IS SELLING MALWARE A FEDERAL CRIME?

MARCELO TRIANA*

Congress enacted the Computer Fraud and Abuse Act (CFAA) to impose criminal penalties for a variety of computer misuse offenses. One provision, 18 U.S.C. § 1030(a)(5)(A), criminalizes hacking and the use of malicious software ("malware") by making it a crime to transmit code (i.e., malware) with "intent to cause damage." Today, § 1030(a)(5)(A) fails to adequately police the black market for malware. The United States Department of Justice has recently used the statute to combat these markets by prosecuting hackers who sold malware. This Note argues that § 1030(a)(5)(A) is ill suited to combat the sale of malware for two reasons. First, certain types of malware do not fit under the CFAA's definition of "damage." Second, selling malware does not necessarily satisfy the statute's "intent" element. Ultimately, the black market for malware needs to be policed, and Congress must amend the CFAA's outdated elements to deal with the dangers of malware attacks on our increasingly connected society.

INTRODUCTION 1312
I. THE EVOLUTION OF FEDERAL COMPUTER MISUSE CRIMES ADDRESSING MALWARE 1316
A. *Early Attempts to Address Cybercrime* 1316
B. *The Computer Fraud and Abuse Act (CFAA)* 1319
1. *The Violent Crime Control and Law Enforcement Act of 1994* 1321
2. *The National Information Infrastructure Protection Act of 1996* 1323
3. *Final Amendments to § 1030(a)(5)* 1325
II. HACKING AND THE RISE OF THE MARKET FOR MALWARE 1326
A. *Differences Between Malware that Steals or Destroys Information* 1327
B. *Malware Markets* 1331
C. *The Department of Justice's Attempts to Expand the Scope of § 1030(a)(5)(A)* 1336
III. FIXING THE CFAA'S INTENT AND DAMAGE REQUIREMENTS 1340

 J.D., 2018, New York University School of Law. I am thankful to all my friends and loved ones for supporting me through the writing and editing process. I also owe my gratitude to the editors of the *New York University Law Review*, especially Ben Perotin and Neelofer Shaikh. I want to also thank Professor Orin S. Kerr, with whom I have never spoken but whose writings provided the inspiration and substantiation for this Note.

A. *Selling Malware Is Not Covered by § 1030(a)(5)(A)'s Intent Requirement* 1340
B. *Not All Malware Is Covered by the CFAA's Definition of "Damage"* 1345
C. *Amending the CFAA to Deal with Selling Malware* . 1348
CONCLUSION 1350

INTRODUCTION

On Friday, May 12, 2017, computer systems around the world were crippled by a malicious software program ("malware") called WannaCry, which encrypted computer files and demanded a $300 ransom to recover files.[1] The attack spread to more than seventy countries, affecting a variety of high-profile targets like FedEx, Britain's National Health Service, Honda, and more.[2] A few hours after the attack commenced, a cybersecurity expert named Marcus Hutchins figured out how to stop WannaCry from spreading. Hutchins surmised that WannaCry could be halted by registering a website domain name[3] hidden in the malware's code that would signal the malware to cease and desist once registered.[4] Before the attack, Hutchins was a relatively unknown cybersecurity researcher who ran a cybersecurity blog called MalwareTech.[5] Afterward, he quickly

---

[1] *What You Need to Know About the WannaCry Ransomware*, SYMANTEC: THREAT INTELLIGENCE BLOG (Oct. 23, 2017), https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.

[2] *E.g.*, *Honda Halts Japan Car Plant After WannaCry Virus Hits Computer Network*, REUTERS (June 21, 2017, 12:12 AM), https://www.reuters.com/article/us-honda-cyberattack/honda-halts-japan-car-plant-after-wannacry-virus-hits-computer-network-idUSKBN19C0EI (providing examples of companies victimized); Nicole Perloth & David E. Sanger, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html (describing how WannaCry affected FedEx, Spanish and Russian telecommunications giants, and Britain's National Health Service).

[3] A domain name is just the name of a website, which is in essence the website's URL. Registering the domain name is the first step to creating a website and requires signing up the name with a registrar (e.g., GoDaddy). Om Thoke, *Know More About Domain Names and the Registration Process*, LIFEWIRE (Feb. 25, 2018), https://www.lifewire.com/domain-names-and-registration-process-3473709.

[4] *See* Samuel Gibbs, *WannaCry Hackers Still Trying to Revive Attack Says Accidental Hero*, GUARDIAN (May 22, 2017, 5:41 AM), https://www.theguardian.com/technology/2017/may/22/wannacry-hackers-ransomware-attack-kill-switch-windows-xp-7-nhs-accidental-hero-marcus-hutchins (describing how Hutchins identified a web address in the WannaCry code that became the "so-called kill switch" for the malware).

[5] Brian Krebs, *Who Is Marcus Hutchins?*, KREBS ON SECURITY (Sept. 5, 2017), https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/ ("Relatively few knew it before his arrest, but Hutchins has for many years authored the popular cybersecurity blog MalwareTech.").

became the hero who stopped a global cybersecurity catastrophe.[6] But his story soon took a dramatic turn.

Two months after the WannaCry attack, Hutchins was indicted in the Eastern District of Wisconsin on six felony counts, two of which were for violating provisions of the Computer Fraud and Abuse Act (CFAA).[7] One of these provisions was 18 U.S.C. § 1030(a)(5)(A)—the CFAA's hacking statute—which prohibits knowingly transmitting malware while intending to cause damage to a computer.[8] Prosecutors alleged that Hutchins conspired with an unnamed defendant to market and sell malware called Kronos, which steals banking credentials.[9] Hutchins's case is part of a larger effort to police the market for malware. The problem with using the CFAA's hacking provision to do this is that not all malware is used for criminal purposes.

In the early days of computers, researchers developed nascent forms of malware as practical jokes on friends or simply as experiments, but today malware is increasingly developed for profit.[10] Malware is a portmanteau of malicious software and is defined as a "program[ ] written with the intent of being disruptive or damaging to (the user of) a computer or other electronic device."[11] The first types

---

[6] *See* Danica Kirka, *Expert Who Beat Cyberattack Says He's No Hero*, ASSOCIATED PRESS (May 16, 2017), https://www.apnews.com/dc60584d4b214f0fa6eb9ef88fdf46a7 (describing how Hutchins has been considered a hero but that he does not consider himself one because fighting malware is "the right thing to do"); Elizabeth Weise, *His Life Got Weird After Saving the Internet: Ransomware Hero Marcus Hutchins*, USA TODAY (May 23, 2017, 7:52 AM), https://www.usatoday.com/story/tech/talkingtech/2017/05/23/ransomware-hero-marcus-hutchins-says-tabloids-invaded/102026238/ (noting that Hutchins has been hailed a hero after stopping WannaCry).

[7] *See* Indictment at 2, 8, United States v. Hutchins, No. 2:17-CR-124 (E.D. Wis. July 12, 2017) (charging Hutchins for conspiring with an unnamed defendant to violate various subsections of 18 U.S.C. § 1030).

[8] *See* 18 U.S.C. § 1030(a)(5)(A) (2012) (penalizing anyone who "knowingly causes the transmission of program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer"); Haeji Hong, Note, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283, 284 n.5 (1997) (citing the 1996 Senate report describing § 1030(a)(5) as a measure to protect against hackers).

[9] *See* Indictment at 3, *Hutchins*, No. 2:17-CR-124 (describing Hutchins's alleged marketing and sale of Kronos); Ben Sullivan, *What Is the Kronos Malware Hutchins Is Accused of Creating?*, WIRED (Aug. 5, 2017), http://www.wired.co.uk/article/what-is-kronos-trojan-malware-marcus-hutchins-hacker (detailing how Kronos allowed attackers to steal banking information by recording key strokes on a victim's computer).

[10] *See* MARC GOODMAN, FUTURE CRIMES 15–16 (2015) (describing how the first hackers were motivated by "lulz," or laughs, and hacked to prove they could do it); Lillian Ablon & Martin Libicki, *Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data*, 82 DEF. COUNS. J. 143, 144 (2015) (describing how criminal enterprises recognized advancing technologies and the world's connectedness as an opportunity for financial gain with less risk).

[11] *Malware*, OXFORD ENGLISH DICTIONARY, http://www.oed.com/view/Entry/267413?redirectedFrom=malware#eid. Malware was first coined in July 1990 by Yisrael

of malware created were computer viruses,[12] and the first known virus, called Elk Cloner, was created by a ninth grader as a joke to play on his friends.[13] Hackers soon started creating dozens of new types of malware,[14] and around the same time they also started realizing they could make money off of their skills creating malware.[15] Major corporations take part in this trend by creating bug bounty programs, whereby they pay hackers tens of thousands of dollars to identify vulnerabilities.[16] Corporations are not alone in buying up malware. Governments around the world also purchase malware but justify doing so by citing public safety or national security.[17] At the

---

Radai as a way to describe Trojans, viruses, worms, and other types of malicious software. Ellen Messmer, *Tech Talk: Where'd It Come from Anyway?*, PC WORLD (June 29, 2017, 9:42 AM), https://www.pcworld.com/article/147698/tech.html.

[12] *See* CHRISTOPHER C. ELISAN, MALWARE, ROOTKITS & BOTNETS: A BEGINNER'S GUIDE 10 (2013) ("Before Yisrael Radai coined the word 'malware' in 1990, malicious programs were collectively called computer viruses.").

[13] In 1982, a ninth grader named Richard Skrenta released the Elk Cloner virus onto his school's computers. Farhad Manjoo, *The Computer Virus Turns 25*, SALON (July 12, 2007, 2:59 PM), https://www.salon.com/2007/07/12/virus_birthday/. Elk Cloner spread by copying itself onto any floppy disk students used on the school's computers. *Id.* It did not do any damage aside from occasionally displaying a joking message. *Id.*

[14] *See* Brian Heater, *Malware: A Brief Timeline*, PCMAG (Mar. 10, 2011, 12:01 PM), https://www.pcmag.com/feature/261678/malware-a-brief-timeline (chronicling several additional viruses created in the late 1980s and early 1990s).

[15] *See* LILLIAN ABLON ET AL., RAND CORP., MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA 32 fig.6.1 (2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf (displaying a timeline on the development of the black market for hacked information and noting how in the late 1980s black markets emerged, particularly in Warsaw Pact countries); *see also* KIM ZETTER, COUNTDOWN TO ZERO DAY 99–100 (2014) (describing one of the first known instances of selling malware, in which a hacker sold unknown computer vulnerabilities, also known as zero-days, on eBay); Ablon & Libicki, *supra* note 10, at 144 ("Cybercrime grew as more of the world gained a digital component. Access to computing technology became more prevalent, and there were more technologically savvy people.").

[16] *See, e.g.*, Kate Conger, *Apple Announces Long-Awaited Bug Bounty Program*, TECHCRUNCH (Aug. 4, 2016), https://techcrunch.com/2016/08/04/apple-announces-long-awaited-bug-bounty-program/ (describing how Apple had reversed its policy of not offering bounties for vulnerabilities and will now offer up to $200,000 for exploits to its products); Kate Conger, *Bug Made It Possible to Take Over Tinder Accounts with Just a Phone Number*, GIZMODO (Feb. 22, 2018, 3:10 PM), https://gizmodo.com/bug-made-it-possible-to-take-over-tinder-accounts-with-1823238474 (describing how a researcher discovered a vulnerability in Facebook and Tinder's systems and how both companies paid him several thousand dollars); Dan Goodin, *Google Pledges $2 Million in Prizes to Hackers Who Exploit Chrome*, ARS TECHNICA (Aug. 15, 2012, 7:37 PM), https://arstechnica.com/information-technology/2012/08/google-pledges-million-in-hacking-prizes/ (noting how Google will pay $60,000 for identifying exploits for its Chrome web browser).

[17] *See, e.g.*, Lily Hay Newman, *A Hacking Group Is Selling iPhone Spyware to Governments*, WIRED (Aug. 25, 2016, 1:46 PM), https://www.wired.com/2016/08/hacking-group-selling-ios-vulnerabilities-state-actors/ (detailing how a company called NSO Group sold iPhone spyware to governments); Jose Pagliery, *This Company Sells Spy Tools to Evil Governments*, CNN: TECH (July 6, 2015, 5:42 PM), http://money.cnn.com/2015/07/06/

same time, a black market developed for criminal organizations to buy malware for committing cyberattacks.[18]

Federal prosecutors have started targeting the black market for malware by expanding § 1030(a)(5)(A)'s reach to prosecute hackers, like Hutchins, for selling malware. But § 1030(a)(5)(A) does not clearly criminalize the sale of malware for two reasons.[19] First, defendants charged with selling malware in violation of § 1030(a)(5)(A) likely do not meet the statute's mens rea requirement. Since hackers selling malware more clearly intend to profit off of their skills, they likely do not meet the mens rea requirement of "intentionally" causing "damage." Second, the statute's definition of "damage" does not clearly capture certain types of malware.[20] Malware is used to steal data or disrupt a user's access to computer data, and courts have split on whether "damage" covers only disrupting access or also covers stealing information. Ultimately, prosecutors risk doing violence to the CFAA by prosecuting hackers for selling malware and thus overextending § 1030(a)(5)(A)'s text and original purpose. Instead, Congress should amend the CFAA to deal with the black market for malware.

This Note builds on previous work by analyzing whether § 1030(a)(5)(A) also penalizes hackers who sell the tools to break into a computer system. Prior work on the CFAA has tended to focus on the statute's distinction between exceeding authorized access and unauthorized access, and not on the markets for malware and hacking tools.[21] Part I details the origins of computer misuse offenses and the

technology/hacking-team-hacked/index.html (describing how a company called Hacking Team sold hacking and spying tools to Ethiopia for $1 million, Egypt for €58,000, and Sudan for $960,000); Kim Zetter, *U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies*, WIRED (Nov. 11, 2014, 6:30 AM), https://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/ (mentioning the government's policy that the NSA disclose software vulnerabilities, unless the vulnerability has a "clear national security or law enforcement" use).

[18] *See* Ablon & Libicki, *supra* note 10, at 144–45 ("[C]ybercrime has become the province of large, highly organized groups, with robust infrastructure and social organization, often connected with traditional crime groups. These groups pursue specific actions such as stealing information or installing malware."); *infra* notes 149–61 and accompanying text describing the development and structure of the black market for malware.

[19] *See infra* Section II.B.

[20] *See infra* Section II.A.

[21] *See, e.g.*, Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442 (2016) (arguing for courts to adopt a narrower, "code-based" approach to interpreting the meaning of exceeding authorized access and unauthorized access); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143 (2016) (developing a framework for distinguishing between authorized and unauthorized access to a computer). There was some discussion of when technology sellers, black market or otherwise, can be guilty of aiding and abetting

creation of the current version of the CFAA. Part II provides background on the types of malware hackers often use, describes the markets through which hackers sell malware, and details the Department of Justice's (DOJ) recent push to prosecute the sale of malware. Part III analyzes how § 1030(a)(5)(A)'s intent and damage requirements do not cover the sale of malware, and provides a way in which Congress can amend the CFAA to deal with the market for malware.

I
The Evolution of Federal Computer Misuse Crimes Addressing Malware

Computer misuse offenses evolved several times since the computer revolution of the 1970s and 1980s. Prosecutors first attempted to address computer misuse by employing common law offenses like theft and trespass. This was an imperfect solution because those offenses focus on the physical world and do not adequately capture how computers function. In 1984, Congress finally created the CFAA to specifically address newfangled, malicious uses of computers. While it was updated several times since its enactment, the CFAA has not been amended in nearly a decade and is now unable to address the malware market.

A. Early Attempts to Address Cybercrime

There are two types of computer crimes. The first is the commission of traditional crimes facilitated by computers; for example, a Ponzi scheme disseminated via email or sharing child pornography on the internet.[22] The second is the commission of computer misuse

liability, but that article did not address how the malware market impacts liability under § 1030(a)(5)(A). Benton Martin & Jeremiah Newhall, *Technology and the Guilty Mind: When Do Technology Providers Become Criminal Accomplices?*, 105 J. Crim. L. & Criminology 95 (2015) (discussing when sellers of technology with criminal uses aid and abet their users' crimes, but not focusing on malware markets, or § 1030(a)(5)(A)'s intent and damage elements).

[22] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1602 (2003). The two categories Professor Kerr adopts originated from Professors Charney and Alexander, but Charney and Alexander had a third category, or offense, in which computers were also used as a storage device for evidence. Scott Charney & Kent Alexander, *Computer Crime*, 45 Emory L.J. 931, 934 (1996). Alternatively, the 1989 version of the Department of Justice's computer crime manual divided computer crime into three categories: the object of the crime, which refers to theft of computer hardware or software; the subject of the crime, which refers to the computer as the subject or site of any damage caused; and the instrument of the attack, which alludes to using computers to execute traditional offenses (e.g., wire fraud or identify theft). Alexander Galicki et al., *Computer Crimes*, 51 Am. Crim. L. Rev. 875, 878, 882 (2014).

crimes, such as interfering with the proper functioning of computers or networks.[23] This Note focuses on the latter. Computer misuse crimes involve disrupting the proper functioning of a computer or network[24]—disruption which, today, is enabled by using malware.

Computer misuse offenses, at an abstract level, occur in one of two ways: exceeding access privileges or denying a user access privileges.[25] Exceeding access privileges can occur when a user who has access to a computer gains unauthorized access to additional files or portions of the computer, or it can occur when someone without access privileges uses the computer.[26] For example, a college student has authorized access to parts of the college's system but exceeds her authorized access when she uses an administrator's password to access the system and change her grade.[27] Denying access privileges is somewhat more self-explanatory and occurs when a hacker denies users their full privileges on a computer or network.[28] For example, someone could deploy a direct denial of service (DDoS)[29] attack to freeze a website, thus denying a user's rights to access the website.[30]

Before Congress enacted specific computer misuse offenses, prosecutors turned to property crimes—like trespass, burglary, and theft—

---

[23] Kerr, *supra* note 22, at 1603 ("We can define computer misuse as conduct that intentionally, knowingly, recklessly, or negligently causes interference with the proper functioning of computers and computer networks."); *see also* Galicki et al., *supra* note 22, 879–81 (noting how one category of computer crime offenses focuses on hackers using malware to disrupt normal computer activity).

[24] Kerr, *supra* note 22, at 1603–04 (describing how computer misuse upsets a user's reliance on their rights and privileges through using hacking, viruses, worms, or denial of service attacks).

[25] *Id.* at 1604.

[26] *Id.* A fair amount of recent scholarship on the CFAA has involved a debate over when a user has accessed a system either while exceeding authorized access or without authorization. *See, e.g.*, William A. Hall, Jr., *The Ninth Circuit's Deficient Examination of the Legislative History of the Computer Fraud and Abuse Act in* United States v. Nosal, 84 GEO. WASH. L. REV. 1523, 1524–26 (2016) (arguing that the Ninth Circuit improperly interpreted "exceeds authorized access" to exclude misappropriation of trade secrets because Congress intended to permit prosecutions of insiders who exceed their authorized access for prohibited purposes); Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 171–81 (2011) (analyzing the differences between unauthorized and exceeding access).

[27] Kerr, *supra* note 22, at 1603–04 (explaining exceeding authorized access with the example of someone hacking into a corporate network and seeing secret files that the person is not supposed to view).

[28] *Id.* at 1604.

[29] A DDoS attack occurs when a large number of computers send data requests to a single server, thus flooding the server with traffic. The high volume of traffic overloads the server's typical internet bandwidth, causing it to seize up. *What Is a DDoS Attack?*, CISCO, https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html (last visited Mar. 14, 2018).

[30] Kerr, *supra* note 22, at 1604.

to address acts of computer misuse.[31] But these property crimes were ill suited to addressing computer misuse. Both criminal trespass[32] and burglary[33] seem analogous to computer misuse crimes because of an intent to enter onto a person's property while possibly intending to cause damage, but both offenses focus on whether the defendant is physically present on the property.[34] As a result, both offenses are difficult to square with computer misuse, since computer misuse often does not entail physical presence on property.[35] Prosecutors also thought theft statutes could address computer misuse under the rationale that hackers committed theft by disrupting computer privileges.[36] Theft statutes presume the existence of identifiable property, the use of which an owner is deprived, but this concept is strained when applied to computers.[37] In early cases, courts held there was a property interest in the mere use of a computer, data stored on a computer, and even the password controlling access.[38] But these interpretations struggled to rationalize how this property interest was

---

[31] *Id.* at 1605–13 (describing how prosecutors considered applying existing property crimes before any legislature enacted a computer crime statute).

[32] Criminal trespass punishes knowingly entering a person's property while on notice that the owner forbids entry. *See* MODEL PENAL CODE § 221.2(1) (AM. LAW INST., 1985) ("A person commits an offense if, knowing that he is not licensed or privileged to do so, he enters or surreptitiously remains in any building or occupied structure . . . ."); Kerr, *supra* note 22, at 1605–06 (explaining how trespass generally punishes knowing entrance or presence on property despite notice that the owner forbids it).

[33] Burglary is the act of breaking and entering with the intent to commit a crime therein, but modern statutes focus on entering a building without license or privilege with the intent to commit a crime inside. *See* MODEL PENAL CODE § 221.1 ("A person is guilty of burglary if he enters a building or occupied structure . . . with purpose to commit a crime therein . . . ."); Kerr, *supra* note 22, at 1606 (recounting the elements of burglary at common law and in modern statutes).

[34] Kerr, *supra* note 22, at 1606–07 (explaining how trespass and burglary statutes require the defendant to pass a property's threshold to commit either offense).

[35] *Id.* at 1607. Some people contend that the CFAA has essentially adopted trespass principles and codified them in a computer crime statute. *See generally* Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477 (2016) (arguing that the CFAA's "without authorization" term incorporates preexisting physical trespass principles).

[36] *See* Kerr, *supra* note 22, at 1609–10; *see also* United States v. Girard, 601 F.2d 69, 71 (2d Cir. 1979) (concluding that the defendant committed theft by taking government computer records); United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) (holding that information on a telecommunications company's system was property, and the defendant defrauded the company of its property by intercepting information from its system).

[37] *See* Kerr, *supra* note 22, at 1610–11 (detailing how courts struggled to rationalize how a defendant's conduct deprived an owner of their property rights in a computer file or program when the owner still had access to those files or programs).

[38] *Id.* at 1610 ("Courts held that the mere use of a computer was property, that the data viewed when using a computer also constituted property, that the data stored in a computer counted as property, and even that the password that controlled access to a computer account was property.").

deprived when someone took only a copy of software or digital records and did not deprive the owner of the property itself.[39] The debate over whether copying data deprives a user of their property interest still exists, but in the CFAA, the debate is over whether copying data fits under the CFAA's definition of damage, a necessary element for most CFAA offenses.[40]

Congress tried solving the imperfections of using property crimes by creating a statute to specifically address computer misuse. The CFAA at first focused on hacking for banking and government information but was later amended to address broader categories of offenses against a wider range of targets such as selling computer passwords or hacking personal computers. The CFAA's hacking provision was, however, drafted in an era when hackers deployed malware to directly attack computers. Today, there are growing markets, both legitimate and illicit, where malware is bought and sold as a commodity. Congress did not envision the development of these markets, and thus did not create a provision to police them.

B. The Computer Fraud and Abuse Act (CFAA)

Congress has expanded the application of the CFAA through multiple amendments to computer misuse statutes.

The earliest computer crime laws were enacted as part of the Comprehensive Crime Control Act of 1984 (CCCA), an omnibus crime bill that revised multiple provisions of federal criminal law.[41] The CCCA established three new crimes, codified at 18 U.S.C.

---

[39] *See id.* at 1610–13 (analyzing several federal and state cases that struggled to rationalize how a property interest in computer data was deprived when a defendant stole the data but the owner still had access to it). Professor Kerr notes that courts were results oriented and held defendants guilty if the victim was harmed in some way. *Id.* at 1611.

[40] *See infra* Section II.A, III.B (discussing malware and how courts have split on whether certain types of malware fall under the statute's definition of "damage").

[41] Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976, 2190–92; *see also* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563–64 (2010) (describing the CCCA as an omnibus crime bill containing the first federal computer crime statute). Legend has it that the CFAA owes its creation to the 1983 movie *WarGames*, where Matthew Broderick starred as a tech-savvy teenager who hacks into the North American Aerospace Defense Command (NORAD). *See* Fred Kaplan, *'WarGames' and Cybersecurity's Debt to a Hollywood Hack*, N.Y. TIMES (Feb. 19, 2016), https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html (describing how federal officials developed cybersecurity policies after Ronald Reagan saw *WarGames* and became concerned with the military's computer vulnerabilities); Jamie Williams, *Congress Needs to Clarify that Password Sharing Is Not a Federal Crime*, ELECTRONIC FRONTIER FOUND. (Nov. 2, 2016), https://www.eff.org/deeplinks/2016/11/congress-needs-clarify-password-sharing-not-federal-crime?page=14 ("Congress passed the CFAA after 'War Games' . . . put the fear of God into lawmakers about the vulnerability of our computer networks.").

§ 1030(1)–(3): computer misuse to obtain national security information,[42] computer misuse to obtain personal financial records,[43] and hacking into U.S. government computers.[44] All three offenses required a mens rea of "knowingly" engaging in the offense.[45]

Congress amended these early provisions with the Computer Fraud and Abuse Act of 1986, the first stand-alone legislation meant to address computer crimes.[46] The CFAA expanded the scope of the CCCA's computer crime laws by adding three new offenses codified at § 1030(a)(4)–(6). § 1030(a)(4) prohibited knowingly accessing a computer without authorization with intent to defraud.[47] § 1030(a)(5) prohibited intentionally accessing a computer without authorization and altering, damaging, or destroying information, thereby causing either a loss of $1000 or more, or impairing the medical diagnosis, treatment, or care of one or more individuals.[48] § 1030(a)(5) has become known as the CFAA's hacking statute because it essentially prohibits deploying any malicious program.[49] And § 1030(a)(6) prohibited knowingly trafficking in computer passwords with intent to defraud.[50] § 1030(a)(4)–(6) contained the mens rea requirement "intentionally" causing damage, instead of or in addition to the "knowingly" requirement in the 1984 version.[51] Congress chose to

---

[42] 18 U.S.C. § 1030(a)(1) (Supp. II 1984) (penalizing "knowingly access[ing] a computer without authorization . . . and by means of such conduct obtain[ing] information that has been determined by the United States Government . . . to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . .").

[43] *Id.* § 1030(a)(2) (criminalizing "knowingly access[ing] a computer without authorization . . . and thereby obtain[ing] information contained in a financial record of a financial institution . . .").

[44] *Id.* § 1030(a)(3) (punishing "knowingly access[ing] a computer without authorization . . . and by means of such conduct knowingly us[ing], modif[ying], destroy[ing], or disclos[ing] information in, or prevent[ing] authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States . . .").

[45] *Id.* § 1030(a)(1)–(3).

[46] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (Supp. IV 1987)).

[47] 18 U.S.C. § 1030(a)(4) (Supp. IV 1987).

[48] *Id.* § 1030(a)(5).

[49] *See* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 913 (2003) (describing § 1030(a)(5) as a "hacking offense" penalizing "those who damaged or altered the data of another"); *see also* S. REP. No. 99-432, at 10 (1986) (noting that § 1030(a)(5) was "aimed at 'outsiders,' i.e., those lacking authorization to access any Federal interest computer").

[50] 18 U.S.C. § 1030(a)(6) (Supp. IV 1987).

[51] *Compare id.* § 1030(a)(4)–(6) (Supp. IV 1987) (requiring intent to defraud or intent to access a computer), *with id.* § 1030(a)(1)–(3) (1984) (Supp. II 1984) (requiring knowingly accessing a computer without authorization); *see also* Skibell, *supra* note 49, at 913–14 ("[§ 1030(a)(4)–(6)] included a mens rea of 'intentionally,' a higher requirement than the level of 'knowingly' which was used throughout the 1984 version of the CFAA.").

raise the mens rea requirement out of concern for criminalizing mistaken or careless acts of unauthorized access of a computer or data therein.[52]

Though it expanded the CFAA by adding three offenses, Congress viewed the CFAA as a limited statute. For example, Congress confined the application of § 1030(a)(4) and 1030(a)(5) to offenses involving "[f]ederal interest computers."[53] Congress limited the statute out of concern for states' powers to proscribe computer crimes,[54] but in so doing Congress limited the CFAA's reach to only a few offenses.[55] In the intervening decades, Congress has shed the idea that federal computer crime law should be limited and instead opted to expand multiple provisions of the CFAA. This Note focuses on Congress's amendments to and expansion of the CFAA's hacking provision, § 1030(a)(5)(A), as well as the limitations of the provision in policing markets for malware.

1. The Violent Crime Control and Law Enforcement Act of 1994

18 U.S.C. § 1030(a)(5) was first revised by the Violent Crime Control and Law Enforcement Act of 1994,[56] another omnibus crime bill, which created several of the elements that still exist in today's version of § 1030(a)(5)(A). The 1994 amendments revised § 1030(a)(5) to make it a crime to, "through means of a computer

---

[52] *See* S. REP. NO. 99-432, at 6–7, 10, 21 (1986) (detailing Congress's concern with penalizing individuals who log onto a computer and inadvertently stumble across files to which the user does not have authorized access).

[53] 18 U.S.C. § 1030(a)(4)–(5) (Supp. IV 1987) (applying the respective offenses only to accessing federal interest computers without authorization). The 1986 amendments defined "[f]ederal interest computer" in two ways. First, a federal interest computer could be a computer used by financial institutions or the United States. 18 U.S.C. § 1030(e)(2)(A) (Supp. IV 1987) (defining a "Federal interest computer" as one used exclusively by a "financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government"). Second, a federal interest computer could be a computer part of a multistate network used to commit the offense. *Id.* § 1030(e)(2)(B) (Supp. IV 1987) (defining a "Federal interest computer" as "one of two or more computers used in committing the offense, not all of which are located in the same State"). The definition, in essence, required a strong federal interest or nexus for an act to fall under the statute.

[54] S. REP. NO. 99-432, at 4 (stating that the Committee rejected the call for a sweeping federal computer crime law because it was "convinced that [its chosen] approach strikes the appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses").

[55] *See* Kerr, *supra* note 41, at 1565 (noting how the federal interest computer requirement was limited, since "it effectively required an interstate offense over an interstate network," and noting that at a "time when use of the Internet remained in its infancy, few crimes would be included in its reach").

[56] Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796. The amendments to § 1030(a)(5) were subtitled the Computer Abuse Amendments Act of 1994. *Id.* § 290001(b), 108 Stat. at 2097–98.

used in interstate commerce or communications, knowingly cause[ ] the transmission of a program, information, code, or command to a computer or computer system" and either intend to or recklessly cause damage.[57]

There were three significant revisions to § 1030(a)(5)(A) from the 1994 amendments. One significant aspect of the 1994 amendments was the creation of felony and misdemeanor penalties. A person committed a felony under the 1994 version of § 1030(a)(5) when she intended for the transmission to "damage, or cause damage to" a computer, network, data, or program "or [intend for the transmission to] withhold or deny . . . the use of [a computer, network, data, or program]."[58] A person committed a misdemeanor by sending a transmission "with reckless disregard of a substantial and unjustifiable risk that the transmission will damage, or cause damage to, [a computer, network, data, or program], or withhold[s] or den[ies] . . . use of [a computer, network, data, or program]."[59] The difference between the felony and the misdemeanor versions of § 1030(a)(5)(A) was based on whether the defendant intentionally or recklessly caused damage. Creating a misdemeanor provision to § 1030(a)(5) was thought to fix the CFAA's perceived failure to cover circumstances where a hacker caused damage with reckless disregard.[60]

Another significant aspect of the 1994 amendments was the deletion and introduction of several statutory elements. The 1994 amendments deleted the phrase "intentionally accessing a Federal interest computer" and replaced it with the phrase "computer used in interstate commerce or communication."[61] The amendments also introduced the "transmission of a program" element.[62] The 1994

---

[57] 18 U.S.C. § 1030(a)(5)(A)–(B) (1994).

[58] *Id.* § 1030(a)(5)(A)(i), (c)(3)(A) (making a violation of (a)(5)(A) punishable by a fine or up to five years in prison, depending on whether the defendant was previously convicted of an offense under this section).

[59] *Id.* § 1030(a)(5)(B), (c)(4) (making a violation of (a)(5)(B) punishable by a fine or up to one year in prison).

[60] *See* A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 83 (2001).

[61] *Compare* 18 U.S.C. § 1030(a)(5) (Supp. IV 1987) (using the phrase "Federal interest computer"), *with* 18 U.S.C. § 1030(a)(5) (1994) (omitting "Federal interest computer" and instead using "computer used in interstate commerce or communication"). This change was motivated by arguments that "Federal interest computers" did not cover hackers who attacked computers in their own state. The 1994 amendments were not accompanied by a congressional report explaining the amendments, but the Senate report to the 1996 amendments explains how the change from "Federal interest computer" to "computer used in interstate commerce or communication" was meant to cover intrastate hacking. S. REP. NO. 104-357, at 10 (1996).

[62] The full statutory language being: "transmission of a program, information, code, or command." 18 U.S.C. § 1030(a)(5) (1994).

amendments required the defendant intend for the transmitted program to damage a computer (or its data) or withhold the user's access.[63] A part of this requirement was proving some financial harm that required showing either a "loss or damage," but Congress did not fully explain this requirement until adding a definition in 1996.[64] And the 1994 amendments introduced the element that to violate the statute, the transmission of a program must occur "without the authorization of the persons or entities who own or are responsible for the computer system."[65]

2. The National Information Infrastructure Protection Act of 1996

Congress again revised § 1030(a)(5) through the National Information Infrastructure Protection Act of 1996.[66] The 1996 amendments retained many elements introduced in the 1994 amendments, but the statute was reorganized into three offenses—(a)(5)(A)–(C)—and has generally retained this structure. Section (a)(5)(A) made it a felony to "knowingly cause[ ] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[ ] damage without authorization, to a protected computer."[67] Section (a)(5)(B) made it a felony to "intentionally access[ ] a protected computer without authorization, and as a result of such conduct, recklessly cause[ ] damage."[68] And section (a)(5)(C) made it a misdemeanor to "intentionally access[ ] a protected computer without authorization, and as a result of such conduct, cause[ ] damage."[69] The 1996 amendments also deleted the phrase "computer used in interstate commerce or communication."[70] But, more importantly, it

---

[63] 18 U.S.C. § 1030(a)(5)(A)(i) (1994).

[64] *See id.* § 1030(a)(5)(A)(i)(I), (B)(i)(II) (requiring that a transmission "damage, or cause damage"); *id.* § 1030(e) (omitting "damage" from definition section of 1994 statute); *id.* § 1030(e)(8)(A) (Supp. II 1997) (defining "damage" as "any impairment to the integrity or availability of data . . . or information" that "causes loss aggregating at least $5000 in value" during a one year period); *see also* S. REP. NO. 104-357, at 11 (1996) ("The 1994 amendment required both 'damage' and 'loss,' but it is not always clear what constitutes 'damage.'").

[65] *Id.* § 1030(a)(5)(A)(ii)(I), (B)(ii)(I).

[66] Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491 (1996).

[67] 18 U.S.C. § 1030(a)(5)(A), (c)(3)(A) (Supp. II 1997) (punishing a first-time violation of 1030(a)(5)(A) with a fine or imprisonment of not more than five years, or both).

[68] *Id.* § 1030(a)(5)(B), (c)(3)(A) (punishing a first-time violation of § 1030(a)(5)(B) with a fine or imprisonment of not more than five years, or both).

[69] *Id.* § 1030(a)(5)(C), (c)(2)(A) (punishing a first-time violation of § 1030(a)(5)(C) with a fine or imprisonment of not more than one year, or both).

[70] Congress replaced the "interstate commerce" language out of concern that it was not as all-encompassing as the previous phrase—"Federal interest computer." *See* S. REP. NO. 104-357, at 10 (1996) (describing the loophole left open by the 1994 amendments). DOJ identified that "interstate commerce" excluded intrastate computers used by financial

defined damage as "any impairment to the integrity or availability of data, a program, a system, or information," that causes an aggregate loss of at least $5000 in a year, modifies or impairs medical treatment of one or more individuals, "causes physical injury to any person," or "threatens public health or safety."[71] Congress wanted the definition to satisfy several areas of concern: significant financial losses, impacts on medical treatment, physical injuries, and threats to public health or safety.[72]

Congress indicated some intent for "damage" to be defined broadly. The Senate report addressed the example of a hacker using a keylogger to steal passwords and then removing the keylogger from the computer.[73] While neither the computer nor its information is "damaged," the passwords are no longer secure, and the system administrator bears the cost of resecuring the system.[74] The report notes that if the loss to the victim satisfied the monetary threshold—$5000 in a one-year period—then the conduct should be criminal.[75]

Congress also explained its rationale for using the "without authorization" language differently in § (a)(5)(A) (for insiders) versus (a)(5)(B) and (C) (for outsiders). Congress intended § 1030(a)(5)(A) to apply to "anyone who intentionally damages a computer, regardless of whether they were an outsider or an insider otherwise authorized to access the computer."[76] Congress wanted to protect insiders to some extent by only making them liable for intending to cause damage, not for recklessly or negligently causing damage; but it wanted to punish hackers for "any intentional, reckless or other damage they caused by

---

institutions or the government. *See* U.S. DEP'T OF JUSTICE, LEGISLATIVE ANALYSIS OF THE 1996 NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT, 2 ELECTRONIC INFO. POL'Y & L. REP. 240, 244 (1997) (describing the unintended side effects of the 1994 changes from "federal interest computer" to "computer used in interstate commerce or communication"). As a result, Congress decided to use the phrase "protected computer," which was defined as a computer "used in interstate or foreign commerce or communication," or a computer used exclusively by a "financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government." *See* 18 U.S.C. § 1030(e)(2) (Supp. II 1997). Congress ultimately solved this definitional problem by copying part of the definition for "Federal interest computer" and placing it under "protected computer" in the 1996 amendments. *Compare* 18 U.S.C. § 1030(e)(2)(A) (Supp. II 1997) (defining "protected computer" as a computer used by a financial institution or the United States government), *with* 18 U.S.C. § 1030(e)(2)(A) (Supp. IV 1987) (defining a "Federal interest computer" as a computer used by a financial institution or the United States government).

71 18 U.S.C. § 1030(e)(8) (Supp. II 1997).

72 S. REP. NO. 104-357, at 11.

73 *Id.*

74 *Id*.

75 *Id.*; *see also id.* at 13 (denoting a monetary threshold of $5000).

76 *Id.* at 10.

their trespass."[77] This means that insiders would not be punished for accidentally causing damage by accessing parts of a computer system without authority, whereas outsiders who invade a computer could be liable for intentionally or accidentally causing damage. The rationale for this distinction was based on the assumption that "anyone who knowingly invades a system without authority"—an outsider—and causes damage should be punished even when the damage was less than intentional.[78] Congress believed an alternative scheme would "invite hackers to break into computer systems, safe in the knowledge that no matter how much damage they cause" their conduct is not criminal unless intentional or reckless.[79]

3. Final Amendments to § 1030(a)(5)

The remaining amendments to § 1030(a)(5) came from the USA PATRIOT ACT of 2001[80] (Patriot Act) and the Identity Theft Enforcement and Restitution Act of 2008.[81] Both acts included formatting changes but very few substantive changes. One change from the Patriot Act was to expand the meaning of "protected computer" to include computers "located outside the United States,"[82] and the 2008 amendments did the same by adding the disjunction that a computer be "used in *or affecting*" interstate commerce.[83] The 2001 amendments defined loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data . . . and any revenue lost, cost incurred, or other consequential damages . . . because of interruption of service."[84] The 2001 amendment's "loss" definition focused on financial harm and distinguished "damage," which was more akin to the destruction of data or withholding access to data.[85]

The current version of § 1030(a)(5)(A) makes it a felony to "knowingly cause[ ] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[ ]

---

[77] *See id.* at 11 (noting the different mens rea levels of culpability for insiders and outsiders).

[78] *Id.*

[79] *Id.*

[80] Pub. L. No. 107-56, 115 Stat. 272.

[81] Pub. L. No. 110-326, tit. II, 122 Stat. 3560.

[82] 18 U.S.C. § 1030(e)(2)(B) (Supp. I 2002).

[83] 18 U.S.C. § 1030(e)(2)(B) (Supp. II 2009) (emphasis added).

[84] 18 U.S.C. § 1030(e)(11) (Supp. I 2002).

[85] *Compare id.* (defining "loss"), *with* S. REP. NO. 104-357, at 11 (1996) (using the example of a hacker using a keylogger to steal passwords and noting that in such an instance there would not be "damage," but there would be "loss").

damage without authorization, to a protected computer."[86] To convict a defendant of violating § 1030(a)(5)(A), prosecutors must prove "(1) the defendant knowingly caused [a] transmission . . . ; (2) the transmitted material caused damage to a protected computer that the defendant was not authorized to cause; and (3) the defendant intended to cause the damage."[87] Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information."[88] And a "protected computer" is either a computer used by "a financial institution or the United States Government"[89] or a computer "used in or affecting interstate or foreign commerce or communication."[90]

The 1986 and 1996 Senate reports to the CFAA amendments noted that given how technology continues to develop at a rapid pace, the CFAA must be continuously revised.[91] Despite that imperative, the CFAA has not been updated in approximately ten years,[92] and § 1030(a)(5) has not been meaningfully revised in almost twenty.[93] As a result, the CFAA's hacking statute is no longer suited to dealing with the current rise in the illicit market for malware.

II

Hacking and the Rise of the Market for Malware

Malware and the market for it have grown in tandem over the past several decades. When malware was created as a practical joke, hackers did not yet think to commercialize their skills.[94] Hackers developed a black market early on in the computer revolution but used it to sell stolen information, like credit card numbers. Hackers today sell their skills and their malware as commodities.

---

[86] 18 U.S.C. § 1030(a)(5)(A) (2012); *id.* § 1030(c)(4)(B) (punishing a first-time violation of § 1030(a)(5)(A) with a fine or imprisonment of not more than ten years, or both).

[87] Scott, *supra* note 60, at 99; *see also* 18 U.S.C. § 1030(a)(5)(A).

[88] 18 U.S.C. § 1030(e)(8).

[89] *Id.* § 1030(e)(2)(A).

[90] *Id.* § 1030(e)(2)(B).

[91] *See* S. Rep. No. 104-357, at 5 (1996) ("As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime."); S. Rep. No. 99-432, at 1–2 (1986) ("During the past several years, the Congress has been investigating the problems of computer fraud and abuse to determine whether Federal criminal laws should be revised to cope more effectively with such acts.").

[92] *See* 18 U.S.C. § 1030 (2012) (providing the most recent version of the CFAA).

[93] Congress last changed § 1030(a)(5)(A) in 1996, amending its structure. *See* 18 U.S.C. § 1030(a)(5)(A) (Supp. II 1997); *supra* Section I.B.2 (describing the 1996 amendments).

[94] *See* Goodman, *supra* note 10, at 15–16 (describing how malware was created just for laughs and was not initially commercialized).

A. Differences Between Malware that Steals or Destroys Information

Malware is a broad category for programs used for malicious purposes. Any malware attack has two parts: exploits and malicious code/executables.[95] Exploits are programs created to leverage a system's security vulnerabilities to plant the malicious code, and exploits do not serve any malicious function aside from providing a hacker with access to a computer.[96] Malicious code, also called the payload, is the program that executes the ultimate malicious goal.[97] To analogize it to burglary, exploits are like the lockpicks used to break into a home, and malicious code is the component that steals or destroys anything once inside a home.

Malware is commonly classified by its functionality and is often labeled a virus, worm, Trojan, rootkit, ransomware, spyware, backdoor, or botnet.[98] Malware today is often a hybrid of these types and has multivariate functionality.[99] Despite these labels, hackers generally deploy malware either by preventing users from accessing their computer data, whether by simply locking the data or deleting it altogether,[100] or by gaining access to a computer to copy or steal the data without destroying or locking out users.[101] The essential difference between these two categories is whether the malware destroys computer data. While technologists generally classify malware by its different functions[102]—and not by this two-part classification—bifurcating a description of malware in this way makes it easier to see when malware falls under the CFAA's damage definition. Several of

---

95 *See* Palo Alto Networks, *Malware vs. Exploits: What's the Difference?*, YouTube (Sept. 2, 2016), https://www.youtube.com/watch?v=a9u8-rNCHUs (describing "malicious executables" and "exploits" as the "two subcomponents of malware").

96 *See* Camilo Gutierrez Amaya, *Myths About Malware: An Exploit Is the Same as Malware*, WeLiveSecurity (Oct. 21, 2014, 2:32 PM), https://www.welivesecurity.com/2014/10/21/myths-about-malware-exploit-is-the-same-as-malware/ (defining exploits as programs that "simply try[ ] to take advantage of an error in the design or programming of a system or application" and noting that while exploits are not on their own malicious, "cybercriminals tend to use them as a component within their malicious code to gain access to a system illegally").

97 *See id.*

98 *See* Elisan, *supra* note 12, at 18.

99 *Cf.* John Aycock, Computer Viruses and Malware 17 (2006) (noting how technology makes it easy to create hybrid malware combining parts of different types of malware).

100 *See supra* notes 25–30 and accompanying text (describing computer misuse offenses focused on restricting a user's access).

101 *See supra* notes 25–30 and accompanying text (recounting computer misuse offenses focused on simply exceeding access privileges).

102 *See* Aycock, *supra* note 98, at 11 ("Malware can be roughly broken down into types according to the malware's method of operation.").

these malware types function to steal or destroy information; others only provide access to steal or destroy information.

Viruses and worms are two common malware programs used to destroy computer data. Viruses and worms are both self-replicating programs, but viruses require a host computer to spread, and worms do not.[103] Viruses operate by infecting a host's files or other programs; they can be immediately executed, lay in wait until a particular program is run, or can infect the computer during its start-up processes.[104] Worms operate in much the same way, but instead of spreading from a host they propagate across a network (e.g., office computers connected via WiFi).[105] One of the earliest examples of this is the Morris Worm, named after its creator, Robert Morris,[106] who released the worm in 1988 and was mostly motivated by intellectual interest.[107] The worm was only programmed to spread itself, not to destroy data, but it nonetheless damaged computers by causing them to freeze when the virus kept multiplying on computers that were already infected.[108]

---

[103] SUSAN W. BRENNER, CYBERCRIME AND THE LAW 36–37 (2012). Viruses have become more and more prevalent; approximately 200 were in circulation in 1990, and experts have estimated that by 2010 there were millions of viruses spreading around the globe. *Id.* at 37.

[104] ELISAN, *supra* note 12, at 11. More specifically, viruses can operate as file infectors, boot-sector viruses, or multipartite viruses. File infectors can immediately infect a file when a virus is executed or they can lay in wait until a particular program is run. *Id.* at 11, 15. A boot-sector virus infects a computer by infecting the computer during its start-up or initialization processes—its boot-sector. *See id.* at 15 (describing that a boot-sector virus "hijack[s] the first instruction in the boot sector to point to itself"); *see also* Tim Fisher, *What Is a Boot Sector?*, LIFEWIRE, https://www.lifewire.com/what-is-a-boot-sector-2625815 (last updated Mar. 12, 2017) (describing how the boot-sector is the space on a drive that contains the "information about how to start the boot process in order to load an operating system"). A multipartite virus is a hybrid with executable and boot-sector components, but when executed the virus looks for files to infect and then looks for the presence of disks in drives and infects their boot-sectors. ELISAN, *supra* note 12, at 11–12.

[105] AYCOCK, *supra* note 98, at 15.

[106] *See* Larry Seltzer, *The Morris Worm: Internet Malware Turns 25*, ZDNET (Nov. 2, 2013, 1:00 PM), https://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/ (describing the Morris Worm as the "first great incidence of malware . . . on the Internet"); *see also* United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (upholding Morris's conviction under the CFAA).

[107] *See* Meghan Holohan, *As the Morris Worm Turned*, CARNEGIE MELLON UNIV. SCH. COMPUTER SCI.: LINK, https://www.cs.cmu.edu/link/morris-worm-turned (last visited May 30, 2018) (noting that the Morris Worm was "[d]esigned to test the size of the Internet").

[108] *Morris*, 928 F.2d at 505–06. Morris did not want the worm to recopy itself unnecessarily to already-infected computers, so he programmed the worm to query whether a computer was infected. If the answer was "no," then the worm would infect it, but if it was "yes," the worm would not duplicate itself. *Id.* at 506. At the same time, Morris was concerned that some programmers could kill the virus by programming their computers to falsely answer "yes," so Morris programmed the worm to duplicate itself every seventh time the worm queried a computer. *Id.* He underestimated how many times a computer would be queried, and in the end computers began freezing as fast as the worm

Trojans and backdoors, on the other hand, do not self-replicate but instead allow hackers to penetrate a computer's security.[109] Trojans allow hackers to access new systems by passing themselves off as harmless programs, thus deceiving users into downloading or opening a Trojan file.[110] Trojans are often used to destroy files, software, or the whole operating system.[111] Trojans can be placed as attachments in emails that appear benign, or they can appear as a bank login screen to trick you into typing in your credentials.[112] Backdoors are avenues to bypass a computer's security safeguards, and they operate in stealth to avoid detection.[113] Remote access Trojans (RATs), also called remote access tools, are a type of backdoor that give an attacker remote administrative access to a computer.[114] RATs are distinguishable from traditional backdoors in that RATs have a user interface that allows the hacker to command the infected computer.[115] RATs allow attackers "to do almost anything" on the compromised computers, including installing malware to steal or destroy data.[116]

Spyware is a broad category of malware used to steal private information.[117] Spyware can be tailored to log any keyboard strokes a user makes, take screenshots of a computer's desktop, or steal information from a computer's memory.[118] They are used to collect banking credentials, corporate secrets, or any other bit of confidential information.[119] Spyware also does not replicate, like a virus or worm,

---

spread. *See id.* (noting that Morris's original calculations resulted in more copying than anticipated).

109 AYCOCK, *supra* note 98, at 13 (noting how backdoors do not self-replicate and are a mechanism for bypassing normal security protocols); GOODMAN, *supra* note 10, at 17 (describing how Trojans do not reproduce and allow hackers access to an infected system).

110 GOODMAN, *supra* note 10, at 17.

111 ELISAN, *supra* note 12, at 25.

112 *See* AYCOCK, *supra* note 98, at 13 (giving an example of a Trojan that provides deceptive password prompts as a way of stealing a user's login credentials).

113 ELISAN, *supra* note 12, at 25.

114 *Id.* at 26.

115 *Id.*

116 *Id.*

117 *See id.* at 27 (describing spyware as "information stealers" that cull basically "anything that the attackers can use to their advantage or monetize").

118 These discrete functions fall into three categories: keyloggers, desktop recorders, or memory scrapers. *Id.* Keyloggers record a user's keystrokes and send them to a remote server used by an attacker. *Id.* Desktop recorders take screenshots of a computer's desktop or the active window on scheduled intervals or when triggered by an event, such as a mouse click or a certain keystroke. *Id.* Memory scrapers steal information from a computer's memory while it is being processed, since data in memory is unencrypted. *Id.*

119 *See* AYCOCK, *supra* note 98, at 16.

but can be installed on a computer by being combined with non-malicious software.[120]

Botnets are distinct from the above types of malware given that they infect computers to create a network of infected computers to achieve some other malicious goal apart from the infection itself. A bot is a program that takes control of an electronic device and uses the device to perform automated functions.[121] Bots form together into botnets, which can consist of millions of devices dispersed across the world.[122] Bots report back to the master computer which controls the bot's functions.[123] Bots spread across the internet and use many of the types of malware described above (e.g., backdoors, rootkits, and worms) to gain access and control over a device.[124] Botnets are often used to send out viruses or spam; steal banking credentials and information for the "master"; perpetrate DDoS attacks by flooding a website with traffic to crash its servers; or execute click fraud schemes, which consist of using bots to click on online advertisements to drive up advertising revenue.[125]

While malware can be programmed to perform almost any function imaginable, the above types display how malware is often deployed not to destroy but to provide hackers with access to computers to steal information. While viruses and worms are often used to destroy computer data, the Morris Worm and Elk Cloner[126] illustrate how a virus or worm does not necessarily have to destroy data to be considered either type of malware. For example, while the Stuxnet worm[127] and the WannaCry virus were both designed to destroy either

---

120 *See id.* at 17 ("Spyware may arrive on a machine in a variety of ways, such as bundled with other software that the user installs, or exploiting technical flaws in web browsers.").

121 *See id.* at 18–19. Bots are also referred to as zombies because they follow commands blindly. *See id.*

122 *What Is a Botnet?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/what-is-botnet (last visited Aug. 24, 2018).

123 *See id.* ("Once the recipient opens the malicious file on his computer, the bot reports back to command and control where the bot-herder can dictate commands to infected computers."); *see also* AYCOCK, *supra* note 98, at 18.

124 Emmanuel Carabott, *Explaining Botnets*, GFI SOFTWARE: TECH TALK BLOG (Apr. 7, 2011), https://techtalk.gfi.com/explaining-botnets/; *see also What is a Botnet?*, NORTON BY SYMANTEC, https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html (last visited May 30, 2018) (stating that botnets are often spread through Trojans).

125 *See* ELISAN, *supra* note 12, at 65–69.

126 *See* Manjoo, *supra* note 13 (noting how Elk Cloner "didn't do much damage" and only ever "so often would display a tittering message on the screen").

127 Stuxnet was designed to infect Windows PCs managing large-scale industrial-control systems used to operate factories and public utility facilities, known as supervisory control and data acquisition systems (SCADA). Gregg Keizer, *Is Stuxnet the 'Best' Malware Ever?*, COMPUTERWORLD (Sept. 16, 2010, 7:47 AM), https://www.computerworld.com/article/2515757/malware-vulnerabilities/is-stuxnet-the—best—malware-ever-.html. It took

physical machinery or digital information, Trojans and backdoors provide hackers ways to exploit vulnerabilities to get into a computer system, and spyware allows hackers to steal the information once they are inside.

B. Malware Markets

The term "hacker" is often misused to connote someone who maliciously attacks computer systems.[128] Hackers are more accurately understood as people fascinated by tinkering with computers and with using their technical skills to overcome computer problems.[129] Hackers first started out by experimenting with computers but eventually turned mischievous as they wanted to further probe technology's limits;[130] at the same time, hacking also became virtuous as some sought to protect computer systems.[131] Hacking today falls into one of three categories: white-hat, black-hat, and gray-hat.[132] White-hat hackers are ethical hackers who work toward the public's interest, for

---

advantage of four previously unknown vulnerabilities to gain access to Windows PCs and multiple features to search for and gain control of SCADA systems. *Id.* Stuxnet was designed to infect Iranian nuclear reactors and damage its nuclear centrifuges, and it was successful given that around sixty percent of infected PCs were in Iran. *See id.* (describing how Iran was the country hardest hit by Stuxnet); *see also* RALPH LANGNER, THE LANGNER GRP., TO KILL A CENTRIFUGE 3 (2013), https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (describing how the Stuxnet code was designed to damage centrifuge rotors).

128 *See* Ben Yagoda, *A Short History of "Hack"*, NEW YORKER (Mar. 6, 2014), https://www.newyorker.com/tech/elements/a-short-history-of-hack (chronicling how the general connotation of the term "hacker" changed over time to mean someone who commits malicious activity). Since "hacker" is often mistakenly used to describe someone engaging in malicious hacking, technologists developed the term "cracker" to signify people who hack for criminal purposes. Margaret Rouse, *Hacker*, TECHTARGET: SEARCHSECURITY, http://searchsecurity.techtarget.com/definition/hacker (last updated Aug. 2017) ("[H]ackers . . . identify flaws in security systems and work to improve them, including security experts tasked with locating and identifying flaws in systems and fixing those vulnerabilities. Crackers . . . are intent on breaching computer and network security to exploit those same flaws for their own gain."). For consistency with various sources that use "hacker" rather than "cracker," this Note will use the term hacker throughout.

129 Rouse, *supra* note 127.

130 *See* Martin & Newhall, *supra* note 21, at 99–101 (describing how early experimentation with computers turned nefarious as hackers pushed boundaries and how virtuous hacking sprouted as a counter-balance).

131 *See* Bobby Hellard, *What is Ethical Hacking? White Hat Hackers Explained*, IT PRO (May 29, 2018), http://www.itpro.co.uk/hacking/30282/what-is-ethical-hacking-white-hat-hackers-explained (describing how white hat hackers "aim to improve security, finding security holes and notifying the victim so they have an opportunity to fix it before a less-scrupulous hacker exploits it"); Donna Lu, *When Ethical Hacking Can't Compete*, ATLANTIC (Dec. 8, 2015), https://www.theatlantic.com/technology/archive/2015/12/white-hat-ethical-hacking-cybersecurity/419355/ (defining white hats as "ethical hacker[s] who expose[ ] vulnerabilities in computer systems to improve cybersecurity").

132 Rouse, *supra* note 127.

example, by helping companies find vulnerabilities in their software.[133] Black-hats intentionally access systems for malicious purposes like stealing data or to vandalize computer systems.[134] Gray-hats occupy a middle ground by engaging in conduct falling into either category.[135] Gray-hats hack computers without permission to raise awareness of major security vulnerabilities, but are also comfortable providing these vulnerabilities to governments.[136] Black-, gray-, and white-hat hackers have all found ways to make money in the malware market.

White hats sell their skills and knowledge to companies through bug bounty programs. Technology companies like Google and Microsoft pay hackers to expose vulnerabilities in their software.[137] Third-party security firms also buy up information on vulnerabilities to sell back to their clients.[138] These security firms use the information to test their clients' security and then privately disclose the vulnerabilities to software vendors.[139] Companies and security firms even host competitions where hackers get paid thousands to hack specific software.[140]

There is also a growing gray market for selling malware to governments.[141] Security firms willing to sell malware and exploits to gov-

---

133 *Id.*

134 *Id.*

135 *Id.*

136 *See* ZETTER, *supra* note 15, at 101 (describing the gray market for vulnerabilities sold to governments); Laura Sydell, *This 'Gray Hat' Hacker Breaks into Your Car – to Prove a Point*, NPR (Feb. 23, 2018, 5:05 AM), https://www.npr.org/sections/alltechconsidered/2018/02/23/583682220/this-gray-hat-hacker-breaks-into-your-car-to-prove-a-point (detailing how a hacker breaks into cars, connected doorbells, drones, and phones to find vulnerabilities).

137 ZETTER, *supra* note 15, at 100.

138 *See, e.g.*, *id.* (describing how a company called HP Tipping Point buys up the vulnerabilities); Liam Tung, *Security Firm 'Guarantees' to Pay More than Google Does for Chrome Exploits*, CSO (July 28, 2015, 9:03 AM), https://www.cso.com.au/article/580580/security-firm-guarantees-pay-more-than-google-does-chrome-exploits/ (discussing how one company pays hackers more than any other bug bounty and provides this information to its customers).

139 *See, e.g.*, ZETTER, *supra* note 15, at 100 (discussing HP Tipping Point's practice of using the vulnerabilities for which it pays hackers to test its clients' security). Tipping Point profits by securing their clients before software companies patch their programs. *Id.*

140 *See, e.g.*, Ms. Smith, *Pwn2Own: Microsoft Edge and Apple Safari Fall on Day 1*, CSO (Mar. 15, 2018, 7:09 AM), https://www.csoonline.com/article/3263766/security/pwn2own-microsoft-edge-and-apple-safari-fall-on-day-1.html (detailing the winning hackers on the first day of the 2018 hacking contest called Pwn2Own).

141 *See, e.g.*, Joseph Cox, *Government Malware Company 'Grey Heron' Advertises Signal, Telegram Spyware*, MOTHERBOARD (Mar. 7, 2018, 11:05 AM), https://motherboard.vice.com/en_us/article/bj54kw/grey-heron-new-spyware-brochure-hacking-team (reporting on a new company advertising malware meant to hack secure messaging apps).

ernments populate the gray market.[142] Multiple branches of the United States government have bought malware for a variety of purposes. The Department of Defense, Central Intelligence Agency, and National Security Agency have purchased exploits for offensive and defensive purposes.[143] The DOJ has even bought malware to help it catch suspected criminals; for example, the FBI disseminated malware from a site on the dark web that trafficked in child pornography to track down more computers possessing this material.[144] Some companies seem to care little about which governments buy their malware and what those governments use it for.[145] Indeed, firms have realized that the gray market could be more profitable than disclosing the vulnerabilities to software companies. For example, at least one company, VUPEN, which sells exclusively to intelligence and law enforcement agencies, refused to tell software companies about the vulnerabilities it identified.[146] VUPEN's CEO joked that he could make more money holding onto vulnerabilities for its customers.[147] The rise in the gray market for malware exploits has coincided with the rise in a black market for the same goods and services.[148]

---

142 *See* ZETTER, *supra* note 15, at 106 (noting that "the really big trade in exploits these days is [ ] done . . . by the security firms and defense contractors who have made the development and sale of exploits for government part of the new military industrial complex").

143 *See id.* at 106–07 (recounting how hackers released private documents from the vulnerability seller, Endgame Systems, revealing that the company was focused on providing advice and support to United States intelligence and military organizations).

144 *See, e.g.*, Kim Zetter, *Everything We Know About How the FBI Hacks People*, WIRED (May 15, 2015, 7:00 AM), https://www.wired.com/2016/05/history-fbis-hacking/ (chronicling the history and techniques of the FBI hacking into suspected criminals' computers); *The Playpen Cases: Frequently Asked Questions*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions#howdidplaypenmalwarework (last visited July 18, 2018) (detailing how the FBI employed malware, called a network investigative technique (NIT), to track down computers with child pornography).

145 Alex Hern, *Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim*, GUARDIAN (July 6, 2015, 7:46 AM), https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim (reporting that a security firm sold spying tools to countries with repressive regimes—Uzbekistan, Bahrain, Sudan, and more—who used those tools to target human rights activists).

146 *See, e.g.*, ZETTER, *supra* note 15, at 112 (discussing how VUPEN refused to sell information to Google about vulnerabilities it had found in Google's Chrome browser).

147 *See id.* (detailing how Google offered VUPEN $60,000 for information on an exploit the company identified, but the CEO preferred to keep it for his customers). VUPEN's CEO, Chaouki Bekrar, has insisted that the company's desire to exclusively work with governments is based on an imperative to help democracies save lives while facing national security issues. *Id.*

148 *See* ABLON ET AL., *supra* note 15, at 27 ("The market for zero-days (black or gray) is gaining in popularity, or at least in recognition, which may mean a potential increase in malware and attacks . . . .").

The malware black market started out as a generic online black market for financial information. In the early days, the black market was made up of small networks of people trying to buy and sell credit card numbers.[149] Sales were highly disorganized; vendors would sell credit card numbers written on notepads, and most hackers were either lone wolves or members of small groups.[150] These markets started transforming in the 2000s when tech-savvy market actors started forming tight-knit networks, and the markets started offering a wide range of goods.[151] The black market became made up of a strict hierarchy of site administrators, buyers, sellers, and intermediaries who facilitate transactions by validating products and participants.[152] The markets first expanded to selling credentials to other digital accounts (e.g., e-commerce and social media accounts), and eventually began selling full-on hacking goods and services.[153] Hackers sell a range of malware and previously unknown exploits, called zero-days, as well as botnets for rent and hackers for hire.[154] These markets have matured enough to look like legitimate markets. For example, the relationship between products and prices on the malware market depends on factors like brand name, quality, or renting versus buying. Prices for exploits depend on whether they are bought outright or rented for a specific shelf life, as well as the quality rather than quantity of the exploits.[155] The market's reach is increasingly global and its offerings only limited by buyers' demands.

Hackers and others in the market come from across the world. At first, many were former government employees of Eastern European countries with training and education but no jobs after the fall of the Berlin Wall.[156] This trend dissipated as future generations grew up with computers and gained increasing technical expertise.[157] Most malware attacks originate in the United States, China, or Russia,[158]

---

149 *See id.* at 4 (noting how the market in the mid-2000s focused on selling credit card data and eventually evolved to e-commerce information).

150 *Id.* at 32 fig.6.1 (depicting the development of the black market for hacking services from the late 1980s to 2013).

151 *Id*.

152 *Id.* at 5. Market administrators sit atop the hierarchy; below them are subject-matter experts (which include researchers, malware writers, and programmers); then come intermediaries and vendors; and at the bottom are buyers. *Id.* at 5, 6 fig.2.1.

153 *Id.* at 4.

154 *Id.* at 10 tbl.2.1.

155 *Id.* at 12.

156 *Id.* at 6.

157 *See id.* (noting how the number of black market participants rose "with the entry of a generation of 'digital natives' who have grown up more skilled").

158 *See* Alissa de Carbonnel, *Hackers for Hire: Ex-Soviet Tech Geeks Play Outsized Role in Global Cyber Crime*, NBC NEWS (Aug. 22, 2013, 4:49 PM), https://www.nbcnews.com/tech/security/hackers-hire-ex-soviet-tech-geeks-play-outsized-role-global-f6C10981346

but some believe Russia leads all others in the quality of its malware.[159] Russia's leadership in malware development is based in part on the Russian government's tolerance for attacks beyond its borders, which means the risk of being prosecuted is low enough to incentivize black hat hacking.[160] Russia's tolerance for attacks is a prime illustration of the need to police malicious hacking, but doing so also requires well-tailored laws for dealing with hacking and the malware black market. The market's offerings are becoming more creative and are limited only by buyers' demands.[161]

Malware markets, gray or black, are likely to grow as hackers try to make more money off of their skills. The number of susceptible targets will increase as corporations and governments rely more on networked data and devices. Cisco Systems projected that by 2020 connected devices will outnumber people six to one.[162] Further complicating things is the fact that technology is frequently designed to emphasize advancement at the expense of security.[163] Former government officials continue to try to raise awareness of the cybersecurity dangers,[164] but to no avail as Congress continues not to address cyber-

---

(noting China and Eastern European countries as major distributors of malware); *see also* 22 SYMANTEC, INTERNET SECURITY THREAT REPORT 65–66 (2017) (detailing how data traffic for a particular attack originated mostly in China (26.5%), the United States (17.7%), and Russia (5.8%)).

159 de Carbonnel, *supra* note 158.

160 *See* Arkady Bukh, *The Real Cybercrime Geography*, TECHCRUNCH (Jan. 4, 2015), https://techcrunch.com/2015/01/04/after-sony-whats-the-real-cybercrime-geography/ (describing how hackers are incentivized to make malware because of low wages in the regular economy in Russia and the low risks of being caught).

161 *See* ABLON ET AL., *supra* note 15, at 34 (projecting that attackers will continuously innovate and change tactics, will shift away from selling financial credentials because they flood the market, and that there will be more hacking services for hire).

162 DAVE EVANS, CISCO INTERNET BUS. SOLS. GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 fig.1 (2011), https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf; *see also* VERIZON, STATE OF THE MARKET: INTERNET OF THINGS 4 (2017), https://www.verizon.com/about/sites/default/files/Verizon-2017-State-of-the-Market-IoT-Report.pdf (citing one report indicating that the number of wireless connected devices, called the Internet of Things (IoT), will rise from 14.9 billion at the end of 2016 to more than 82 billion in 2025).

163 *See* Laura Hautala, *Spectre and Meltdown: Details You Need on Those Big Chip Flaws*, CNET (Jan. 8, 2018, 11:51 AM), https://www.cnet.com/news/spectre-meltdown-intel-arm-amd-processor-cpu-chip-flaw-vulnerability-faq/ (explaining how microprocessors in every electronic device are designed to speed them up, which creates inherent vulnerabilities).

164 *See, e.g.*, Chris Bing, *Former CIA Director Calls on Public to Demand Cybersecurity Legislation*, CYBERSCOOP (June 15, 2017), https://www.cyberscoop.com/former-cia-director-calls-public-demand-cybersecurity-legislation/ (reporting on former CIA Director John Brennan's call for Congress to deal with cybersecurity issues); *Counterterrorism, Cybersecurity, and Homeland Security*, COUNCIL ON FOREIGN RELATIONS (Jan. 10, 2017, 8:30 AM), https://www.cfr.org/event/counterterrorism-cybersecurity-and-homeland-security (reporting an interview with Lisa Monaco, former Assistant to the President for

security. In the face of congressional intransigence, the DOJ has started using the CFAA—namely, § 1030(a)(5)(A)—to combat the malware black market.[165]

C. The Department of Justice's Attempts to Expand the Scope of § 1030(a)(5)(A)

Before the DOJ started indicting hackers under § 1030(a)(5)(A) for selling malware, there were some pushes to amend the CFAA. In 2015, President Obama presented a legislative proposal to enhance cybersecurity, which included provisions calling for greater cooperation between the private sector and government; standardizing data breach reporting; and giving prosecutors more tools to prosecute hackers, such as making it a crime to sell malware.[166] Congress never came close to amending the CFAA to grant prosecutors more authority to prosecute hackers, possibly because several digital rights and privacy groups raised concerns about aggressively prosecuting hackers.[167] While advocating for President Obama's legislative proposal, the DOJ admitted that the CFAA does not clearly criminalize

---

Homeland Security and Counterterrorism, in which she discussed national security threats, cybersecurity being a major threat); Emily Tillett, *Jeh Johnson Worries U.S. Still "Vulnerable" to Election Meddling*, CBS NEWS (Aug. 6, 2017, 1:21 PM), https://www.cbsnews.com/news/jeh-johnson-concerned-u-s-still-vulnerable-election-meddling/ (noting that former Secretary of Homeland Security Johnson feels "that the cyber threat . . . is 'going to get worse before it gets better'" and has called for a national campaign to deal with the risks).

165 *See, e.g.*, Indictment, United States v. Huddleston, No. 1:17-CR-34 (E.D. Va. Feb. 28, 2018); Indictment, United States v. Hutchins, No. 2:17-CR-124 (E.D. Wis. July 11, 2017); Indictment, United States v. Yücel, No. 1:13-CR-834 (S.D.N.Y. June 24, 2015).

166 Press Release, Office of the White House Press Sec'y, Securing Cyberspace – President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat ("[The proposal] would allow for the prosecution of the sale of botnets, . . . [and] would expand federal law enforcement authority to deter the sale of spyware used to stalk or commit ID theft . . . ."). The DOJ advocated for adopting President Obama's legislative proposal to criminalize the sale of malware—which it termed, selling "means of access." *Prosecuting the Sale of Botnets and Malicious Software*, U.S. DEP'T OF JUSTICE (Mar. 18, 2015), https://www.justice.gov/archives/opa/blog/prosecuting-sale-botnets-and-malicious-software [hereinafter *Prosecuting the Sale*].

167 *See, e.g.*, *EFF Statement on President Obama's Cybersecurity Legislative Proposal*, ELECTRONIC FRONTIER FOUND. (Jan. 13, 2015), https://www.eff.org/deeplinks/2015/01/eff-statement-president-obamas-cybersecurity-legislative-proposal (arguing the EFF's position that prosecutors should have tools to investigate, disrupt, and prosecute cybercrime, but the government does not need more authority to conduct digital surveillance or prosecute criminals); Dustin Volz, *President Obama's New Cybersecurity Proposal is Already Facing Skepticism*, NAT'L J. (Jan. 13, 2015, 5:58 AM), https://www.nationaljournal.com/s/33607/president-obamas-new-cybersecurity-proposal-is-already-facing-skepticism ("Congress has repeatedly come up short on passing substantial cybersecurity packages, in part because of concerns from privacy groups.").

the sale of certain types of malware.[168] Given this admission, and that it is now prosecuting hackers for selling malware, the DOJ has arguably conceded that it is pushing the boundaries of § 1030(a)(5)(A).

The DOJ has thus far indicted three hackers for selling malware. The first was Alex Yücel, who was indicted on November 25, 2013, in the Southern District of New York.[169] Yücel was charged with violating § 1030(a)(5)(A), among other provisions, for running an organization called Blackshades that marketed and sold a RAT online.[170] Prosecutors stated that thousands of cybercriminals bought the RAT and used it to infect over half a million computers.[171] Yücel moved to dismiss the charges on the grounds that "protected computer," "damage," and "without authorization" were void for vagueness.[172] The district court disagreed and held that the statute's terms were not void.[173] Because Yücel did not argue that he had insufficient intent to commit the offense, the court did not interpret the statute's intent

---

168 The DOJ specifically stated that the CFAA might not cover selling botnets because selling or renting an existing botnet does not establish that the seller or renter was the party that hacked into the bots. *Prosecuting the Sale*, *supra* note 166 ("Current criminal law prohibits the creation of a botnet because it prohibits hacking into computers without authorization. It also prohibits the use of botnets to commit other crimes. But it is not similarly clear that the law prohibits the sale or renting of a botnet.").

169 Indictment, *Yücel*, No. 1:13-CR-834.

170 *Id.* at 3 (charging Yücel with violating § 1030(a)(5)(A) for selling "malicious software to others, enabling them to infect and remotely control victims' computers"); Press Release, U.S. Attorney's Office for the S. Dist. of N.Y., Manhattan U.S. Attorney and FBI Assistant Director-In-Charge Announce Charges in Connection with Blackshades Malicious Software that Enabled Users Around the World to Secretly and Remotely Control Victims' Computers (May 19, 2014), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection (stating Yücel owned the Blackshades organization and sold the RAT).

171 Press Release, U.S. Attorney's Office for the S. Dist. of N.Y., *supra* note 170.

172 Memorandum in Support of Defendant's Motion to Dismiss Count II as Void for Vagueness at 5–8, United States v. Yücel, 97 F. Supp. 3d 413 (S.D.N.Y. 2015) (No. 1:13-CR-834).

173 *Yücel*, 97 F. Supp. 3d at 416–22.

requirement.[174] In March 2015, Yücel pleaded guilty to violating § 1030(a)(5)(A).[175]

The second hacker prosecuted was Taylor Huddleston, who was indicted in the Eastern District of Virginia on February 16, 2017.[176] Huddleston marketed and sold licensing software called Net Seal—which hackers use to prevent malware buyers from pirating their malware—and a RAT called NanoCore.[177] Prosecutors alleged that Huddleston conspired to violate § 1030(a)(5)(A) by selling Net Seal to "cybercriminals" who would use it to prevent their customers from copying and distributing their malware without paying.[178] Huddleston allegedly gave Net Seal to a separately charged defendant, Zachary Shames, who used it in selling a keylogger to other people.[179] Shames made over a thousand PayPal payments to Huddleston for Net Seal.[180] Huddleston also advertised NanoCore on a hacker forum and distributed it to more than 350 people that he knew would use the program.[181] Almost five months after being indicted, Huddleston pleaded guilty to distributing NanoCore,[182] while prosecutors eventually dismissed the counts relating to Net Seal sales.[183]

---

174 *See* Memorandum in Support of Defendant's Motion to Dismiss Count II as Void for Vagueness, *Yücel*, 97 F. Supp. 3d 413 (No. 1:13-CR-834). Arguments about insufficient intent are likely to arise only at trial since this is a jury question. *See* COMM. ON FED. CRIMINAL JURY INSTRUCTIONS OF THE SEVENTH CIRCUIT, PATTERN CRIMINAL JURY INSTRUCTIONS OF THE SEVENTH CIRCUIT 53 (2012) (stating that trial judges' instructions as to intent will depend on the precise mental state required by a particular statute); NINTH CIRCUIT JURY INSTRUCTIONS COMM., MANUAL OF MODEL CRIMINAL JURY INSTRUCTIONS FOR THE DISTRICT COURTS OF THE NINTH CIRCUIT 89–93 (2010) (defining several mens rea elements for instructing juries); *see also* Ann Hopkins, *Mens Rea and the Right to Trial by Jury*, 76 CALIF. L. REV. 391, 397 (1988) (stating that when the Constitution was ratified, the "presence or absence of mens rea was a jury question").

175 Transcript of Plea Hearing, United States v. Yücel, No. 1:13-CR-834 (S.D.N.Y. June 24, 2015).

176 Indictment at 1, United States v. Huddleston, No. 1:17-CR-34 (E.D. Va. Feb. 23, 2018). Huddleston was specifically indicted for aiding and abetting computer intrusion. *Id.* While this Note focuses on direct liability under § 1030(a)(5)(A) for selling malware, there is also a question whether selling malware satisfies aiding and abetting liability given that federal courts have applied varying standards of whether an accomplice must act purposefully or knowingly. *See* Martin & Newhall, *supra* note 21, at 117–27 (discussing various theories for aiding and abetting liability, and the Supreme Court's complicity in creating the confusion).

177 Indictment at 4, *Huddleston*, No. 1:17-CR-34.

178 *Id.* at 2. Huddleston reportedly received over 25,000 payments for Net Seal. *Id.* at 4.

179 *Id.* at 4.

180 *Id.*

181 *Id.* at 10. NanoCore was allegedly used in a spear phishing scheme in which victims were tricked into downloading malware disguised as benign email attachments. *Id.* at 11.

182 Plea Agreement, *Huddleston*, No. 1:17-CR-34.

183 Motion to Dismiss, United States v. Huddleston, No. 1:17-CR-34 (E.D. Va. July 25, 2017).

The DOJ's third prosecution is against Marcus Hutchins, the hacker mentioned in the introduction, who was indicted on July 11, 2017, in the Eastern District of Wisconsin.[184] He was charged with six felony counts, only two of which were for violating § 1030(a)(5)(A).[185] Prosecutors alleged that Hutchins conspired with an unnamed, separately charged defendant to advertise and sell a banking malware called Kronos.[186] Kronos would install itself onto a victim's web browser and record keystrokes in an effort to steal banking credentials.[187] Hutchins reportedly created a video showing Kronos's functionality, continued to advertise it on forums throughout 2014, and eventually sold a version of Kronos in 2015 for $2000.[188] Hutchins's case is currently in the discovery phase.[189] If successfully defended, it could provide a framework for challenging the DOJ's attempts to expand the scope of § 1030(a)(5)(A).

In all the above cases, there are two fundamental problems with using § 1030(a)(5)(A) to prosecute the sale of malware. First, it is not clear that the hackers who sold malware satisfy § 1030(a)(5)(A)'s intent element.[190] Hackers who sell malware may only intend to profit from their skills; these individuals might know, but not intend, that their malware would be used to cause damage. Additionally, the structure and legislative history of § 1030(a)(5)(A) indicate that it was meant to punish defendants who directly hacked into computers rather than individuals who facilitated hacking by selling malware.[191] Second, it is unclear whether some types of malware in use today cause the type of harm that satisfies the CFAA's definition of "damage."[192]

---

184 Indictment, United States v. Hutchins, No. 2:17-CR-124 (E.D. Wis. July 11, 2017).

185 *Id.* Hutchins was also accused of violating 18 U.S.C. §§ 2511–12, which are not addressed in this Note. *Id.* at 7.

186 *Id.* at 3.

187 Sullivan, *supra* note 9. Kronos began appearing on Russian cyber black markets in 2014 and would cost around $7000. *Id.*

188 Indictment at 3, *Hutchins*, No. 2:17-CR-124.

189 *See* United States' Response to Motion to Compel Discovery, *Hutchins*, No. 2:17-CR-124 (responding to a defense motion seeking the government's evidence to help prepare for Hutchins's defense).

190 *See* Orin Kerr, *The Kronos Indictment: Is It a Crime to Create and Sell Malware?*, WASH. POST: VOLOKH CONSPIRACY (Aug. 3, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/08/03/the-kronos-indictment-it-a-crime-to-create-and-sell-malware/?utm_term=.3189c6088685 ("Hutchins and X [probably] knew that whoever bought the malware would use it illegally. But under the statute, mere knowledge isn't enough. For Hutchins and X to be liable on this count, causing the impairment of the availability and integrity of information must have been their goal.").

191 *See infra* Section III.A.

192 *See infra* Section III.B (explaining how some types of malware are not covered by the CFAA's definition of damage).

III
Fixing the CFAA's Intent and Damage Requirements

The difficulty with using § 1030(a)(5)(A) to prosecute the sale of malware is that hackers might simply intend to make money off of their skills rather than cause damage—and thus only have knowledge that damage could occur. Further complicating the analysis, only a handful of courts have examined § 1030(a)(5)(A)'s intent requirement. These cases and the CFAA's legislative history nonetheless provide a framework for understanding the statute's mens rea requirement. The CFAA's definition of damage presents similar problems given that some courts have interpreted the definition to cover cyberattacks when information is accessed but not destroyed, and some courts have not. The dual problems with using § 1030(a)(5)(A) to police the black market for malware leave Congress with the imperative to amend the statute if it wants to criminalize selling malware used for criminal purposes.

A. Selling Malware Is Not Covered by § 1030(a)(5)(A)'s Intent Requirement

Understanding the CFAA's mens rea element requires looking at the Model Penal Code's (MPC) descriptions of mens rea. While federal law does not wholly adopt the MPC's definitions (which are of course nonbinding), the CFAA's legislative history suggests that Congress was incorporating the MPC's mens rea formulations.[193] For example, according to the MPC, a person acts with intent when "it is his conscious object . . . to cause such a result,"[194] and the 1986 Senate report to the CFAA stated that intentional conduct must be the "person's conscious objective."[195] The 1986 report also describes knowledge as an awareness that "the result is practically certain to follow from [the defendant's] conduct, whatever his desire may be as

---

193 *See* S. Rep. No. 101-544, at 9 (1990) (stating that the "standard for recklessness used in the bill is taken from the Model Penal Code"); S. Rep. No. 99-432, at 5–6 (1986) (using the MPC's phrasing when referring to knowledge and intent); Orin S. Kerr, Computer Crime Law 100 (2d ed. 2009) ("[T]he legislative history of § 1030 suggests that its drafters wished to incorporate the MPC's mens rea provisions.").

194 Model Penal Code § 2.02(2)(a) (Am. Law Inst., 1962) (stating that a person acts with intent when "it is his conscious object to engage in conduct of that nature or to cause such a result").

195 S. Rep. No. 99-432, at 6 (1986) (stating how an intentional standard "designed to focus . . . prosecutions on those whose conduct evinces a clear intent to enter . . . computer files or data belonging to another" and how this standard means the "conduct or the causing of the result must have been the person's conscious objective").

to that result,"[196] while the MPC defines knowledge as an awareness "that it is practically certain that [the defendant's] conduct will cause such a result."[197]

Congress changed § 1030(a)(5)'s mens rea requirement in 1986, from knowledge to intent, for two reasons. First, Congress wanted to punish intentional, rather than mistaken, unauthorized access of a computer.[198] Second, Congress was worried the knowledge standard would risk imposing liability on someone who inadvertently stumbled into another person's computer files.[199] The 1986 report summed up these points by stating that the intent standard is "designed to focus Federal criminal prosecution on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another."[200]

The 1996 report drew a similar distinction between insiders and outsiders, but it also noted that insiders only face liability if they intend to cause damage, whereas outsiders could be guilty of causing damage at any mens rea.[201] The 1996 report framed § 1030(a)(5) as an offense for prosecuting the defendant's trespass on a computer, whether intentionally or otherwise.[202] The 1986 and 1996 reports evince Congress's focus on hackers who themselves broke into computers, rather than malware sellers.

Most federal courts that have interpreted the CFAA have done so in hacking cases that do not involve malware sellers,[203] and those courts that have dealt with violations of § 1030(a)(5)(A) have not delved deeply into the statute's mens rea element.[204] The most mean-

---

196 *Id.* (describing a mens rea of knowingly, which requires that one be aware "that the result is practically certain to follow from his conduct, whatever his desire may be as to that result" (quoting United States v. U.S. Gypsum Co., 438 U.S. 422, 445 (1978)).

197 MODEL PENAL CODE § 2.02(2)(b) (stating that a defendant acts knowingly when either "he is aware that his conduct is of that nature or that such circumstances exist" or "that it is practically certain that his conduct will cause such a result").

198 S. REP. NO. 99-432, at 5–6 (1986).

199 *Id.* at 6.

200 *Id.*

201 S. REP. NO. 104-357, at 11 (1996).

202 *Id.*

203 *See, e.g.*, Pulte Homes, Inc. v. Laborers' International Union North America, 648 F.3d 295 (6th Cir. 2011) (denying a motion to dismiss in a case where the defendant flooded the plaintiff's email inbox and phone voicemail, thus freezing its communications systems); Arience Builders, Inc. v. Baltes, 563 F. Supp. 2d 883 (N.D. Ill. 2018) (denying a motion to dismiss where a company alleged that a former employee deleted data without authorization prior to leaving the company to compete in a separate business); Exec. Sec. Mgmt., Inc. v. Dahl, 830 F. Supp. 2d 883 (C.D. Cal. 2011) (partially denying a motion for summary judgment where a company alleged that a former employee used a program to delete the company's data).

204 *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006) (interpreting whether deleting files falls under "transmission"); *Baltes*, 563 F. Supp. 2d at

ingful analysis of the statute's intent requirement comes from a Third Circuit case, interpreting the statute's mens rea requirement, and two district court cases, applying the Circuit's holding. In *United States v. Carlson*, the Third Circuit reviewed whether a defendant, Allan Carlson, violated § 1030(a)(5)(A) by sending thousands of emails to several addresses associated with Philadelphia sports journalists and the Philadelphia Phillies in hopes of informing journalists and the team's management of his perceived issues with the team.[205] Carlson specifically appealed on the grounds that he did not intend for the email addresses he spoofed—which he used to send the emails in the first place—to be damaged by a torrent of return emails.[206] The Third Circuit stated that to prove a violation of § 1030(a)(5)(A), prosecutors have to establish that the defendant "*deliberately* caused an impairment to the integrity or availability of data, a program, a system, or information."[207] The court held that there was sufficient circumstantial evidence for the jury to conclude that Carlson intended to cause damage to the spoofed addresses given Carlson's actions and his "internet savvy."[208]

Two district courts in Pennsylvania later used *Carlson* as a basis for interpreting § 1030(a)(5)(A)'s intent requirement. In *United States v. Prugar*, a court in the Middle District of Pennsylvania reviewed whether the defendant, Dariusz Prugar, intended to cause damage to his former employer's computer by deleting a log of his unauthorized computer access.[209] Prugar argued that he only intended to cover his tracks by deleting the access log, and that he did not intend for the system to malfunction.[210] The *Prugar* court cited *Carlson*'s interpretation of intent and ruled against Prugar on the grounds that the CFAA's definition of damage covered the access log he deliberately destroyed.[211] According to the court, whether Prugar intended to

884 (same); First Fin. Bank, N.A. v. Bauknecht, 71 F. Supp. 3d 819, 850–51 (C.D. Ill. 2014) (interpreting whether defendant caused damage by deleting files).

205 209 Fed. App'x 181, 183 (3d Cir. 2006). Carlson masked his email address so that the sender of the emails appeared to be from other entities—e.g., the FBI and the Phillies organization itself. *Id.* For example, on November 7, 2001, Carlson sent over 1000 emails titled, "The Mariner's[sic] Didn't Trade A–Rod" from the email address "SpecialProsecutor@fbi.gov" to six writers at a Philadelphia newspaper. *Id.* And on November 11, 2001, Carlson sent over 5000 emails titled, "Sign JASON GIAMBI" to one address at the Philadelphia Phillies. *Id.*

206 *Id.* at 185.

207 *Id.* at 184 (emphasis added).

208 *Id.* at 185.

209 No. 1:12-CR-267, 2014 WL 4716382, at *9 (M.D. Pa. Sept. 22, 2014).

210 *Id.*

211 *Id.*

cause a system malfunction was irrelevant because intending to delete the log was enough to make him guilty of violating the statute.[212]

Several years later, a court in the Eastern District of Pennsylvania examined *Carlson* and *Prugar* in a civil CFAA case, *QVC, Inc. v. Resultly, LLC*, while reviewing a motion to dismiss.[213] QVC sued Resultly, an advertising agency, alleging that Resultly used a program to overload QVC's servers by flooding it with web traffic.[214] The court examined *Carlson* and *Prugar*, noting that both cases hold that alleging a violation of § 1030(a)(5)(A) requires proof that "the defendant knew his actions would cause damage *and* that it was his conscious desire to take those actions."[215] The court ultimately dismissed the § 1030(a)(5)(A) count on the bases that Resultly's program could have flooded traffic because of a malfunction, and Resultly was not incentivized to shutdown QVC's website since it would not be able to make commissions on QVC online sales.[216] While these cases focused on instances in which the defendant was the direct attacker, they provide a framework for analyzing § 1030(a)(5)(A)'s intent requirement.

Looking to these three cases and the MPC definition of intent, the question becomes: in selling malware to someone who may or may not use it to attack another computer, is it a hacker's conscious object to cause damage? Put another way, does a hacker intend to cause damage by selling malware to someone who may use it to attack another computer, or does the seller simply have knowledge that damage will occur?[217] Given that hackers are increasingly aware that they can profit from making malware and selling it online, the answer to these questions appears to be that at least some hackers have the conscious objective only to make money by selling their skills via online markets.[218] Malware is often used for malicious activity and is clearly sold online to criminals who engage in cyberattacks.[219] But saying that malware is only sold to criminals and is only used for malicious activity ignores the multiple purposes it now serves. Hackers often want to get their hands on new malware to unpack it and further

---

[212] *Id.* at *10.

[213] 159 F. Supp. 3d 576 (E.D. Pa. 2016).

[214] *Id.* at 581.

[215] *Id.* at 593 (emphasis added).

[216] *Id.* at 594.

[217] *See* Kerr, *supra* note 189 (questioning whether Marcus Hutchins intended to cause damage or merely had knowledge damage would occur by selling Kronos malware).

[218] *See supra* notes 128–61 and accompanying text (recounting the development of white, gray, and black markets for computer vulnerabilities).

[219] *See supra* notes 149–61 and accompanying text (describing the black market for malware and the criminal organizations that populate these markets).

understand how it works or create defensive measures to fend it off.[220] It is possible, however, that a hacker who sells malware may have some basis to know that the malware will be used to damage another computer; their knowledge could depend on the type of malware sold and on what hacker forum.[221] But the problem with that proposition is that the hacker only has knowledge and not necessarily intent for the malware to cause damage. In using § 1030(a)(5)(A) to prosecute the sale of malware, the DOJ risks making bad law by conflating interpretations of knowledge and intent, and in turn, doing violence to the language of § 1030(a)(5)(A).

In addition to this textual problem with § 1030(a)(5)(A)'s intent requirement, there is also a basis to believe that Congress did not intend for this section to be used for prosecuting the sale of malware. The two congressional reports to the CFAA indicate that Congress envisioned § 1030(a)(5) as applying to individuals who commit malware attacks themselves and not those who traffic in programs that facilitate attacks. The 1986 Senate report described § 1030(a)(5) as a provision aimed at addressing attacks from outsiders, but it envisioned prosecuting defendants "whose conduct evinces clear intent to enter, without proper authorization, computer files or data belonging to another."[222] Congress's worry about potential insiders who were *using* a computer and mistakenly exceeding their authorization demonstrates its intent to cabin the statute to just those who used malware.[223] The 1986 alteration provides some basis for the notion that Congress tried limiting the CFAA's reach.

The 1996 Senate report noted how that year's amendments distinguished between damage by insiders and outsiders and indicated that liability would differ if someone trespassed as an outsider. The report explained that the amendments envisioned that "outside hackers who

---

220 *See* Martin & Newhall, *supra* note 21, at 99–101 (describing virtuous hacking); *see also* ZETTER, *supra* note 15, at 21–22, 118–19 (describing two cybersecurity experts who became fascinated with encryption and the cat-and-mouse game of intrusion detection); *supra* notes 136–39 and accompanying text (addressing bug bounty programs and third-party security firms who provide information on computer vulnerabilities to their private clients).

221 *See* Kim Zetter, *Dozens Nabbed in Takedown of Cybercrime Forum Darkode*, WIRED (July 15, 2015, 4:48 PM), https://www.wired.com/2015/07/dozens-nabbed-takedown-cybercrime-forum-darkode/ (reporting on an online forum, called Darkode, that catered to cybercriminals buying and selling hacking tools); Press Release, U.S. Dep't of Justice, AlphaBay, the Largest Online "Dark Market," Shut Down (July 20, 2017), https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down (disclosing that prosecutors shut down a dark web market, AlphaBay, where people sold malware, as well as guns, drugs, and counterfeit goods).

222 S. REP. NO. 99-432, at 6 (1986).

223 *Id.* at 5–6 (explaining the reasons for changing the scienter requirement from "knowingly" to "intentionally").

break into a computer could be punished for any intentional, reckless, or other damage they cause by their *trespass*."[224] The report further explained that "anyone who knowingly *invades* a system without authority and causes significant loss to the victim should be punished . . . ."[225] By using words like trespass or invade, Congress provided some basis to think of § 1030(a)(5)(A) as an offense where the defendant was the person who directly attacked, trespassed, or invaded the computer system.

The DOJ's attempt to expand the scope of § 1030(a)(5)(A) to circumstances of selling malware risks expanding the scope of the statute in ways that Congress did not intend. Prosecutors attempted something similar when they used common law crimes as a basis for attempting to prosecute early computer crimes.[226] However, these cases reached mixed results, in which judges were outcome oriented, and there was little coherence to computer crime prosecutions.[227] Prosecutors risk creating a similar situation of disparate decisions if they continue using § 1030(a)(5)(A) without updating the CFAA.

