# "Anyone Else Seeing this Error?": Community, System Administrators, and Patch Information

1st Adam Jenkins
*School of Informatics*
*University of Edinburgh*
*Edinburgh, UK*
*adam.jenkins@ed.ac.uk*

2nd Pieris Kalligeros
*School of Informatics*
*University of Edinburgh*
*Edinburgh, UK*
*pieriskalligeros@yahoo.gr*

3rd Kami Vaniea
*School of Informatics*
*University of Edinburgh*
*Edinburgh, UK*
*kami.vaniea@ed.ac.uk*

4th Maria K. Wolters
*School of Informatics*
*University of Edinburgh*
*Edinburgh, UK*
*maria.wolters@ed.ac.uk*

***Abstract*—Applying regular patches is vital for the timely correction of security vulnerabilities, but installing patches also risks disrupting working systems by potentially introducing unknown errors. System administrators must manage the challenges of patching using a combination of reliance on best practice and available information to best match their organizations' needs. In this work, we study how patch-related activities are supported by the mailing list of the website PatchManagement.org which is dedicated to the task. We qualitatively coded 356 list emails sent between March and July, 2018, to understand how members interact with the list community. Based on our results, we argue that the mailing list is an example of an Online Community of Practice, where practitioners engage in communal learning and support. We find that the community supports members in multiple phases of the patching process by providing workarounds before a patch is available, guidance prioritizing released patches, and helping with post-patch trouble. Additionally, the community provides help around tool selection and facilitating discussions.**

***Index Terms*—Human factors, Security usability, Technology social factors**

## 1. Introduction

Patch management is a difficult task, requiring system administrators (sysadmins) to have a strong understanding of their system components, obtain good information about potential patches, and apply them to the systems without incident. The task is also difficult because of the unknowns around how a system will react to a patch.

The Meltdown [1] and Spectre [2] patches are a good example of the security importance related to updates, as well as the uncertainty as to the outcome of patching. In January 2018, the two new critical vulnerabilities were announced. They affected all modern processors, allowing malicious programs to access and read information stored in memory, including memory used by other programs running on the same processor. Large vendors, such as Google, Apple, Microsoft, and IBM quickly released patches (aka updates) to protect users. The following week, Microsoft was forced to pull its patches due to users complaining about unbootable PC's [3]. Hoax websites also started appearing offering malware laden Meltdown/Spectre patches [4].

Patching is crucial to security, the majority of compromises involve an exploited vulnerability for which a patch exists, but has not yet been installed [5], [6]. From a purely security viewpoint, installing patches quickly is vitally important. Official patch advice, such as the UK Government's "Cyber Essentials" scheme recommends that patches be applied within two weeks of release [7]. Yet, in the wild we still do not see critical patches being as widely installed as they should be. For example, the WannaCry malicious software took several UK National Health Service trusts offline blocking patients from accessing health care. The associated patch had been available for a full two months before the attack, but had not been installed [8]. Similarly, HeartBleed – a serious vulnerability that provides anyone with a dump of current server memory – was still an issue three years after the patch release as a third of systems had still not applied the patch patch [9]. Recent work shows that this situation has not improved [10].

Despite the security positives of patch installation, sysadmins are still nervous about installing them. Patches have a long history of coming not only with security improvements, but also with problems [11]. Code Red, a computer worm from the early 2000's, famously featured a faulty patch solution, followed by a second less faulty patch which most people installed, and finally a third good patch that few installed because the second one mostly worked [12]. More recently, a Windows 10 update in 2018 created chaos for users when the patch caused serious data loss by deleting the Documents folder [13]. One of the roles of a sysadmins is to balance the security needs of patching quickly against the risks of installing a problematic patch, which can be challenging [14]. A recent Avast report [15] found that 55% of software was out of date, raising serious concerns about the nature and current state of patch management policies, and signalling to academia that more must be done to understand the nuances of patch management [16].

Our work aims to expand on the research community's understanding of sysadmins' information seeking behaviors around patch management by conducting a qualitative analysis of the prominent mailing list: PatchManagement.org. Recent work has indicated that similar information sources are being used by sysadmins during the initial stages of assessing a patch [17], and we present the first analysis of such a data source. This mailing list is dominated by Microsoft related content, as seen


DOI 10.1109/EuroSP48549.2020.00015

in Figure 1, so we provide a contextual focus to the information shared on the list by narrowing our focus to that of Windows Update.

In this work, we qualitatively code 356 list emails sent between March and July, 2018, to understand how the list community interacts. Based on our results, we argue that the mailing list is an example of an Online Community of Practice, where practitioners engage in communal learning and support.

Our primary questions when analyzing the list were:

- RQ1 In what ways do contributing members of PatchManagement.org engage with the list?
- RQ2 What types of information is shared or requested by sysadmins in the community?

We find that the PatchManagement.org community supports members in multiple phases of the patching process from providing guidance on pre-patch mitigation, information to support patch prioritization, suggesting workarounds for error-prone patches, and sourcing information on potential errors. We detail the community effort in contributing advice on tool selection and facilitating discussions of best practice approaches to patch management.

## 2. Related Work

### 2.1. SysAdmins and Their Work Practices

Most of what we know about the day-to-day activities of sysadmins is based on a sequence of ethnographic studies [18]–[27] which were later compiled into a book [28]. The studies show that beyond the obvious technical requirements, the role also requires extensive collaboration and communication with other sysadmins. The systems that sysadmins work on can have many components that cross boundaries between teams, organizations, and expertise. Consequentially, their work depends on establishing *grounding* [29]–[31], where they form a common understanding of the behavior of a system with other sysadmins. This is followed by a joint understanding of who will do what work, when, and how they will go about it. The grounding activity is vital because each sysadmin involved may have only a fractional view of the system as well as access control limitations on their potential actions. Grounding is necessary, partially because sysadmin work represents a *distributed cognitive system* [18], [32] where multiple members of a group work together to complete a task as a single cognitive unit.

