# Quantifying the Reflective DDoS Attack Capability of Household IoT Devices*

Minzhao Lyu†, Daniel Sherratt†, Arunan Sivanathan†,

Hassan Habibi Gharakheili†, Adam Radford⋆, Vijay Sivaraman†

†Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia
⋆Cisco Systems, Sydney, Australia
{m.lyu,a.sivanathan}@student.unsw.edu.au,dgsherratt@gmail.com,h.habibi@unsw.edu.au,aradford@cisco.com,
vijay@unsw.edu.au

## ABSTRACT

Distributed Denial-of-Service (DDoS) attacks are increasing in frequency and volume on the Internet, and there is evidence that cyber-criminals are turning to Internet-of-Things (IoT) devices such as cameras and vending machines as easy launchpads for large-scale attacks. This paper quantifies the capability of consumer IoT devices to participate in reflective DDoS attacks. We first show that household devices can be exposed to Internet reflection even if they are secured behind home gateways. We then evaluate eight household devices available on the market today, including lightbulbs, webcams, and printers, and experimentally profile their reflective capability, amplification factor, duration, and intensity rate for TCP, SNMP, and SSDP based attacks. Lastly, we demonstrate reflection attacks in a real-world setting involving three IoT-equipped smart-homes, emphasising the imminent need to address this problem before it becomes widespread.

**ACM Reference format:**
Minzhao Lyu†, Daniel Sherratt†, Arunan Sivanathan†,
Hassan Habibi Gharakheili†, Adam Radford⋆, Vijay Sivaraman†. 2017.
Quantifying the Reflective DDoS Attack Capability
of Household IoT Devices[1]. In *Proceedings of WiSec '17 , Boston, MA, USA, July 18-20, 2017,* 6 pages.
DOI: 10.1145/3098243.3098264

## 1 INTRODUCTION

The first wide-scale attack that involved home IoTs was uncovered in early 2014 [15] – hackers broke into more than 100,000 consumer devices including TVs and fridges to target enterprises and individuals worldwide with malicious emails. Over the past year, we have routinely seen IoT devices leveraged to launch DDoS attacks –weaponisation of IoTs has led to 558 attacks generating sustained traffic over 100 Gbps, often peaking at 800 Gbps, representing an annual growth of 150% in frequency and 60% in size [1]. These attacks are cumulatively estimated to impose an hourly cost of $30,000 to the victim organisation [16].

Many of these large-scale attacks [19, 23] have paralyzed popular Internet services (such as the DynDNS provider in the U.S.) by hijacking thousands of Internet accessible IoT devices (such as cameras), injecting malware (e.g. Mirai) into these devices and turning them to botnets that flood unwanted traffic to servers. This has to-date been easy because many IoT devices are shipped with little or no hardening against attacks; for example, they often allow remote access via SSH or FTP protocols, and use insecure default credentials (e.g. combination of 'root' and 'admin') that are not modified by the user. Moreover, several of these IoT devices are openly accessible on the Internet, and are not secured behind NAT or Firewall gateways [11]. Slowly, manufactures are reacting to the growing threat of IoT bonets, and are starting to limit or block remote access to their devices, raising the barrier for attackers to infiltrate these devices for the purpose of injecting malware that can launch attacks.

Even if an IoT device is not compromised, it can be employed in an "reflection" attack, whereby the attacker sends it a short query message (such as SSDP m-search, SNMP get-next/get-bulk, or TCP syn) with a spoofed source IP address, to which the device responds with a long reponse to the victim. In effect, the attacker uses the IoT device to reflect the attack, while amplifying the volume to inflict greater damage on the victim. Arbor Networks reports that reflection techniques (using SSDP, NTP, DNS, and SNMP) have already been used in several massive DDoS attacks [2, 3], and the growing ubiquity of IoT makes them attractive to attackers seeking to amplify their attacks.

