Google nest

July 28, 2017

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

Submitted electronically to counter_botnet_RFC@ntia.doc.gov

Google Inc. (Google) and Nest Labs, Inc. (Nest) are pleased to provide comments in response to the National Telecommunications & Information Administration's (NTIA) Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats (RFC).  Google and Nest appreciate the NTIA's specific focus on this concrete, clearly-scoped, and important security issue.

While there is no such thing as perfect data security, as the Federal Trade Commission (FTC) has frequently observed,[1] there is a long and growing list of best practices that companies can employ to reasonably secure connected devices and help ensure they do not become part of a botnet facilitating an automated, distributed attack.

Our submission focuses on three areas.  First, we describe our involvement in the IoT space, which includes manufacturing devices, developing protocols and operating systems, and maintaining platforms for third-party developers.  We then describe some of the key security best practices we follow and believe the private sector can adopt more broadly to mitigate the risks of botnets and automated attacks.  Lastly, we discuss some recommendations on what government can do.  While the current legal regime, including vigorous FTC enforcement, already encourages businesses to adopt reasonable security measures, more can be done through voluntary public-private partnerships to enable consumers to make informed, security-conscious decisions when purchasing and using connected devices.  Such collaboration should work to ensure that those companies that invest in security are rewarded for their efforts.

## I. About Google and Nest

Google and Nest each manufacture and sell Internet-connected devices to consumers.

For example, Google Home is a voice-activated speaker powered by Google Assistant that acts as a point of control for other connected home devices; allows consumers to get real-time information about weather, traffic, finance, sports, local businesses; place calls; play music; and much more.  Google Wifi provides a "mesh" network of routers that communicate wirelessly to each other to create a single WiFi

[1] Fed. Trade Comm'n, *Commission Statement Marking the FTC's 50th Data Security Settlement* 1 (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

network that provides a blanket of connectivity. This allows consumers to have multiple sources of powerful WiFi blanketing their home.

Google also develops and maintains the Android Things operating system and platform, which enables third-party developers to build smart devices and applications using Android APIs and Google services.[2] This will allow developers to take advantage of the security built into the Android operating system,[3] including over-the-air security updates.[4]

Nest manufactures connected home products to create a thoughtful home that takes care of the people inside it, while also addressing societal challenges such as energy use, life safety, and personal security. The Nest Learning Thermostat is a smart thermostat that, through onboard sensors, user interaction, and advanced algorithms, can learn a household's temperature preferences to help consumers stay comfortable and save energy. Nest Protect is a smoke and carbon monoxide alarm that uses advanced sensor and communications technology and intelligent algorithms to alert users to smoke and carbon monoxide emergencies, speak verbal warnings, and provide mobile notifications through the Nest app. Nest Cam, Nest Cam Outdoor, and Nest Cam IQ are home security cameras that provide 24/7 live streaming to customers' phones to help them monitor their homes, find out if something is wrong, watch their pets, or simply to know if a package has arrived.

Via the Works with Nest program, third-party developers can obtain access to the Nest cloud API to build integrations between Nest products and services and third-party products and services.

## II. Google and Nest's Approach to Securing Connected Devices

Google and Nest share NTIA's concern over the threat of botnets to wage automated, distributed attacks. Malicious actors target vulnerable computers or connected devices, which are then infected with malware. The compromised devices—a "botnet"—can be remotely commanded to undertake a number of tasks, including mounting distributed denial of service (DDOS) attacks against the ultimate targets.[5] This is done by causing the botnet to generate a flood of traffic to overwhelm a web domain. The use of connected devices makes it especially difficult for the web domain to mitigate attacks by identifying and screening requests from compromised devices because each device has its own IP address and the requests appear legitimate. If the DDOS attack successfully targets a key piece of infrastructure, such as a

[2] *See* Android Things, https://developer.android.com/things/index.html.

[3] *See* Android Source, *Security*, https://source.android.com/security/.

[4] *See, e.g.*, Android Things, *Update Builds for an Android Things Product*, https://developer.android.com/things/console/update.html#push-a-build.