To illustrate these issues, Kandogan et al. [28, p.19-49] provide a case study of a web admin, "George," attempting to set up a new server, but running into an error. Notably, in George's example, he has to communicate with many other sysadmins to solve the problem partially because each sysadmin he contacts has a different set of knowledge, view of the system, or access control rights. The Firewall team, for example, has the ability to change firewall settings which George's server needs. The software vendor knows about the weird intricacies of their system that may not be in documentation. To succeed, George must build an understanding of how the system works (situational awareness) and facilitate communication among the people helping him to build a communal shared knowledge of the problem (information broker).

**Situational Awareness.** Having a strong "sense of their system" supports sysadmins engaging in troubleshooting behaviors as it helps them pinpoint likely sources of problems. Tools are also used to view the current system status with sysadmins putting strong emphasis on the accuracy, verification, reliability, and credibility of tools they use [33], resulting in team members using very different sets of tools in an effort to match their needs [34].

As systems grow in size, so do the challenges of maintaining situational awareness. Hrebec and Stiber [35] surveyed 54 sysadmins who reported, on average, a 77% understanding of their systems. They also found that 86% of respondents were self-taught. When asked how they would troubleshoot for an issue they did not already know how to solve, answers included: researching technical documentation (23.58%), web, bulletin board systems, and newsgroups (43.47%), and consultation with others with experience (24.75%).

**Information Brokers.** The term "Technical Brokers" was coined by Velasquez and Weisband [36] to highlight the role sysadmins play in "translating" technical information and knowledge into a digestible format for their organizations. They found that sysadmins broker information between end users, members of their technical community, and the systems they work with. De Souza, Pinhanez, and Cavalcante [37], [38] studied outsourcing organizations and similarly found that sysadmins collect information from a range of sources when solving problems, including: customers, customer account brokers, and other employees who work with customers. Similar to others, they also find a prominence of communication and collaboration tools (e.g. instant messenger etc.) to facilitate communication with 59.36% stating they used these tools when dealing with incidents.

### 2.2. Security and Sysadmins

Sysadmins who focus on security tasks are often more event driven, with a high focus on collaboration to help spread the load of highly complex scenarios and associated risks. Additionally, due to the rapid developing nature of cyber-security, security admins have a steeper learning curve [23], [26]. Kramer and Carayon [39] interviewed 16 sysadmins (8 security admins and 8 network admins) on the human and organizational factors related to cyber-security, and analyzed the data using models of human error and macro-ergonomics to interpret accidental errors. They found that organizational factors were the most prominent aspect. Other works have focused on task specific usability issues or solutions, such as configuration languages [40]–[42], the deployment of HTTPS [43], and the diagnosing of security issues [44]. These results indicate that much work is still required to make these tools, and process usable, with consideration for the unique workload and flow required by sysadmins.

**2.2.1. Updates and SysAdmins.** Relatively little is known about sysadmins' needs and work practices around software updating. Crameri et al. [45] surveyed 50 sysadmins as part of their development of Mirage, a distributed

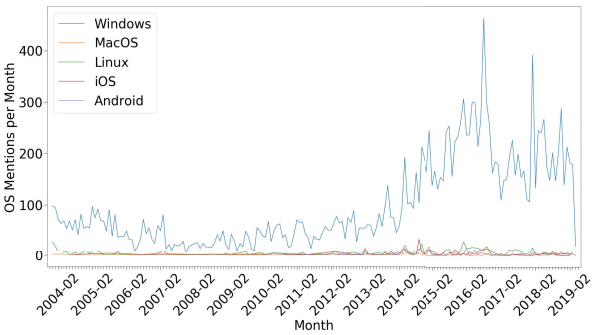


Figure 1: Number of times each OS was mentioned in list emails per month.

framework for patch deployment. The survey found that 90% of sysadmins applied patches once a month or more to their systems, and reported security fixes as the main purpose of applying updates. They also found that 70% of sysadmins would avoid or delay updating if problems arose, and when asked to estimate the failure rate of patches, the average was 8.6%. More recently, Li et al. [17] conducted a survey of 102 sysadmins, and performed a further 17 in-depth interviews to determine their process, and its impact on patching effectiveness. They found that information impacted patching decisions, but there was no centralized hub of information, forcing sysadmins to find information from a range of sources including: official vendor notifications (71%), security advisories (78%), professional mailing lists (54%), online forums (53%), news (39%), and blogs (38%). The survey also found that sysadmins continued to source information through various means after installation, such as 55% reporting that problematic updates were found through end-users of clients complaints. In the post application state where errors were present, the strategy used by the majority of sysadmins was to uninstall the offending update (47%) resulting in a functional but insecure system state. Sysadmins then had to scramble to find workarounds or fixes by themselves, or with software vendors.

### 2.3. End-Users and Updates

While sysadmins are generally aware of the link between updates and security, there is a lack of end-user awareness as to the security critical nature afforded to updates [16], [46]–[50]. This difference has been highlighted repeatedly, with IT security experts rating software updates as an effective security practice [51]–[53] while end users do not list [51]. It therefore comes as no surprise that end-users avoid or delay updating, inadvertently increasing their vulnerability time frame [48], [54]. Reasons for the circumventing updates include annoying interruptions to users' workflows [47], [49], [55], or confusing and unwelcome UI alterations [48], [54], [56], [57].