What is particularly scary about reflection attacks is that unlike a botnet, the attacker does not need to hijack the IoT device for the reflection attack – all they need is to be able to send it a spoofed query message to which it will respond. The aim of this paper therefore is to conduct a reality check on the feasibility and efficacy of reflective DDoS attacks, using a range of techniques on a number of consumer IoT devices available in the market today. Our **first** contribution addresses the complacency around NAT/firewall protection in home networks – we show that malware (in the form of computer code, browser script, and mobile app) can penetrate the home to identify the IoT devices within, and reconfigure the

[1]Funding for this project was provided by the Australian Research Council (ARC) Linkage Grant LP150100666


*WiSec '17 , Boston, MA, USA*

DOI: 10.1145/3098243.3098264

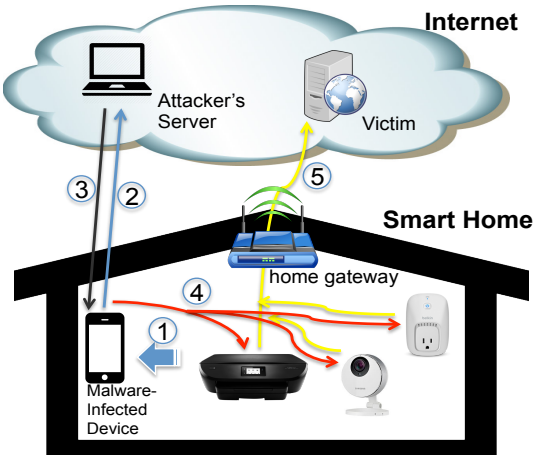


**Figure 1: Internal source of attack traffic**

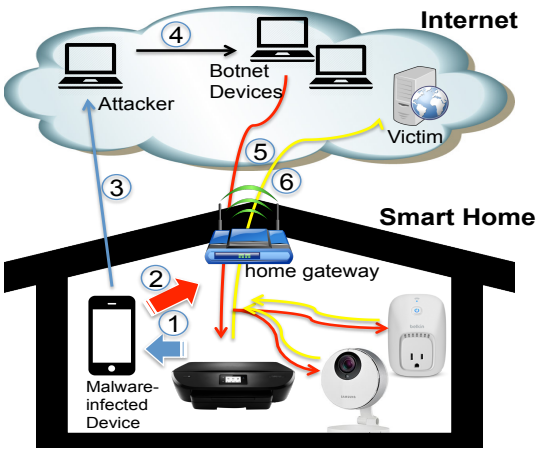


**Figure 2: External source of attack traffic**

home gateway to expose these IoT devices to internal and external reflection without the user's knowledge, in effect making every home device a potential reflector. Our **second** contribution is to profile the reflective capability of eight consumer IoT devices available today, in terms of their amplification factors, traffic capacity, and sustained durations for SSDP, TCP, and SNMP-query based attack traffic. Our **third** contribution is to deploy these IoT devices in three homes equipped with different IoT devices, using different models of home gateways, and served by different ISPs, to demonstrate their combined capability to amplify a DDoS attack by a factor of 20 over a sustained 24-hour period. Our work is the first to empirically evaluate the risk of reflection DDoS attacks using household IoT devices, pointing to the urgent need to identify and mitigate them before they cause widespread damage.

The remainder of the paper is organized as follows: §2 summarizes relevant prior work on DDoS attacks. In §3 we show how malware can penetrate the NAT/firewalls in home gateways to expose household IoT devices as reflectors, while in §4 we quantify the strength of reflective DDoS attacks from numerous consumer IoT devices. We demonstrate the aggregation of reflection attacks from our lab setup as well as three households and quantify its performance in §5, and conclude the paper in §6.

## 2 RELATED WORK

Methods for reflective DDoS attacks have been studied in the research literature. The work in [6, 24] identifes 14 different UDP-based protocols related to network services (SSDP, SNMP, DNS, NTP, NetBios), legacy protocols (CharGen, QOTD), P2P (BitTorrent, Kad) and Gaming (Quake 3, Steam) that can be reflected and amplified. Kührer *et al* [12] scan and discover publicly accessible Internet devices, including servers, home routers, and embedded devices that respond to UDP reflection requests. The work is extended in [14] to include attacks based on 13 common TCP-based protocols (FTP, HTTP, IPP, IMAP, SSH, etc.) – and about 2% of over 20 million hosts scanned on the Internet were found to have an amplification factor greater than 20x.

Prior works have only considered reflection agents publicly accessible over the Internet, while we additionally show that consumer IoT devices secured behind home gateways can also be exposed. Further, prior works have largely focused on measuring reflections of single packets, while we quantify sustained attacks from individual IoT devices as well as aggregated households.

