Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources[1]

Version 1.0 (February 2020)

I. Introduction

The Cybersecurity Unit (CsU) prepared this document in response to questions posed by private organizations about the legality of specific cybersecurity measures.[2] It includes contributions from other components of the Department of Justice, such as the National Security Division, and other federal agencies.[3] Consistent with the CsU's mission, this document is intended to help organizations adopt effective cybersecurity practices and to conduct them in a lawful manner.

This document focuses on information security practitioners' cyber threat intelligence-gathering efforts that involve online forums in which computer crimes are discussed and planned and stolen data is bought and sold. It also contemplates situations in which private actors attempt to purchase malware, security vulnerabilities, or their own stolen data—or stolen data belonging to others with the data owners' authorization—in Dark Markets.[4] It is not, however, intended to

[1] This document confers no rights or remedies and does not have the force of law. *See United States v. Caceres*, 440 U.S. 741, 752-753 (1979). This document is also not intended to have any regulatory effect.

[2] This document focuses on activities conducted by private actors. Additional legal and policy issues not addressed in this document may arise when government actors engage in the activities discussed herein. Government actors should consult agency or department counsel or contact the CsU for advice regarding their activities.

[3] The Department of Justice's Federal Bureau of Investigation (FBI), the Department of Homeland Security's United States Secret Service (U.S. Secret Service), and the Treasury Department's Office of Foreign Asset Control (OFAC) provided valuable input to this paper.

[4] Dark Markets are found on the TOR ("the Onion Router") network, which is a collection of computers designed to obfuscate the origin of online communications. The TOR network encrypts and routes communications through a series of relays around the world to thwart efforts to trace their origin. TOR hidden services, also called the "Dark Web," are sites that may only be accessed using a TOR browser. Because the location of sites operating as TOR hidden services is concealed and difficult to trace, TOR hidden services are a preferred technique for hosting sites associated with illegal activities.

cover intelligence or evidence gathering involving other types of criminal forums, such as forums that traffic in child pornography[5] or illicit drugs.

The scenarios referenced in this document are derived from practices that the CsU's private sector outreach and engagement suggest are commonly used by the cybersecurity community to gather intelligence, retrieve stolen data, and obtain malware samples and security vulnerabilities. The legal concerns discussed herein are likely to arise when information security practitioners engage in those activities. While this document is intended to provide assistance in identifying potential legal issues, it does not—and cannot—comprehensively address all the legal issues that practitioners may face in every circumstance, particularly because minor changes in facts can substantially alter the legal analysis. Accordingly, we strongly recommend that consumers of this document consult with legal counsel to make proper use of its recommendations and analysis.[6]

Two Rules to Always Follow

1. Don't Become a Perpetrator: Some of the activities discussed in this document implicate federal criminal law and may violate State law and/or create civil liability. Organizations anticipating they will engage in those activities should consult with their legal counsel to assess the legality of planned activities. It may also be beneficial in some circumstances to cultivate a relationship with local FBI and U.S. Secret Service field offices if contemplating these types of operations. Contact information is provided at the end of this document.

2. Don't Become a Victim: The cybersecurity activities discussed in this document may involve interacting with sophisticated criminal actors. They should not be undertaken without a deliberate assessment of risk. An organization planning to engage in these activities should remain vigilant, institute appropriate security safeguards, and adhere to cybersecurity practices that will minimize the risk that it will be victimized.

The legal discussion in this document is limited to U.S. federal criminal law. It does not focus on civil liability, state law, or the law of countries other than the United States, nor does it cover potential regulatory restrictions.

II. Scenario Assumptions

The scenarios discussed below are premised on the activities of private sector information security practitioners who gather information from Dark Market forums as part of their cybersecurity activities. They are based upon legally significant assumptions about the way practitioners conduct their activities and the practitioners' intent.

[5] The legal analysis for gathering information from forums that traffic in child pornography or related illegal activities would likely differ from the analysis provided here, because it is illegal to use the Internet or cell phones to knowingly advertise, distribute, receive, or possess child pornography, or to access it intentionally. *See* 18 U.S.C. §§ 2251, 2252, and 2252A. Therefore, conducting intelligence gathering and other operations on those forums would involve different legal considerations.

[6] This document can serve as a starting point for a security practitioner's discussion with his or her organization's legal counsel. Fact-specific application of the considerations highlighted in this document will allow an organization to tailor its plans to fit its individualized assessments of legal benefits and risks before proceeding.

Tips on Lawfully Collecting Intelligence in Online Forums

- Passively Collecting Intelligence Typically Is Not Illegal: Doing nothing more than passively gathering information from an online forum, even one on which criminal conduct related to computer crime is conducted, is unlikely to constitute a federal crime, particularly when done without any criminal intent. However, accessing such a forum without authorization or surreptitiously intercepting communications occurring on that forum could raise legal concerns under the Computer Fraud and Abuse Act (18 U.S.C. §1030) (CFAA) and the Wiretap Act (18 U.S.C. § 2511).