## 3. Windows Update and Patch Tuesday

As mentioned previously, a large percentage of the PatchManagement.org emails focus on Microsoft-related patches (Figure 1) which are released in monthly cycles. This focus on Microsoft makes sense as it is still the most popular Operating System (OS), running on around 88.80% of all desktop platforms [58]. We give an overview of Microsoft's patching process to help the reader understand the context the email list exists within.

Microsoft's patching process has been through many variations. Prior to Windows 98, patches were only posted on a website where users could download them, but no Microsoft-produced automated process existed for downloading and installing them. With the release of Windows 98, the Critical Update Notification Utility [59] was added as a background process that would automatically check the website for new "Critical" patches and notify the user if they were found. In 2000, Windows ME shipped with "Automatic Updates", a tool that automatically checked for patches, but only once the user had opted-in for the feature. Windows XP SP2 changed the default settings to automatically download and install patches with users having the right to opt-out [49]. As a result of the defaults change, Microsoft saw Windows XP patching rates jump from 5% to 90% [60].

On the administration side, before Windows XP and 2000, there was no easy way to centrally deploy or manage patching. Then, around 2003, Microsoft released the Software Update Service (SUS) for Windows XP and 2000 [61]. SUS provided control and centralisation by allowing administrators to run their own local "Windows Update" servers which allowed them to select which patches should and should not be deployed in their organisation. The Automatic Update software on the organization's computers would then point at the local update server and automatically install the sysadmin's selected patches. SUS was a powerful tool, but it still lacked many crucial features, such as varying patching platform (i.e. servers or desktop), which wouldn't arrive until the release of SUS's successor Windows Server Update Service (WSUS) in late March 2005. Additionally, WSUS allowed sysadmins to implement staged deployment of patches for testing purposes before a full deployment.

Starting October 2003, all Microsoft product updates are released on the second Tuesday of every month, unofficially dubbed "Patch Tuesday". On Patch Tuesday all available patches are released at once between the hours of 17:00 and 18:00 UTC, with related information such as Knowledge Base (KB) articles following soon after. The KB articles are important because they provide a unique number for the patch as well as documentation such as the update's purpose, related system or platform, known issues, and workarounds.

Historically, the second Tuesday was chosen as it was theorized that it would allow sysadmins the full Monday to fix any issues found in their system over the weekend, before having to manage the updating process. The scale and dominance of Patch Tuesday has resulted in some companies piggybacking off of the model, with Adobe also releasing their patches on the same day. Attackers have also normalized to the cycle, with the next day now unofficially called "Exploit Wednesday." They also download and analyze the patches, find changes the patch makes (vulnerability locations), and then develop exploits to target unpatched platforms.

Prior to Windows 10, patches were released separately for each issue and sysadmins could select which patches

to install or not. With the release of Windows 10 Microsoft switched to a cumulative updating model for all Windows versions where each version of Windows theoretically receives only two patches each month: the cumulative patch and the security-only patch. Installing the cumulative patch installs all outstanding updates for the system for the current month and prior months. Installing the security-only update will only patch security issues for the current month. Cumulative updates are potentially problematic for security because they force sysadmins into an all-or-nothing situation. Previously they could selectively block patches that were having issues while installing the others, but with the cumulative model, if any of the changes cause problems, the whole patch must be blocked and they have no option of installing non-problematic elements.

## 4. PatchManagement.org

PatchManagement.org, has been in existence since December 2003, and is the first mailing list dedicated to the topic of patch management. It was designed to be used by network and sysadmins along with security professionals to discuss the latest events and information related to patching, with no restriction on vendor or operating system. It encourages discussion of a range of topics including experiences with released patches, and "how-to" questions regarding deployment or assessment of patches. The list's charter does have some restrictions on post content. Most notably for this research, is the restriction of announcements regarding vulnerabilities, unless they are accompanied with a mitigation.

Moderation is provided by several key members of the patching community, from whom we have received consent to conduct community-respectful research using the mailing archive. Furthermore, research we have produced is being shared with them to allow for feedback and validation. The list is hosted by Ivanti, and the emails posted through the mailing list are stored on MARCive online. In April 2019, after data collected for this study was completed, the list re-located to a Google Group.

### 4.1. List Data Collection

We scraped the PatchManagement.org mailing list archive in April of 2019 using a custom Python script to automatically download the emails from MARCive and stored them and accompanying metadata in a secure PostGreSQL database. We used the Beautiful Soup library [62], to strip HTML and extract the plain text. The study design was certified by our ethics panel (#84622).

Sender emails were also processed to ensure that multiple presentations of the same sender were linked together. Host information was then extracted from email addresses and used to determine the likely country of origin and the sector using FortiGuard's Web Filter [63]. Out of respect for the list community, we avoid any discussion of specific organizations, and instead focus on sector and region of the world to describe members.

### 4.2. List Demographics

We collected a total of 63,536 emails with send dates ranging from December 2003 to April 2019. Figure 2

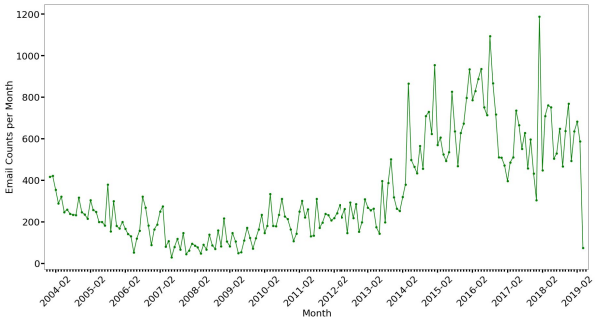


Figure 2: Total number of emails sent per month for the whole history of the list.

