Patch Pilgrimage: Exploring the Landscape of TCP Reflective Attacks and User Patching Expedition

Joost Oortwijn
Delft University of Technology
Delft, The Netherlands
J.Oortwijn@student.tudelft.nl

Carlos H. Gañán
Delft University of Technology
Delft, The Netherlands
C.HernandezGanan@tudelft.nl

ABSTRACT

The proliferation of Internet-connected devices has led to a concerning increase in cyberattacks. Among these, a novel attack technique has emerged, which involves the use of TCP reflective amplification attacks to launch large-scale Distributed Denial of Service (DDoS) assaults. This technique has proven to be more effective than UDP-based amplifiers, underscoring the pressing need for immediate attention. In this study, we delve into the heart of this vulnerability by examining the characteristics of vulnerable devices and the security practices of their users. Our findings highlight two critical aspects: first, devices can remain unpatched for extended periods, and second, their amplification rates can exceed those of traditional DDoS amplification vectors. Through network scans, we identified over 30,000 vulnerable devices within a single Internet Service Provider (ISP). These devices encompass a wide range of types, from alarm systems to energy monitors. In collaboration with the ISP, we conducted semi-structured interviews with the users of these vulnerable devices. Our interviews revealed that while vulnerability notifications have the potential to motivate end-users to update their devices, comprehensive descriptions are essential for accurate identification and the subsequent implementation of necessary software and firmware updates.

CCS CONCEPTS

• **Security and privacy → Vulnerability scanners**.

KEYWORDS

Vulnerability patching; IoT security; DDoS

ACM Reference Format:
Joost Oortwijn and Carlos H. Gañán. 2024. Patch Pilgrimage: Exploring the Landscape of TCP Reflective Attacks and User Patching Expedition. In *The 39th ACM/SIGAPP Symposium on Applied Computing (SAC '24), April 8–12, 2024, Avila, Spain.* ACM, New York, NY, USA, Article 4, 10 pages. https://doi.org/10.1145/3605098.3635982

1 INTRODUCTION

The rapid proliferation of internet-connected devices has revolutionized numerous aspects of our lives, facilitating seamless communication, efficient data transfer, and unparalleled convenience [24]. However, the widespread connectivity also brings forth substantial cybersecurity challenges as malicious actors seek to exploit vulnerabilities within these interconnected systems. Among the myriad of threats, Distributed Denial of Service (DDoS) attacks continue to be a major concern [13], capable of paralyzing online services and inflicting significant financial losses.

Traditionally, DDoS attacks have predominantly relied on User Datagram Protocol (UDP)-based protocols for their amplification and reflection techniques [23]. However, the DDoS landscape is constantly evolving, unveiling new attack vectors that necessitate exploration. One such emerging threat is the exploitation of Transmission Control Protocol (TCP) reflective amplification, offering attackers novel opportunities to launch large-scale DDoS assaults [2]. This newly discovered attack vector capitalizes on the sophisticated functionalities of middleboxes, such as firewalls and network address translators, to amplify and redirect TCP traffic toward targeted systems.

This study delves into the specific properties associated with TCP reflective amplification attacks and how to mitigate vulnerable devices. While prior studies have primarily focused on UDP-based attacks, the characteristics and implications of TCP reflective amplification remain relatively unexplored. By examining vulnerable devices, comprehending end-user security behaviors, and assessing the effectiveness of vulnerability notifications, we bridge the gaps in understanding and provide valuable insights into mitigating this emerging threat.

We conduct extensive research around two key areas of exploration. Firstly, we conducted scans within our partner ISP's network, revealing key insights. Employing two distinct scanning methods, we observed fluctuating counts of vulnerable devices across autonomous systems, with energy monitors accounting for a substantial portion of devices. The initial spike of vulnerable devices was followed by a decrease, suggesting successful mitigation efforts. Furthermore, our analysis highlighted the variable lifetimes of vulnerable devices, with some devices remaining vulnerable for more than a year. Amplification factors exhibited substantial diversity, with an average factor of approximately 37.45 and notable outliers exceeding 5000, underscoring the urgency of addressing these vulnerabilities within our partner's network.

Secondly, we analyze end-user behavior patterns concerning patching vulnerable devices, shedding light on their actions, update practices, and potential security implications. Our results show that the majority of the users of these vulnerable devices check for updates when prompted. However, some took no action, citing generic content or unclear patching information. A minority sought help, while a few boosted overall security without directly addressing the issue. For device updates, automatic updates were common, along

SAC '24, April 8–12, 2024, Avila, Spain

ACM ISBN 979-8-4007-0243-3/24/04.
https://doi.org/10.1145/3605098.3635982

with notifications-triggered updates. A few proactively checked for updates, while others left it to third parties. Conversely, reasons for not updating ranged from unawareness to perceived unnecessary updates or concerns about disruptions. The main contributions of this paper are as follows:

- We conducted large-scale scans within the autonomous systems of an ISP to identify devices vulnerable to TCP reflective amplification attacks. Over a period of one and a half years, we identified a total of 30,821 vulnerable devices.
- We characterized these devices, identifying each type and its amplification factor. Our results show that the amplification factor averages around 38, with a maximum of almost 10,000.
- We modeled the patching time of each of these devices using Kaplan-Meier survival curves. The results show a median patching time of less than 10 days, but with a maximum of more than a year for devices that are never patched.
- We conducted fifteen semi-structured interviews with the owners of these vulnerable devices. Our results show a diverse set of reasons for not patching, ranging from not being aware to neglecting the threat because the device was working properly.

2 RELATED WORK

2.1 DDoS attacks

Distributed Denial-of-Service (DDoS) attacks are orchestrated attempts to disrupt the normal operation of servers, services, or networks by overwhelming them with excessive internet traffic [13]. The execution of DDoS attacks involves several stages [12, 13, 19] and victims [28]. Initially, attackers must recruit internet-connected devices, or bots, to launch the attack. These bots can be any internet-enabled device, and their recruitment methods depend on the specific DDoS attack type. Attackers often exploit vulnerabilities to gain partial control over these devices. Once recruited, the bots can be remotely manipulated by the attacker to either initiate attacks or enlist additional bots, forming a botnet. The attacker then leverages this botnet to orchestrate a continuous flood of traffic toward a target, rendering its services inaccessible to legitimate users.

Amplification reflection attacks on services using the TCP protocol differ from attacks on UDP-based services. UDP protocols are attractive for amplification reflection attacks due to their one-way traffic nature, allowing attackers to abuse services that employ this transportation protocol [1, 18, 22]. Commonly exploited UDP-based services include SSDP, SNMP, DNS, NTP, and NetBios. Attackers can generate reflection by sending a short query message to a vulnerable service, which responds with a large reply packet directed at the victim.

