25 September 2019

(U//FOUO) *A NorCal Regional Perspective: The Dark Web*

(U) Prepared by the Department of Homeland Security Intelligence Enterprise (DHS IE), Field Operations Division, Central Pacific Region.

(U//FOUO) **Scope:** This Regional Perspective (RP) highlights the accompanying Reference Aid from the DHS IE Cyber Mission Center (CYMC) that provides an overview of the dark web. This RP is intended to inform state and local law enforcement of the international criminal drug activity and domestic terrorist threats occurring on the dark web and impacting the Northern California Area of Responsibility (AOR).

(U//FOUO) The dark web is a portion of the internet that provides anonymity for a range of licit and illicit activities, requiring specialized software to access, and employing multi-layer encryption, rendering it nearly impossible to trace activity back to its originator. The dark web hosts criminal marketplaces that offer tools and services to commit cybercrime and facilitate the purchase of illicit items such as drugs, weapons, counterfeit identification, personally identifiable information, and illegal pornography. Cyber actors worldwide continue to utilize the dark web to conduct illicit activities, some of which occurs within the Northern California AOR according to Department of Justice arrests and DHS open source reporting.

- (U//FOUO) On August 6, 2018, a social media user posted a hyperlink to the social media account of an Antifascist (Antifa) group active in Berkeley, California that was discussing the white supremacist extremist* presence at a rally, according to DHS open source reporting. The link resolved to a text storage website on the dark web containing a message titled, "Berkeley, Philadelphia Antifa" that threatened violence against a list of alleged Antifa members.[1]

- (U) On 26 January 2018, a formerly San Francisco-based USPER was sentenced to five years and 10 months in prison for drug trafficking on the dark web marketplace AlphaBay.[2] The USPER was a large-scale heroin, fentanyl, and methamphetamine distributor who received orders on AlphaBay, mailed the narcotics from a post office in San Francisco to customers throughout the United States, and then received payments in Bitcoin, according to court documents.[3]

- (U) On 15 March 2017, a grand jury in the Northern District of California indicted two Russian Federal Security Service (FSB) officers who allegedly utilized the dark web to contact and direct criminal hackers to steal Yahoo, Google, and other webmail credentials of specific targets, including Russian journalists and Russian and U.S. Government officials, according to court documents.[4][5]

- (U) On 29 May 2015, a UPSER from San Francisco, California was sentenced to life imprisonment for owning and operating Silk Road, the first large scale dark web criminal marketplace. The marketplace enabled thousands of drug dealers to sell narcotics worldwide, facilitated money laundering operations, and offered computer hacking services until it was shut down by law enforcement in 2013.[6]

(U//FOUO) Featured Product: DHS, Reference Aid, **(U)** ***"The Dark Web,"*** dated 20 June 2019.

* (U//FOUO) DHS defines White Supremacist Extremists as groups or individuals who facilitate or engage in acts of unlawful violence directed at the federal government, ethnic minorities, or Jewish persons in support of their belief that Caucasians are intellectually and morally superior to other races and their perception that the government is controlled by Jewish persons.

[1] (U//FOUO); DHS; OSIR-04001-1086-18; 8 AUG 2018; DOI 8 AUG 2018; (U//FOUO); Post-rally threat of stalking and violence against antifascist protesters in CA and PA posted to Dark Web.; Extracted information is U//FOUO; Overall document classification is U//FOUO.
[2] (U); DOJ; Press Release; "Dark-Web Drug Traffickers Sentenced in Separate Cases to 80 Months and 70 Months in Prison"; 16 JAN 2018; https://www.justice.gov/usao-edca/pr/dark-web-drug-traffickers-sentenced-separate-cases-80-months-and-70-months-prison; accessed on 19 JUN 2019.
[3] (U); DOJ; Press Release; "Trafficker Of Fentanyl, Heroin, And Methamphetamine On Dark Web Marketplace Alphabay Pleads Guilty To Drug Distribution Charge"; 16 OCT 2017; https://www.justice.gov/usao-edca/pr/trafficker-fentanyl-heroin-and-methamphetamine-dark-web-marketplace-alphabay-pleads ; accessed on 19 JUN 2019.
[4] (U); DOJ; Press Release; "Canadian Hacker Who Conspired With And Aided Russian FSB Officers Pleads Guilty"; 28 November 2017; https://www.justice.gov/usao-ndca/pr/canadian-hacker-who-conspired-and-aided-russian-fsb-officers-pleads-guilty; accessed on 12 SEP 2019.
[5] (U); DOJ; Press Release; "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts"; 15 March 2017; https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions; accessed on 12 SEP 2019.
[6] (U); DOJ; Press Release; Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison; 29 May 2015; https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison; accessed on 13 August 2019.