## 3 EXPOSING HOUSEHOLD IOT DEVICES AS REFLECTORS

Attackers today commonly use publicly available services such as DNS and NTP as reflectors [13]. While the high traffic capacity of such servers makes them attractive as reflectors, their limited number makes them easier to safeguard. By contrast, household IoT devices individually have low traffic capacity, but their aggregation in large numbers can easily sustain very high attack volumes, making them attractive agents for the next wave of reflection attacks. The presence of home gateways with NAT/Firewall offers some protection to household IoT devices from being used as reflectors, but in this section we show that this protection can be circumvented relatively easily, making real the risk that tens of millions of such devices can become reflection agents.

Our attack is inspired by prior work that has shown that it is relatively easy to inject malware into downloaded software [18], browser plug-ins [9], and mobile apps [8], that the user can reasonably be expected to be running within their home inside of the home gateway. Specifically, [9] has shown that malicious scripts can be embedded in browser extensions to send packets on the home network, and [20] has shown that a malicious mobile app (approved by Apple) can discover IoT devices within the home and configure port forwarding on the home gateway to allow external access to these devices. We now describe two methods by which such malware can expose household IoT devices as reflectors to attackers.

The first (and somewhat naive) method is depicted in Fig. 1. In step ① our malware scouts for reflection-vulnerable UDP ports (1900 SSDP, 161 SNMP) and common TCP ports (22 SSH, 23 Telnet, 80

| Device Type | SSDP Reflection | SNMPv1 Reflection | SNMPv2c Reflection | TCP SYN Reflection |
|---|---|---|---|---|
| Samsung smart cam | Unsupported | Unsupported | 4.65 | 5 |
| Wemo power switch | 24.44 | Unsupported | Unsupported | 5 |
| Philips Hue lighbulb | 15.13 | Unsupported | Unsupported | 6 |
| Belkin NetCam | 43.3 | Unsupported | Unsupported | 6 |
| HP ENVY 5540 printer | Unsupported | 1.33 | Unsupported | 5 |
| Wemo motion sensor | 27.47 | Unsupported | Unsupported | 5 |
| SmartThings hub | Unsupported | Unsupported | Unsupported | 4 |
| Withings Smart sleep sensor | Unsupported | Unsupported | Unsupported | 6 |

**Table 1: Protocol vulnerability and amplification factors**

HTTP, 443 HTTPS) on IoT devices that are present in the home network. It then transfers collected information to the outside attacker in step ②. Upon receiving a trigger message from the attacker (step ③), our malware in step ④ becomes part of the botnet that generates IP-spoofed traffic (by forging the packet header so it contains a victim's address as sender) to IoT devices inside the local home network. The IoT devices will respond (step ⑤) to amplify and reflect these packets to the victim machine in the Internet.

Though the attack above is feasible (as demonstrated later in this paper), it has some limitations. Firstly, IP-spoofing is not possible in some platforms – for instance, Apple iOS does not allow developers to access and modify raw packet information. Secondly, this attack relies on the insider botnet device (containing the malware) to be present and online in the home network. On the flip side, the reflection sourced from an internal botnet can be quite efficient since an UDP-based query can be broadcasted to multiple IoT devices in the home network, triggering them all to reply to the victim, thereby achieving high amplification.

A more sophisticated version of our attack is shown in Fig. 2, which requires an one-off action from the malware to identify and expose household IoT devices to external botnets. The malware first discovers IoT devices in the house (step ①) as before. It then reconfigures the home gateway using an UPnP SOAP command (step ②) to enable port-forwarding, so that query packets from the Internet get forwarded to a specific port of appropriate IoT device in the home that responds to (and amplifies) the query. This will be demonstrated in subsequent sections for multiple IoT devices across multiple home gateway models. Our malware then informs the attacker in step ③ on the public IP address, protocols and port numbers to use for reflecting attacks from this house. The attacker instructs botnet devices (step ④) to source traffic towards this house (step ⑤), which the household IoT devices now amplify and reflect to the victim on the Internet (step ⑥).