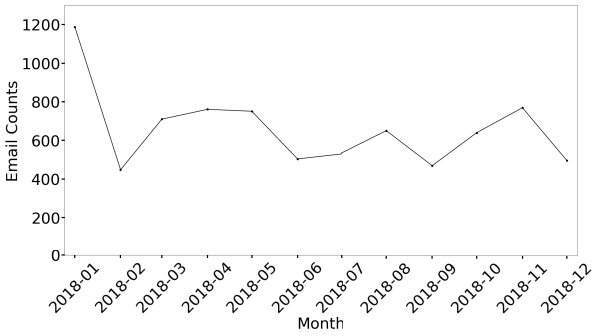


Figure 3: Total number of emails sent per month in 2018.

shows the total numbers of emails sent per month for the whole dataset, and Figure 3 shows emails sent only in 2018. Both figures show the wide variation of month-to-month email counts. Figure 2 also illustrates how the list has shrunk and then grown over time, with the recent up-tick in emails roughly corresponding to the increased focus on patching as a preventative security practice as well as the industry-wide shift towards making patching automated [48], [51]. Taking a closer look at the most recent complete year, 2018, Table 1 and Figure 2 show that the number of overall emails are increasing, with a slightly higher number of total emails, senders, and email threads with no replies.

We searched the emails for Operating System names (Windows, MacOS, Linux, iOS, and Android) to understand their relative representation. Windows is by far the most discussed operating system (Figure 1).

To understand the variety of organizations represented, we looked at the host names of all 870 unique email senders in 2018 along with their sector according to FortiGuard. We identified a total of 670 unique email domains, 94% of which were associated with only one email address. In other words, most organizations represented have only a single sysadmin engaged with this community. We found a total of 24 unique country top level domains from the UK, US, Canada, Australia, New Zealand, Europe, Asia, and South America. The top three sectors by sender were: Business (n=191), Education (n=119), and IT (n=110). Other notable sectors included: Government and Legal Organisations (n=59), Health and Well-being (n=62), Financial (n=60), and Private Domains (n=165) which include email addresses such as @gmail.com and

TABLE 1: Comparison between 2018 and other years (04-18) in terms of the number of *emails* sent across the list, the number of unique *senders*, and the number of emails sent that had *no reply*.

| # of | 2018 | All Years | | | |
|---|---|---|---|---|---|
| | | Avg. | Std. Dev. | Max | Min |
| Emails | 7908 | 4075.93 | 2718.25 | 9538 | 1217 |
| Senders | 870 | 670.60 | 201.51 | 1200 | 476 |
| No Reply | 538 | 342.67 | 153.82 | 620 | 178 |

@hotmail.com. In short, the list represents sysadmins located world wide in a range of sectors.

## 5. Qualitative Coding Methodology

### 5.1. Codebook Design

Before creating the codebook, the two authors conducting the qualitative analysis (AJ and PK) reviewed the full content of 13 randomly selected threads from 2018, comprising 106 emails in total. Based on this review, we decided that similar to other work [64], the analysis would focus only on the initial email of a thread. The content of the full thread was interesting, but provided minimal additional information about the reasons people engaged with the list.

To create the codebook, two authors open coded [65, p.100] the same 50 randomly selected initial thread emails from throughout 2018 and individually created potential codebook structures. They then met, discussed the observed themes and created a combined codebook. One interesting observation was the difference between emails where the primary goal was information seeking versus sharing. So the codebook explicitly had separate codes based on the perceived intention of the email sender. Both coders then individually applied the codebook to a new random set of 50 emails, this time writing memos as they went. Both the memos and results were reviewed and discussed resulting in a refinement of the codebook. Coding conflicts were resolved within these sessions through continual discussion with issues reviewed until agreement was reached. This process was repeated six more times (350 emails in total) before the coders felt they had sufficient agreement and were no longer seeing new themes emerge (saturation). Interrater agreement as measured by Cohen's Kappa was 0.88 (2 s.f.) for the last set of emails, which is considered to be a very high level of agreement [66]. Table 2 details the codes present in the codebook along with their descriptions.

### 5.2. Qualitative Coding

The codebook was applied to all emails sent from the beginning of March to the end of July 2018. The dates were chosen for three reasons. First, they are from the most recent full year, 2018. Second, Meltdown and Spectre, headline worthy vulnerabilities, were announced in January 2018, so we selected a start date of two months later to allow the list to return to a normal state. Third, the chosen dates avoid major holidays that might impact patch behavior.

A total of 380 initial thread emails were sent within the chosen five months, representing 0.05% of all emails in 2018. The emails were then divided up with 45% given to each coder. The remaining 10% were given to both coders and placed at the end of their coding list. This 10% (n=38) overlap was used to measure the drift as the two coders coded separately. The resulting $\kappa$=0.79 (2 s.f.) shows a continued high-moderate agreement [66]. Of the 380 initial thread emails 24 were removed after coding as they were deemed to not be initial thread emails.

## 6. Results

What follows is a discussion of the 356 initial thread emails and the codes applied from our developed codebook. Overall, there was a total of 188 information requests, 150 examples of information sharing, and 18 off-topic emails. We present the codes below by collecting them into similar thematic areas, such as updates and errors, and the associated tasks, such as troubleshooting. We illustrate each code with examples edited for readability, as well as the total number of emails coded from the final set, and percentage. Table 2 has further statistics, including total numbers of URLs shared, and KBs mentioned.