[5] *See, e.g.*, John Leyden, *Mysterious Hajime Botnet Has Pwned 300,000 IoT Devices*, The Register (Apr. 27, 2017), https://www.theregister.co.uk/2017/04/27/hajime_iot_botnet/; Lily Hay Newman, *The Botnet that Broke the Internet Isn't Going Away*, Wired (Dec. 9, 2016), https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/; Michael Kan, *An IoT Botnet Is Partly Behind Friday's Massive DDOS Attack*, PCWorld (Oct. 21, 2016), http://www.pcworld.com/article/3134056/hacking/an-iot-botnet-is-partly-behind-fridays-massive-ddos-attack.html.

dynamic domain name service provider—as occurred following the Mirai attack on Dyn in October 2016—the attack is capable of taking down sizable portions of the Internet.[6]

To counter such threats, companies should use reasonable security measures in building and supporting connected devices. There is no "one size fits all" approach to combating such threats. What is reasonable or appropriate security can vary significantly depending on the environment in which a technology will be deployed, the types of products in question, the sensitivity of data involved, and the risks associated with malicious intrusion.[7] IoT, in particular, spans an enormous range of ecologies, each with its own individualized security needs. The security measures appropriate for the electrical grid, for example, are vastly different from the those appropriate for a connected toaster or a wearable fitness tracker. Nest and Google respectfully recommend that NTIA and other U.S. Government actors consider these variations in context, and the balance of this comment is focused on technologies developed for residential use.

In residential IoT, the following is a non-exhaustive list of security practices, which Google and Nest follow for their connected devices, that can help mitigate the risk of automated, distributed security attacks:

- *Secure Coding*. Companies should follow "security by design," that is, integrating secure coding practices into the development and testing lifecycle for IoT devices. This is a vital step because botnets often take advantage of well-known and avoidable software vulnerabilities. Additionally, considering security in the design phase encourages software architecture that limits security risks by, for example, prohibiting administrative access to the device or limiting the information exposed to or transmitted over the public network. Companies can leverage secure coding principles from a number of authorities, such as the Open Web Application Security Project,[8] the Department of Homeland Security,[9] and Google.[10]

- *Strong Authentication and Password Practices*. Strong authentication is one of the most important bulwarks against the conscription of connected devices into botnets.

    - *No Default Passwords.* Recent events have shown the risk that many consumers will not change default passwords.[11] As a consequence, default passwords can open a path for

[6] *See, e.g.*, Newman, *supra*; Nicky Woolf, *DDoS Attack that Disrupted Internet Was Largest of Its Kind in History, Experts Say*, The Guardian (Oct. 26, 2016), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[7] *See* Fed. Trade Comm'n, *Security Check: Reducing Risks to Your Computer Systems* 2 (June 2003), https://www.ftc.gov/system/files/documents/plain-language/bus58-security-check-reducing-risks-your-computer-systems.pdf.

[8] *See* OWASP, https://www.owasp.org/index.php/Main_Page.

[9] *See* U.S. Dep't of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT)*, Nov. 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

[10] *See* Google Outsourcing, *Web Application Security Requirements for Google Providers*, https://partner-security.withgoogle.com/docs/webapp_requirements.

[11] *See* U.S. Computer Emergency Readiness Team, *Heightened DDoS Threat Posed by Mirai and Other Botnets* (Oct. 14, 2016, last revised Nov. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA16-288A; *see also, e.g.*, Fred Kaplan, *Vulnerability Is the Internet's Original Sin*, Slate (Oct. 25, 2016),

    malicious attackers to compromise large numbers of devices with a single set of credentials. That is why Nest and Google products do not ship with default passwords. Rather, users setting up a Nest or Google account must create an individualized password during the account creation process.

    - *Multi-Factor Authentication.* Enabling multiple forms of verification ("multi-factor authentication") to access applications with control capabilities over devices further reduces the opportunity for malicious attackers to compromise large numbers of devices remotely. For example, Nest and Google account holders have the option of enabling two-factor authentication for added account security.

    - *No Hardcoded Credentials.* Devices and services should not have hardcoded credentials ("backdoors"). Any process for a factory reset or lost password on a device should include a physical presence test, such as pressing a button or connecting a jumper. All credentials that allow access to the device should be documented and should be user-configurable.

- *Encryption Best Practices*. Of course, strong authentication provides no protection if untrusted sources can control IoT devices over the network or obtain credentials by monitoring network traffic. Therefore, secure protocols, such as Transport Layer Security (TLS), should be used to encrypt traffic to and from external networks. Although the computations necessary to implement TLS can pose a problem for IoT devices with limited device computing resources, the security benefits it brings will generally outweigh such concerns. Additionally, connected device manufacturers should ensure they reap the benefits of this and other security protocols by ensuring that all cryptographic credentials (such as a TLS certificate) that are presented outside the device use private keys that are (1) unique to the specific device or service, and (2) replaceable in the event of expiration, compromise, or other business need.[12]

- *Network Security*: The best way to maintain a service's network security is to expose as little of that service as possible to the public Internet, which means that any service not required for the proper functioning for the device or service should not be exposed on a network interface. Any services that must be exposed should not include undocumented extra functionality that can pose a security risk.

- *Enabling Security Updates.* IoT providers can also follow practices that promote the broad and prompt availability of security updates and mitigate the risk of compromise during the update process. For example:

    - *Updates Should be Automatic*. Devices should, generally speaking, be capable of automatic software updates so that they can receive security updates without user action. This is necessary for categories of devices that are not capable of such interaction (e.g.,

http://www.slate.com/articles/news_and_politics/war_stories/2016/10/the_dyn_ddos_attack_shows_how_vulnerable_we_ve_made_ourselves.html.

[12] This does not apply to certificates that are never presented *outside* of the device, such as those used to verify a firmware update or to perform a verified boot process.

  those without integrated displays or remote application control). Even for devices with integrated displays or other means of control, automatic updates promote the broadest possible release of security upgrades to prevent the introduction or persistence of vulnerabilities that could compromise devices or other Internet-connected systems.

  - *Update Process Should be Secure.* IoT device manufacturers should also ensure that their method for providing security updates is verifiable. To avoid the risk of introducing malware onto IoT devices, all firmware updates should be cryptographically signed using asymmetric cryptography, and devices must verify the signature before installing the update.

- *Bug Bounty Programs.* In addition to pre-launch testing to identify vulnerabilities, many companies—including Google and Nest—have had success identifying and remediating security vulnerabilities through "bug bounty" programs, which provide incentives for outside security researchers to submit vulnerability reports.[13] At minimum, however, companies should maintain and monitor dedicated security channels for outside individuals, including security researchers, to submit vulnerability reports in their products.[14]

These security practices show some of the steps that the private sector can take to address the risks of botnets and automated attacks. This list is neither exhaustive nor meant to suggest any future regulatory approach. Google and Nest also recognize that best practices may evolve over time and may depend on the specific ecosystem or technology in question. Practices like these, however, show the results that are possible when the IoT technology industry takes security seriously and innovates to implement robust security.

## III. What Government Can Do

Google and Nest appreciate NTIA's interest in fostering the adoption of these practices, and applaud the careful, thoughtful approach NTIA has taken to this issue. We believe it is important for government to incentivize and encourage the adoption of best practices like these, while ensuring that it continues to foster a pro-innovation climate, particularly in a space as nascent as IoT. Just as policymakers in the 1990s accorded the Internet room to develop, policymakers today should adopt an approach that enables IoT to flourish and grow. Google and Nest therefore agree with the FTC's longstanding recommendation against IoT-specific legislation.[15]

[13] *See, e.g.*, Bugcrowd, *Bug Bounty List*, https://www.bugcrowd.com/bug-bounty-list/; HackerOne, *Bug Bounty Programs*, https://hackerone.com/bug-bounty-programs.

[14] *See, e.g.*, Google, *Report a Security Vulnerability*, https://www.google.com/appserve/security-bugs/m2/new?rl=&key=; Nest, *Keeping Data Safe at Nest*, https://nest.com/privacy/data/.

[15] *See* Fed. Trade Comm'n Staff, *Internet of Things: Privacy & Security in a Connected World* 48-49 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Existing law already requires manufacturers of connected devices to employ reasonable security measures to avoid substantial consumer injury.[16] The FTC and the States actively enforce these and other security and privacy mandates.[17]

Rather than impose new legal mandates, government can and should encourage the marketplace to do more to reward those who invest in good security practices and punish those that do not. Device and network security are, by their nature, complex and difficult for ordinary consumers to ascertain and understand. In addition, while Google and Nest share the FTC's goal of preventing misleading statements about security, strong enforcement action may unintentionally deter companies from providing more specific information about their security practices. As a consequence, the government should consider ways to create an environment in which businesses are more inclined to voluntarily provide information about their security practices and increase consumer awareness of good security practices they can follow. As consumers are informed in a clear manner about the elements of sound security, and the security of specific products, they can more readily factor security into their decisions about whether to purchase and how to use products. This, in turn, should spur more companies to prioritize security.

NTIA has also recognized the value of greater transparency regarding security practices.[18] We commend the NTIA's work to convene a wide variety of stakeholders to consider ways to encourage consumers to consider security as they decide what smart devices to buy and how to use them.

Government of course can also play an important role in sharing information about vulnerabilities in devices, software or other parts of the IoT ecosystem that can lead to security breaches. The government should leverage the Vulnerability Equities Process, CERTS, and other mechanisms to help industry keep users secure. At the same time, government should refrain from attempting to require manufacturers, developers and others in the ecosystem to implant backdoors for surveillance purposes. Doing so necessarily compromises security for users, and undermines the trust that is necessary if IoT is to reach its potential.

We also believe it is critical to ensure that consumers are making informed decisions about their own digital hygiene practices, which can reduce the likelihood of successful botnet attacks. One example of this is the National Cyber Security Alliance's (NCSA) Lock Down Your Login campaign (sponsored by Google),[19] which highlights six discrete steps that consumers can take to improve the security of their data and devices:

- Protect accounts with strong authentication
- Keep software updated
- Avoid phishing attempts

[16] *See, e.g.*, 15 U.S.C. § 45(a).

[17] In addition, to Section 5 of the FTC Act and comparable state prohibitions on unfair and deceptive acts and practices, IoT companies are subject to a host of more targeted laws, such as the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, the data breach notice laws of 48 states, and the substantive data security requirements of fifteen states .

[18] NTIA, Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security. .

[19] *See* National Cyber Security Alliance, *Lock Down Your Login*, https://www.lockdownyourlogin.org.

- Use unique passwords
- Protect mobile devices
- Use trusted security tools

The recent partnership between the Department of Justice's Criminal Division Cybersecurity Unit and the Consumer Technology Association to produce user-centric guidelines is another example of how the public-private partnership model can succeed.[20] Government and industry should explore similar opportunities to promote consumer awareness in the IoT space.

Finally, government is uniquely positioned to encourage experts from industry, academia, and other key sectors to establish a collaborative approach to new security standards and protocols. The security practices detailed above are important tools that can mitigate the risk presented by botnets and other automated threats, but such risks are constantly evolving and so too must the protocols to address them. Cybersecurity professionals from wide-ranging organizations, working together, are best suited to this task and to develop robust, practical, and interoperable new security protocols. Government should use its unique convening power to promote and highlight such collaboration.

## IV. Conclusion

Google and Nest appreciate NTIA's careful, targeted approach to the important issue of botnets and the risk of DDOS and other automated attacks. The need to adjust security measures as appropriate for the risks of each class of IoT product, the rapidly shifting IoT landscape, and the adapting strategies of attackers for exploiting IoT devices all counsel in favor of encouraging an environment that supports innovation and allows flexibility in developing security protocols for IoT devices. Google and Nest appreciate the opportunity to comment on securing IoT devices against being used for automated attacks and stand ready to work with NTIA and other stakeholders on this important issue.

Respectfully submitted,

Danielle Osler

Danielle Osler
Public Policy & Government Relations Counsel
Google Inc.

Richard J. Lutton, Jr.
General Counsel
Nest Labs, Inc.

[20] *See* Department of Justice, Criminal Division, Computer Crime & Intellectual Property Section, Cybersecurity Unit, and Consumer Technology Association, *Securing Your "Internet of Things" Devices* (July 2017), https://www.justice.gov/criminal-ccips/page/file/984001/download.