Attn: Evelyn L. Remaley
National Telecommunications and
Information Administration (NTIA)
U.S. Department of Commerce
1401 Constitution Avenue NW., Room 4725,
Washington, DC 20230

July 28th, 2017

Comments of New America's Open Technology Institute:

Promoting Stakeholder Action Against Botnets and Other Automated Threats

New America's Open Technology Institute (OTI) welcomes the opportunity to respond to the National Telecommunications and Information Administration (NTIA) Notice and Request for Comments on this important issue. We also appreciate the Multistakeholder Process that the NTIA is currently undertaking on this issue. Our comments will focus specifically on recommendations for ways to better secure end-points, especially IoT devices, to help protect them against botnet attacks.

Introduction

Botnets, especially "botnets of things" have become one of the biggest threats to cybersecurity. Over the past decade the Internet of Things (IoT) industry has expanded dramatically, with the FTC predicting that there will be 50 billion connected devices by the year 2020.[1] This has swelled dramatically, far beyond what we could've predicted even ten years ago. The cameras that allow you to check in on your pets while at work; systems that provide home automation functions like opening the garage door or turning off the light; and bracelets that track your sleep patterns are all connected to the internet, and are potential targets for attack. But not all of the IoT devices under threat are toys or convenience items—technology in infrastructure and critical industry is under threat as well. And botnets created by harnessing these devices can attack anything connected to a network. This threat is only going to become more concerning as the industry expands, so steps need to be taken now to manage this risk.

The size and complexity of the Internet of Things makes it difficult to regulate. IoT devices have constituted a plurality of all internet-connected devices since 2014, and are expected to outnumber tablets, smartphones, and PCs combined by next year.[2] Even conceptualizing the nature of a regulatory system that could encompass the whole scope of IoT is challenging, and the logistics of enforcing legal standards on an industry as diversified this one, with so many actors working across inter- and intra-national jurisdictions on the same product, is daunting. In recognition of these challenges, the Department

[1] https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[2] David McCandless, "The Internet of Things – An Interactive Primer," *Information Is Beautiful*, November 23, 2016, http://www.informationisbeautiful.net/visualizations/the-internet-of-things-a-primer/.

of Commerce[3] and the Communications Security, Reliability and Interoperability Council[4] have promoted the adoption of voluntary guidelines, rather than enforceable regulations. There is reason to be optimistic about the potential for government participation in, and coordination of, the establishment of voluntary principles, even in the absence of enforcement mechanisms: a group of researchers studying botnet infection patterns concluded that "the malware problem is fundamentally a *cultural* problem."[5] Physical security is widely understood and highly valued by producers and consumers, but digital security is less so. Government can look to the work of projects like the Digital Standard, a collaboration between groups such as Consumer Reports and Ranking Digital Rights, for practicable guidelines that will improve device security.[6] Working with consumer protection and advocacy groups to create straightforward guidelines for vendors can help to guide the design process and shift the expectations and priorities of consumers towards greater security.

Seven Recommendations to Help Secure Internet of Things Devices

1. Use rewards to reduce vulnerabilities in IoT products

An effective way to limit the spread of botnet attacks is to reduce the number of vulnerabilities that allow them to infect devices. In the rush to get highly-lucrative IoT products to market, (especially inexpensive ones), those items do not necessarily receive the same level of security review and testing as the more established products. Industries like car manufacturers and healthcare technologies generally face more stringent review processes than producers of toasters or connected cameras. These big, better regulated companies also struggle with vulnerabilities in their products, but they have established processes for finding and patching them - hopefully (but not always) before they create widespread damage.