# 4 QUANTIFYING THE REFLECTION CAPABILITY

We evaluate traffic reflection using the attack models presented in the previous section applied to eight consumer IoT devices: these include the Samsung smart camera[21], Wemo power switch[5], Wemo motion sensor[5], Philips Hue lighbulb[17], Belkin NetCam[4], HP ENVY 5540 printer[10], SmartThings hub[22], and Withings Smart sleep sensor[25], all chosen as they have fairly high adoption among consumers today. In our laboratory setup all IoT devices are connected to a TP-Link home router model Archer C7 v2 that runs OpenWrt firmware release Chaos Calmer (15.05.1, r48532) and serves as the gateway to the Internet. We wrote Python script that emulates the malware, running on a Macbook Air laptop connected to the LAN side of the home router. Our attacker is an Ubuntu machine (running a PHP script), the victim is a Windows7 laptop, and the external botnet device is a Kali Linux desktop (running python script), all of which are directly connected to the campus network offering public IP addresses.

## 4.1 Attack Amplification

Our first attack is from the internal botnet, which sends a broadcast `M-SEARCH` request for SSDP, and `get-next` request for SNMPv1 (as broadcast request), `get-bulk` request for SNMPv2c (as broadcast request), and unicast `SYN` packet for TCP. For the TCP reflection scenario, we inhibit the victim from sending a `RST` packet to the reflector (which is the likely case when it is overloaded with DDoS attack traffic [14]), which makes the reflector retransmit the TCP `SYN-ACK` repeatedly (4-6 times for the IoT devices we used).

Each IP-spoofed packet generated by the botnet device causes one (in the case of SNMP) or many (in the case of SSDP and TCP) packets to get reflected to the victim. Table 1 shows reflection types (SSDP refleciton, SNMPv1 reflection, SNMPv2c reflection and TCP SYN reflection) supported by each IoT device considered, along with their amplification factor where applicable, which is the ratio of size(s) of reflected packet(s) to the size of the original spoofed request packet. It is seen that all eight IoT devices considered can reflect TCP SYN packets, though the amplification factor is relatively low in the range of 4-6 (arising from retransmissions of the `SYN-ACK`). SNMP is reflected by only two of eight devices considered, again with a relatively low amplification factor, with the SNMPv2 `get-bulk` being more effective than the SNMPv1 `get-next` request. SSDP, supported by half the devices considered, by far yields the highest amplification: for example the Belkin NetCam and Wemo motion sensor amplify attacks by factors of 43.3 and 27.47 respectively. This is because the SSDP response typically contains device information including IP address, name, UUID, management URL, functionalities, etc.; this information can vary among devices, for example the Philips Hue lightbulb's response is about one third of the Belkin NetCam's in bytes.

We also verified that the same attacks work from an external botnet, once the malware has crafted UPnP packets to enable port forwarding on the home gateway. The amplification factors are identical, the only difference being that in the case of SSDP and SNMP the