### 6.1. Patch Prioritization (n=76, 21.3%)

Two crucial activities after a patch is released are learning about its release and, if there are multiple patches, deciding which ones to prioritize [17]. This prioritization includes understanding the changes the patch is likely to make, risks of not patching (vulnerabilities), and likely impacts on sysadmins' systems. Similar to the related work, we found that patch prioritization is a common activity for list members.

**6.1.1. Update Info (n=51, 14.3%).** This code was predominantly related to the announcement of a patch's release, usually with URLs to the KB articles. Table 2 highlights URL usage with only 51 emails containing 287 KBs and 355 URLs. While the majority of content was focused on Microsoft, announcements were made for a range of products including Apple and Adobe. Announcements included, re-releases or hotfixes, and even online murmurs of a patch's upcoming release. The sender would provide URLs, and often quote important information directly from the source along with any other observations, as seen in the example below:

> "[URL to MS Support Article KB4090913]
> This update includes quality improvements. No new operating system features are being introduced in this update. Significant changes include the following:
> -Addresses issue where some USB devices and onboard devices, such as a built-in laptop camera, keyboard, or mouse, stop working. This may occur when the Windows Update servicing stack incorrectly skips installing the newer version of some critical drivers in the cumulative update and uninstalls the currently active drivers during maintenance.

TABLE 2: Codebook for initial emails with counts, percentage, thread length statistics, and counts of KBs and URLs mentioned in the emails.

| Theme | Code | Count | % | Thread Length | | | | Total counts | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Mean | Std. Dev. | Max | Min | KB# | URLs |
| Patch Prioritization | Update Info | 51 | 14.3 | 6.43 | 7.54 | 34 | 2 | 287 | 355 |
| | Update Query | 25 | 7.0 | 9.48 | 9.73 | 34 | 2 | 17 | 5 |
| Errors and Troubleshooting | Update Error Info | 46 | 12.9 | 7.93 | 8.71 | 42 | 2 | 45 | 46 |
| | Update Error Query | 13 | 3.7 | 7.85 | 6.63 | 22 | 2 | 10 | 11 |
| | Patching Problems | 86 | 24.2 | 9.29 | 8.25 | 36 | 2 | 69 | 22 |
| Threats on the Radar | Vulnerability and Attack Query | 4 | 1.1 | 7.00 | 6.88 | 17 | 2 | 0 | 1 |
| | Attack and Vulnerability Info. | 12 | 3.4 | 5.50 | 2.91 | 10 | 2 | 1 | 16 |
| How-to and Tools | Scenario/Situation Request | 15 | 4.2 | 8.73 | 7.19 | 30 | 3 | 5 | 3 |
| | Tool Info. | 19 | 5.3 | 6.16 | 4.57 | 16 | 2 | 0 | 21 |
| | Tool Query | 29 | 8.1 | 7.69 | 7.56 | 37 | 2 | 3 | 4 |
| Mechanics and Documentation | Update Mechanism Query | 14 | 3.9 | 5.21 | 3.07 | 12 | 2 | 123 | 122 |
| | Update Mechanism Info. | 12 | 3.4 | 8.00 | 8.82 | 33 | 2 | 8 | 16 |
| Vendor Behaviour | Windows MS Information | 10 | 2.8 | 14.40 | 19.63 | 55 | 2 | 0 | 14 |
| | Windows MS Query | 2 | 0.6 | 5.50 | 4.95 | 9 | 2 | 0 | 0 |
| Off Topic and Community | Community | 7 | 2.0 | 11.14 | 10.90 | 32 | 2 | 0 | 5 |
| | List Info | 3 | 0.8 | 5.67 | 3.21 | 8 | 2 | 0 | 1 |
| | List Query | 3 | 0.8 | 9.00 | 5.29 | 15 | 5 | 0 | 0 |
| | Off Topic Info | 5 | 1.4 | 4.60 | 3.21 | 9 | 2 | 0 | 52 |

> -Addresses issue where some devices may fail to boot with "INACCESSIBLE_BOOT_DEVICE".
> Release notes updated to reflect that this DOES address the inaccessible boot device issue."

On Patch Tuesday, external groups, such as GHacks, system administrator subreddits, and AskWoody, create lists of Microsoft patches with prioritization-related information such as: platforms impacted, severity of vulnerability, URLs to KB articles, and even an executive summary with advice regarding the patches to prioritize for that month. For example:

> "...
> Executive Summary
> Security updates are available for all supported versions of Windows (client and server). Other Microsoft products with security updates are: Internet Explorer, Microsoft Edge, Microsoft Exchange Server, PowerShell Core, Adobe Flash, Microsoft Office. No critical vulnerabilities for Windows versions but for Microsoft Edge and Internet Explorer. Microsoft lifted the antivirus compatibility check on Windows 10 version 1607, 1703 and 1709.
> Operating System Distribution
>
> - Windows 7: 21 vulnerabilities of which 21 are rated important
> - Windows 8.1: 20 vulnerabilities of which 20 are rated important
> - Windows 10 version 1607: 29 vulnerabilities of which 29 are rated important
> - Windows 10 version 1703: 28 vulnerabilities of which 28 are rated important
> - Windows 10 version 1709: 24 vulnerabilities of which 24 are rated important
>
> ..."

**6.1.2. Update Query (n=25, 7.0%).** In this code, the sender is looking for information about a particular patch with the goal of gathering information as opposed to fixing a problem. These emails are generally asking the community for patch information not found in documentation or asking for the community's opinion about a patch.

For example, the below request asks if a particular patch still exists. Patches can go in and out of circulation as Microsoft removes and replaces error inducing patches and the sender is uncertain if that is what they are seeing.