INTELLIGENCE ENTERPRISE

REFERENCE AID

Homeland Security

20 June 2019

(U) Cyber Mission Center

(U) The Dark Web

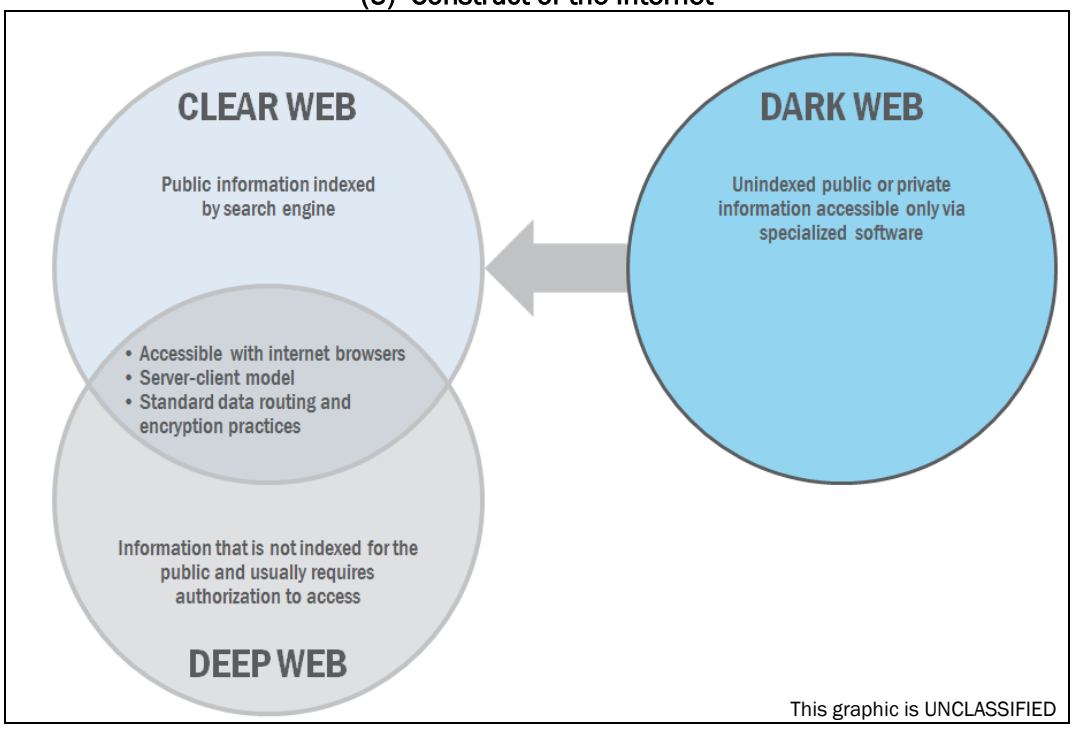
(U//FOUO) Scope. This *Reference Aid* provides an overview of the dark web, a portion of the internet that provides anonymity for a range of licit and illicit activities and individuals—including platforms for privacy rights activists and individuals living in countries with strict censorship laws, as well as venues for criminals and malicious cyber actors seeking to conduct illegal activity. The information cutoff date for this *Reference Aid* is 29 January 2019.

(U//FOUO) Prepared by the DHS Intelligence Enterprise (DHS IE) Cyber Mission Center (CYMC). Coordinated with CBP, CWMD, FEMA, ICE, NCCIC, S&T, TSA, USCG, USSS, CIA, DIA, Department of Energy, Department of State, Department of the Treasury, FBI, NASIC, NGA, NIC, and NSA.

(U) Executive Summary

(U) The internet is a network of networks that extends far beyond what we can access with a search engine. This *Reference Aid* explains the difference between the clear, deep, and dark webs, and provides insight into how the dark web operates and what it is used for.