However, sometimes these in-house information security departments aren't enough to find critical vulnerabilities. To address this, many companies, ranging from Microsoft to Uber, have looked to independent researchers to help secure their products and services. Hundreds of companies have formalized programs that they use to attract researchers who find vulnerabilities, assure them that there will be a reasonable voice on the other end of the line, and provide a secure means to submit reports.[7] Some of them pay out monetary rewards, but they don't have to. Called "Vulnerability Rewards Programs," or the more catchy "Bug Bounty Programs," some of these schemes pay out hundreds of thousands of dollars to experts outside of the formal information security market. Companies are in a constant battle to secure their products, and bounties are seen as one way to attract the best and the

---

[3] "White House Announces Public-Private Partnership Initiatives to Combat Botnets," Government, *United States Department of Commerce*, (May 30, 2012), http://2010-2014.commerce.gov/news/press-releases/2012/05/30/white-house-announces-public-private-partnership-initiatives-combat-b.html.

[4] "The CSRIC III initially tasked Working Group 7, Botnet Remediation, with proposing a set of voluntary practices that would constitute the framework for a voluntary program for ISPs to follow to mitigate the botnet threat...through voluntary participation." Michael O'Reirdan et al., "U.S. Anti-Bot Code of Conduct (ABC) for Internet Service Providers (ISPs): Barrier and Metric Considerations," Working Group 7 Botnet Remediation (Communications Security, Reliability and Interoperability Council, March 2013), 3, https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf; *c.f.*, Working Group 8, "Internet Service Providers (ISP) Network Protection Practices" (The Communications Security, Reliability and Interoperability Council, November 2011), 5, http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

[5] Brett Stone-Gross et al., "Your Botnet Is My Botnet: Analysis of a Botnet Takeover," in *Proceedings of the 16th ACM Conference on Computer and Communications Security: November 9 - 13, 2009, Chicago, Illinois, USA* (ACM Conference on Computer and Communications Security, New York, NY: ACM, 2009), 635–47, 646, http://delivery.acm.org.ezproxy.princeton.edu/10.1145/1660000/1653738/p635-stone.pdf?ip=128.112.200.107&id=1653738&acc=ACTIVE%20SERVICE&key=7777116298C9657D%2ECCADDB884D0A3BC7%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=790503970&CFTOKEN=90635074&__acm__=1501164648_13e9f7f7dbfa4b672f48b3ff8b486f3d.

[6] "Digital Standard," *The Digital Standard*, 2017, https://www.thedigitalstandard.org/.

[7] Andi Wilson, "Squashing Car Bugs: What Chrysler's New Bounty Program Means For Vulnerabilities Research," New America's Open Technology Institute, July 18, 2016, https://www.newamerica.org/oti/blog/squashing-car-bugs-what-chryslers-new-bounty-program-means-vulnerabilities-research/.

brightest eyes and to find a greater number of bugs before they can be exploited.[8] Although the vendors that developed the first bounty programs were multi-billion dollar corporations,[9] these programs are valuable to a wide range of industries—even startups and small businesses.[10] Some companies have used rewards in the form of airline points,[11] "swag,"[12] or even just "hall of fame"[13] recognition as rewards for successful bounty-hunters.[14] This opens the potential for participation by companies that can't necessarily pay out large sums in exchange for assistance securing their products. Even better, the process of implementing a vulnerability rewards program puts a company in a security frame-of-mind, encouraging deeper thought about products and design. The fewer vulnerabilities a product has, the stronger its protection against botnets.

2. Randomize default credentials and allow users to customize login information

In order to make IoT devices more secure against botnet attacks, end-users should be able to change their usernames and passwords. When you buy technology like a router, it comes with factory default information, often common to many devices and sometimes unable to be customized. The Mirai botnet, which was used in a DDoS attack against DNS service provider Dyn in October 2016, was able to infect 380,000 devices like printers, webcams, and DVRs[15] using fewer than 70 common combinations of usernames and passwords. These products were still set to factory default, which made them extremely vulnerable.[16] As IoT devices become more common, allowing end-users to change their login credentials on devices they purchase is a crucial step in ensuring security of the broader network. The Department of Homeland Security has recommended that devices be sold with "unique, hard to crack default usernames and passwords" in order to protect them from this type of attack.[17] The ability to modify login credentials should not be taken as a replacement for the implementation, where possible, of unique passwords for every device sold, but it is a good first step toward securing technology like routers that have been commonly harnessed by botnets.[18] Educating consumers is also an important step in reducing the vulnerability caused by common and/or unchangeable passwords—even experts sometimes fail to engage in good information security practices. A 2014 survey of 653 IT professionals found that only 30% change the default passwords on their wireless routers.[19] In order to address this human error component, vendors can also suggest or require users to create new passwords when setting up a device, or provide clear instructions on how to change credentials after setup.