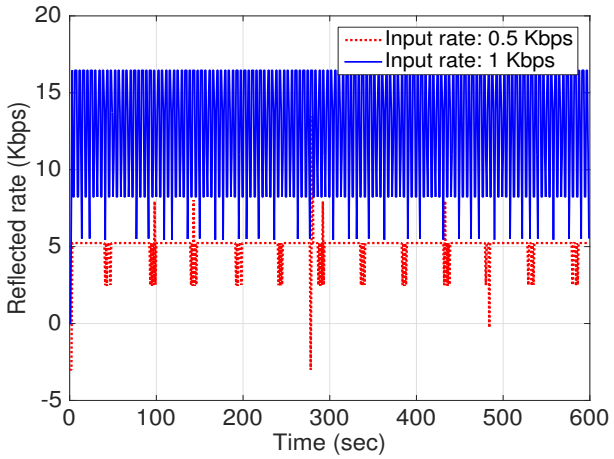


**Figure 3: Reflected SSDP traffic pattern of Philips Hue lightbulb**

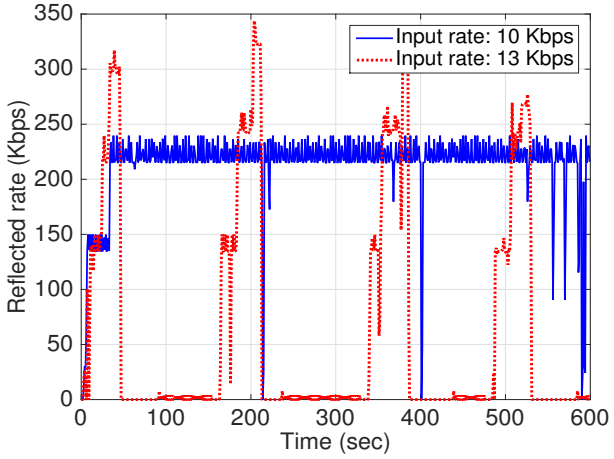


**Figure 4: Reflected SSDP traffic pattern of Wemo power switch**

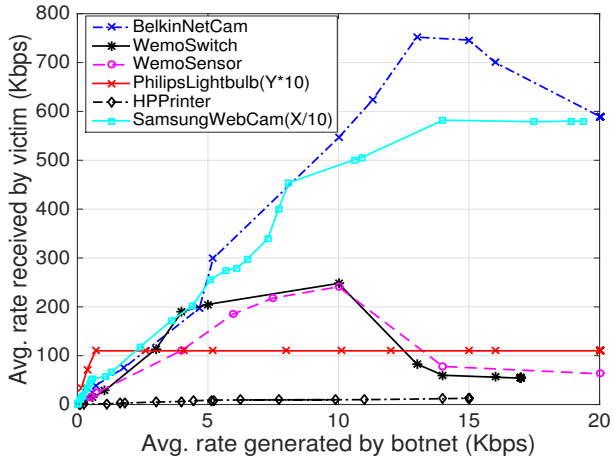


**Figure 5: Input/Output average rate in sustained UDP reflection attack**

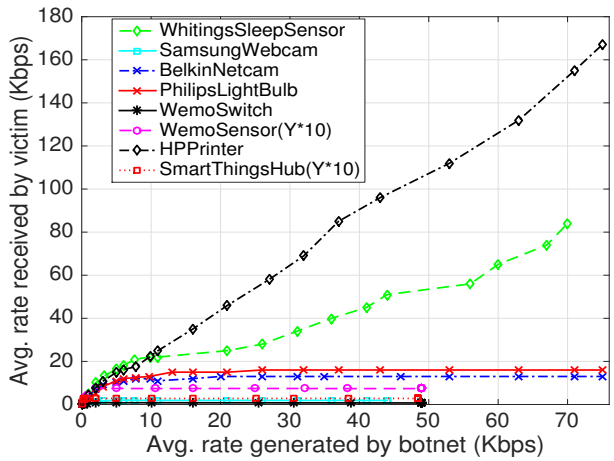


**Figure 6: Input/Output average rate in sustained TCP reflection attack**

`M-SEARCH`, `get-next`,`get-bulk` requests have to be unicast messages (addressed to the home gateway's public IP address on the appropriate port) rather than a LAN broadcast.

## 4.2 Sustaining Attacks

IoT devices are resource-constrained, and we do not expect them to be able to amplify arbitrary volumes of attacks. In this section we therefore quantify the maximum rate and duration for which each IoT device can sustain a reflection attack. We subject each IoT device to bombardment of attack traffic at various rates for a duration of 10 minutes (by adjusting the inter-packet delay and using multi-threading where needed), and observe how its reflected traffic pattern and amplification change with time and traffic rate.

**UDP-based Reflection:** One may note from Table 1 that each IoT device considered supports at most one of the UDP protocols (SSDP or SNMP). We therefore subject these devices to the appropriate UDP traffic at increasing rate. Fig. 3 shows a time-series of the reflected rate from the Philips Hue lightbulb when subjected to two SSDP query rates: when the request rate is 0.5 Kbps, it reflects at around 5 Kbps (dashed red line in plot) and when subject to 1 Kbps it reflects at 12 Kbps (solid blue line). The resulting sustained amplification is therefore around 10-12, which is slightly lower than the amplification of 15 obtained from a single packet (as reported in Table 1, signifying that the efficacy of amplification can fall at higher rates. Indeed, when we increased the query rate above 1 Kbps, the reflected traffic rate and traffic pattern over time do not change, signfying that the device has saturated in its ability to sustain the rate.

In Fig. 4 we show the reflected traffic pattern from the Wemo power switch when subjected to SSDP queries. When the query rate is around 10 Kbps, the device is able to sustain a reflection rate of around 220 Kbps, corresponding to an amplification factor of around

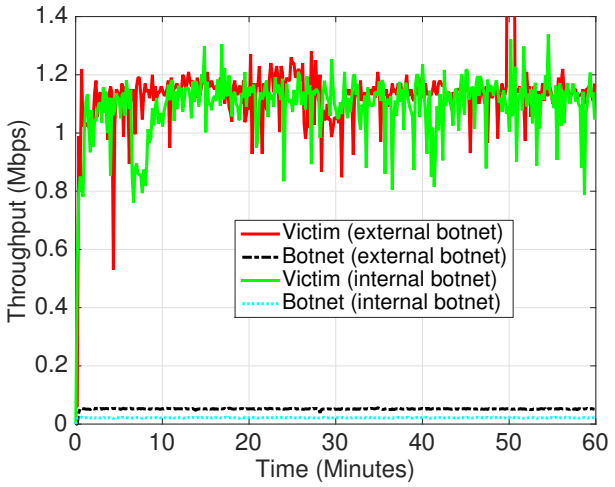


**Figure 7: Aggregated attack traffic from external and internal botnets**

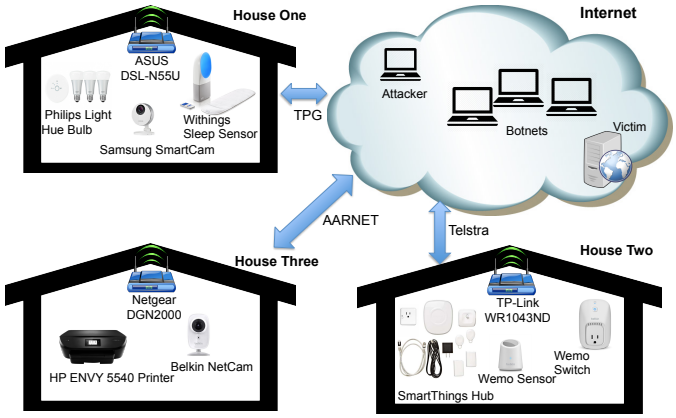


**Figure 8: Residential deployment**

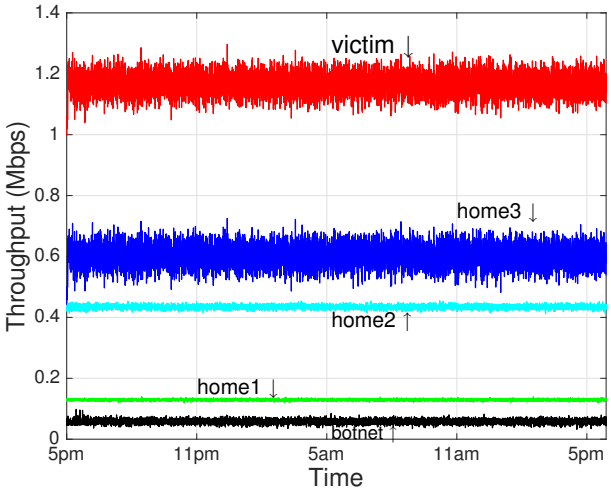


**Figure 9: Reflected aggregated traffic pattern**

22 (consistent with the number of 24 reported on a per-packet basis in Table 1). However, in this case increasing the query rate further causes the device to falter – the figure that at an input rate of 13 Kbps, the device reflects traffic for only about 30 seconds before it becomes unresponsive (itself becoming a victim of a DoS attack!), and requires around 100 seconds to recover back before the cycle repeats. As astute attacker would know the rate to which a device can be pushed so as to sustain the DDoS attack over longer periods. Fig. 5 summarizes the ability of each IoT device considered to sustain attacks, by plotting the average reflected traffic rate (received by victim) as a function of the average input traffic rate (generated by botnet) – the slope of each curve is indicative of the amplification factor. Devices such as the Samsung SmartCam (using SNMPv2c), Philips lightbulb (using SSDP), and HP printer (using SNMPv1) saturate in their ability to reflect attacks (at respective input rates of 140, 0.7 and 15 Kbps), while other devices such as the Belkin Netcam, Wemo motion sensor, and Wemo power switch (all using SSDP) drop markedly in their rate when subject to input traffic in excess of 13, 10, and 10 Kbps respectively.