> "Did Microsoft withdraw the 1709 July 10 CU? On endpoints with the July 10 SSU (KB4339420) installed, WU is not offering the July CU (KB4338825)."

In the next example, the sender points out the number of side-effects of installing the patch, asks if installing it is really worth it, and then subtly asks if anyone is aware of an upcoming replacement patch with less side effects.

> "I know this may be old news for some of you but I generally wait a day or so before applying patches. When I read about this patch and see the known issues and workarounds -
> [URL to MS Support Article KB4088878]
> - is this patch really necessary? Looks like side effects after taking a drug that will fix one thing but make you suicidal. And when is Microsoft going to provide this update...in a future release? And we're supposed to limp along?"

## 6.2. Errors and Troubleshooting (n=145, 40.8%)

The largest theme found in our dataset was focused on the errors and troubleshooting caused by newly released patches. Moreover, the mailing list attempts to keep track of and announce any indications of updates causing problems that may have been observed elsewhere on the web. Due to the cyclical nature of Patch Tuesday, each month we would see the latest error trends. For example, March and April had reoccurring issues with patches impacting the Network Interface Controller (NIC). The community was continually on the look out for information regarding errors, and this could be sourced through citations to blogs, or forums, or through the problems brought to the list by community members. This citation behaviour

is shown through the count of KB Numbers, and URLs found within this code, as seen in Table 2. These initial pieces of data would accumulate and eventually be recognised by Microsoft, through official statements, and proposed workarounds. These would then be fed back into the community as a double confirmation of the issues.

**6.2.1. Patching Problems (n=86, 24.2%).** This code was assigned to emails where the sender found themselves in the debugging stage following the application of a patch. The sender would be focused entirely on receiving information that would explain and alleviate the symptoms of the offending patches. The majority of these emails followed a very similar structure, in which the sender would describe the observation they had made, and the context in which it had appeared, such as in testing environments or in production systems. The sender would elaborate in great detail on the context of the error, such as the system version, the deployment method, the patches applied (usually referenced using KB number), and even the work they had performed to work out what was going on. This could take the form of scripts or listing commands they had run. The sender would also describe any online research they may have conducted, often indicating reaching out on the list was their last hope. For example:

> "I patched my Dev/Test environment last night and I have 6 servers that failed. I deployed through SCCM, most of them showed an error description of Software update execution timeout. So, I changed the max run time on the updates to 90 minutes. This morning, I ran manual update scans on these servers, they all found and downloaded the updates, but 6 of 8 failed again, this time with an error code of 0x800705b4. Looking this up, it refers to Windows Defender. I found one article, saying to verify Windows Defender service is running, which it is on all of these servers
> Is anyone else seeing this issue?"

The final call for any similar observation or workarounds was another prominent feature of this code, and was complimented by other senders who would refer to older emails made in that month or previous, which had similar error features to their own issues. For example,

> "After a patch install on Wednesday night, we saw about 6 virtual W2012R2 servers stuck at the loading windows stage. The servers had obviously tried to auto reboot, but didn't come back up properly. The VM's had to be reset and then came up normally - no NIC issues.
> The patches installed were: KB4088876, KB4089187, KB4088785 and KB4088879. Nothing in the eventlog, known issues section and I don't remember seeing anything on this list.
> Anybody else seen boot issues on W2012R2? I'm guessing it might be either KB4088876 or KB4088879 (or both) but I have no evidence for this.
> ..."

**6.2.2. Update Error Query (n=13, 3.7%).** We distinguished Update Error query from Patching Problems by ensuring the sender did not explicitly state that they were currently troubleshooting. Instead, the sender was requesting more information regarding rumors of errors discussed elsewhere or by clients/ other colleagues. As seen here where the sender lists errors they have observed:

> "Please note this is not happening to all systems.
> I have updated two home pcs to 1803 with no issues
> But am seeing forums and consultants starting to report some issues. Wondering if anyone else is seeing anything similarly and if so can you email me directly so we can grab some log files?
> 1. Symptom: Desktop is unavailable
> [URL to Windows10Forum Thread on 'Desktop Unavailable' Error]
> [URLs to TomsHardWare Thread 'Desktop Unavailable' on Error] ...
> It looks like this: [URL to Twitter, Picture of Error]
> 2. Roll back loop [URL to Reddit Thread on Windows 10 Roll Back Loop Error]
> ..."

Senders would ask if community members had any further information pertinent to the described bug. The focus was on actionable intelligence, such as workarounds or contextual triggers for bugs, like the offending patch and the applications it interfered with. Asking the community for this information allowed the the sender to perform a risk analysis, as to whether the known issue was anything they would have to worry about in their patching strategies.

> "[URL to MS Support Article KB4103718]
> For those of you that did suffer a loss of networking after the May updates, what exact nic card did you have?
> What brand of computer?"

**6.2.3. Update Error Info (n=46, 12.9%).** Here the sender shares information regarding the existence of potential errors found in that month's batch of patches. This information could take the form of forum thread discussion of problems, to news or blog articles detailing problematic patches. Often, these URLs could also be sourced from other online communities (Technet, MS Answers, Reddit, Twitter, etc.), or the patch documentation. For example:

> "I just wanted to pass this along and wondered If anyone else has come across this issue yet..?
> We haven't but apparently many others are now:
> [URL to Reddit Thread on Error following July Updates] "

Data could also come directly from the sender's system, however they would not explicitly ask for help troubleshooting. Their intention was to make the community aware of a problematic patch, as they may have already raised the issue with Microsoft, or had simply uninstalled the patch. For example:

> "We are running Office Professional 2016 64bit (msi install) on Windows 10 Enterprise v.1703 and encountered the Word has stopped error

when double clicking a Word file in File Explorer to open it. You can start Word and open files within Word without the issue.
...
Uninstalling the patch resolved the issue"

If available, they would hint at a possible workaround or suggested mitigation strategies for the errors. If this was not available, the sender would often ask for thoughts, or if anyone else had first hand experience with this issue.