---

[8] Andi Wilson, Ross Schulman, Kevin Bankston, and Trey Herr, "Bugs in the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications," *New America's Open Technology Institute* (July 2016), 18, https://na-production.s3.amazonaws.com/documents/Bugs-in-the-SystemFinal.pdf.

[9] Esben Friis-Jensen, "The History of Bug Bounty Programs," *Cobalt*, April 10, 2014, https://blog.cobalt.io/the-history-of-bug-bounty-programs-50def4dcaab3; Kim Zetter, "With Millions Paid in Hacker Bug Bounties, Is the Internet Any Safer?" *Wired*, November 8, 2012, https://www.wired.com/2012/11/bug-bounties/.

[10] "Bug Bounty Programs: The most exhaustive list of known Bug Bounty Programs on the internet, *HackerOne*, https://hackerone.com/bug-bounty-programs.

[11] United Airlines Bug Bounty Program, https://www.united.com/web/en-US/content/Contact/bugbounty.aspx.

[12] Cloudflare Vulnerability Disclosure Policy, https://www.cloudflare.com/disclosure/.

[13] Fitbit, *Bug Crowd*, https://bugcrowd.com/fitbit.

[14] "Bug Bounty List, *Bug Crowd*, https://www.bugcrowd.com/bug-bounty-list/.

[15] Brian Kerbs, "Did the Mirai Botnet Really Take Liberia Offline?" *Krebs on Security,* November 4, 2016, https://krebsonsecurity.com/tag/mirai-botnet/.

[16] Steve Ragan, "Here Are the 61 Passwords That Powered the Mirai IoT Botnet," *CSO Online*, accessed July 26, 2017, http://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html; "IoT Botnet Highlights the Dangers of Default Passwords," *PC World*, n.d., https://www.pcworld.idg.com.au/article/607908/iot-botnet-highlights-dangers-default-passwords/.

[17] U.S. Department of Homeland Security, "Strategic Principles for Securing the Internet of Things (IoT)" (U.S. Department of Homeland Security, November 15, 2016), 5, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

[18] "Security News This Week: A Botnet Takes Down Nearly a Million German Routers," Wired, December 3, 2016, https://www.wired.com/2016/12/security-news-week-botnet-takes-nearly-million-german-routers/.

[19] "80% of SOHO Routers Contain Vulnerabilities," *Infosecurity Magazine*, February 22, 2014, https://www.infosecurity-magazine.com/news/80-of-soho-routers-contain-vulnerabilities/.

3. Design devices so that they can be patched and updated

In order to make IoT devices more secure against botnet attacks they must be designed in such a way that they can be patched or updated. Vulnerabilities are to be expected in hardware and software development, and development and issuance of patches is key to maintaining secure products in the long term.[20] But the low-power batteries in many inexpensive IoT devices are unable to support the demands of downloading an update through an encrypted link, meaning the device cannot be patched.[21] These devices provide a critical point of weakness that botmasters can exploit. The brand of baby monitor which was hacked in August of 2013, allowing hackers to see and speak to the baby being monitored, was one such low-power device which could not be updated securely over Wi-Fi; when the hack occurred, only 1% of users had updated the firmware which patched the vulnerabilities responsible.[22] On online forums, consumers expressed frustration with the inability to update securely over Wi-Fi, with some "willing to take [the] risk" and download the update over an insecure connection.[23]