**TCP-based Reflection:** Table 1 indicates that a TCP SYN packet sent to an IoT device gets amplified by a factor of 4-6. However, experimentation revealed that six of the eight IoT devices considered could not sustain even a few Kbps of TCP SYN requests, and their reflected attack rates never exceed 20 Kbps (i.e. SmartThings hub, Wemo power switch, Wemo motion sensor, Samsung SmartCam, Belkin Netcam and Philips Light Hue bulb are not able to generate sustained attack rates more than 0.3, 0.7, 0.8, 1.9, 13 and 16 Kbps respectively), as depicted in Fig. 6. This is because these IoT devices are not able to maintain more than a few concurrent connections open, possibly because their memory resources get exhausted, and size of each TCP SYN-ACK packet is relatively small (i.e. about several tens of Bytes). The figure also shows that the HP Printer (black dotted line) and the Whithings sleep sensor (green dotted line) are the only ones that can sustain higher reflection rates; however, their amplification factors when reflected average rates exceed 20 Kbps (approximately 2 and 1 respectively) are much lower than expected from Table 1, indicating that the state maintenance in TCP imposes a higher burden on the IoT device, leading to much lower amplification for TCP compared to UDP traffic. Attacks using UDP are therefore more effective, except when the IoT device does not support any UDP reflection (such as the Smart Things hub and Whithing sleep sensor).

## 5 AGGREGATED REFLECTIVE DDOS ATTACK

Having quantified the individual reflection capabilities of the eight consumer IoT devices, we deployed them in aggregate, first in the lab, and then distributed across three homes (belonging to authors on this paper), in order to validate their combined behavior in the real-world.

### 5.1 Lab Environment

All eight IoT devices are connected to a home gateway in our lab, and attack traffic is generated first from internal and then from external botnets. The internal botnet is able to broadcast its SSDP queries (to address `239.255.255.250`) and SNMP v1/v2c requests (to address `192.168.0.255` in our setup), while for the external botnet appropriate port forwarding rules are enabled by the malware to direct queries as unicasts to each device. For the SSDP reflection, the standard M-SEARCH is a broadcast request, our botnet device instead sends unicast UDP packets with the same payload as M-SEARCH request to get it routed to the home gateway. We did not make an overly great effort to optimize the query rates to each specific device – our results in the previous section indicate that every device we considered can sustain input traffic of 10 Kbps, so we kept the rate uniform at this number for UDP and TCP requests across all devices.

In Fig. 7 we show the average reflected traffic rate received by the victim (a computer on campus) over an 1-hour period, and find it to be roughly 1.1 Mbps for both internal and external botnet attacks. The external botnet traffic rate is around 50 Kbps (corresponding to an amplification of over 20), while the internal botnet rate is a lot lower at 20 Kbps, since it broadcasts its queries on the home LAN, giving it a higher amplification factor of over 100.

### 5.2 Residential Environment

We now distributed our IoT devices across three households (belonging to the authors), as depicted in Fig. 8, each having a different home gateway (ASUS, Netgear, and TP-Link) and a different ISP. Python scripts were executed in each household to emulate the malware that discovered available reflective ports of household devices and enabled port forwarding on the respective gateways, and the attacker was hosted on an Ubuntu machine, a Kali Linux machine located on campus representing an external botnet device. Fig. 9 shows the traffic sourced from the botnet device (the bottom black line, averaging at just under 60 Kbps), and the traffic reflected from each of the three houses to the victim was measured (home-1 green line 0.14 Mbps, home-2 light-blue line 0.42 Mbps, home-3 dark-blue line 0.6 Mbps), and found to total 1.16 Mbps (top red line). Further, this amplification of around 20 was sustained for 24 hours from 5pm on 6 Feb 2017 till 5pm on 7 Feb 2017.

## 6 CONCLUSIONS

This paper has explored the feasibility and efficacy of DDoS attacks that use consumer IoT devices as reflectors. We have shown that home gateways can be bypassed by malware inside the home to expose IoT devices as reflectors to external botnets. We have profiled the reflective power of eight popular consumer IoT devices in terms of their amplification factors and sustained rates. We have deployed these IoT devices in real homes to amplify an attack by a factor of 20 to inflict 1.2 Mbps of unwanted traffic on an Internet victim for 24 continuous hours. It is not inconceivable in the near future that 8 million (rather than just eight) IoT devices, mistakenly assumed to be safely hidden behind NAT gateways, are used as reflectors to inflict damage on victims in the form of Terabit-per-second DDoS attacks. While we cannot proffer a ready solution, attempts at limiting the network behavior of IoT devices [7] are worth considering.

