FIRSTRESPONDER'STOOLBOX

(U//FOUO) Cyber Threats to First Responders are a Persistent Concern

(U//FOUO) We assess with moderate confidence that cyber actors, including those who support violent extremism, are likely to continue targeting first responders on the World Wide Web, including by distributing personally identifiable information (PII) for the purpose of soliciting attacks from willing sympathizers in the homeland, hacking government websites, or attacking 911 phone systems to hinder first responders' ability to respond to crises.

(U) **SCOPE**: The purpose of this product is to promote general awareness of cyber tactics that might be employed against US first responders and some general considerations for first responders to harden themselves against attack.

- (U//FOUO) In January 2017, police in Washington, DC discovered multiple disruptions to their surveillance cameras as a result of ransomware infections. Hackers compromised 70% of the cameras across the city, eight days before the Presidential Inauguration, which prevented officials from accessing the command and control center of the surveillance system. The infected cameras were configured with default remote access passwords, according to FBI reporting.

- (U) In October 2016, a telephony denial of service attack to the 911 network impacted emergency call centers in at least 12 states. Several centers reported they were inundated with fake phone calls. As a result, authorities were in danger of losing service to their switches and operators had difficulty in distinguishing fake incoming calls from legitimate calls for service. Authorities arrested a US person for the cyber attack, and charged him with three counts of felony computer tampering.

- (U//FOUO) In March 2016 there were two doxing attacks in the US. In early March, the pro-ISIS Caliphate Cyber Army (CCA) posted PII of 50 police officers from New Jersey. The PII included the officers' names, home and work addresses, and phone numbers. In mid-March, prior to merging with other hacking groups to form the United Cyber Caliphate (UCC), the CCA hacking group posted a "kill list" containing the PII of 36 Minnesota police officers. According to the FBI, it is investigating threatening phone calls to law enforcement officials, possibly resulting from CCA postings.

24 JULY 2017
AUTHORED BY NCTC, DHS, FBI

(U) **POTENTIAL CYBER-ATTACK TACTICS AGAINST FIRST RESPONDERS:** With the expanding use of Internet-connected technology, first responders should be aware of existing and emerging tactics and technologies used by cyber actors with malicious intent.

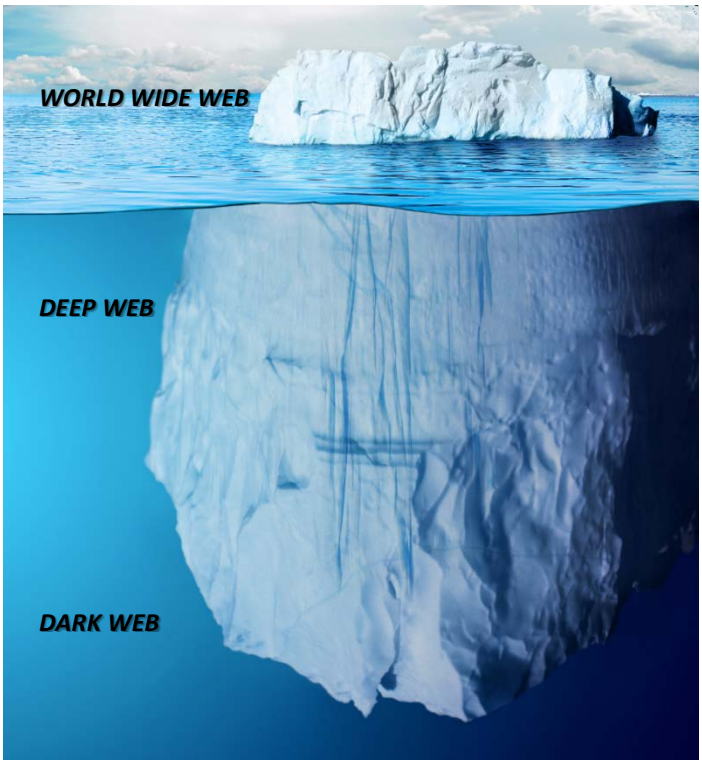
- (U) **DOXING:** The process of gathering information about a person or business using online public sources including social media profiles, reverse phone lookup, and search engines.
- (U) **RANSOMWARE:** An attack that typically propagates through one of two mechanisms: user-initiated actions such as clicking on a malicious link in a spam e-mail or on a website, or through malvertising[a] and drive-by downloads,[b] which do not require any user interaction. Clicking on links, especially in emails from unknown senders, could instigate a ransomware program which will lock and encrypt the computer until a fee is paid.
- (U) **PHISHING:** The act of scamming a user, typically through email, into surrendering private information that will be used for identity theft. These attacks tend to focus on convincing the subject to provide personal information, such as bank account numbers or social security numbers.
- (U) **SPEAR-PHISHING:** A type of phishing attack that focuses on a single user or department within an organization to obtain sensitive information such as login IDs and passwords. Spear phishing targets a department by creating an email that appears to come from the organization (for example, human resources) asking the subject to reset his or her user name and password.
- (U) **WHALING:** A type of phishing attack directed at high-level individuals or executives within a company.
- (U) **SOCIAL ENGINEERING:** The act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information which the individual does not realize will be used to attack a computer network.
- (U) **TROJAN:** A destructive program that masquerades as a benign application. These programs are typically sent as a link within an email that the sender tries to convince the subject to click on.
- (U) **DENIAL OF SERVICE (DoS):** A malicious attack on a network designed to disable the network by flooding it with useless traffic, making it unable to process legitimate traffic. Malicious actors may direct computer traffic to the subject's website to slow down or disrupt the site's ability to function.
- (U) **TELEPHONY DENIAL OF SERVICE (TDoS):** Occurs when malicious actors seek to overwhelm an agency's phone system by flooding the agency's telephone switches with repeated calls from spoofed numbers, clogging lines, and inhibiting real callers from connecting.
- (U) **DISTRIBUTED DENIAL OF SERVICE (DDoS)**: A type of DOS attack in which multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a denial of service.
- (U) **PORT SCANNING:** The act of systematically scanning a computer's ports to find a weakened access point to break into a computer. Malicious actors may use this technique to find weak access points a subject's computer uses to access the Internet. Once found, the actor will attempt to hack the computer and gain access to the subject's computer network.