Even when a device can be patched, users frequently neglect to do so.[24] Vendors can provide or recommend tools to users, which will notify IoT device owners of updates and assist with their installation, such as those submitted to the FTC's IoT Home Inspector Challenge.[25] This is another point at which human error introduces insecurity, as patching as a security measure depends on the cooperation of users, unless a vendor has the capability to automatically push updates onto users' devices. To address this, the FCC and Department of Homeland Security have both recommended configuring IoT devices to automatically install critical safety patches.[26] However, implementing automatic updates may have an adverse effect on the effectiveness of security patches. Some users resist updating software because they dislike the other changes that come along, such as to a user interface. This was the case when Windows users turned off all updates—including patches—to avoid the automatic update from Windows 7 and 8 to Windows 10.[27]

4. Establish a support window and end-of-life procedures

---

[20] A typical piece of software may have up to 25 vulnerabilities per 1,000 lines of code. Critical software like that inside of pacemakers can run 80,000 lines long, and the programs controlling smart cars run into the millions. Paul E Black et al., "Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy" (Gaithersburg, MD: National Institute of Standards and Technology, November 2016), 2, doi:10.6028/NIST.IR.8151. "When Code Can Kill or Cure," *The Economist*, June 2, 2012, http://www.economist.com/node/21556098; Jason Paur, "Chevy Volt: King of (Software) Cars," *WIRED*, accessed July 28, 2017, https://www.wired.com/2010/11/chevy-volt-king-of-software-cars/.

[21] "For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries." Article 29 Data Protection Working Party, "Opinion 8/2014 on the on Recent Developments on the Internet of Things," September 16, 2016, 9, http://link.springer.com/chapter/10.1007/978-3-319-32156-1_13, qtd. in FTC Staff Report, "Internet of Things: Privacy and Security in a Connected World" (Federal Trade Commision, January 2015), n. 55, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[22] Kashmir Hill, "How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old," *Forbes*, accessed July 28, 2017, https://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/.

[23] "slingster," "Reason Why Not to Upgrade Firmware via Wireless?," *Foscam Forum*, January 4, 2015, http://foscam.us/forum/reason-why-not-to-upgrade-firmware-via-wireless-t12033.html.

[24] "Of the nearly 46,000 [infected] Foscams," a brand of baby monitor, "over 40,000 have not updated their systems to fix the vulnerability." Kashmir Hill, "'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users," *Forbes*, August 27, 2013, https://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/, cited in FTC Staff Report, "Internet of Things: Privacy and Security in a Connected World" (Federal Trade Commision, January 2015), n. 56, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[25] "IoT Home Inspector Challenge," *Federal Trade Commission*, July 26, 2017, https://www.ftc.gov/iot-home-inspector-challenge.

[26] U.S. Department of Homeland Security, "Strategic Principles for Securing the Internet of Things (IoT)" (U.S. Department of Homeland Security, November 15, 2016), 7, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf; Working Group 8, "Internet Service Providers (ISP) Network Protection Practices" (The Communications Security, Reliability and Interoperability Council, November 2011), 16, http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

[27] "Fearing Forced Windows 10 Upgrades, Users Are Disabling Critical Updates Instead," *PCWorld*, May 27, 2016, http://www.pcworld.com/article/3075729/windows/fearing-forced-windows-10-upgrades-users-are-disabling-critical-updates-at-their-own-risk.html.

In order to make IoT devices more secure against botnet attacks, vendors must establish end-of-life plans. This includes establishing the extent of the support window (if there is one) after which the device will no longer receive patches from the vendor, and conveying that information to users so that they can decide how to proceed. For example, devices like fitness trackers, which tend to be replaced on a regular basis, may be able to have a somewhat short support window without it posing a significant security challenge. However, technology like connected refrigerators, which are often more expensive and less frequently replaced, would need to have a much longer support window in order to continue to be secure for the lifespan of the appliance.[28] Both of these types of devices may pose significant security risks as these regularly replaced IoT items are sometimes produced by startups or new companies that may not have the capacity to maintain consistent technical support, and companies that produce home appliances may be new to the world of connected technology. Support windows, and clear consumer education about them, are crucial to protect all of these devices against botnet attacks.