TCP-based services are less vulnerable to amplification reflection attacks due to the three-way handshake principle, which verifies sender IP addresses. However, TCP services can still be exploited for such attacks. Recent research by Bock et al. (2021) focuses on leveraging vulnerable middleboxes, like firewalls and intrusion detection systems, for TCP reflective amplification attacks [2]. Middleboxes have characteristics favorable for this attack, responding to incomplete handshakes and forbidden URL requests, facilitating amplification. TCP reflective amplification attacks involving vulnerable Internet of Things (IoT) devices operate similarly but with distinctions. In IoT devices, amplification occurs at the destination device, not intermediaries. Improper TCP configurations in IoT devices cause them to respond to incomplete handshake requests with HTML landing pages. Bock et al. [2] identified millions of IP addresses for TCP amplification attacks, with 82.9% being middleboxes and the rest various internet-connected devices. These attacks result in high amplification factors, often exceeding UDP-based attacks, attributed to victim-sustained loops and routing loops when vulnerable middleboxes are involved, generating substantial traffic towards victims.

2.2 Consumer Vulnerability Management

Vulnerability notifications aim to inform end-users about vulnerable or malware-infected devices for remediation. While earlier studies (e.g., [14], [26], [4], [5]) have demonstrated the positive impact of notifications on patching when detailed information is directly provided to network operators, the inadequacy of security advice persists [27], resulting in vulnerable devices.

However, trust in the sender is crucial for notification effectiveness, with various studies highlighting the role of sender reputation [7], [20], [25]. Notification channels, including email, telephone calls [10], postal mail, walled garden, instant messaging, SMS, and web browser notifications, vary in effectiveness and feasibility. Combining multiple channels can improve remediation rates [15].

Notification content should be clear, easily understandable, and tailored to end-users. While some studies suggest comprehensive content (e.g., [6], [17]), others advocate simplicity [9]. Understanding end-users' technical abilities is crucial, as indicated by Rodríguez et al. [20, 21].

3 METHODOLOGY

The methodology employed in this paper utilizes a mixed methods approach, i.e., we combine quantitative data gathered via large-scale Internet measurements and qualitative interviews with end-users. The quantitative analysis involves conducting `NMAP` scans, landing page analysis, and manual scanning to gather information on the characteristics of vulnerable devices. The qualitative interviews provide insights into end-users' behavior and perception of vulnerability notifications. This comprehensive approach enables a more holistic understanding of the remediation of consumer-grade vulnerable devices, enhancing the validity and reliability of the findings.

3.1 Data Sources

We leverage three distinct data sources. Firstly, quantitative data on vulnerable middleboxes or IoT devices is obtained from a third-party organization called *The Shadowserver Foundation*. The second data source consists of quantitative data acquired through network scanning of IP addresses with vulnerable devices. The third source is qualitative data obtained through semi-structured interviews conducted with end-users of vulnerable devices.

The Shadowserver data serves as the initial point for this paper, offering insights on IP addresses assigned to vulnerable devices from April 25th, 2022, to February 19th, 2023. Additionally, the IP addresses reported by Shadowserver serve as input for IP scans, which constitute the second data source.

Network scans provide quantitative data on the characteristics of vulnerable devices. This data facilitated the setup of an experiment. In this experiment, end-users of vulnerable devices are notified about the vulnerability through a vulnerability notification. Subsequently, interviews are conducted with these users.

3.1.1 Vulnerable DDoS Middlebox reports. Shadowserver initiated daily reporting on vulnerable middleboxes in April 2022. Scans are performed similarly to the method described by Bock et al. [2], involving the identification of vulnerable middleboxes through custom TCP packet scanning. The scans are executed by sending two types of custom TCP packets to port 80: a `SYN` packet with an `HTTP GET` payload for a forbidden URL (e.g., pornography or gambling sites) and a SYN packet followed by a `PSH + ACK` packet with an `HTTP GET` payload request for a forbidden URL, using sequence numbers.

The daily reports from Shadowserver allow this research to track IP addresses with vulnerable devices over time. These reports include the observed amplification factor, IP address, basic geographical information, and are filtered to include only IP addresses of interest. It is important to note that while Shadowserver scans for vulnerable middleboxes, the results suggest that the reported IP addresses may also include IoT devices with broken TCP implementations. Therefore, the data provided by Shadowserver serves as the starting point for identifying IP addresses and end-users analyzed in this research.

3.1.2 Network Scans. Mapping information on vulnerable devices is achieved through three types of scans conducted in a chronological order.

- **NMAP:** NMAP [16] is utilized to identify open ports, services running on these ports, and other device information. Scanning the IP addresses reported by Shadowserver with NMAP helps identify the characteristics of most vulnerable devices.
- **Landing Page Analysis:** To complement the NMAP scan data, the URL landing pages of the IP addresses (accessible via port 80) are analyzed. These landing pages provide insights into the device type and brand name, further characterizing the devices.
- **Manual Scanning:** As the identified and analyzed IP addresses are based on Shadowserver's reports of vulnerable middleboxes, additional scanning is required to validate the findings. Manual scanning involves sending custom TCP packets using a Python script. Unlike Shadowserver's scans, the script sends packets with a normal URL instead of a forbidden one, aiming to determine if devices are exclusively middleboxes or other IoT devices. The responses from vulnerable IP addresses are captured using tcpdump and analyzed. This data validation process identifies the devices causing the reported amplification, based on the captured HTML pages after sending the custom TCP packets.

3.1.3 End-User Interviews. Interviews are conducted with end-users who owned vulnerable devices within our partner ISP's network. The purpose of these interviews is to examine the efficacy of vulnerability notifications, explore end-user updating behavior, understand their characteristics, perception of notifications, and actions taken. The interview protocol comprises an introduction and content sections about the purpose of the research. Conducted over the phone, interviewees are unaware of the research or vulnerability until notified. Thus, a comprehensive introduction precedes semi-structured questions. To ensure quality, the protocol drew insights from prior partner ISP studies and underwent expert review.

In total, 31 end-users were contacted, with a 48.4% response rate. Interviews averaged 11 minutes and 20 seconds. This adheres to established best practices that suggest the inclusion of 12-20 participants to offer substantial guidance for forthcoming quantitative research and to craft recommendations that can be broadly applied in the field [11]. Thematic analysis using Atlas.ti software identified themes such as end-user characteristics, device identification, actions taken, update behavior, and incentives for updating.