## 6.3. How-To and Tools (n=63, 17.7%)

We observed that senders were seeking the advice and suggestions from the community for a range of patching related tasks. These codes appeared to be eliciting the experiences of the community to inform their current process, or to aid with proposed future changes. For example, we saw situations in which the sender was seeking the recommendations of tools for a given task, such as Automatic Deployment Rules (ADR), or asking for for PowerShell scripts that were shared amongst the community. Asking the community for these recommendations, or experiences, allows community members to better understand, and develop their systems and patching process.

**6.3.1. Scenario/Situation Request (n=15, 4.2%).** In this code, the sender would set out a patching scenario, or a situation they needed guidance on. Senders would give future planned changes to their systems, or their current set-up, and look for suggested plans, or the thoughts of the community. For example:

"We are setting up a WSUS server for Windows 10 systems. The current plan is to limit access to only new or upgraded devices so the old system can sunset with older systems. This should also help with the different management styles of the newer OS, and the storage requirements.
How would you manage this transition?"

Sender's may also enquire about how community members tackle certain aspects of patch management, such as system upgrades, updating portable machines, or getting to grips with monitoring patching levels. Senders were looking to elicit the experiences of list members, and to gain from the knowledge of others. For example:

"While we have the majority of our systems in-house, there are a handful of portable machines that leave our LAN frequently. Currently utilizing WSUS for internal machines with a GPO pointing towards it for both reporting and update feed. On the portable machines however I set a GPO for them to download from Microsoft directly since they are usually not here. Problem is, there are a few patches that we either do not want installed, or Microsoft can't figure out how to get them to work properly which I would like to filter out. Just wanting to get some pros and cons of which way or another you all have experienced."

Given the scale of Microsoft, gaining from the knowledge of others is highly valuable, and allows sysadmins the opportunity to avoid pitfalls and follow in the steps of those with more experience.

**6.3.2. Tool Info (n=19, 5.3%).** Here the sender would share the announcement of a tool, service, or script, which they deemed potentially useful in the patching process. We did not include direct discussion of patches for tools in this code, and instead only considered examples where new features or announcements of intended products pushed a sender to share with the community. For example,

"WAC or Windows Admin Center creates a new method for managing PC's for help desk functions. Update management is included in this. Have any of you tested this? It looks like it is only compatible with Chrome and Edge and 2012 and newer OS. Oh, and it doesn't replace RSAT or MMC completely.
[URL to Microsoft Cloudblogs WAC Announcement]"

It could also take the form of settings and tricks that a sender had found, and was willing to share with the community.

"I'm in the middle of creating a reference image for 1709 and have found a way of disabling the silently installed apps and removing the associated tiles from start. These changes need to be applied to the ntuser.dat in C:/users/default. It may help someone:
Windows Registry Editor Version 5.00
`[HKEY_LOCAL_MACHINE\defuser`
`\Software\Microsoft\Windows`
`\CurrentVersion\Conte$\DeliveryManager]`
`"FeatureManagementEnabled"=dword:00000000`
`"OemPreInstalledAppsEnabled"=dword:00000000` …"

**6.3.3. Tool Query (n=29, 8.1%).** Here, a sender would pose a question regarding a tool, software (SCCM, ConfigMgr), or script related to an element of patching. This could take the form of feedback regarding a particular tool, or looking for suggestions of an alternative. It should be noted that this code was not limited to only Microsoft products, as a number of third party software and vendors were routinely discussed. The sender would often detail the intricacies of their systems and indicate exactly what they wished the tool to do. For example:

"Can anyone recommend an alternative to Ivanti/Shavlik for a small business (just 12 licences). We've been very happy with it since the days of hfnetchk, but it seems neither the reseller or Ivanti themselves want our business any more - must be too small - so we're looking for an alternative. Ideally agentless and cost effective without too much admin input or scripting. Can't use an MS offering as we have moved away from Windows servers, so it needs to run on a workstation and not need AD."

Alternatively, the code contained examples where senders were working out errors, or best practices with the tool in question. For example:

"I currently use Automatic Deployment Rules in SCCM to deploy and manage Windows updates/patches. In the event that an emergency patch is released to the WU que, how do I push this update through. My current ADR is set to run each patch Tuesday with a deadline of 7 days after."

### 6.4. Threats on the Radar (n=16, 4.5%)

SysAdmins must be constantly vigilant for new, and potentially devastating vulnerabilities that could impact in their systems. Being aware of these issues will allow them to plan their patching accordingly, as well as mitigate the risks of yet unpatched vulnerabilities. Cyber Security is constantly adapting as new vulnerabilities are found everyday, and hence the community attempts to remain current through their information collaboration. As with previous themes, there were popular topics discussed, such as fallout from the Meltdown and Spectre patches released earlier in the year (but not released within our chosen window). Clarification would be sought on whether vulnerabilities had been plugged following the released patches, or if there was potentially more needing to be done to prevent successful attacks on their systems.