[a] (U) Malvertising (malicious advertising) refers to the use of online advertising to spread malware.
[b] (U) Drive-by downloads infect computers from visiting websites running malicious code.

- (U) **ZOMBIE:** A computer that is under the control of a malicious hacker without the knowledge of the computer owner.

(U//FOUO) **POTENTIAL COUNTERMEASURES AND OTHER CONSIDERATIONS:** First responders are highly encouraged to minimize their online footprint on social media accounts, by removing or securing information to limit the release of potentially sensitive information on public-facing platforms. The following recommendations for increased online security are provided for consideration. Additionally, the information that cyber actors may glean from first responders may be used on the "Dark Web," unindexed "invisible" sections of the Internet, which enable anonymous communication. The use of the Dark Web by cyber actors may further hinder awareness that a cyber attack against a first responder has even occurred.

- (U//FOUO) Regularly perform online searches to determine what information is available about you and your family on the open Internet; however, be aware that the location from which you perform your search (for example, police or fire station) may reveal police or fire IP addresses;
- (U//FOUO) Be familiar with and set the strongest privacy controls possible on social media sites;
- (U//FOUO) Remove address, date of birth, phone number, email address, and other PII from social media profiles;
- (U//FOUO) Audit all personal and family photographs accessible on the Internet and attempt to remove, if possible;
- (U//FOUO) Search for personal and family photographs posted/tagged by "friends" and "friends of friends" on social media and remove yourself from the tag list;
- (U//FOUO) Follow strict password security protocols on all devices and online accounts; update regularly;
- (U//FOUO) Use two-factor authentication whenever possible;



(U) Per a Congressional Research Service report, the layers of the Internet go far beyond the surface content that many can easily access in their daily searches. The other content is that of the Deep Web, content that has not been indexed by traditional search engines. The furthest corners of the Deep Web, segments known as the Dark Web, contain content that has been intentionally concealed. The Dark Web may be used for legitimate purposes as well as to conceal criminal or otherwise malicious activities. It is the exploitation of the Dark Web for illegal practices that has garnered the interest of officials and policymakers.

- (U//FOUO) Monitor credit reports; consider purchasing year-round credit monitoring through trustworthy services or directly from the credit bureaus;
- (U//FOUO) Be aware of social engineering tactics and scams aimed at obtaining PII or sensitive information;
- (U//FOUO) Implement sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices; and
- (U//FOUO) Install operating system updates when they are available.

(U) **ADDITIONAL RESOURCES:**

- (U) DHS's Computer Emergency Readiness Team, also known as US-CERT, lists helpful resources describing techniques to apply when posting information on social networking websites, including:
  - (U) "Staying Safe on Social Networking Sites" (https://www.us-cert.gov/ncas/tips/ST06-003)
  - (U) "Socializing Securely: Using Social Networking Services" (https://www.us-cert.gov/security-publications/socializing-securely-using-social-networking-services)

- (U) To report suspicious activity, law enforcement, fire, EMS, private security personnel, and emergency managers should follow established departmental protocols. All other personnel should call 911 or contact local law enforcement. For more information on suspicious activity reporting, visit http://nsi.ncirc.gov/resources.aspx.

- (U) To file a complaint with the Internet Crime Complaint Center visit www.IC3.gov.

- (U) State, local, tribal and territorial governments can report cyber incidents and receive free assistance around the clock, from the Multi-State Information Sharing & Analysis Center (MS-ISAC), by contacting the Security Operations Center at 1-866-787-4722 or by e-mail at soc@msisac.org.

- (U) For additional federal resources related to cyber reporting, visit: https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

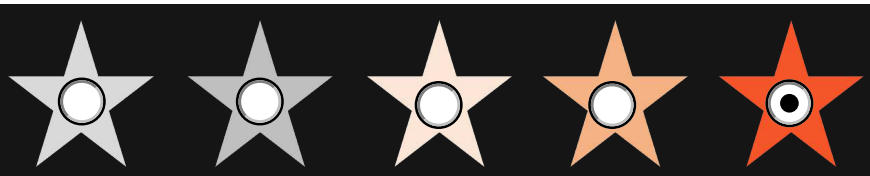
PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and/or ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: Cyber Threats to First Responders are a Persistent Concern

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS. HOW DOES JCAT MAKE PRODUCTS BETTER?

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT