ON THE COST OF BOTNET ATTACKS: INCREASING IOT MANUFACTURER ACCOUNTABILITY

Nicholas Eitsert

A. INTRODUCTION

On October 21st, 2016, domain name registration service Dyn, Inc. experienced a significant outage severing access to major internet services throughout North America and Europe.[1] Users were unable to reach popular websites such as Amazon.com and Twitter.com for as long as twelve hours before Dyn staff resolved the issue. Similar phenomena occurred several other times in 2016. In November, roughly 900,000 customers of German telecommunications company Deutsche Telekom experienced an internet blackout as popular internet routers simultaneously failed.[2] During the same month, internet infrastructure in Liberia crashed, resulting in a full internet blackout.[3] These outages, and many others, have one commonality: they were caused by intentional attacks carried out using armies of hijacked internet devices known as botnets.

Botnet attacks typically block authorized users from utilizing internet services by performing distributed denial of service (DDoS) attacks. DDoS attacks knock websites offline by consuming as many network resources as possible and crashing the application or occupying all available bandwidth. Hackers with more hijacked internet devices at their disposal can consume more network resources and increase the damage caused by an attack.

Hackers have historically used personal computers to perform DDoS attacks. Since the early 2000s, a new, more vulnerable target for infection has emerged. The Internet of Things (IoT) refers to the global network of connected devices featuring Internet Protocol (IP) connectivity. Electronics and appliance manufacturers have become increasingly enthusiastic about creating IoT devices by adding internet connected features to a variety of non-traditional devices. These include smart refrigerators, security cameras, and printers. In fact, the number of non-traditional connected IoT devices has nearly tripled over the past five years. To meet the growing demand, IoT devices must be developed swiftly and inexpensively, which often

---

[1] Tim Greene, *How the Dyn DDoS attack unfolded*, NETWORK WORLD (Oct. 26, 2016, 7:52 P.M.), https://www.networkworld.com/article/3134057/how-the-dyn-ddos-attack-unfolded.html.

[2] Eduard Kovacs, *German ISP Confirms Malware Attacks Caused Disruptions*, SECURITY WEEK (Nov. 29, 2016), https://www.securityweek.com/german-isp-confirms-malware-attacks-caused-disruptions.

[3] John Leyden, *Mirai IoT botnet blamed for 'smashing Liberia off the internet'*, REGISTER (Nov. 4, 2016, 4:40 P.M.), https://www.theregister.co.uk/2016/11/04/liberia_ddos/.

results in the creation of consumer products that are poorly secured. These products often suffer from security failures as simple as open configuration ports,[4] hardcoded backdoors,[5] and unchanged factory default passwords.[6] Hackers have developed malware specifically designed to exploit common vulnerabilities of IoT devices and create botnets.

The effects of botnet-based cyberattacks are far more serious than brief interruptions from 21st century conveniences. In July of 2014, Microsoft assistant general counsel Richard Boscovich addressed the Senate Judiciary Committee on Crime and Terrorism on the emerging threat of botnet attacks. Boscovich described $500 million in losses caused by the Citadel botnet and $70 million resulting from the Zeus botnet.[7] FBI Director Christopher Wray addressed the Homeland Security and Government Affairs Committee of the United States Senate in 2017, outlining threats to the U.S. resulting from botnet-conducted cybercrime. Director Wray estimated the annual losses to the U.S. economy from botnet attacks lying "in the order of several billion dollars" per annum.[8] Most of these costs fall on companies and consumers that are unable to rely on web-based services or participate in web-based sales and web hosting providers that are tasked with resolving service issues. Meanwhile, the IoT manufacturers whose unsecure devices provide hackers with the power to execute these attacks are responsible for little, if any, of the resulting costs.

B. BOTNET PREVENTION: EXISTING LAW

1. Enforcement of 18 U.S.C.S. § 1030 (CFAA) Against Botnet Operators

The most obvious remedy for recovering losses due to botnet attacks is for the government to criminally prosecute botnet operators

---

[4] Johannes B. Ullrich, *TR-069 NewNTPServer Exploits: What we know so far*, SANS ISC INFOSEC F. (Nov. 29, 2016), https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/.

[5] Paul Ducklin, *D-Link router flaw lets anyone login through "Joel's Backdoor"*, NAKED SECURITY (Oct. 15, 2013), https://nakedsecurity.sophos.com/2013/10/15/d-link-router-flaw-lets-anyone-login-using-joels-backdoor/.

[6] Douglas Bonderud, *Leaked Mirai Malware Boosts IoT Insecurity Threat Level*, SECURITY INTELLIGENCE (Oct. 4, 2016), https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/.

[7] *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 113th Cong. (2014) (statement of Richard Domingues Boscovich, Assistant General Counsel, Microsoft Digital Crimes Unit).

[8] *Threats to the Homeland: Hearing Before the S. Comm. on Homeland Security and Gov. Affairs*, 115th Cong. (2017) (statement of Christopher A. Wray, Director of the FBI).

and demand restitution as a part of sentencing. The Computer Fraud and Abuse Act (CFAA), 18 U.S.C.S. § 1030, provides the framework for such a resolution.

In 2004, an FBI Cyber Crimes squad nabbed a group of hackers known as the "DDoS Mafia" in Operation Cyberslam. Four US citizens and one UK citizen were accused of performing a ten-day long DDoS attack on websites of competitors of businessman Jay Echouafni and charged with violating the CFAA.[9] The hackers reportedly unleashed their 38,000 IoT bots on Echouafni's competitors for just $1,000 USD.[10] Unfortunately for the hackers, the DDoS attack was so potent that it erroneously blocked access to other services hosted by the service provider, Speedera, including the US Department of Homeland Security website. This likely brought increased scrutiny from the FBI and landed the group an additional charge under 18 U.S.C. § 371. Given the severity of the charges, the members of the 'DDoS mafia' fared well. Of the five members, only two were sentenced to prison and for no more than two years.[11] Despite these lenient sentences, Operation Cyberslam has been called "the first successful investigation of a large-scale distributed denial of service attack (DDoS) used for a commercial purpose in the United States."[12]

In *United States v. Gasperini*, Fabio Gasperini, an Italian citizen and resident of the Netherlands, used his botnet to perpetrate click fraud.[13] Gasperini was convicted of misdemeanor computer intrusion under 18 U.S.C. § 1030(a)(2) for infecting at least 2,000 devices in the US with his botnet software and was sentenced to the statutory maximum of twelve months imprisonment and a $100,000 fine.[14] While this may seem like a success for the CFAA and the FBI, Gasperini's twelve-month sentence is negligible compared to the seventy years he faced.

---

[9] Complaint at 2–3, United States v. Ashley (Aug. 25, 2004), https://www.reverse.net/operationcyberslam.pdf (charges following this complaint were dropped, but further action was taken in 2006).

[10] *Id*. at 18.

[11] *See* United States v. Roby, No. 04-704(c) (C.D. Cal. 2005); Brian Krebs, *Hired Internet Gun Sentenced to Two Years*, WASH. POST (May 1, 2006, 3:07 P.M.), http://voices.washingtonpost.com/securityfix/2006/05/hired_internet_gun_sentenced_t_1.html.

[12] Lucian Constantin, *European Botnet Runners Indicted in the FooNet DDoS Case*, SOFTPEDIA NEWS (Oct. 4, 2008, 11:03 A.M.), https://news.softpedia.com/news/European-Botnet-Runners-Indicted-in-the-FooNet-DDoS-Case-94919.shtml.

[13] United States v. Gasperini, No. 16-CR-441, 2017 U.S. Dist. LEXIS 114166, affrm'd, United States v. Gasperini, 729 Fed. Appx. 112 (2d Cir. 2018).

[14] Press Release, U.S. Dep't Justice, Cybercriminal Convicted of Computer Hacking and Sentenced to Statutory Maximum (Aug. 9, 2017), https://www.justice.gov/usao-edny/pr/cybercriminal-convicted-computer-hacking-and-sentenced-statutory-maximum.

After trial, Gasperini's defense team enthusiastically pointed out where the prosecution erred. CQURE Academy, analysts for the defense, claimed that the FBI collected incomplete evidence and failed to follow correct procedure. Specifically, "due to the international cooperation with several countries[, e]ach of these countries used their own procedure for evidence collection."[15] Gasperini's experts were easily able to draw attention to flaws in the government's evidence and have Gasperini acquitted on all five felony charges he faced, leaving only the lesser-included misdemeanor offense of computer intrusion. Perhaps most importantly, extraterritorial prosecutions under the CFAA require international cooperation. The prosecution of Gasperini would have been impossible if not for the Netherlands Ministry of Security and Justice and the Italian Postal and Telecommunications Service. Had Gasperini resided in a country with hostility towards the US, he never would have been extradited to face trial in the first place.