Even computers, which tend to be manufactured and maintained by vendors with more technical expertise, suffer from vulnerabilities due to an insufficient support window. An international survey found that 52% of businesses still have at least one machine running Windows XP (support ended in April, 2014), and 9% still have at least machine running Windows Vista (support ended in April, 2017).[29] Although it is to be expected that even Microsoft cannot maintain support for software that over 10 years old, users may choose not to update their computers or operating systems past that point. Continued use of out-of-date, unsupported devices and software is more common among governments and hospitals, which may have specialized systems designed for that particular interface which cannot be easily updated.[30] In response to the WannaCry ransomware attack Microsoft took the extremely unusual step of releasing Windows XP patches, three years after support ended, because so many computers were still at risk.[31]

5. Let users know what security features are available, and which are not

In order to make IoT devices more secure against botnet attacks, users should be made aware of the security features are available to them on the device, including those enabled by default. They should also be provided information that explains what these features are, and why they are important. For example, it should be clear to users if their data is transmitted with end-to-end encryption, and what this means, so that they may make educated decisions about how they share data. Users may not be aware that their data is being served insecurely, or that their account is not protected by "lock-outs" after incorrect login information is entered multiple times.[32] A survey of ten of the most popular IoT devices found that only three encrypted communications with the internet and just four used encryption when downloading software updates.[33] Meanwhile, eight of the ten devices and associated cloud/mobile

---

[28] Andrew Cunningham, "LG Threatens to Put Wi-fi in Every Appliance it Introduces in 2017," *Ars Technica*, January 4, 2017, https://arstechnica.com/gadgets/2017/01/lg-puts-amazons-alexa-in-a-fridge-and-wi-fi-in-everything-else/.

[29] Spiceworks Inc, "Windows 10 Adoption Surges, yet Businesses Still Hang on to Windows XP and Vista," *The Spiceworks Community*, April 3, 2017, https://community.spiceworks.com/networking/articles/2628-windows-10-adoption-surges-yet-businesses-still-hang-on-to-windows-xp-and-vista; "Windows Lifecycle Fact Sheet," *Microsoft Support*, May 24, 2017, https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet; "Support for Windows XP Ended," *Microsoft*, April 8, 2014, https://www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support.

[30] Patrick Howell O'Neill, "Windows XP a Security Nightmare, Yet Still Used by Hundreds of Millions", *Cyberscoop*, November 1, 2016, https://www.cyberscoop.com/windows-xp-us-government-duo-security-october-2016/; Steve Ranger, "Windows XP: Why Hospitals Are Still Using Microsoft's Antique Operating System," *ZD Net*, December 8, 2016, http://www.zdnet.com/article/windows-xp-why-hospitals-are-still-using-microsofts-antique-operating-system/.

[31] Patrick Howell O'Neill, "Microsoft Patches Windows XP Due to 'heightened Risk' of Nation-state Activity," *Cyberscoop*, June 13, 2017, https://www.cyberscoop.com/windows-xp-patches-wannacry-microsoft/.

[32] Mario Ballano Barcena and Candid Wueest, "Insecurity in the Internet of Things," *Security Response, Symantec*, 2015, 5, https://pdfs.semanticscholar.org/6d7f/60b16adead96aafa9e975207980eb32671b5.pdf.