- Access Forums Lawfully: Accessing a forum in an unauthorized manner, such as by exploiting a vulnerability or by using stolen credentials, can implicate the CFAA and statutes like the Access Device Fraud statute (18 U.S.C. § 1029).

- Do Not Assume Someone Else's Identity without Consent: Using a fake online identity to gain access to or participate in a forum where criminal conduct is occurring, standing alone, is typically not a violation of federal criminal law. However, assuming the identity of an actual person without his or her permission rather than manufacturing a false persona can cause legal problems.

A. Security Practitioners

This document focuses on private sector information security practitioners who obtain information (i.e., cyber threat intelligence, stolen data, security vulnerabilities, and malware) from Dark Markets where tools and services associated with the commission of computer crimes are bought and sold and stolen data is available for purchase. It assumes these activities are conducted within the jurisdiction of United States and in a manner that renders them subject to U.S. federal criminal law.[7] It also assumes the practitioners obtain information solely so that it can be used and shared for legitimate cybersecurity purposes (e.g., to help others identify and defend against cybersecurity threats) and with no criminal or malicious intent or motive.

Practitioners engaged in these types of online activities frequently use pseudonyms and fabricated identities while operating on forums for security and personal safety reasons. As discussed below, fake identities should be entirely fabricated and not involve assuming the identity of actual people without their authorization. Fabricated online identities should also not involve falsely

[7] The application of federal criminal law to activities occurring online can be complicated. Some cybercrime statutes have broad jurisdictional reach: for example, the Computer Fraud and Abuse Act (CFAA) covers cyber attacks and intrusions against computers that are used in or affect interstate or foreign commerce and communications, even when the targeted computers are outside the United States. *See* 18 U.S.C. § 1030(e)(2)(B). Other criminal prohibitions have more limited reach and many have no extraterritorial application at all. *See, e.g.*, *European Cmty. v. RJR Nabisco, Inc.*, 764 F.3d 129, 141 (2d Cir. 2014), *rev'd on other grounds*, 136 S.Ct. 2090 (quoting *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 264 (2010)) (Second Circuit holding that 18 U.S. § 1343 (the wire fraud statute) does not apply to wholly extraterritorial activity). The issue of applicability of federal criminal law to online conduct is unavoidably fact-dependent and requires a statute-specific analysis. For the most part, the scenarios in this document presume federal jurisdiction and that the federal criminal law being discussed extends itself to the facts being considered. It does not, however, address whether the activity may implicate the law of other countries, such as locations where forums may be hosted, which may be implicated by the activities.

claiming to be someone with any special status, such as a government official.[8]

B. The Forums

The forums on which cybersecurity practitioners gather cyber threat intelligence vary. Most are found on the Dark Web on sites accessible through the TOR network as hidden services.[9] Some of these Dark Market forums are invitation-only sites known in information security circles for being used to obtain illegal services and purchase stolen financial and personal data. Others are openly accessible on the Dark Web, relying on the anonymity furnished by TOR to shield their operators. The discussion threads in some of these forums include topics of general interest related to coding and malware; however, the sites of greatest interest to security practitioners openly advertise illegal services and the sale of stolen credit card numbers, compromised passwords, and other sensitive information.[10]

C. Accessing the Forums

The manner in which a forum is accessed can be legally material. Accessing forums using legitimate credentials provided by forum operators is the best way of avoiding legal issues concerning the means of access. Gaining access to forums using unauthorized means could violate federal criminal law. For instance, using stolen credentials to access the forum could constitute a violation of, *inter alia*, the CFAA.[11] Also, using an exploit or other technique to access and gather information from a server or system on which the forum operates rather than through intended (and therefore authorized) means could violate the CFAA and possibly other federal criminal statutes that govern electronic surveillance.[12] Accessing forums contrary to a forum's policies may likewise raise legal issues about lawful access under the CFAA.[13]

Forums operated by criminal actors may require proof that someone seeking access to the forum has bona fide criminal intent. For instance, the forum operator may require the purchase

---

[8] *See infra* p. 6 and note 17.

[9] *See supra* p. 1 and note 4.

[10] As noted at the outset, this paper does not address sites that traffic in or otherwise involve child pornography. *See supra* p. 2.

[11] *See United States v. Nosal*, 930 F.Supp.2d 1051, 1061 (N.D.Ca 2013) (unauthorized use of other employee's passwords supported charges under 18 U.S.C. § 1030(a)(4)); *Global Policy Partners, LLC v. Yessin*, 686 F.Supp.2d 631 (E.D.Va 2009) (a husband's access to wife's email account using her password without permission was a violation of section 1030). Also, the CFAA may be implicated if the forum administrators levy specific requirements that must be met for authorized access to the forum.

[12] For instance, if electronic communications were intercepted without the communicants' consent using a surreptitiously installed "sniffer" or similar program installed on the host server, the Wiretap Act (18 U.S.C. § 2511 *et seq*.) could apply. Such activities could also violate other laws and the privacy of innocent parties whose web sites share space on the same server.

[13] Accessing an online site contrary to its access policies can raise questions about the lawfulness of such access. *Compare hiQ Labs, Inc. v. LinkedIn Corp*., 938 F.3d 985 (9th Cir. 2019) (holding web scraping of publicly accessible web site was not violation of CFAA where there was no circumvention of access permissions) *with Konop v. Hawaiian Airline, Inc*., 302 F.3d 868, 876 (9th Cir. 2002) (discussing in dicta potential for web site access restrictions to affect lawful access).

Best Practices I

- Create "Rules of Engagement": If your organization conducts activities described in this document, or is planning to do so, it should prepare "rules of engagement" or a "compliance program" with protocols that outline acceptable conduct for its personnel and contractors who interact with criminals and criminal organizations. Following deliberately crafted protocols that weigh legal, security, and operational considerations beforehand will discourage rash decisions that could put an organization, its employees, and its data in jeopardy. Having documented rules may also prove useful if the organization ever faces criminal, civil, or regulatory action.

- Be Prepared To Be Investigated: In situations covered by this document, federal investigators may be unable to readily distinguish between criminals and innocent parties engaged in intelligence gathering. Consequently, it is possible that individuals engaged in legitimate cybersecurity may become the subject of a criminal investigation. Therefore, it may be beneficial to build an ongoing relationship with the local FBI field office or Cyber Task Force and the local U.S. Secret Service Electronic Crimes Task Force. Having trusted lines of communication established in advance can avoid misunderstandings about intelligence-gathering activities.

- Practice Good Cybersecurity: In the situations discussed in this document, information is exchanged with cyber criminals. There is no such thing as being "too suspicious" in those circumstances. Practice good cybersecurity at all times and use systems that are not connected to your company network and are properly secured when communicating with cyber criminals.

or delivery of malware or stolen personal information. As explained below, complying with such requests may place a practitioner in legal jeopardy.[14]

The way intelligence is gathered after accessing a forum can also raise legal questions. As discussed further below, collecting information using screen captures and other commonly used methods of memorializing online information that do not bypass security features of the site or access information in an unauthorized manner may avoid potential violations of law.

III. Cyber Threat Intelligence Gathering

Using cyber threat intelligence to prepare for or respond to cyber incidents can mitigate the impact of malicious cyber incidents, or in some cases even prevent them altogether. Timely, accurate threat intelligence can protect an organization and its customers from known cybersecurity threats and vulnerabilities. As the CsU has learned during its outreach about active defense to industry, many cybersecurity organizations consider gathering cyber threat intelligence to be among the most fruitful of cybersecurity activities.[15]

Private sector organizations that disseminate cyber threat intelligence gather it from multiple sources, including in some cases from online forums and other communication channels where illegal activities are planned and malware used to commit illegal acts and stolen data are sold. Information gleaned from those sources can be a rich source of cyber threat intelligence and network defense information

[14] *See infra* pp. 7-9.
[15] *See* CSIS/DOJ Active Cyber Defense Experts Roundtable (March 10, 2015), available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/05/18/CSIS%20Roundtable%205-18-15.pdf

about past, current, or future cyber attacks or intrusions; malware samples; criminals' tactics, tools, and procedures that are in current use or under development; and aliases and identities of individuals engaged in attacks and intrusions. But when private parties join or participate in these online forums to collect information for lawful purposes, the line between gathering threat intelligence and engaging in criminal activity can be hard to discern. The following discussion of different scenarios are intended to help organizations plan to conduct their intelligence gathering activities in a manner that reduces the potential of violating federal criminal law.

A. Scenario 1: "Lurking" in Forums to Gather Cyber Threat Intelligence

If a practitioner reads and collects communications posted openly on the forums but does not respond to forum communications or otherwise communicate with others on or through the forums, there is practically no risk of federal criminal liability. Standing alone, posing as a fictitious person or using a pseudonym to gain entry to and communicate on the forums does not violate federal criminal law, so long as that conduct is not a means of committing fraud or other crimes and access is gained in an authorized manner.[16] That said, assuming the identity of an actual person without permission could prove legally problematic. Depending upon the actual person being impersonated and the actions taken under the assumed identity, a practitioner could face criminal and civil legal action.[17]

B. Scenario 2: Posing Questions on Criminal Forums

If a practitioner decides to more aggressively gather intelligence by posting inquiries on the forum seeking information about illegal activities, the practitioner's actions will increase the risk of becoming the subject of a criminal investigation. While asking general questions poses only marginal legal risk, that risk increases substantially if a practitioner's postings appear to solicit the commission of a crime. Soliciting or inducing the commission of a computer crime can expose a practitioner to criminal liability.[18]

If a practitioner does not intend to use information obtained on a forum to commit a federal criminal violation, asking questions and soliciting advice on the forum is unlikely to constitute a crime. However, law enforcement investigates forums where criminal activity is taking place and asking questions and soliciting advice about criminal conduct is an indication that a crime may be occurring. Consequently, there is a possibility that the practitioner's inquiries and exchanges with others on the forum that appear to involve discussions of criminal conduct could implicate the practitioner in a criminal investigation of the forum or its members.

---

[16] *See supra* Section II.C.

[17] For example, the impersonation of an officer or employee of the United States is a violation of federal criminal law. *See* 18 U.S.C. § 912. Some states have also created civil causes of action for online impersonation. *See, e.g.*, WA ST 4.24.790 (June 7, 2012) (Washington State statute for "electronic impersonation—Action for invasion of privacy).

[18] The crime of solicitation involves seeking another person to engage in a specified criminal act. *See, e.g.*, Cal. Penal Code § 653(f) (West 2016). There are few federal solicitation statutes that could apply to solicitation of activity that could constitute a computer crime. *See, e.g.*, 18 U.S.C. § 2512(1)(c) (advertising of unlawful electronic interception device). There are, however, many state solicitation statutes that might apply if the relevant conduct occurs within the jurisdiction of that state. In addition, a solicitation could lead to aiding and abetting a federal crime or conspiracy to commit a federal crime. *See, e,g.,* 18 U.S,C. §§ 2(a), 371.

This could subject the practitioner to investigative scrutiny. Practitioners and organizations can take steps to mitigate that risk, though.

For instance, they can document their operational plans for conducting cyber threat intelligence gathering and keep records of their online activities and how information was gathered and used. In the event of a criminal investigation, such records may help establish that their conduct was legitimate cybersecurity activity and help law enforcement determine that a practitioner's actions were executed in furtherance of the company's legitimate cybersecurity operations, as opposed to the actions of a rogue employee engaged in illegal conduct.

An organization should also establish policies and protocols that have been vetted with its legal counsel to guide its employees' and contractors' activities on forums (and anywhere else).[19] Having vetted "rules of engagement" or a "compliance program" can help prevent personnel from accidentally or unintentionally put their organization and its employees in legal jeopardy or risk compromising its security. It may also be beneficial to inform law enforcement before engaging in these intelligence-gathering activities by building an ongoing relationship with the local FBI field office or Cyber Task Force and the local U.S. Secret Service field office or Electronic Crimes Task Force. Early engagement with law enforcement may also help ensure that a practitioner's activities do not unintentionally interfere with an ongoing or anticipated investigation by law enforcement. Contact information is provided at the end of this document.

C. Scenario 3: Exchanging Information with Others on the Forum

If a practitioner becomes an active member of a forum and exchanges information and communicates directly with other forum members, the practitioner can quickly become enmeshed in illegal conduct, if not careful. It may be easier for an undercover practitioner to extract information from sources on the forum who have learned to trust the practitioner's persona, but developing trust and establishing bona fides as a fellow criminal may involve offering useful information, services, or tools that can be used to commit crimes. Engaging in such activities may well result in violating federal criminal law.

Whether a crime has occurred usually hinges on an individual's actions and intent. A practitioner must avoid doing anything that furthers the criminal objectives of others on the forums. Even though the practitioner has no intention of committing a crime, assisting others engaged in criminal conduct can constitute the federal offense of aiding and abetting.[20] An individual may be found liable for aiding and abetting a federal offense if her or she takes an affirmative act—even an act that is lawful on its own—that is in furtherance of the crime and conducted with the intent of facilitating the crime's commission.[21] Actively participating in a

---

[19] Such policies and procedures—sometimes called rules of engagement or a compliance program—may give direction on topics like gaining access to online forums, creating an online persona, and engaging in potentially criminal conduct.

[20] Under the federal aiding and abetting statute, one who "aids, abets, counsels, commands, induces or procures its commission" or "willfully causes an act to be done which if directly performed by him or another would be an offense against the United States" may be guilty of aiding and abetting and is punishable as the principal. *See* 18 U.S.C. § 2.

[21] *Rosemond v. United States*, 572 U.S. 65, 71 (2014).

criminal venture with full knowledge of the circumstances involved—even if the actor does not agree with all aspects of that criminal venture—is sufficient to establish aiding and abetting liability.[22]

For instance, a practitioner who provides members of the forum with technical assistance regarding malware knowing the advice will help them breach a network could violate the federal criminal aiding and abetting statute, if the forum members execute their plan–even if the practitioner did not intend to help commit that *particular* crime. Moreover, even if the practitioner does not intend to aid the commission of a crime and ultimately is not charged with committing a crime, such assistance might bring unwanted and costly investigative scrutiny.

Best Practices II

- Information about an ongoing or impending computer crime uncovered during intelligence gathering activities should be promptly reported to law enforcement through contacts—ideally already established— at the local FBI field office or Cyber Task Force and the local U.S. Secret Service field office or Electronic Crimes Task Force (ECTFs).
- In some criminal forums, participants may be required to establish their criminal bona fides by assisting in a criminal act or furnishing proof that they have committed a prior offense. Do not provide any valid, useful information that can be used to facilitate a crime. Doing so could result in civil or criminal liability.
- Involve your legal department in operational planning. They may be able to spot legal issues and provide guidance that can avoid legal problems.

A practitioner must also avoid violating the federal conspiracy statutes.[23] The conspiracy statutes apply when an individual enters into an agreement with at least one other person to commit a federal crime; some statutes also have as an element that someone make any overt act in furtherance of that crime.[24] So, even if providing information to an individual on a forum is not itself a federal criminal offense, the practitioner could still have engaged in a criminal conspiracy, if the practitioner agreed that a crime would occur, regardless of whether it actually happens or not.[25] The general federal conspiracy statute requires some member of the conspiracy to act in furtherance of the conspiracy, but that act need not itself be a crime, nor must the act be performed by the person charged.[26] The CFAA has its own conspiracy provision that only requires an agreement to commit a violation of the CFAA without the commission of any overt acts in furtherance of the conspiracy.[27] Even so, if the practitioner does not intend to commit an offense

[22] *See id.* at 78.
[23] 18 U.S.C. § 371. The federal conspiracy statute makes it a crime for "two or more persons [to] conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy…." *Id.*
[24] *Braverman v. United States*, 317 U.S. 49, 53 (1942).
[25] *See Ocasio v. United States*, 136 S. Ct. 1423, 1432 (2016) ("It is sufficient to prove that the conspirators agreed that the underlying crime *be committed* by a member of the conspiracy who was capable of committing it. In other words, each conspirator must have specifically intended that *some conspirator* commit each element of the substantive offense.").
[26] *See Braverman*, 317 U.S. at 53 ("The overt act, without proof of which a charge of conspiracy cannot be submitted to the jury, may be that of only a single one of the conspirators and need not be itself a crime.").
[27] *See* 18 U.S.C. § 1030(b).

and has not in fact agreed with another party to achieve a criminal objective, the practitioner has not participated in a criminal conspiracy under federal law.[28]

In sum, a security practitioner should take care to avoid taking any action that would assist others in the commission of a crime or agreeing that a crime should occur. Practitioners engaged in these sorts of intelligence gathering activities should remain mindful that their communications and actions are occurring in the context of an online site that exists to facilitate criminal conduct and with individuals who may be planning to commit crimes. The practitioner should avoid providing any true, accurate, or useful information that could advance such crimes.

In the event the practitioner becomes the target of a federal criminal investigation, investigators will likely attempt to determine intent, in part, using extrinsic and circumstantial evidence. Consequently, as suggested above, a practitioner and his or her employer should maintain records that document the practitioner's actions on the forums and the legitimate business purpose for the practitioner's activities so they can establish a legitimate motive and the steps taken to avoid furthering illegal activities.

IV. Purchasing Stolen Data and Vulnerabilities for Cybersecurity Purposes

Some cybersecurity firms monitor Dark Markets for specific types of information as a service to their customers. They may search for customer records or other types of sensitive customer data being offered for sale, because the sale of such information in Dark Markets can be a sign of a previously undetected data breach. They may also search for malware or security vulnerabilities that target their customers' networks or products, which may indicate that a customer's data and assets are ripe for exploitation. When these types of information are discovered for sale online, a cybersecurity organization may attempt to purchase them or broker a deal with the seller for their removal from a Dark Market.

Negotiating with anonymous parties engaged in selling stolen property or security vulnerabilities on the Dark Web creates substantial risk of producing an array of undesirable outcomes: the seller may take the purchaser's payment without producing the promised data; may breach the agreement by selling copies of the data to others; may not have possession or control of all copies of the stolen data and, therefore, be unable to stop it from being further disseminated; may use the proceeds to fund more crimes; or may even produce a trojanized version of the data or vulnerability intended to compromise the purchaser's systems. These risks are compounded by the fact that a merchant selling illicit goods may anticipate that an organization cheated out of its money after striking a deal with a Dark Market merchant will be reluctant to report the incident to the authorities.

An organization that is swindled out of its money by a Dark Market merchant is also likely to have little legal recourse because the seller will often be anonymous; located in a country beyond the reach of U.S. courts; and/or was paid using an untraceable, irrevocable

[28] *United States v. Mahkimetas*, 991 F.2d 379, 383 (7th Cir.1993) (A federal conspiracy requires an agreement among individuals who intend to carry out the agreed-upon criminal act).

payment method. For all of these reasons, organizations should be wary of attempting to obtain stolen data and security vulnerabilities in this manner.

Still, some organizations may be willing to assume these risks because, on balance, they anticipate that there will be commensurate benefits. For instance, they may only seek to obtain a copy of their stolen data so they can assess the nature and scope of a previously undetected data breach and patch their networks to avoid further loss. Also, cybersecurity firms may be able to use the stolen information to create intelligence reporting that others can use to protect their networks better.

Setting aside questions about effectiveness and practicality, purchasing one's own stolen data—or, in the case of a cybersecurity firm, the data of a party that authorizes the purchase of its stolen data—raises legal concerns that warrant consideration. At the outset, federal prosecutors have not typically brought charges against parties who merely attempt to purchase their own stolen data or buy a security vulnerability. However, a party engaged in those activities faces legal risks discussed below that should be considered.

A. Scenario 1: Purchasing Stolen Data

The scenarios in this section focus on different aspects of purchasing stolen data, each of which can have an impact on the legal analysis:

- Whether the purchaser is the legitimate owner of the data: Is the stolen data being purchased by the data owner or the data owner's authorized agent?
- The type of data being sold: Is the stolen data the type of information whose transfer or possession is prohibited by federal law (e.g., stolen credit card information or trade secrets)?
- The identity of the seller: Is the seller someone with whom federal law prohibits the data owner from transacting business?

Each of the scenarios below uses the same assumptions discussed in the intelligence gathering scenarios discussed above: i.e., assumptions about the security practitioners, the nature of the forums accessed, and the means of accessing such forums.[29] However, the discussion here focuses on practitioners who discover data for sale that appears to belong to their cybersecurity company's customers. In these hypothetical cases, the practitioners contact the seller as instructed on the Dark Web site and, with the customer's authorization, offers to purchase the data. These hypotheticals also assume that payment is made and the seller produces the data as agreed.[30]

1. The Ownership of the Data

As mentioned above, purchasing one's own stolen data typically poses little risk of federal prosecution. However, while reviewing the stolen data, the purchaser discovers that the

[29] *See infra* pp. 2-4.

[30] For the sake of this legal analysis, it is necessary to presume that the transaction is successful. For the reasons outlined above, there are no guarantees that an effort to purchase stolen goods online will produce the desired outcome.

tranche of data produced by the Dark Market seller includes data that belongs to other companies. It turns out, the purchaser's stolen data is commingled with data that was likely stolen from other data breach victims.

If the purchaser did not know, and had no reason to know, that the stolen data being bought belonged to others, there is little chance of facing criminal prosecution for purchasing it. Subject to the exceptions discussed below, criminal liability for possessing or handling stolen data generally requires the intent to use the data in an unlawful manner, which this document presumes the practitioner lacks. For instance, the access device fraud statute requires an intent to defraud and the theft of trade secrets statute requires an intent to convert the information to the economic benefit of anyone other than its owner.[31]

But purchasing another party's stolen information without permission or authority can raise questions about the purchaser's intent that invite investigative scrutiny to determine the purchaser's motive. To manage this risk, upon recognizing that the purchased data contains information that it does not have the right to possess, the purchaser should promptly sequester it and not further access, review, or use it. The purchaser should then either immediately contact law enforcement and provide it with the data and/or inform the actual data owner, to the extent it can be determined, that it is in possession of its data. These steps will help demonstrate the lack of any criminal intent that would merit criminal prosecution. When contacting someone whose stolen data has ended up in your possession, avoid communicating in a manner that could be misconstrued to be an extortionate demand.[32]

2. The Nature of the Data

The type of stolen data being sold will also determine whether any criminal statutes prohibit it from being purchased. As noted above, many of the federal criminal statutes associated with the type of stolen data that tends to be sold in Dark Markets—e.g., passwords, account numbers, and other personally identifiable information—only apply if there is intent to further another crime: for instance, an intent to use the information to defraud.[33] For this reason, a purchaser of the stolen data who lacks a criminal motive is unlikely to face prosecution under those statutes.

While unwittingly purchasing another party's stolen information is also typically unlikely to pose a risk of criminal liability, knowingly purchasing another party's stolen data without that party's authorization can pose some legal risk. It is much more likely to raise questions about the purchaser's motives and result in scrutiny from law enforcement and the legitimate data owner, particularly if a trade secret is involved.[34]

---

[31] *See* 18 U.S.C. §§ 1029(a)(1)-(8), (10); 18 U.S.C. § 1832(a).

[32] A party whose stolen data has ended up in the possession of a cybersecurity practitioner could interpret a practitioner's effort to impose conditions on the return of the stolen data to be an extortionate demand. Practitioners should avoid making the return of stolen data dependent on purchasing the practitioner's services or satisfying a demand for anything else of value.

[33] *See* 18 U.S.C. §§ 1029(a)(1)-(8), (10).

[34] "[T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes,

Accidentally purchasing a trade secret would not violate the Theft of Trade Secrets Act (the Act), but receiving, buying, or possessing a trade secret[35] knowing that it was stolen or obtained without authorization can violate it, if other elements of the statute are met. The Act prohibits the transfer or other handling of a trade secret that is converted to the benefit of anyone other than the rightful trade secret owner, intending or knowing that doing so would injure the owner of the trade secret.[36] So, any use of that information would merit examination by the authorities or the trade secret owner. The Act includes a civil cause of action, so a trade secret owner could pursue civil action, even if a criminal prosecution is declined.

As recommended above, the best means of mitigating the risk of being investigated and prosecuted for unintentionally purchasing stolen data that belongs to others—other than by ensuring the seller does not produce material that does not belong to the purchaser—is by promptly contacting and surrendering such extraneous data to law enforcement and/or the rightful data owner. Doing so will minimize the risk that a purchaser's unintended possession of such data will be misinterpreted as a criminal act and could help mitigate civil liability.

3. The Nature of the Seller

Engaging in a financial transaction with certain individuals or organizations can violate the law. For instance, 18 U.S.C. § 2339B prohibits providing material support, or attempting or conspiring to provide material support, to a group that has been designated a foreign terrorist organization.[37] A violation of section 2339B requires a subject to know about the organization's connection to terrorism. It does not, however, require that the subject have the specific intent to further the organization's terrorist activities.[38] Therefore, if a practitioner bought the stolen data knowing the seller was a member of such a foreign terrorism group, the practitioner would violate section 2339B.

Under the International Emergency Economic Powers Act (IEEPA),[39] a similar prohibition would bar the purchaser from buying the stolen data from certain individuals or

---

methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."

18 U.S.C. § 1839(3).

[35] 18 U.S.C. § 1832(a)(3).

[36] Section 1832(a)(2) prohibits unauthorized copying, duplication, sketching, drawing, uploading, altering, destroying, photocopying, replication, transmission, delivery, sending, mailing, communicating, or conveying a trade secret to the economic benefit of anyone other than the owner thereof, and intending or knowing that the doing so will injure any owner of that trade secret.

[37] Liability under section 2339B attaches when a person has knowledge that an organization has been designated a terrorist organization under section 219 of the Immigration and Nationality Act, that the organization has engaged or engages in terrorist activity as defined in section 212(a)(3)(B) of the Immigration and Nationality Act, or that the organization has engaged or engages in terrorism as defined in section 140(d)(2) of the Foreign Relations Authorization Act.

[38] *Holder v. Humanitarian Law Proj.*, 561 US 1, 17 (2010).

[39] 50 U.S.C. § 1705.

entities designated by the U.S. Government. In the last several years, the U.S. Government has issued executive orders sanctioning Iranian, North Korean, and Russian individuals and entities for national security reasons, including cyber-related misconduct.[40] These executive orders and regulations, among other things, prohibit any trade or economic transaction with designated targets. Among other things, IEEPA criminalizes willful violations of these executive orders and regulations and their prohibitions on economic and trade transactions.

The Department of Justice's National Security Division prosecutes criminal violations of IEEPA. IEEPA's willfulness standard would pose significant barriers for criminally prosecuting a practitioner under IEEPA based on the facts of the scenario. Because the identity of anyone selling stolen data in a Dark Market is likely to be masked by a pseudonymous online persona, it is unlikely that the true identity of the seller of stolen data will be known or knowable to a buyer. Where a buyer does not know the identity of the seller and, therefore, does not know the buyer is the subject of economic or trade sanctions, a criminal prosecution requiring proof of willful intent might not be possible to bring. The National Security Division's Counterintelligence and Export Control Section can be reached at (202) 233-0986.

Civil liability, however, can also be imposed under IEEPA. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is responsible for civil enforcement of U.S. economic and trade sanctions regimes. OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals. Civil enforcement of IEEPA may be imposed on the basis of "strict liability," meaning a party could be civilly liable even if it did not know it was engaging in a transaction with an individual or entity that was the subject of trade or economic sanctions. Unauthorized transactions under OFAC's IEEPA-administered regulations may result in a civil monetary penalty. The statutory maximum civil penalties are adjusted annually for inflation.[41]

Companies should make every effort to ensure they are not dealing with an individual or entity subject to economic or trade sanctions. OFAC encourages companies to implement a risk-based compliance program to mitigate the risks of dealing with persons, regions, or countries subject to economic or trade sanctions prohibitions. To assist the public, OFAC published on its website a document, *A Framework for OFAC Compliance Commitments*, intended to provide organizations with a framework for the five essential components of a risk-based sanctions compliance program.