Criminal enforcement under the CFAA ultimately fails to dissuade botnet operators from performing attacks and is unsuccessful at recovering damages for injured parties because botnet operators typically reside and house assets beyond the jurisdiction of the US, most frequently in countries unfriendly towards the US.[16] Further, even those operating within the US lack the assets to cover the damages caused and typically receive light penalties.

2. Federal Trade Commission Enforcement of 15 U.S.C. § 45

A more obscure method for preventing botnet attacks involves incentivizing manufacturers to secure IoT devices against unauthorized breaches by botnet operators. The Federal Trade Commission (FTC), the US agency charged with preventing unfair competition and unfair or deceptive acts or practices in or affecting commerce, incentives IoT manufacturers with the threat of litigation. In 2015, The United States Court of Appeals for the Third Circuit decided *FTC v. Wyndham Worldwide Corp*., wherein the FTC attempted to exert its regulatory power over Wyndham Worldwide Corp to force the maintenance of stronger cybersecurity standards.[17] The Court, rejecting a variety of arguments raised by Wyndham, denied Wyndham's motion to dismiss and suggested that unsafe cybersecurity practices violate 15 U.S.C. § 45(a).[18] Wyndham later

---

[15] Paula Januszkiewicz, *How we helped keep an alleged "hacker" out of 70 years in prison*, CQURE ACADEMY (Aug. 2017), https://cqureacademy.com/blog/identity-theft-protection/fabio-gasperini-case.

[16] Lesley Stahl, *The growing partnership between Russia's government and cybercriminals*, CBS NEWS (Apr. 21, 2019), https://www.cbsnews.com/news/evgeniy-mikhailovich-bogachev-the-growing-partnership-between-russia-government-and-cybercriminals-60-minutes/.

[17] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

[18] *Id*. at 16–21.

settled the case, and the FTC has since used this regulatory power to check the cybersecurity standards of IoT device manufacturers.

FTC v. AsusTeK Computer, Inc.

Asus released a new feature for its wireless routers called "AiCloud" in 2012. AiCloud allowed users to access removable media connected to their wireless router from anywhere with an internet connection. AiCloud, however, contained several security vulnerabilities that allowed anyone with the router's easily discoverable IP address to login to the portal without a username or password.[19] An attacker could subsequently access the removable media and the router's configuration settings.

The FTC filed a formal complaint against Asus over security vulnerabilities relating to AiCloud and other well-known router exploits in 2014.[20] The complaint stated five counts, the first four asserting that Asus made misrepresentations relating to the security of its router. The FTC's final allegation, titled "Unfair Security Practices," simply states that Asus "failed to take reasonable steps to secure the software for its routers . . . . This practice is an unfair act or practice," suggesting that the FTC views poor security standards as an inherently unfair practice.[21] Asus settled the complaint with the FTC in 2016 by agreeing to conduct biannual, independent security audits for the next twenty years.[22]

Asus routers had also been exploited by botnet operators, but the FTC failed to introduce such evidence in this complaint. Rather, the FTC focused primarily on the AiCloud vulnerabilities that allowed hackers to access personal files, including pictures, tax returns, and emails. The FTC likely chose to ignore evidence of Asus routers being compromised by botnet operators due to the difficulty of proving injury to consumers. 15 U.S.C.S. § 45(n) states, "[the FTC] shall have no authority . . . to declare unlawful an act or practice . . . unless the act or practice causes or is likely to cause substantial injury to consumers . . . ." If the FTC cannot prove injury to consumers, it cannot declare a practice unlawful. While open, unsecured access to personal information by unauthorized third parties drastically increases a consumer's likelihood of falling victim to identity theft or ransomware and thus clearly causes injury to consumers, consumers are typically not targeted by botnet operators. Rather, botnet operators use compromised consumer devices to perform attacks against

[19] Complaint at 2–3, In Re ASUSTek Computer, 705 Fed. Appx. 956 (Fed. Cir. 2017), https://www.ftc.gov/system/files/documents/cases/160222asuscmpt.pdf.
[20] *Id*.
[21] *Id*. at 10.
[22] Agreement Containing Consent Order at 6, In Re ASUSTek Computer, 705 Fed. Appx. 956 (Fed. Cir. 2017), https://www.ftc.gov/system/files/documents/cases/160222asusagree.pdf.

websites and other internet services indirectly associated with Asus's consumers.

FTC v. D-Link

The routers and cameras produced by D-Link were also riddled with vulnerabilities. The FTC filed a complaint against D-Link relating to IoT device security just months after the settlement with Asus was approved.[23] Borrowing from the success of the grievance against Asus, the FTC developed a complaint against D-Link that is almost a mirror image. After having a motion for summary judgement denied, D-Link settled and agreed to conduct biannual, independent security audits and maintain a software security program. Again, the FTC chose to focus on risks directly harming consumers rather than botnet creation.

Review of FTC's Enforcement of 15 U.S.C. § 45

While the FTC has significantly broadened its regulatory authority to encourage IoT manufacturers to adopt strengthened security standards, the FTC's regulatory authority and jurisdiction are not broad enough to promote lasting change in the security policies of the IoT industry. First, the FTC is limited to regulating unfair or deceptive acts. While the FTC may wish to interpret poor security policies as an unfair practice per se, the courts have suggested that this is not the case. A California district court judge partially dismissed the FTC's case against D-Link during litigation, without prejudice, because "[t]he FTC [did] not identify a single incident where [a consumer] suffered any harm or even simple annoyance and inconvenience from the alleged security flaws in the DLS devices. . . . [T]he FTC cannot rely on wholly conclusory allegations about potential injury to tilt the balance in its favor."[24] Thus, poor cybersecurity standards alone are not enough to satisfy the court, and the FTC cannot prove unfairness unless it can show direct, real harm to consumers. Since *Asus* and *D-Link* both involved stolen files and identity theft, the FTC easily amended its complaints to overcome the judge's objection. A matter solely concerning poor security policies that result in the creation of botnets would be considerably more difficult to prosecute as botnet attacks rarely cause direct harm to Asus's customers.

Second, the settlement agreements signed in *Asus* and *D-Link* are too lenient. The FTC imposed no monetary penalty, criminal

[23] Complaint, FTC v. D-Link Sys., Inc., 2018 U.S. Dist. LEXIS 199023, (N.D. Cal. 2018), https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf.

[24] Mallory Locklear, *FTC lawsuit over D-Link's lax router security just took a big hit*, ENGADGET (Sept. 21, 2017), https://www.engadget.com/2017/09/21/ftc-lawsuit-d-link-lax-router-security-took-hit/.

charge, or injunction on the defendants. Instead, these manufacturers are solely bound to maintain basic security policies. This is hardly an adequate punishment and provides little encouragement for other manufactures to adopt these policies proactively.

C. BOTNET PREVENTION: PROPOSED LAW

Internet of Things Cybersecurity Improvement Act

The Internet of Things (IoT) Cybersecurity Improvement Act was first introduced in the Senate in 2017. Rather than relying on criminal penalties to deter botnet operators, the IoT Cybersecurity Improvement Act of 2017 required that government departments and contractors only purchase IoT devices that meet basic security standards.[25] In doing so, the sponsors of the bill trusted that the immense purchasing power of the federal government would ignite an industry-wide change in security standards. As expressed by CNET Magazine, "[t]he hope is that by improving security standards for the federal government, one of the largest customers available, standards for the entire IoT market would improve along with it."[26]

The IoT Cybersecurity Act of 2017 would primarily require federal agencies to add clauses in contracts with suppliers that prevent the utilization of IoT devices with known vulnerabilities listed in the National Vulnerability Database (NVD) in government projects. The NVD, which is maintained by the National Institute of Standards and Technology (NIST), contains over 120,000 known vulnerabilities, including those that allow botnet operators to easily infect IoT devices.[27] Clauses in the IoT Cybersecurity Act of 2017 would force government contractors to employ IoT devices that only accept trusted updates from the vendor, use up-to-date industry protocols, and do not include any hard-coded credentials.

The IoT Cybersecurity Improvement Act was praised by the internet community. Popular science fiction author Bruce Sterling, writing for Wired Magazine, stated that "[t]his legislation probably makes way too much sense to ever get passed by the current Congress."[28] Despite strong industry support, the bill died in the

---

[25] Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S. 1691, 115th Cong. (2017).

[26] Alfred Ng, *Congress introduces bill to improve 'internet of things' security*, CNET (Mar. 11, 2019, 3:42 P.M.), https://www.cnet.com/news/congress-introduces-bill-to-improve-internet-of-things-security/.

[27] NATIONAL VULNERABILITY DATABASE, NIST, https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&search_type=all (last visited Nov. 6, 2019).

[28] Bruce Sterling, *Spime Watch: the fact sheet for the Internet of Things Cybersecurity Improvement Act of 2017*, WIRED (Aug. 11 2017, 5:02 A.M.), https://www.wired.com/beyond-the-beyond/2017/08/spime-watch-fact-sheet-internet-things-cybersecurity-improvement-act-2017/.