[33] Mats Andersson, "Use Case Possibilities with Bluetooth Low Energy in IoT Applications," White paper, (2014), http://www.spezial.de/sites/default/files/bluetoothlowenergy-iot-applications_whitepaper_ubx-14054580.pdf.

applications "failed to require passwords of sufficient complexity and length."[34] Educating users on provided security features, and their benefit, may also provide the secondary benefit of building norms within the industry about including features like end-to-end encryption in new products. Vendors who promote the security of their products may also be able to attract customers through these features. Surveys have shown that consumers value products with quality certifications, such as organic and free trade foods.[35] Consumers demonstrate the same habits with more expensive purchases as well: condominiums in LEED-certified buildings sell for 21% more than analogous properties without the certification.[36]

6. Connect consciously

In order to make IoT devices more secure against botnet attacks, vendors should be conscious of the potential threats of connecting a device to the internet. They should also consider the type of data transfer which a device will perform when choosing the connection method. For example, devices working over a short range and transferring small amounts of data, such as key fobs or smart home devices, could use Bluetooth Low Energy.[37] No protocol is perfectly secure, and vendors should make clear which protocol a device uses and the security risks thereof, as well as what data is stored or transferred. For devices that do not require internet connectivity for their core functionality, vendors should consider allowing users to selectively toggle the device's connection on and off without powering down the device itself or utilizing a different method of connectivity such as Bluetooth or cellular.[38] Smart home devices such as juicers[39] or *sous-vide* precision cookers[40] augmented with IoT features can perform their core functionality equally well with or without internet connection. Vendors can include instructions on how to enable AP Isolation mode on the guest network on a user's home network router, which creates a second, separate network which allows devices to communicate with the router but not with one another. This intervention could prevent a poorly secured, low-end hacked IoT device from infecting other devices on that network that resisted initial infection thanks to stricter security measures[41] Ensuring that infections do not spread between devices within a single network becomes more and more urgent as IoT devices become more common in cars[42], fire alarms[43], and even guns.[44] Infecting these types of devices can create physical dangers if they are insecure, whereas using an AP isolated guest network to separate poorly secured IoT

---

[34] Hewlett Packard Enterprise, "Internet of Things Research Study" (Hewlett Packard, November 2015), 4 http://h20195.www2.hpe.com/V4/getpdf.aspx/4aa5-4759enw.

[35] Nancy Gagliardi, "Consumers Want Healthy Foods--And Will Pay More For Them," *Forbes*, accessed July 28, 2017, https://www.forbes.com/sites/nancygagliardi/2015/02/18/consumers-want-healthy-foods-and-will-pay-more-for-them/; Jens Hainmueller, Michael J. Hiscox, and Sandra Sequeira, "Consumer Demand for Fair Trade: Evidence from a Multistore Field Experiment," *The Review of Economics and Statistics* 97, no. 2 (June 24, 2014): 242–56, doi:10.1162/REST_a_00467.

[36] Kerry Curry, "People Are Paying a 20% Premium for 'Green' LEED-Certified Condos," accessed July 28, 2017, http://www.mansionglobal.com/articles/26952-people-are-paying-a-20-premium-for-green-leed-certified-condos.

[37] Mario Ballano Barcena and Candid Wueest, "Insecurity in the Internet of Things," *Security Response, Symantec*, 2015, 19, https://pdfs.semanticscholar.org/6d7f/60b16adead96aafa9e975207980eb32671b5.pdf.

[38] Mats Andersson, "Use Case Possibilities with Bluetooth Low Energy in IoT Applications," White paper, (2014), http://www.spezial.de/sites/default/files/bluetoothlowenergy-iot-applications_whitepaper_ubx-14054580.pdf.

[39] Ellen Huet and Olivia Zaleski, "Silicon Valley's $400 Juicer May Be Feeling the Squeeze - Bloomberg," News, Bloomberg Technology, (April 19, 2017), https://www.bloomberg.com/news/features/2017-04-19/silicon-valley-s-400-juicer-may-be-feeling-the-squeeze.

[40] Brian Feldman, "I'm So Excited to Precision-Cook Meat While Also Remotely Attacking Websites," Select All, July 11, 2017, http://nymag.com/selectall/2017/07/im-so-excited-to-join-a-botnet.html.

[41] Chris Hoffman, "Lock Down Your Wi-Fi Network With Your Router's Wireless Isolation Option," *How-To Geek*, January 6, 2014, https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless-isolation-option/.