B. Not All Malware Is Covered by the CFAA's Definition of "Damage"

Federal courts have struggled to settle on how much harm satisfies the CFAA's definition of "damage." While the CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information,"[228] some courts have interpreted it broadly to encompass instances where data on a computer was only stolen and not made inaccessible. In *Yücel*, the court held that the definition required prosecutors to prove both that a computer no longer operated as it did when the owner first possessed it and that the damage would negatively impact the economic value of the computer.[229] This interpretation sweeps far enough to cover the act of breaching the confidentiality or integrity of information on a system, and does not require preventing a user from accessing the informa-

---

[224] S. REP. NO. 104-357, at 11 (1996) (emphasis added).

[225] *Id.* (emphasis added).

[226] *See supra* notes 32–40 and accompanying text (chronicling the early days of using common law offenses to prosecute computer misuse).

[227] *See* Kerr, *supra* note 22, 1610–13 (noting that "courts tended to reach results-oriented outcomes" when faced with tough questions about how property crimes covered computer misuse).

[228] 18 U.S.C. § 1030(e)(8) (2012).

[229] United States v. Yücel, 97 F. Supp. 3d 413, 420 (S.D.N.Y. 2015).

tion.[230] The court examined the 1996 Senate report to § 1030(a)(5) and determined that Congress intended "damage" to be broad since it meant to capture using a keylogger that required expending resources to resecure the system.[231] The Ninth Circuit took a similarly broad view of "damage" in *United States v. Middleton*.[232] Middleton was charged with violating § 1030(a)(5)(A) for gaining unauthorized access to an administrative computer belonging to his former employer, then changing administrative passwords, altering the computer's registry, and deleting billing data.[233] In rejecting Middleton's argument that the jury was improperly instructed as to the definition of "damage," the Ninth Circuit held that "damage" included any loss of data, or the cost to restore or resecure the computer.[234]

Several courts have taken the opposite view of "damage," finding that damage only occurs when the computer data is destroyed or no longer accessible. In *Trademotion, LLC v. Marketcliq, Inc.*,[235] a district court in the Middle District of Florida analyzed whether a company "damaged" a competitor's computer by causing the plaintiff's former vice president to delete the plaintiff's computer files and insert code onto the plaintiff's online software that would divert prospective clients from the plaintiffs to the defendants.[236] The court focused on the term "integrity" in the definition of "damage," and it reasoned that integrity "requires 'some diminution in the completeness or usability of data or information on a computer system.'"[237] Several judges in the Northern District of Illinois have reached a similar conclusion, holding that "merely copying electronic information from a computer system does not satisfy the 'damage' element because the CFAA only recognizes damage to a computer system when the viola-

230 *See id.* ("The government is expected to offer evidence that when the Blackshades RAT is surreptitiously loaded onto a computer, the computer no longer operates only in response to the commands of the owner.").

231 *Id.* at 420–21 ("The Report's example [of a password stealing program] is strikingly similar to the RAT's keylogger function, which also copied passwords to Blackshades users' computers.").

232 231 F.3d 1207 (9th Cir. 2000).

233 *Id.* at 1209.

234 *Id.* at 1213; *see also* Matthew Andris, Comment, *The Computer Fraud and Abuse Act: Reassessing the Damage Requirement*, 27 J. MARSHALL J. COMPUTER & INFO. L. 279, 287 (2009).

235 857 F. Supp. 2d 1285 (M.D. Fla. 2012).

236 *Id.* at 1288.

237 *Id.* at 1292 (quoting Resdev, LLC v. Lot Builders Ass'n, No. 6:04-CV-1374ORL31DAB, 2005 WL 1924743, at *5 n.3 (M.D. Fla. Aug. 10, 2005)). The court ultimately held that the plaintiffs failed to establish damage by simply arguing they needed to only plead loss, and not damage as well, under the CFAA. *Id.*

tion causes a diminution in the completeness or usability of the data on a computer system."[238]

These competing interpretations are problematic because some forms of malware neither delete data nor make it inaccessible. Ransomware, which has characteristics of a worm and a virus, is a clear example of malware that makes computer files inaccessible, which it does through encrypting the data until the victim pays a ransom.[239] Other forms of malware—like keyloggers, Trojans, or backdoors—function quite differently in that they steal, but do not destroy, information.[240] Information stealers, such as keyloggers, only surreptitiously send private information back to an attacker.[241] As courts have disagreed on whether "damage" covers any impairment of the security of computer data or just the deletion or inaccessibility of the data, some forms of malware seem to fall under the CFAA and some are outside its scope.

While reasonable courts have differed on interpreting "damage," the stronger argument appears to be that "damage" does not adequately cover some types of malware. While the 1996 Senate report speaks broadly on keyloggers and the insecurity of data, it states that "'damage' will require . . . significant financial losses,"[242] which evinces a focus on financial harm and not mere insecurity of information. A majority of courts have essentially adopted this position, reasoning that merely copying information is not damage[243] and that the CFAA "is not intended to expansively apply to all cases where a trade

---

238 Cassetica Software, Inc. v. Computer Scis. Corp., No. 09-C-0003, 2009 WL 1703015, at *3 (N.D. Ill. June 18, 2009); *see also* Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l, Inc., 616 F. Supp. 2d 805, 811 (N.D. Ill. 2009) ("[C]opying electronic files from a computer database . . . is not enough to satisfy the damage requirement of the CFAA; there must be destruction or impairment to the integrity of the underlying data."); Motorola, Inc. v. Lemko Corp., 609 F. Supp. 2d 760, 769 (N.D. Ill. 2009) ("The plain language of the statutory definition refers to situations in which data is lost or impaired because it was erased or because (for example) a defendant smashed a hard drive with a hammer.").

239 *See* SYMANTEC: THREAT INTELLIGENCE BLOG, *supra* note 1 (describing how ransomware, specifically WannaCry, functions); 22 SYMANTEC, *supra* note 157, at 58–62 (analyzing how ransomware is typically disseminated, how it affects businesses, and current trends in recent attacks).

240 *See supra* notes 109–20 and accompanying text.

241 *See* AYCOCK, *supra* note 98, at 13–14, 16–17 (explaining the ways Trojans, backdoors, and spyware are used to steal information); Sullivan, *supra* note 9 (describing the Kronos keylogger malware that stole banking credentials).

242 S. REP. NO. 104-357, at 11 (1996).

243 *See* Peter J.G. Toren, *Computer Fraud and Abuse Act*, LANDSLIDE, May/June 2017, at 42, 44 (noting courts are split on whether copying amounts to damage but that a majority position holds that it is not).

secret has been misappropriated by use of a computer."[244] In concluding that merely copying information does not constitute damage, courts have held that copying information does not impair the integrity of that data, and that data must be destroyed or impaired for "damage" to occur.[245] In sum, the CFAA's definition of "damage" is increasingly inappropriate for the reality we live in today, where criminals use information stealers to acquire private information, like banking credentials or corporate secrets.

C. Amending the CFAA to Deal with Selling Malware

Prosecutors risk doing violence to the CFAA's language if they continue using it to prosecute hackers selling malware. Firstly, Congress evinced its intent to have § 1030(a)(5)(A) used against hackers who directly used malware, not those who sold it.[246] Prosecutors also risk conflating knowledge and intent, making bad law for the CFAA, by altering the meaning of intent not only in § 1030(a)(5) but also in § 1030(a)(2), as the 1986 Senate report stated that the mens rea requirements in both provisions are supposed to match.[247] Secondly, prosecutors risk creating inconsistent outcomes given that some malware does not fit the definition of "damage." For example, prosecutors may be able to go after hackers, like Hutchins or

---

244 U.S. Gypsum Co. v. LaFarge N. Am., Inc., 670 F. Supp. 2d 737, 744 (N.D. Ill. 2009); *see also* Landmark Credit Union v. Doberstein, 746 F. Supp. 2d 990, 993 (E.D. Wis. 2010) (stating that seemingly every court in the Seventh Circuit has held that copying information does not constitute damage under the CFAA). Courts that have held as much have done so based on three premises: First, the CFAA is not intended to apply to cases where trade secrets were misappropriated; second, merely copying data does not impair the integrity of information; third, and relatedly, courts require the data be destroyed or impaired. *See, e.g.*, NetApp, Inc. v. Nimble Storage, Inc., No. 5:13-CV-05058-LHK (HRL), 2015 WL 400251, at *11–12 (N.D. Cal. Jan. 29, 2015) (collecting cases holding that merely copying data does not state a claim for damage under the CFAA, and describing the three premises on which those cases are based).

245 *See, e.g.*, New S. Equip. Mats, LLC v. Keener, 989 F. Supp. 2d 522, 530 (S.D. Miss. 2013) ("[T]he mere copying of electronic information from a computer system is not enough to satisfy the CFAA's damage requirement.") (citation omitted); Capitol Audio Access, Inc. v. Umemoto, 980 F. Supp. 2d 1154, 1157–58 (E.D. Cal. 2013) (rejecting the assertion that "access to a publication and the disclosure of its information satisfies the CFAA's definition of damage"); Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l, Inc., 616 F. Supp. 2d 805, 811 (N.D. Ill. 2009) (reasoning that copying files from a database is insufficient to satisfy the CFAA's damage requirement); Worldspan, L.P. v. Orbitz, LLC, No. 05 C 5386, 2006 WL 1069128, at *5 (N.D. Ill. Apr. 19, 2006) (rejecting the plaintiff's argument that taking information constitutes damage); *see also NetApp, Inc.*, 2015 WL 400251, at *11–12 (collecting cases holding that copying information does not impair its integrity).

246 *See supra* notes 76–79 and accompanying text.

247 S. REP. NO. 99-432, at 10 (1986) ("The 'intentional' standard is the same as that employed in Section 2(a)(1) and 2(b)(1) of the bill.").

Huddleston, but unable to go after someone selling a botnet.[248] And if § 1030(a)(5)(A) is incapable of addressing malware markets, we can only deal with this newfangled problem by amending the statute.

Policing the black market for malware requires a different conceptual basis than the one for § 1030(a)(5)(A). The CFAA's hacking statute was focused on outsiders who broke into or trespassed on a computer,[249] but since selling malware does not involve that conduct, policing the black market requires a statute to focus on transactions for malware. One starting point is President Obama's legislative proposal. The legislative proposal would have criminalized selling the "means of access" to another computer by adding this language to § 1030(a)(6)—which punishes "knowingly and with intent to defraud traffic[king] . . . in any password or similar information through which a computer may be accessed without authorization."[250] The proposal would also replace the "intent to defraud" requirement with a requirement that the government prove that the defendant knew or should have known that the "means of access" would be used to hack a computer or cause damage.[251] The legislative proposal also attempts to address the problems with the definition of "damage" by allowing the government to prove knowledge that the means of access would be used to hack a computer, but not require proof of a statutorily defined type of damage.[252] An amended statute should, ultimately, punish whoever sells the means of accessing a protected computer while knowing, or acting with reason to know, that the means would be used to enter the protected computer without authorization.

The United Kingdom crafted a similar statute that can serve as a template for amending the CFAA. In 2006, Parliament enacted the Police and Justice Act, which made it a crime to "suppl[y] or offer[ ] to supply any article believing that it is likely to be used" to commit or aid in the commission of another hacking offense.[253] When it was passed, the statute was criticized because of its less demanding mens rea of "belief," which critics argued could be used to go after ethical

---

[248] *See Prosecuting the Sale*, *supra* note 165 (pointing out that selling a botnet does not clearly fit under the CFAA's proscriptions).

[249] *See supra* notes 76–79 and accompanying text.

[250] 18 U.S.C. § 1030(a)(6) (2012).

[251] *Prosecuting the Sale*, *supra* note 165.

[252] *See id.* (stating that an element of the proposed statute would be that the defendant "knew or should have known that the means of access would be used to hack or damage a computer").

[253] Police and Justice Act 2006, c. 48, § 37 (Eng.), https://www.legislation.gov.uk/ukpga/2006/48/contents (amending the Computer Misuse Act 1990 by adding section 3A, which consisted of three new offenses; section 3A(2) made it a crime to supply malware with a "belief" it could be used to commit a hacking offense). The statute defined "article" as "any program or data held in electronic form." *Id.*

hackers given that a "belief" mens rea is more demanding than mere suspicion but less than knowledge.[254] While Congress would likely face similar criticisms if it amended the CFAA, a "knowingly" mens rea strikes a balance between an intent and recklessness standard that would, respectively, either make it too difficult or too easy to go after hackers. A "knowingly" mens rea would hold hackers liable when they had a basis to know their malware would be used to access another computer but at the same time not overly penalize them when they sell their malware without indicia that it would be used maliciously. The strength of a knowingly standard, nonetheless, may depend on how expansive a view courts take on what evidence proves knowledge.

Conclusion

The CFAA must be revised to address the rise in malware attacks for illicit financial gain. The malware black market has created a space in which malware can be bought and sold as a commodity. Its value on the black market will only continue to rise as more black market participants realize it is a more stable commodity than banking credentials, which is a reality that poses a greater risk to people everywhere. But § 1030(a)(5)(A)'s text and legislative history illustrate how inadequately it criminalizes the sale of malware. Congress must not shirk its responsibilities, and it must revisit proposals to amend § 1030(a)(5)(A) to address this problem.

---

254 *See* Alisdair A. Gillespie, Cybercrime 72–73 (2015) (describing criticisms of section 3A(2)'s mens rea of "belief" that could be used to go after people who create malware for legitimate tasks).