(U) Construct of the Internet



(U) Accessing the Dark Web

(U) The dark web requires specialized anonymization software to access, such as Tor or Invisible Internet Project .[a] Tor uses multi-layer encryption to route internet traffic through randomly generated nodes—decrypting traffic one layer at a time at each node—making it nearly impossible for activity to be traced back to the originator.[1,2]

(U) Dark Web Purpose and Content

(U) The dark web is used to anonymously obtain the following items.

(U) Dark Web Service	(U) Explanation	(U) Example
(U) Drugs	» (U) Make up a large portion of illicit online transactions. » (U) Vendors reviewed and rated.	(U) A dark web drug vendor in October 2018 was arrested and $400,000 of cocaine confiscated.[3]
(U) Weapons	» (U) Commonly available. » (U) Used by people who cannot obtain weapons legally or who want to make anonymous weapons purchases.	(U) DHS agents in September 2018 intercepted a 9mm pistol, suppressor, and 150 rounds of ammunition that had been purchased by a man in Scotland from a vendor in the United States.[4]
(U) Counterfeit Identification	» (U) Widely available. » (U) Passports, driver's licenses, and other identification.	(U) Counterfeit US passports sell for $1,000-2,000.[5]
(U) Personally Identifiable Information (PII)	» (U) Social security numbers. » (U) Names/addresses. » (U) Health records. » (U) Used to steal identities to commit fraud.	(U) PII is used to fraudulently file tax returns; the money is routed to the criminals rather than the victims. Even infants have been victims of identity theft.[6,7]
(U) Illegal Pornography	» (U) Specialized forums cater exclusively to child pornography. » (U) Other obscene material is also available.	(U) The FBI in 2017, along with international law enforcement partners, arrested more than 900 suspects who were using a dark web child pornography forum called Playpen.[8]

[a] (U) Tor is derived from an acronym for the original software project name, "The Onion Router."

(U) Dark Web Cyber-Specific Criminal Services

(U) Some criminal marketplaces sell tools and services specifically used to commit cybercrimes.

(U) Dark Web Service	(U) Explanation	(U) Example
(U) Malware-as-a-Service	» (U) Criminals license the use of malware and receive support. » (U) Allows low-tech criminals to conduct cyber attacks without investing in the development of malware.	(U) Especially popular for criminals operating ransomware; ransomware-as-a-service platforms are available for as low as $39.[9]
(U) Hacking for Hire	» (U) Criminal marketplaces function like bulletin boards for hacking jobs. » (U) Typical jobs include compromising a website or stealing account credentials.	(U) Hacking-for-hire sites also exist on the clear web.[10]
(U) Botnets	» (U) Used for spam, scanning, and DDoS attacks. » (U) A DDoS attack with a botnet of 1,000 workstations averages $25 an hour.[11]	(U) Necurs is a multifunctional botnet available for rent in underground markets.[12] It has been used to distribute Dridex and TrickBot, as well as ransomware, including Locky, Scarab and Jaff, via spam e-mail messages that can number in the tens of millions per day.[13]
(U) Crypting[b]	» (U) Customized obfuscation service that encrypts, encodes, and otherwise obfuscates code so that it can evade detection by antivirus programs.	(U) The website reFUD[.]me allows users to upload files to determine if the files are detectable by antivirus software.[14]

(U//FOUO) State-Sponsored Actors and the Dark Web

(U) In addition to cybercriminals, nation-state actors use the dark web to conduct cyber operations.

(U) Dark Web Service	(U) Explanation	(U) Example
(U) Nation-State/Criminal Cooperation	» (U) Nation-states direct criminal elements to act on their behalf. » (U) Dissociates the government from the attack to create plausible deniability.	(U) The US Department of Justice in 2017 indicted two Russian Federal Security Service (FSB) officers, alleging that they "protected, directed, facilitated, and paid criminal hackers to collect information through computer intrusions in the United States and elsewhere."[15]

[b] (U) Crypting is scrambling the binaries of files so they cannot be easily detected by antivirus software.