[42] Federal Bureau of Investigation, Department of Transportation, and National Highway Safety Administration, "Motor Vehicles Increasingly Vulnerable to Remote Exploits," Government, *Internet Crime Complaint Center*, (March 17, 2016), https://www.ic3.gov/media/2016/160317.aspx.

[43] Earlence Fernandes, *Fake Alarm Attack [Final v1]*, Streaming, 2016, https://www.youtube.com/watch?v=RnGcrOixzbI&feature=youtu.be; Earlence Fernandes, Jaeyeon Jung, and Atul Prakash, "Security Analysis of Emerging Smart Home Applications," *University of Michigan*, 2016, https://iotsecurity.eecs.umich.edu/.

[44] Andy Greenberg, "Hackers Can Disable a Sniper Rifle—Or Change Its Target," *WIRED*, July 29, 2015, https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/; Runa A Sandvik and Michael Auger, "When IoT Attacks: Hacking a Linux-Powered Rifle" (Powerpoint, Black Hat Hacker Conference, Las Vegas, August 2015), https://www.blackhat.com/docs/us-15/materials/us-15-Sandvik-When-IoT-Attacks-Hacking-A-Linux-Powered-Rifle.pdf.

devices from home computers, and from one another, would inhibit the ability of botmasters to launch massive ransomware attacks on or harvest personal information.

7. Support the products which support best practices

In order to make IoT devices more secure against botnet attacks government actors can "walk the walk" by purchasing and endorsing secure products. It may not be possible to enforce standards on the industry writ large, but it is far easier to model good practices and purchase compliant products through government contracts. The federal government can commit itself to the use of secure IoT devices which meet certain security standards, and support states and municipalities that do the same. Experts estimate that 2.3 billion devices will be connected in "smart city" infrastructures by the end of 2017, and the smart city IoT market will reach $930 billion to $1.7 trillion by 2025.[45] Only giving lucrative government contracts to vendors practicing effective security practices both protects government technology from attack and incentivizes companies who want to work with the government to improve the security of their products. The importance of making sure that key government services are not made vulnerable to being taken over by botmasters cannot be overstated. Data breaches or system takeovers could be disastrous. There were 300 cyberattacks on critical infrastructure in 2015, and the growth of IoT in smart cities only makes the attack surface larger. European researchers found that smart parking meters, bike sharing systems, and public transport ticketing can all be completely circumvented in 50 Italian cities.[46] Government has a special responsibility to protect information, and can model best practices for IoT endpoint protection in doing so.

Conclusion

OTI's recommendations focus on ways to secure endpoints, but doing this requires taking action on the technological AND human level. Only so much "security by design" can be accomplished if users make poor choices about how they interact with technology. Vendors need to make their products more secure by eliminating dangerous vulnerabilities, ensuring that devices can be patched and updated, and installing security features like encryption. Users need to be educated about which features exist, how they work, and why they are important. Governments need to model good security practices by purchasing IoT technology with the security features necessary to protect their networks, and to incentivize companies to improve the security of their products. Only when the three stakeholders work together can we address the threat of "botnets of things." We thank NTIA for their attention to this important issue.

For questions or additional information, please contact:
Andi Wilson, Policy Analyst, New America's Open Technology Institute, wilson@opentechinstitute.org

[45] "Building Smarter Cities," *CompTIA*, August 26, 2016, https://www.comptia.org/resources/building-smarter-cities.

[46] Matteo Beccaro and Matteo Collura, "(Ab)using Smart Cities: The Dark Age of Modern Mobility" (HITB GSEC, InterContinental, 2016), 15, 4, http://gsec.hitb.org/materials/sg2016/whitepapers/Abusing%20Smart%20Cities%20-%20Matteo%20Beccaro%20and%20Matteo%20Collura.pdf; Mirko Zorz, "Hacking Smart Cities: Dangerous Connections," *Help Net Security*, August 18, 2016, https://www.helpnetsecurity.com/2016/08/18/hacking-smart-cities/.