolkit," a resource that both emergency managers and senior leaders can use to discuss roles and responsibilities during incidents.

Senior leaders and policy makers play a critical role in incident management. The particulars of the role vary widely across the nation according to local laws and authorities. Stakeholders have asked for assistance developing materials to assist their senior leaders.

FEMA understands local personnel best understand the specific roles and responsibilities within their jurisdiction. For this reason, FEMA released these documents as customizable templates so local emergency managers can revise them according to their local authorities and procedures.

The templates in the toolkit include:

- Elected Officials/Senior Executives Quick Reference Guide.
- Department Head Quick Reference Guide.
- National Incident Management System Senior Leader Briefing Template.

This toolkit can help bridge the gap between those who work primarily in the emergency management field and elected officials or senior leaders who may not be well versed with best practices in emergency management.

(Source: FEMA)

Webinars: complex coordinated attacks; securing houses of worship

The International Public Safety Association (IPSA) is offering two free webinars in May:

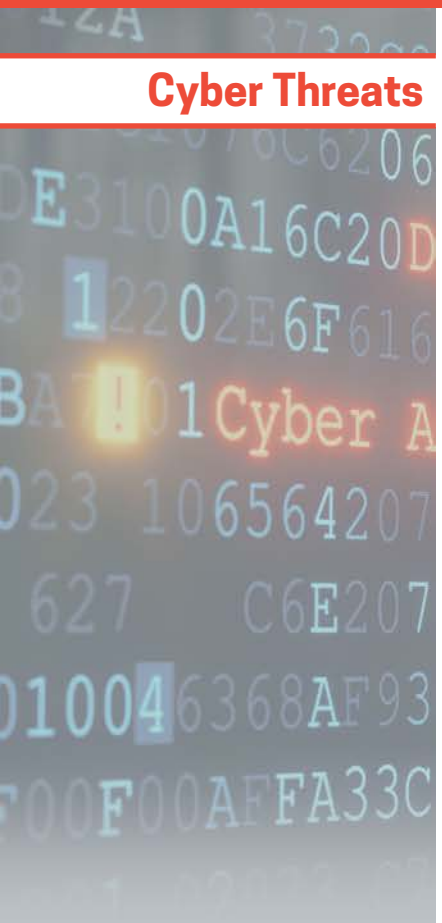
"Church Security: How to make places of worship safe without compromising the core mission," scheduled for Tuesday, May 21, 2019, from 1-2 p.m. Eastern. The instructor will cover the why and how of securing houses of worship. This webinar will cover lessons learned, tools and techniques, and how an in-house security plan can complement law enforcement response and protocols.

"Preparing First Responders for a Complex Coordinated Attack" will discuss common themes in complex coordinated attacks, preparedness challenges, domestic preparedness activities. This webinar is scheduled for Wednesday, May 22, 2019, from 1-2 p.m. Eastern.

Registration is required, see the link to each webinar for details. Participants will receive a certificate of attendance.

(Source: IPSA)

Cyber Threats



FBI: Indicators of Compromise Associated with Ryuk Ransomware

A recent FLASH report from the FBI lists signs common to a Ryuk ransomware attack (PDF, 654 KB). This is a technical document listing things to look for in the registry, file names and host based indicators.

The FBI is also requesting information from agencies, departments or companies that are victims of Ryuk ransomware. The FLASH report lists the requested details and the FBI's contact information.

(Source: FBI)

Openings available in Cybersecurity Virtual Table Top Exercises

The Emergency Management Institute (EMI) Virtual Tabletop Exercise (VTTX) program has **openings in its upcoming cybersecurity exercise scenario**. Available dates are June 11, 12, and 13, 2019 and August 27, 28, and 29, 2019. The exercises run 12-4 p.m. Eastern on each day.

The scenario will focus on increasingly complex and severe cyber threats (PDF, 360 KB), beginning with information on a potential security risk and culminating with containment, eradication and recovery from a cyber incident. Participating organizations and jurisdictions will have a choice of beginner, intermediate or advanced complexity related to one or several different threats.

To participate, send an email to Doug Kahn at douglas.kahn@fema.dhs.gov or call 301-447-7645. Also, send a courtesy copy email to the Integrated Emergency Management Branch at fema-emi-iemb@fema.dhs.gov or call 301-447-1381.

(Source: EMI VTTX)

9 types of malware and how to recognize them

People tend to play fast and loose with security terminology. However, **it's important to get your malware classifications straight** because knowing how various types of malware spread is vital to containing and removing them.

This malware refresher covers viruses; trojans; worms; hybrids and exotic forms; ransomware; fileless malware; and adware.

(Source: CSOonline)

What do tech giants know about you? This tool will tell you

Do you read online privacy policies when you join a website? With over 7.2 billion accounts held across the services studied, including platforms like Google, Facebook, Amazon, and Tinder, **how many of us are aware of the finer details of the privacy policies that we automatically accept**?

Online security platform vpnMentor has delved through the privacy policies of some of the most popular applications, creating an interactive tool that shows how these companies track our every move.

(Source: zdnet)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.