4 CHARACTERIZING VULNERABLE DEVICES

To identify devices vulnerable to TCP reflection attacks, we employ a scanning process utilizing custom TCP packets crafted to elicit amplified responses. Our scanning initiative encompasses IPv4 addresses on the specific country where the partner ISP operates, deploying two distinct methods:

- The first method entails dispatching a `SYN` packet with sequence number 's', immediately followed by a `PSH + ACK` packet with sequence number 's+1'. This `PSH + ACK` packet contains an `HTTP GET` payload request specifically targeting a forbidden resource as configured by the middlebox.
- The second method involves sending a `SYN` packet comprising an `HTTP GET` payload request for a forbidden resource in the same middlebox configuration context.

4.1 Number of vulnerable devices

Figure 1 represents the number of vulnerable devices for the top five autonomous systems (ASes) with the most vulnerable devices within the targeted country. The data spans from April 25, 2022, to July 31, 2023. During this period, the number of vulnerable devices per AS fluctuated, with some ASes consistently having a high number of vulnerable devices while others experienced fluctuations in device counts. AS-0 has the highest count of vulnerable devices, with a mean of approximately 1,448 vulnerable devices per day. On the other hand, AS-3 has only 458 vulnerable devices per day, with a mean count of 205.84, closely followed by AS-4 with 460 vulnerable devices per day and a mean count of 2038.50. AS-2 and AS-1 have mean counts of 416.03 and 207.85 vulnerable devices per day, respectively. The standard deviation is relatively low for AS-1, AS-2, and AS-3 at 68.87, 35.22, and 35.43, respectively, suggesting less variability in daily vulnerable device counts within these ASes. AS-4, with a standard deviation of 658.92, demonstrates more variability. The minimum daily amount of vulnerable devices across all ASes is 12, while the maximum is 246. Our partner ISP comprises different ASes, one of them being the one with the largest number of vulnerable devices at the start of the monitoring period.

It is worth noting that during some periods, other ASes had a considerably higher number of vulnerable devices compared to the top five autonomous systems. This could imply that smaller or less prominent autonomous systems collectively contributed to a significant portion of the vulnerable devices.

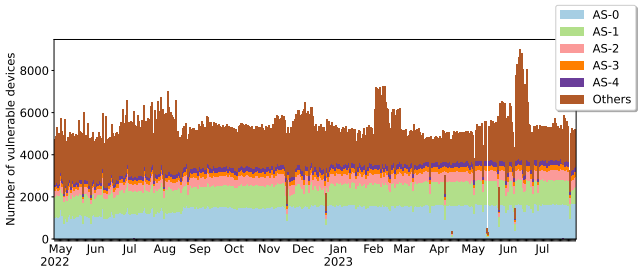

Figure 1: Daily number of devices vulnerable to TCP amplification attacks

4.2 Vulnerable device types

In this section, we delve into the diverse range of vulnerable devices identified within the ASes of our partner ISP. We identified various device types that can potentially lead to TCP reflected amplification attacks. The distribution of these devices is shown in Table 1.

Table 1: Distribution of Vulnerable Devices

Device Type	Distribution
Energy Monitor	23.2%
Firewall	18.1%
Building management system (BMS)	6.5 %
Digital video recorder (DVR)	5.2%
Router	6.5 %
Washing machine	1.5%
Alarm system	1.3 %
WiFi extender	1.0%
Others	38.7%

Our analysis reveals a wide array of device types, and notably, not all of them fit the typical description of a middlebox. Within the identified devices, energy monitors are the primary contributors to observed amplification, accounting for a significant percentage of the devices. These energy monitors share the same brand and type, designed for monitoring household energy consumption. The second most common type of vulnerable device are firewalls which is more aligned with the concept of middlebox. Beyond energy monitors and firewalls, the representation of other vulnerable device types is comparatively lower. We observed the presence of building management systems (BMS) in a smaller proportion, along with a limited number of alarm systems, washing machines, WiFi extenders, and DVRs. Notably, no significant brand similarities were identified among these devices, except for energy monitors and a couple of BMS units.

To ensure the accuracy of our findings, we conducted manual scanning to pinpoint vulnerable devices, including energy monitors, alarm systems, washing machines, WiFi extenders, and BMS units. However, it is important to note that manual validation was not possible for all IP addresses. This limitation may arise from occasional device power-offs, causing intermittent disconnection from the internet. During interviews, one such incident was observed when an end-user turned on their washing machine, leading to a response when manually scanning the corresponding IP address, confirming the washing machine as the source of the problem. While we assume that devices identified through `nmap` scans, URL landing page analysis, and interviews are causing the issues, this conclusion cannot be drawn with absolute certainty.

4.3 Amplification factor

Figure 3 shows the cumulative distribution function (CDF) for amplification factors in devices vulnerable to TCP-amplification attacks. With a total of 30,821 vulnerable devices, these exhibit an average amplification factor of approximately 37.45, highlighting the potential for significant amplification within this group. Around 90% of these devices had an amplification factor of 100 or lower. It is important to note the relatively high standard deviation of 222.50, indicating a wide range and variability in amplification factors. At the lower end, we see a minimum amplification factor of 0.76, emphasizing that even the smallest factors are noteworthy. In terms of quartiles, the 25th percentile reveals a median amplification factor of 8.44, suggesting that a substantial portion of devices maintains relatively low amplification. The median itself, at 8.56, reinforces this trend. The 75th percentile, at 10.80, hints that some devices can achieve notably higher amplification factors. Interestingly, the dataset's maximum amplification factor peaks at an astonishing 9,299, indicating the presence of outliers with exceptionally high amplification capabilities.

Next, we break down the amplification factor per device type. In Figure 2, we provide a visual representation of the distribution amplification factors depending of the type of device. This graph is split into five amplification ranges, showing the highest observed amplification factors for each device type and the number of devices contributing to these levels of amplification.

The observed amplification factors, as illustrated in Figure 2, indicate that the majority of the identified devices generate amplification factors of up to 500. Of significance is the presence of a peak in energy monitors within the range of 1001-5000. Additionally, an alarm system, WiFi extender, and BMS are also found within this range. This observation highlights the existence of multiple vulnerable devices within the ISP's network, capable of significant TCP reflection amplification, with amplification factors surpassing 1000 at the time of this study. Furthermore, three devices exhibited amplification factors exceeding 5000, although they can be considered outliers due to their substantial deviation from the others, with the firewall in this range even reaching an amplification factor of over 150,000.

We determined that the average maximum amplification factor is 2801, a notably higher value compared to average amplification factors observed in commonly used UDP-based protocols. Second, the presence of three significant outliers in the data significantly elevates the average maximum amplification factor. Even without these outliers, the average remains relatively high.

Third, we observed notable variation in amplification among energy monitors, which is linked to the presence of a password-protected mechanism. Despite the identical nature of these devices, the responses generated by scanning queries are contingent upon the presence or absence of a password. In the absence of a password, the HTML response includes a more extensive display, showcasing

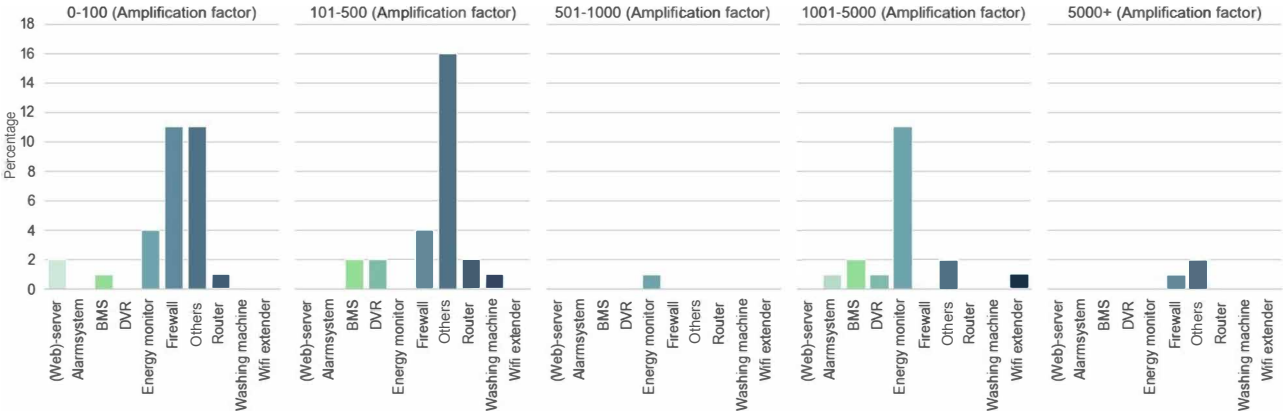

Figure 2: Distribution of the amplification factor per device type

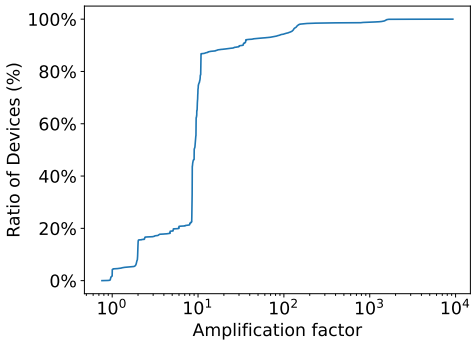

Figure 3: CDF of the amplification factor per device.

the entire landing page of the device with various energy values for monitoring. This results in an amplification factor of approximately 1600. Conversely, when a password is in place, the device generates a more concise landing page, resulting in an amplification factor of approximately 71. The latter landing page only contains a login mechanism, in contrast to the comprehensive landing page displayed without a password, resulting in significantly smaller amplification.

Finally, it is worth noting that a majority of the IP addresses are not reported daily during the time period between their initial and final appearances in the abuse data. On average, only 62.5% of the days between a vulnerable IP's first and last appearance in the abuse data are reported by Shadowserver. This can be partially attributed to devices not being consistently powered on. However, some devices are expected to remain connected to the internet at all times. The IP scans revealed that devices do not respond to every scan, necessitating multiple custom TCP packets to elicit a response, leading to amplification. The reason behind these devices' unresponsiveness to Shadowserver scans, despite no modifications being made to them, remains unclear. Nonetheless, this explains why vulnerable devices are not reported by Shadowserver every day.

5 DEVICE VULNERABILITY LIFETIME

Our dataset spans 462 days and tracks vulnerable devices over this period, shedding light on crucial aspects of vulnerability management. One of the key takeaways from the data is the notable persistence of vulnerabilities. The mean lifetime of vulnerable devices in the dataset stands at ten days, indicating that, on average, a vulnerable device remains at risk for more than seven months. However, some vulnerable devices persisted for as long as 400 days, highlighting a concerning trend where vulnerabilities can endure for extended duration, posing a continuous risk to organizations.

Another significant observation is the gradual decline in the number of vulnerable devices over time. This decline suggests that ISP subscribers patched or remediated vulnerable devices, albeit at varying rates. It underscores the importance of timely vulnerability management practices to reduce the overall exposure to threats.

To further gain insights into the duration of the vulnerability, we employ the Kaplan-Meier estimator to analyze the temporal dynamics of device vulnerabilities within an organizational context. The Kaplan-Meier estimator is a powerful non-parametric method widely used in survival analysis to estimate the probability of an event, in this case, the resolution of device vulnerabilities, occurring at various points in time. This statistical technique enables us to elucidate the survival probabilities of vulnerabilities over time, providing a formal representation of their persistence and the effectiveness of vulnerability management strategies.

The Kaplan-Meier estimator, denoted as $\hat{S}(t)$, estimates the survival probability at a specific time point t. It is calculated as follows:

$$\hat{S}(t) = \prod_{i:t_i<t} \left(1 - \frac{d_i}{n_i}\right)$$

Where: $\hat{S}(t)$ = Estimated survival probability at time t. t_i = Time of occurrence of the i-th event (in our case, vulnerability resolution). d_i = Number of events (vulnerabilities resolved) at time t_i. n_i = Number of devices (vulnerabilities at risk) just prior to time t_i.

This formula allows us to quantitatively assess the survival probabilities of vulnerable devices over time and investigate the factors influencing their persistence or resolution. The results of the estimation are shown in Figure 4. We noticed that a significant drop in

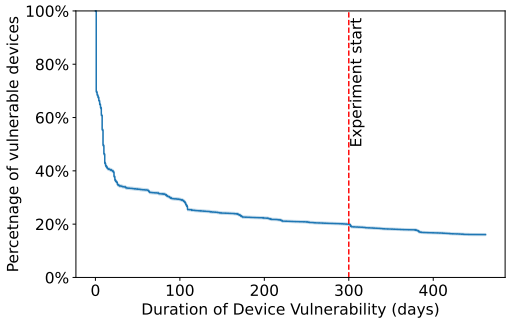

Figure 4: Kaplan-Meier Survival Estimates

the number of vulnerable devices occurred within the first week, primarily attributed to the issuance of an automatic patch by Palo Alto to address their PAN-OS vulnerable software (CVE-2022-0028). This swift response resulted in approximately 60% of vulnerabilities being remediated, showcasing the organization's rapid mitigation capability for critical vulnerabilities. Subsequently, over the course of 30 days, an additional 10% of vulnerabilities were resolved, indicative of an ongoing, albeit slower, remediation process, possibly involving less critical or more complex fixes. Further analysis revealed that after six months, an additional 5% of vulnerabilities were addressed, with the remaining 5% being remediated after a year. Leaving around 20% of vulnerable devices to this type of amplification attacks for more than a year. This long tail of vulnerable devices is the one we studied in the qualitative analysis by contacting their owners through the ISP.

6 END-USER ANALYSIS

In this subsection, we examine the results of interviews conducted with 15 users identified as the owners of the vulnerable devices via a partner ISP. These interviews focused on understanding the user's Internet-connected device update practices and perceptions regarding the security notifications.

6.1 User characteristics

During the interviews, an array of questions was posed to discern the characteristics of the end-users. Previous research (e.g., [3]) has shown that age and gender can impact cybersecurity behavior. First and foremost, the age distribution of the interviewees was ascertained, revealing that the average age of respondents was 60 years old. This age demographic slightly exceeded the average age of the wider population of customers, which stood at 55 years old. Remarkably, only one interviewee (R11), constituting the youngest participant at 34 years of age, represented an outlier within this relatively senior cohort. This disparity emphasized the skew towards higher age averages, with respondent 12 at the other end of the spectrum, being 86 years old, serving as another conspicuous outlier.

The second facet explored during the interviews pertained to the gender distribution of the interviewees. Of the 15 participants, 12 identified themselves as male, whereas the remaining 3 (comprising 20% of the total) identified as female. This gender distribution indicated an overrepresentation of males within the subset of interviewed customers compared to the broader gender distribution among the customer population, where men accounted for 55.64%, women 41.38%, and the remaining 2.98% fell under the category of 'unknown.'

The third dimension under scrutiny involved assessing the interviewees' self-perceived competence in computer security on a scale from 0 to 5. On average, respondents regarded their computer security skills as relatively proficient, with an average score of 3.9. Remarkably, the self-assessed scores corresponded closely with the interviewees' perceptions of their own abilities. Notably, several respondents (specifically respondents 1, 5, 6, and 14) disclosed backgrounds in ICT or cybersecurity. Nonetheless, some interviewees demonstrated a certain dissonance between their self-perceived ability to manage device security and their actions. For instance, respondent 2 stated feeling uncertain about handling computer security matters, despite self-rating at 3 on the scale. This phenomenon was also observed with respondents 8 and 9, who, while expressing reservations about their technical proficiency, similarly assigned themselves a score of 3 on the 0 to 5 scale.

The interviews also aimed to determine the nature of end-users in terms of their internet usage –whether for business or personal purposes. The overwhelming majority of interviewees indicated that their internet connection was used for personal, rather than business, purposes. Two participants confirmed the utilization of their internet connection for commercial purposes.

6.2 User's Identification of Vulnerable Devices

As part of the interviews, we asked the users to identify what devices they thought would be the vulnerable ones as detected by our scans. Given the diverse array of devices susceptible to misuse, it was anticipated that not all end-users would successfully pinpoint the vulnerable device.

Challenges in Identifying Vulnerable Devices: The first challenge for the users was to even remember which of their devices were connected to the Internet. In general, end-users possess multiple smart devices within their residences. The collective average, when considering all interviewed end-users, is four smart devices per household. It is worth emphasizing that this estimation is grounded in the devices specifically identified by the interviewees themselves. However, it is important to note that not all interviewees possessed a comprehensive understanding of what constitutes a smart device. For instance, respondent 2 admitted, *'My husband does not think it [BMS] has been updated; I myself had never realized that it was using WiFi.'* To obtain a more accurate count, interviewees were prompted and provided with suggestions during the interviews to identify as many smart devices as possible. Nevertheless, it is conceivable that the actual number of smart devices within the households of the interviewees is higher.

Interviews also highlighted difficulties in correctly identifying the specific vulnerable device. Only four out of eleven interviewees successfully located the device mentioned in the email. However, it is worth noting that two of these interviewees, during the interview, identified the vulnerable device but also cited numerous other devices they believed could potentially be problematic. For instance, respondent 5 stated, *'After reading the email, I did not know what*

the device could be; you would be surprised how much of that junk you have in your house these days. But the first devices at which I took a look were the energy monitor and the camera system as those were explicitly mentioned.' Respondents 8 and 15 were the sole interviewees who directly identified the vulnerable device. However, both respondents clarified that their identification was not based on the information provided in the notification. Respondent 8 explained, *'We do not have smart devices in our home except our washing machine. This device must be the cause of the problem as we opened all ports to be able to use it. I know it is not safe, but it is the only way to make that thing work.'* Despite the washing machine not being explicitly mentioned in the email, this respondent identified the device based on the fact that it was the only smart device in the household. Respondent 15 identified the vulnerable device by deducing that it must be the new device recently installed shortly before receiving the email notification.

The remaining seven respondents encountered difficulties in identifying the device responsible for the problem. These respondents often relied on their own reasoning rather than the examples of devices provided in the notification. Among these interviewees, four identified a device that did not have the specific vulnerability. Curiously, all four of these end-users shared a common rationale for their identification: they had recently purchased a new device, and shortly thereafter, they received the security notification from the ISP, leading them to conclude that the new device was likely the source of the problem. Two of the seven interviewees simply did not inspect any of their devices, either due to their lack of computer security knowledge (respondent 9) or the perception that the issue was not urgent (respondent 7). The remaining interviewee (respondent 3) mistakenly believed the router to be the vulnerable device. It is conceivable that this respondent did not explore other potential devices mentioned in the email due to incomplete reading.

Remarkably, respondents tended to pinpoint devices they had purchased themselves rather than devices provided by third parties, such as routers provided by an ISP. Ten out of the eleven respondents revealed that they had personally acquired the devices. However, two respondents clarified that they were not responsible for the installation and management of the devices, despite purchasing them. These two respondents were respondent 2 and respondent 4, who owned a vulnerable building management system and alarm system, respectively. Although they had acquired these systems themselves, they were not in charge of installing or managing them. The sole exception was respondent 7 who employed the internet connection for business purposes. This respondent explained, *'I was not here yet when this heating system was installed or bought, so I don't know.'*

6.3 User's Remediation Actions

Respondents were asked about their performed actions after reading the security notification.[1] The different actions are shown in Table 2. It could be that an interviewee performed multiple actions; therefore, the total number of executed actions is higher than the number of interviewees.

[1]Note that four participants did not receive a notification due to the lack of contact details.

Table 2: Performed actions after receiving notification.

Action	*# Users*
Check software update device	5
No action performed	3
Ask someone for help	2
Set password (smart) device	1
Execute port scan	1
Install anti-virus software	1

The most mentioned action was in line with the vulnerability notification, which advised looking for updates for the suggested (vulnerable) devices. Five of the 11 interviewees checked a device for updates, assuming it might be causing the problem. However, none of these five interviewees installed a software update, as their devices were already up-to-date. For example, respondent 1 stated, *'After reading the email, I visited the website of the manufacturer of the energy monitor to see if they have something mentioned about this issue there, but there was nothing there and it explained that my device is already up-to-date.'* The action of checking for software updates was the intended behavior of the interviewees after receiving a notification. However, only respondents 8 and 15 checked the device perceived as vulnerable to TCP reflective amplification attacks. The other three respondents checked for updates on devices that are likely not the problem, thus not fully addressing the issue discussed in this paper.

Other interviewees (n=3) mentioned that they did not perform any action in response to the notification. The reasoning differs among these three interviewees for not doing anything. Respondent 4 explained, *'The information provided was really generic, also when clicking on the exclamation mark in the email you get directed to a standard ISP commercial page. This made that whole email lose all its power as it made me think that nothing serious is happening on my internet connection.'* Respondent 7 did not perform any actions as he/she did not receive the email because it was sent to another email address. The person who received the email explained that he/she deleted the email simply because: *'I'm only responsible for the financial part of the internet connection and not the technical part.'* The one responsible for the internet connection (respondent 7) was never notified by this person. Respondent 11 mentioned that he/she did not perform any actions because he/she thought that sending a large file was the 'trigger' for the ISP to send an email. Additionally, there were two interviewees that asked someone for help after receiving the notification.

Finally, it should be noted that some interviewed participants (n=3) took actions aimed at enhancing the security of their internet connection but did not address the issue of TCP reflective amplification attacks. For instance, Respondent 5 secured his/her energy monitor by setting a password. The respondent stated, *'I decided to use the password functionality for the energy monitor. I already knew that it was possible to use a password but I didn't think it was scary for that device to be open to the internet.'* This action did not fix the broken TCP protocol, thus the device can still be used for launching TCP reflective amplification attacks. Nonetheless, the amplification factor is substantially smaller when the password functionality is

used. Respondent 2 and Respondent 6 implemented measures to enhance the security of their network. Specifically, Respondent 2 installed a virus scanner, while Respondent 6 performed a port scan to identify vulnerabilities in his/her network. Although these actions represent steps in the right direction towards securing their own internet connection, they did not address the issue of a device with a broken TCP protocol in their network. As such, the desired impact was not realized. However, it is noteworthy that these measures had the positive side effect of enhancing the overall security of their internet connection.

6.4 User's Device Update Behavior

The respondents were surveyed regarding their approaches to updating their Internet-connected devices. Given that the interviewees often possess numerous devices within their households, different devices may require distinct updating protocols. For instance, automatic updating may be suitable for one device, while manual checking may be necessary for another. As such, interviewees may describe multiple practices for updating their (smart) devices. These different practices are visualized below in Table 3.

Table 3: User practices to update their devices

Update practices	*R1*	*R2*	*R3*	*R4*	*R5*	*R6*	*R7*	*R8*	*R9*	*R10*	*R11*	*R12*	*R13*	*R14*	*R15*
Update automatically	X		X	X	X	X			X	X	X	X	X	X	X
Update after notification	X	X	X					X		X		X		X	X
Update after check						X				X					
Not updating devices							X								
Device managed by 3rd party		X		X									X		

Interviewees (n=12) rely on automatic updates for their smart devices or believe that their smart devices are automatically updated, although they may not be entirely certain. Even if end-users are aware that not all devices are updated automatically, they may not fully comprehend the associated risks or are willing to take those risks. For example, respondent 11 stated: *'I always set the devices of the big brands to be done automatically, and I have to be honest; then I also blindly assume that this is also done automatically. I have to say that sometimes I find out by chance that that doesn't happen, but I don't actively check it.'* Respondent 4 explained that: *'I also have devices that I do not update, I wonder if my router amplifier can be automatically updated. I assume all equipment is just automatically updated. I do not check whether updates are available for the smart equipment but assume that it just happens.'* Only respondents 4 and 11 exclusively stated that they rely completely on automatic updates, while others, who also mentioned that updates occur automatically, also explained that they do not depend solely on this feature.

Another update practice for smart devices, as mentioned by interviewees (n=9), is to install updates in response to notifications indicating the availability of an update. Only respondent 8 indicated that he/she exclusively relies on these notifications. This can be explained by the fact that the same respondent stated that he/she only has one smart device within their household. Seven out of nine interviewees indicated during the interview that they not only rely on updating their smart devices after receiving notifications but also possess devices that update automatically. This observation might suggest a heightened level of awareness regarding which devices can be updated in their households, as they can differentiate between varying updating practices. In contrast, those interviewees who rely solely on one updating practice may have a comparatively lower level of awareness.

Only few interviewees (n=2) do actively check if their smart devices are up to date with the latest software or firmware. However, this is probably often done on an ad-hoc basis. For example, respondent 6 stated: *'I don't look at it every day, but for example when I have time during the weekend, I go through everything. That way I keep it all a bit up to date.'* Another interviewee, respondent R10, mentioned: *''Coincidentally, I did update the energy monitor a few weeks ago because new firmware was available,'* but later the same respondent explained that: *''I was already busy with it [energy monitor], and then I saw somewhere that a new update was available.'*

According to interviewees (n=3), the task of updating some smart devices falls to a third party, even if end-users own the devices themselves. These devices were found to be part of alarm systems and building management systems that were installed by a third party. Therefore, these interviewees suggested that the responsibility for updating these devices rests with the third party.

Incentives for Updating: The interviewees expressed multiple incentives for updating smart devices in their households. These different incentives are displayed below in Table 4, including the number of times the interviewees named these incentives for updating their smart devices.

Table 4: Reasoning interviewees for updating smart devices

Reasons for Updating	*R1*	*R2*	*R3*	*R4*	*R5*	*R6*	*R7*	*R8*	*R9*	*R10*	*R11*	*R12*	*R13*	*R14*	*R15*
Externally prompted updating	X	X	X		X			X	X	X	X	X	X		X
Security	X	X				X	X		X			X		X	
Happens automatically			X								X			X	
New functionalities		X													
Device does not work							X								

Interviewees (n=11) emphasized that their decision to update their smart devices was influenced by external incentives, although they did not specify a particular rationale for doing so. They mentioned updating in response to receiving a notification or based on the fact that updates are always suggested or recommended. For example, respondent 10 stated: *'Actually, from all the devices I have at home, I get a ping when new firmware is available; in fact, the software and firmware of every device mentioned is up to date because I already do that.'* Similarly, respondent 6 explained: *'... and then I usually get a message that an update is available. And I do that by default if devices support it.'* Often, interviewees also mentioned that they update their smart devices for security reasons; this was mentioned by 7 interviewees. Respondent 9 expressed this by stating: *'Because it [updating] is recommended. Lately, you are getting scared of all those hacks that are being performed, so I try to secure everything as well as possible.'* Another interviewee, respondent 1, who also mentioned security as a reason, used different reasoning for the explanation: *'I update that because it's safe and because it's recommended. I'm pretty into it [the topic of computer security] myself, so I'm pretty sharp on that.'*

Other interviewees (n=3) explained that (some) smart devices are updated automatically and did not further specify their reasoning

for updating. For example, respondent 4 states: *'... I just assume everything happens automatically.'* Only one interviewee mentioned that he/she updates for new functionalities, although respondent 2 was talking about his/her tablet when stating: *'I always do the updates myself when I get a message stating that it [tablet] would work better and that it is [tablet] better secured.'* Finally, it is worth noting that only one interviewee provided an explanation for not updating their smart devices, stating that he/she does not update his/her devices as long as the devices continue to perform their intended functions satisfactorily: *'... to be honest, it [smart devices] works, and I didn't really think about it [not updating] being a security issue, so for the church, that was the most important thing, and for me, that was the reason I didn't consciously do this [updating] in the past.'* However, the respondent expressed concern about the security issue during the interview and mentioned that he/she will take action for security reasons afterward.

Incentives for Not Updating: In addition to expressing incentives for updating their smart devices, interviewees were also asked for their reasons for not updating their smart devices. The different responses are shown in Table 5.

Table 5: Reasons given by interviewees for not updating devices.

Reasons for Not Updating	*R1*	*R2*	*R3*	*R4*	*R5*	*R6*	*R7*	*R8*	*R9*	*R10*	*R11*	*R12*	*R13*	*R14*	*R15*
Unaware of update capability		X	X	X	X	X			X		X	X			
No reason for not updating	X							X		X			X	X	X
Interrupts daily business					X						X				
It already works							X								

The interviewees (n=14) explained that they do updates unless they are unaware that a particular device can be updated. Nonetheless, respondent 7 argued that as long as the smart devices performed satisfactorily, he/she did not see the need for updating the device. Additionally, respondents (n=2) contended during the interviews that end-users can refrain from updating their smart devices due to disruptions in their devices' performance. Nevertheless, both interviewees clarified that they only delay the updating process rather than entirely abstain from it. Interestingly, respondent 3 mentioned during the interview: *'If I'm going to update and reset, then I'm afraid I'll end up in a pandemic of adjustments where I'll need my son again, so I'm very hesitant to do that.'* As this interviewee did not explicitly mention this when asked about his/her reasoning for not updating, it is not included in Table 8. Nonetheless, this perspective offers valuable insights into why the participant may choose to postpone or overlook the installation of a specific update.

Finally, interviewees were asked whether they think a notification by the ISP helps them with updating their smart devices. The respondents (n=9) explained that a notification might help them remember to update. Respondent 5 explains: *'I think so. It's a warning anyway, and you don't want there to be a problem, so that's good.'* On the other hand, the other interviewees (n=6) do not perceive any benefit from receiving a notification. The majority of these individuals clarified that they already make an effort to keep their smart device software up to date and thus consider such notifications by the ISP redundant. For example, respondent 4 argues: *'No, I already do it [updating], that is why this would appear redundant to me.'*

7 DISCUSSION

In this paper, we have investigated the issue of vulnerable middleboxes and IoT devices that can be exploited for TCP reflective amplification attacks, focusing on understanding the types of vulnerable devices and end-user behavior within an ISP's network. Amplification factors originating from vulnerable IoT devices are considerably significant, surpassing those typically associated with widely-used UDP-based protocols. This underscores the potential threat posed by these relatively few devices, despite their limited quantity.

Our research positions this vulnerability type at different stages within the patching life cycle. Middleboxes affected by this vulnerability are mostly closer to the resolution phase, with some devices having received and implemented patches remotely. In contrast, vulnerable IoT devices in a consumer network that are at an earlier stage of the life cycle, with no identified patches available, remain vulnerable for longer periods of time.

When manual patching is the only path to vulnerability remediation, users play a critical role. Our interviews showed that while end-users exhibit motivation and capability in keeping their devices up to date, they require comprehensive information to accurately identify the device in need of remediation. Notably, end-users express a preference for receiving extensive information when notified of vulnerabilities. While this observation is based on a limited sample size, it suggests that comprehensive vulnerability notifications may be more effective, challenging the notion that simplicity is always preferred. This desire for additional information may be influenced by end-users' high perceived proficiency in computer security.

Our study uncovers a unique challenge related to third-party management of vulnerable devices. In cases where third parties oversee device management, it can be unclear who bears responsibility for updates. This complicates the effectiveness of vulnerability notifications, as end-users may not feel accountable for devices managed by third parties. Finally, our research highlights the predicament of certain devices that cannot be remediated due to the absence of available updates. This raises questions about the role of device manufacturers in ensuring product security and prompts consideration of alternative notification methods beyond email, such as walled garden notifications, to compel end-users to remove vulnerable devices from the internet.

Limitations: Despite these valuable insights, our study is not without its limitations. These limitations include a limited sample size, which restricts the generalizability of findings, and our study's focus on a single ISP's consumer market, limiting the broader applicability of results. Certainly, we acknowledge that our research possesses high ecological validity due to our engagement with real-world operational settings within the ISP's abuse department. This approach allowed us to work directly with genuine data, processes, and professionals involved in addressing security issues, enhancing the authenticity and applicability of our findings to practical contexts. Lastly, the characterization of vulnerable devices is limited to those identified during the study period, which may not account for devices vulnerable before our research commenced.

Ethics Our interview protocol received approval from our institution's human research ethics committee. Participants consented

to anonymous participation and call recording, with the option to withdraw. Adhering to the Menlo Report [8], we respected privacy and legal principles by following our ISP partner's guidelines and keeping all data on their premises. Anonymized datasets were created in collaboration with the ISP. Unfortunately, the ISP did not allow public data release. Justice was maintained by offering equal opportunities to all infected customers for sharing their experiences. For beneficence, all subscribers with vulnerable devices were notified. Interviews aimed to enhance ISP customer support and contribute to understanding how users handle persistent vulnerable devices for societal benefit.

8 CONCLUSIONS

This paper has shed light on the issue of vulnerable devices susceptible to TCP reflective amplification, underscoring that the problem goes beyond middleboxes used for censorship and also affects consumer-grade devices. By performing network scans, we identified two distinct categories of vulnerable devices: vulnerable middleboxes, often used for business purposes, and consumer IoT devices with broken TCP protocol implementations, predominantly utilized in broadband networks. While middleboxes have seen significant progress in remediation through automated patching, the persistent absence of available updates to address broken TCP protocols in consumer IoT devices continues to pose a substantial risk.

Our results showed that devices with automatic update mechanisms are patched faster, normally within ten days since the release of the patch, while devices that require manual patching can last more than a year without patching. For these devices, the intervention of the ISP can play a major role and security notifications can lead to mitigation in a wide majority of cases. By conducing interviews with the owners of these devices, we also revealed that end-users are motivated and capable of performing updates when they are aware of their availability, often in response to notifications. However, the effectiveness of vulnerability notifications depends on their specificity and the presence of actual updates.

ACKNOWLEDGMENTS

This work is supported by the Dutch Research Council (NWO) under the RAPID project (Grant No. CS.007).

REFERENCES

[1] Radu Anghel, Swaathi Vetrivel, Elsa Turcios Rodriguez, Kaichi Sameshima, Daisuke Makita, Katsunari Yoshioka, Carlos H. Gañán, and Yury Zhauniarovich. 2023. Peering into the Darkness: The Use of UTRS in Combating DDoS Attacks. In *European Symposium on Research in Computer Security (ESORICS)*.

[2] Kevin Bock, Abdulrahman Alaraj, Yair Fax, Kyle Hurley, Eric Wustrow, and Dave Levin. 2021. Weaponizing middleboxes for TCP reflected amplification. In *30th USENIX Security Symposium (USENIX Security 21)*. 3345–3361.

[3] Dawn Branley-Bell, Lynne Coventry, Matt Dixon, Adam Joinson, Pam Briggs, et al. 2022. Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies* 2022 (2022).

[4] FO Çetin, C Gañán, EM Altena, Takahiro Kasama, Daisuke Inoue, Kazuki Tamiya, Ying Tie, Katsunari Yoshioka, and MJG van Eeten. 2019. Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai. In *Network and Distributed System Security Symposium (NDSS) 2019*.

[5] Orçun Çetin, Carlos Gañán, Lisette Altena, Samaneh Tajalizadehkhoob, and Michel Van Eeten. 2019. Tell me you fixed it: Evaluating vulnerability notifications via quarantine networks. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 326–339.

[6] Orcun Cetin, Carlos Gañán, Maciej Korczynski, and Michel van Eeten. 2017. Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning. In *16th Workshop on the Economics of Information Security (WEIS 2017)*.

[7] Orcun Cetin, Mohammad Hanif Jhaveri, Carlos Gañán, Michel van Eeten, and Tyler Moore. 2016. Understanding the role of sender reputation in abuse reporting and cleanup. *Journal of Cybersecurity* 2, 1 (2016), 83–98.

[8] David Dittrich and Erin Kenneally. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research.

[9] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. 2016. Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 97–111.

[10] Artur Geers, Aaron Ding, Carlos Gañán, and Simon Parkin. 2023. Lessons in Prevention and Cure: A User Study of Recovery from Flubot Smartphone Malware. In *Proceedings of the 2023 European Symposium on Usable Security (EuroUSEC '23)*. Association for Computing Machinery, New York, NY, USA, 126–142.

[11] Greg Guest, Arwen Bunce, and Laura Johnson. 2006. How many interviews are enough? An experiment with data saturation and variability. *Field methods* 18, 1 (2006), 59–82.

[12] Nazrul Hoque, Dhruba K Bhattacharyya, and Jugal K Kalita. 2015. Botnet in DDoS attacks: trends and challenges. *IEEE Communications Surveys & Tutorials* 17, 4 (2015), 2242–2270.

[13] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and other botnets. *Computer* 50, 7 (2017), 80–84.

[14] Frank Li, Zakir Durumeric, Jakub Czyz, Mohammad Karami, Michael Bailey, Damon McCoy, Stefan Savage, and Vern Paxson. 2016. You've got vulnerability: Exploring effective vulnerability notifications. In *25th USENIX Security Symposium (USENIX Security 16)*. 1033–1050.

[15] Jason Livingood, Nirmal Mody, and Mike O'Reirdan. 2012. *Recommendations for the Remediation of Bots in ISP Networks*. Technical Report. https://www.rfc-editor.org/rfc/rfc6561

[16] Gordon Lyon. 2008. Nmap Network Scanning. (2008).

[17] Arman Noroozian, Elsa Turcios Rodriguez, Elmer Lastdrager, Takahiro Kasama, Michel Van Eeten, and Carlos H Gañán. 2021. Can ISPs help mitigate iot malware? A longitudinal study of broadband ISP security efforts. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 337–352.

[18] Rebaz Rashid Nuiaa, Sivasankar Manickam, and Ali Hussein Alsaeedi. 2021. Distributed Reflection Denial of Service Attack: A Critical Review. *International Journal of Electrical and Computer Engineering (IJECE)* 11, 6 (2021), 5327.

[19] Elsa Rodríguez, Radu Anghel, Simon Parkin, Michel Van Eeten, and Carlos Gañán. 2023. Two Sides of the Shield: Understanding Protective DNS adoption factors. In *32nd USENIX Security Symposium (USENIX Security 23)*. 3135–3152.

[20] Elsa Rodriguez, Max Fukkink, Simon Parkin, Michel van Eeten, and Carlos Gañán. 2022. Difficult for Thee, But Not for Me: Measuring the Difficulty and User Experience of Remediating Persistent IoT Malware. In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*. 392–409.

[21] Elsa Rodríguez, Susanne Verstegen, Arman Noroozian, Tomohiko Inoue, Daisukie-and Kasama, Michel van Eeten, and Carlos H. Gañán. 2021. User Compliance and Remediation Success After IoT Malware Notifications. *Journal of Cybersecurity* 7, 1 (2021). https://doi.org/10.1093/cybsec/tyab015

[22] Christian Rossow. 2014. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In *Proceedings 2014 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2014.23233

[23] Haris Sinanovic and Srdjan Mrdovic. 2017. Analysis of Mirai Malicious Software. In *2017 25th International Conference on Software, Telecommunications and Computer Networks*. 1–5. https://doi.org/10.23919/SOFTCOM.2017.8115504

[24] Statista. 2022. *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030*. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[25] Ben Stock, Giancarlo Pellegrino, Michael Backes, and Christian Rossow. 2018. Didn't You Hear Me? - Towards More Successful Web Vulnerability Notifications. In *Proceedings 2018 Network and Distributed System Security Symposium*.

[26] Ben Stock, Giancarlo Pellegrino, Christian Rossow, Martin Johns, and Michael Backes. 2016. Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification. In *USENIX Security Symposium (USENIX Security 16)*. 1015–1032.

[27] Veerle van Harten, Carlos Gañán, Michel van Eeten, and Simon Parkin. 2023. Easier Said Than Done: The Failure of Top-Level Cybersecurity Advice for Consumer IoT Devices. *arXiv preprint arXiv:2310.00942* (2023).

[28] Swaathi Vetrivel, Arman Noroozian, Daisuke Makita, Katsunari Yoshioka, Michel van Eeten, and Carlos H Gañán. 2023. Birds of a Feather? A Comparative Analysis of DDoS Victimisation by IoT Botnet and Amplification Attacks. In *22nd Workshop on the Economics of Information Security (WEIS 2023)*.