115th Congress. Similar bills were presented in 2018 and 2019 with the latter still pending in the House and the Senate.

Review of Proposed Law

The IoT Cybersecurity Improvement Act allows the NIST to maintain a dynamic database of vulnerabilities that government IoT devices must be protected against. Since hackers are constantly finding new weaknesses in IoT devices, it is logical to allow the NIST to maintain up-to-date security standards. However, if the NIST produces security standards that are too stringent, the market for IoT devices will simply split their IoT product lines into two categories: one for government sector devices and another for consumer sector devices. The concept of economies of scale suggests that manufacturers will only segment the market if the cost of implementing these security standards increases the cost of preserving uniformity between consumer and government devices beyond the benefit. Thus, it is vital that the NIST promotes standards which are economically achievable.

The 2019 bill is narrowly tailored to attack the root of the IoT problem without imposing criminal liability or regulating non-governmental activity. This narrowness creates its own issues, however, as some companies may be indifferent to regulations imposed on US government contractors. Companies based in Russia and China, for example, rarely succeed in obtaining US government contracts when US-based alternatives exist. The IoT Cybersecurity Improvement Act provides no incentive for manufacturers in these countries to increase the security of their products. Considering that demand for consumer grade electronics is highly elastic, these companies could increase their market share by continuing to offer unsecure, but inexpensive, IoT products in the US. This could lead to a segmented market with a consumer market dominated by unsecure products produced by foreign manufactures and a government market served by more secure, more expensive brands. Thus, while the IoT Cybersecurity Act of 2019 is an excellent attempt at reducing the prevalence and cost of botnet attacks, more complete legislation that considers the market economics for consumer electronics should be proposed.

D. BOTNET PREVENTION: PROPOSED SOLUTION

Building on the analysis of the botnet prevention schemes discussed above, this author has pinpointed five areas to be addressed by comprehensive anti-botnet legislation necessary to ensure that botnet operators face an appropriate deterrent effect and that device manufacturers share the costs that their unsecure devices impose on society.

1. Prohibition of Default Authentication Credentials

IoT device manufacturers must be prohibited from offering devices with preloaded default passwords or hardwired master keys. It was preloaded default passwords that created several of the most successful botnets, including Mirai. This prohibition must apply to all methods of interface, including the device's web interface portal and telnet services.

2. NIST Database of Vulnerabilities

Hackers are continuously discovering new vulnerabilities that assist in the creation of botnets. Statutory declarations lack the pace and flexibility to prevent these vulnerabilities from being exploited without appearing overly broad. Instead, a dynamic, up-to-date database is required for listing these vulnerabilities so that manufactures have proper notice of what they must protect against. The NIST already manages such a database that could easily be molded to govern consumer grade IoT devices. The computer scientists at the NIST should be tasked with administering a dynamic database with the input of IoT manufacturers while ensuring partiality and reasonableness.

Further, IoT device manufactures must be required to periodically patch devices with security updates when conditions so require. Vulnerabilities are often discovered after a device has already been mass-produced and sold to consumers. Legislation governing only the pre-sale conduct of manufacturers fails to prevent malware from exploiting these newly exposed vulnerabilities.

3. Modernized CFAA

Since many botnet operators operate beyond the jurisdiction of the US (often in countries hostile towards the US), the imposition of criminal liability will never be an effective deterrent on such individuals. The CFAA can still be useful in the fight against botnets, however, since operators, accomplices, and command and control servers do occasionally exist in the US. A modernized CFAA must provide appropriate criminal penalties against botnet operators.

4. Increased FTC Regulatory Power

It is the FTC's responsibility to regulate the conduct and practices of interstate business. Device manufacturers must not be allowed to market IoT devices as 'secure' unless those devices truly do contain beefed up security policies. By declining to punish Asus or D-Link with monetary penalties the FTC missed an opportunity to increase the cost of manufacturing devices with poor security standards. Competitors to Asus and D-Link may continue to produce unsecure devices, knowing that even if caught, the costs imposed by the FTC are minimal.

Perhaps the greatest difficultly for the FTC in prosecuting device manufacturers incorporating weak security standards is the requirement to prove harm to consumers imposed by 15 U.S.C.S. § 45(n). As described earlier, botnets typically do not cause direct harm to consumers. An especially liberal interpretation of § 45(n) would be required for the FTC to satisfy this requirement. Section 45(n) could be modified or interpreted in such a way that "likely to cause substantial injury to consumers" implies "likely to cause substantial injury to commerce."