Having a reasonable compliance program (or "rules of engagement") in place that includes measures for checking whether foreign parties with whom business is transacted are subject to economic and trade sanctions is a prudent way of avoiding criminal liability under IEEPA and may mitigate the likelihood of civil liability as well. OFAC also furnishes tools to help identify Specially Designated Nationals and Blocked Persons who are subject to U.S.

---

[40] *See, e.g.*, Blocking the Property of Certain Persons Engaged in Significant Malicious Cyber-Enabled Activities, Exec. Order No. 13694, 80 Fed. Reg. 18077 (April 1, 2015).

[41] The statutory maximum is set by the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, Sec. 701 of Public Law 114-74.

sanctions, such as the Sanctions List Search[42] and the Resource Center web pages for Sanctions Programs and Country Information.[43] These resources may be consulted to mitigate exposure to civil or criminal liability under IEEPA and other sanctions-related statutes. The public is also encouraged to review the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501 Appendix A, for more information regarding OFAC's enforcement of U.S. economic sanctions, including OFAC's voluntary self-disclosure program and the factors OFAC generally considers when determining an appropriate response to apparent violations.[44]

The public can contact OFAC directly by calling the OFAC Hotline toll free at 1(800) 540-6322 or locally at (202) 622-2490 or by sending an email to *ofac_feedback@treasury.gov*. Additionally, requests for specific licenses may be submitted online at OFAC's website at *www.treasury.gov/ofac*. Inquiries regarding pending license requests may be made at (202) 622-2480.

Scenario 2: Purchasing Vulnerabilities

If, while gathering cyber threat intelligence in Dark Markets, a practitioner discovers security vulnerabilities being offered for sale, the practitioner may decide to purchase them so that they may be disclosed to the relevant vendor or develop a patch to prevent the vulnerabilities from being exploited, particularly if the vulnerabilities target a practitioner's customers. Some practitioners also search for new variants of malware being sold in Dark Markets so they can be analyzed and signatures can be developed for use in virus scanning products.

While security vulnerabilities and malware are frequently used to commit computer crimes and it is a federal crime when they are sold in support of criminal conduct, the mere *purchase* of security vulnerabilities or malware is not generally illegal, standing alone and without any criminal intent. There are, however, two exceptions that warrant mention. First, the possession or sale of software designed to intercept electronic communications surreptitiously may violate the Wiretap Act, which prohibits the intentional possession of any "electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications."[45] Certain malware designed to intercept electronic communications may fall within this definition and, therefore, be unlawful to possess.[46] The best way of minimizing legal risk if purchasing malware that may fall under section 2512 is to coordinate with law enforcement before any transaction occurs.

---

[42] Available at https://sanctionssearch.ofac.treas.gov/

[43] Available at https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx and https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.

[44] Available at https://www.ecfr.gov/cgi-bin/text-idx?SID=093f4d5ea37955ea6a767ad337f4f75d&mc=true&tpl=/ecfrbrowse/Title31/31cfr501_main_02.tpl

[45] 18 U.S.C. § 2512(1)(b)

[46] *See, e.g.*, *Luis v. Zang*, 833 F.3d 619, 635 (6th Cir. 2016) (Upholding civil claim under section 2512 against manufacturer of software used to intercept online communications surreptitiously and husband who used the software to capture wife's communications). For more information about the application of the Wiretap Act, consult prior CCIPS publications on computer crime. *See, e.g.*, U.S. Department of Justice Office of Legal Education, *Prosecuting Computer Crimes* 59-72 (2009).

The second exception is when the purchase is prohibited because the seller is a designated foreign terrorist organization or an individual or entity that is subject to economic or trade sanctions under IEEPA. These concerns are the same ones that arise when purchasing stolen data. See the discussion above explaining legal liability under an authority such as IEEPA and how best to address it.

V. Conclusion

This paper is intended to help private sector cybersecurity practitioners by identifying steps they can take and issues they should consider to avoid violating federal criminal law while conducting cybersecurity activities involving criminal forums. When properly conducted, such activities can improve organizations' cybersecurity readiness and help prepare them to respond to cybersecurity threats effectively and lawfully.

How to Contact Law Enforcement

- If you have a pre-established relationship with your local FBI or U.S. Secret Service field office, notify your usual point of contact of your plans to conduct intelligence gathering and recovery of stolen data or report any information concerning an impending, ongoing, or past crime.
- Find your local FBI or U.S. Secret Service field office by visiting:
  https://www.fbi.gov/contact-us/field-offices
  https://www.secretservice.gov/contact/
- For additional information and resources, please visit:
  https://www.justice.gov/criminal-ccips