## REFERENCES

[1] Arbor Networks. 2017. Insight into the Global Threat Landscape. https://www.arbornetworks.com/insight-into-the-global-threat-landscape. (2017).
[2] Arbor Networks. 2017. No end in sight for DDoS attack size growth. https://pages.arbornetworks.com/rs/082-KNA-087/images/WISR_Infographic_NoEndInSight_FINAL.pdf. (2017).
[3] B. Prince. 2015. DDoS Attacks Using SSDP Spike in Q1: Arbor Networks. http://www.securityweek.com/ddos-attacks-using-ssdp-spike-q1-arbor-networks. (2015).
[4] Belkin International, Inc. 2017. NetCam HD Wi-Fi Camera with Night Vision. http://www.belkin.com/au/F7D7602-Belkin/p/P-F7D7602. (2017).
[5] Belkin International, Inc. 2017. Wemo Switch + Motion. http://www.belkin.com/au/p/F7C027au/#Features. (2017).
[6] C. Rossow. 2014. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. *Network and Distributed System Security Symposium* (2014).
[7] Cisco Systems. 2016. Manufacturer Usage Description Framework. https://tools.ietf.org/pdf/draft-lear-mud-framework-00.pdf. (2016).
[8] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. 2011. A Survey of Mobile Malware in the Wild. *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices* (2011), 3–14.
[9] S. Heule, D. Rifkin, A. Russo, and D. Stefan. 2015. The Most Dangerous Code in the Browser. *Proceedings of the 15th USENIX Conference on Hot Topics in Operating Systems* (2015), 23–23.
[10] HP Development Company, L.P. 2017. HP ENVY 5540 Wireless All-in-One Printer. http://store.hp.com/ukstore/merch/product.aspx?opt=ABU&sel=prn&id=J6U66A. (2017).
[11] J. Condliffe. 2016. How the Internet of Things took down the internet. https://www.technologyreview.com/s/602713/how-the-internet-of-things-took-down-the-internet/. (2016).
[12] M. Kührer, T. Hupperich, C. Rossow, and T. Holz. 2014. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks. *Proceedings of the 23rd USENIX Conference on Security Symposium* (2014), 111–125.
[13] L. Constantin. 2014. Attackers use NTP reflection in huge DDoS attack. http://www.computerworld.com/article/2487573/network-security/attackers-use-ntp-reflection-in-huge-ddos-attack.html. (2014).
[14] M. Kuhrer and T. Hupperich and C. Rossow and T. Holz. 2014. Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks. *USENIX Workshop on Offensive Technologies* (2014).
[15] Market Watch. 2016. Proofpoint uncovers Internet of Things (IoT) cyberattack. http://www.marketwatch.com/story/proofpoint-uncovers-internet-of-things-iot-cyberattack-2014-01-16. (2016).
[16] Arbor Networks. 2017. *DDoS: The Stakes Have Changed. Have You?* Technical Report.
[17] Philips Lighting B.V. 2017. Philips Hue bridge. http://www2.meethue.com/en-au/productdetail/philips-hue-bridge. (2017).
[18] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu. 2007. The Ghost in the Browser Analysis of Web-based Malware. *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets* (2007), 4–4.
[19] S. Khandelwal. 2016. Friday's massive DDoS attack came from just 100,000 hacked IoT devices. http://thehackernews.com/2016/10/ddos-attack-mirai-iot.html. (2016).
[20] V. Sivaraman, D. Chan, D. Earl, and R. Boreli. 2016. Smart-Phones Attacking Smart-Homes. *Proc. ACM WiSec* (2016).
[21] SmartCam. 2017. SmartCam Products: SNH-P6410BN. https://www.samsungsmartcam.com/web/. (2017).
[22] SmartThings, Inc. 2017. Samsung SmartThings Hub. https://www.smartthings.com/works-with-smartthings/hubs-and-kits/samsung-smartthings-hub. (2017).
[23] T. Seals. 2017. Leet IoT Botnet Bursts on the Scene with Massive DDoS Attack. https://www.infosecurity-magazine.com/news/leet-iot-botnet-bursts-on-the-scene/. (2017).
[24] United States Computer Readiness Team. 2014. UDP-based amplification attacks. https://www.us-cert.gov/ncas/alerts/TA14-017A/. (2014).
[25] Withings SA. 2017. Sleep Sensor Accessory. https://www.withings.com/fr/en/products/aura/sleep-sensor-accessory. (2017).