(U) Obtaining Malware	» (U) State-sponsored cyber actors use malware available on dark web environments as-is, or modify it as needed. » (U) Provides a solution without the need to create a new tool. » (U) Disguises the source of the attack.	(U) Russian Government actors modified the Petya ransomware and used it to destroy thousands of machines in Ukraine and elsewhere.[16,17]

(U) Reporting Computer Security Incidents
(U) To report a computer security incident, either contact NCCIC at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the NCCIC Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) Tracked by: HSEC-1.1, HSEC-1.2, HSEC-1.5, HSEC-1.8

[1] (U); VPNmentor: "The Ultimate Guide to Tor Browser (with Important Tips)"; 2019"; http://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/; accessed on 21 MAY 2019.
[2] (U); Digital Citizenship and Surveillance Society; "Invisible Internet Project (I2P); 19 NOV 2015; https://dcssproject.net/i2p/; accessed on 22 MAY 2019.
[3] (U); Nulltx; "UK Darknet Vendor has Nearly $400,000 in Cocaine Seized During Raid"; 19 OCT 2018; https://nulltx.com/uk-darknet-vendor-has-nearly-400000-in-cocaine-seized-during-raid; accessed on 14 FEB 2019.
[4] (U); DeepDotWeb; "Software Engineer Sentenced to Five Years After Ordering a Gun Over the Dark Web"; 28 JAN 2019; https://www.deepdotweb.com/2019/01/28/software-engineer-sentenced-to-five-years-after-ordering-a-gun-over-the-dark-web; accessed on 14 FEB 2019.
[5] (U); Darknetmarkets.co; "Counterfeit Passports Selling Cheaper on the Darknet, but Buyer Beware"; 08 JUN 2017; https://darknetmarkets.co/counterfeit-passports-selling-cheaper-on-the-darknet-but-buyer-beware; accessed on 14 FEB 2019.
[6] (U); Symantec; "Tax Fraud: What You Need to Know"; 2017; https://www.lifelock.com/learn-fraud-tax-fraud.html; accessed on 22 MAY 2019.
[7] (U); CNN; "Infant Social Security numbers are for sale on the dark web"; 22 JAN 2018; https://money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html; accessed on 14 FEB 2019. IRS;
[8] (U); FBI; "'Playpen' Creator Sentenced to 30 Years"; 05 MAY 2017; https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years; accessed on 14 FEB 2019.
[9] (U); NakedSecurity; "5 ransomware as a service (RaaS) kits – SophosLabs investigates"; 13 DEC 2017; https://nakedsecurity.sophos.com/2017/12/13/5-ransomware-as-a-service-raas-kits-sophoslabs-investigates; accessed on 14 FEB 2019.
[10] (U); HireAnHacker; "#1 Best place to Hire Hackers"; 2019; https://hireanhacker.com; accessed on 14 FEB 2019.
[11] (U); Security Affairs; "How Much Cost a DDoS Attack Service?"; 26 MAR 2017; https://www.securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html; accessed on 29 APR 2019.
[12] (U); AppRiver; "Necurs Botnet Launching Massive Ransomware Attacks"; 29 DEC 2017; https://blog.appriver.com/2017/12/necurs-botnet-massive-ransomware-attacks; accessed on 14 FEB 2019.
[13] (U); Infosecurity Magazine; "Necurs Fuels Massive Valentine's Day Spam Campaign"; 12 FEB 2018; https://www.infosecurity-magazine.com/news/necurs-fuels-massive-valentines; accessed on 14 FEB 2019.
[14] (U); BleepingComputer; "Man Admits to Creating Crypting Service Cryptex and reFUD.me Scanner"; 16 JAN 2019; https://bleepingcomputer.com/news/security/man-admits-to-creating-crypting-service-cryptex-and-refudme-scanner/; accessed on 15 FEB 2019.
[15] (U); DOJ; "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts"; 15 MAR 2017; https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions; accessed on 14 FEB 2019.
[16] (U); DHS; "Alert (TA17-181A)"; 01 JUL 2017; https://www.us-cert.gov/ncas/alerts/TA17-181A; accessed on 14 FEB 2019.
[17] (U); White House; "Statement from the Press Secretary"; 15 FEB 2018; https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/; accessed on 14 FEB 2019.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U) The Dark Web

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- ☐ Drive planning and preparedness efforts, training, and/or emergency response operations
- ☐ Observe, identify, and/or disrupt threats
- ☐ Share with partners
- ☐ Allocate resources (e.g. equipment and personnel)
- ☐ Reprioritize organizational focus
- ☐ Author or adjust policies and guidelines
- ☐ Initiate a law enforcement investigation
- ☐ Intiate your own regional-specific analysis
- ☐ Intiate your own topic-specific analysis
- ☐ Develop long-term homeland security strategies
- ☐ Do not plan to use
- ☐ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name: *Position:*
Organization: *State:*
Contact Number: *Email:*

Submit Feedback

Privacy Act Statement