**6.4.1. Attack and Vulnerability Info (n=12, 3.4%).** This code captured information shared regarding the existence of a newly discovered vulnerability or attack in the wild. This could include the announcement of a new vulnerability, for example:

> "Another Spectre/Meltdown type vuln.
> [URL to US-Cert Alert (TA18-141A)]
> [URL to Verge Article on CPU Vulnerability]"

It could also include discussion of the emergence of attacks, and proof of concept code, such as:

> "In the past 12 hours, "XPN" has released and updated exploit code for Total Meltdown.
> [URL to XpnSec Blog on Meltdown]
> Kevin Beaumont has confirmed that it works.
> [URL to Twitter Post]
> Win7 and Server 2008R2 systems are left with few options.
> [URL to Ask Woody Meltdown Post]"

**6.4.2. Vulnerability and Attack Query (n=4, 1.1%).** Senders would ask the community for information regarding known vulnerabilities or new attacks in the wild. These requests were linked to some observations, such as news articles or blogs, that spur them to enquire further. This could also take the form of an observation made about their system, as they seek a verification from the list. Senders would often ask for clarification regarding the technicalities of the vulnerability, or the best mitigation strategies. For example:

> "Just when it seemed like 2018 couldn't get any worse for IT, does anyone have information re: this threat?
> Googling vpnfilter will source several reliable resources that this is a legit threat.
> Based on my reviews of available information I'm not sure at this point just how the stage1 succeeds. If a device does not have remote management enabled that should address this problem - unless there is a flaw that is being exploited on the device itself.
> Can anyone comment on how the exploit succeeds and what if any are the mitigating factors?
> Particular to this new headache it would seem worth asking what devices out of the box allow for remote access? None that I know of or have worked with."

### 6.5. Mechanics and Documentation (n=26, 7.3%)

Patching is a complicated business with multiple sources of information, with documentation, and definitions of vendor terminology. However, due to the scale, and complexity of updates, community members would find themselves confused around terminology and their real-world impact, i.e. how patches actually worked. Inconsistencies in documentation would result in senders looking to the community for reassurance or clarification regarding terms, and the mechanics of patching mechanisms like WSUS, or how different branches of releases were delivered. These codes would contain URLs to the offending documentation, with a total of 138 found within this theme. Understanding the documentation, and therefore how patches were intended to work, is vital to a successful patching schedule. Given the scope of Microsoft, we can see that mistakes in clarity are possible.

**6.5.1. Update Mechanism Info (n=12, 3.4%).** Windows Update Service adapts with time, with changes being made to the inner workings of both patches and patching services. Information sourced in this code could include blog posts made by specific teams within Microsoft, as senders keep the list aware of intended changes to the patching landscape:

> "Office 365 is changing its build numbers to a five-digit format.
> [URL to MS Support Article on Office 365 Changing Build number Format]"

Community members would also monitor discussions found on the list, and be compelled to correct or direct the list to sources which would explain patch mechanics:

> "I've seen several list members recently noting that computers with settings to the contrary are being forced to 1709. Please see KB4023814, particularly this paragraph:
> 'Windows 10 version 1607 and version 1703 are not yet at 'end of service.' However, they must be updated to the latest versions of Windows 10 to ensure protection from the latest security threats.'
> Woody wrote a piece yesterday on Computerworld saying the telemetry level setting is also a factor on who gets the forced upgrade.
> [URL to ComputerWorld Article on Telemetry Settings]
> We're a SMB, Microsoft does not care what I think. But to those of you that have lots of seats and TAMs, is this acceptable to you? It seems unconscionable to me that you follow all Microsoft's latest rules for reg settings and group policy to defer updates, and despite running a version of Windows that had not yet reached EOL, they update you anyway."

**6.5.2. Update Mechanism Query (n=14, 3.9%).** We found that changes or subtle inconsistencies in the wording surrounding the description of technical aspects of

documentation and patches would cause senders to look for clarification. Patching is extremely detail orientated, therefore anything which did not fit into the sender's mental map of how patches are constructed, applied, or delivered, would cause them to reach out to the community to verify. For example:

> "If I go here: [URL to Microsoft Windows 10 Release Information]
> I see Semi-Annual Channel (Targeted) is 1709 and Semi-Annual Channel is 1803. This seems backwards to my understanding of those terms. Am I missing something?"

Update mechanisms also captured misunderstandings regarding how patch delivery mechanism worked and what terminology meant in patching scenarios. As seen here:

> "We are looking at upgrading our Windows 10 fleet and yes we do have a mix bag from 1511 to 1803. We use Configuration Manager 1710 with WSUS.
> Windows 10 1511 is now out of support as we all know, does that mean we cannot upgrade the 1511 (and even 1607) Windows 10 to 1803 via WSUS? I think the answer is yes, and wanted to check with the experts as I am sure we are not the only company that lets say a little slow to the Windows 10 upgrade party.
> Let me know if you need any more information and thanks in advanced"

## 6.6. Vendor Behaviour (n=12, 3.4%)

We observed information regarding Microsoft as a company, its direction, or its policies related to patching. As a sysadmin, one must navigate the relationship with the vendor, as press statements and announcements of intent are indicators of potential shifts and alterations in the patching landscape. Keeping aware of company announcements and internal changes is useful as it allows for anticipation of the changes as opposed to being caught in the cold. We found that these discussions would routinely cover what was believed to be inadequate responses of Microsoft, with many using these to justify their beliefs and patching strategies. The responses were overwhelmingly negative, and it was clear in our community that Microsoft is not seen as a communicative partner. For example, through our error codes we saw passing remarks regarding the state of Microsoft's testing of patches, with some stating, "Do they even test these?!"

**6.6.1. Windows/Microsoft Info (n=10, 2.8%).** This code captured the sharing of information regarding the behaviour of Microsoft. Announcements made by Microsoft and were regularly found to be unsatisfactory. The sender would react negatively to a decision or response from Microsoft, and would appear to vent regarding the "disregard" Microsoft was showing towards them and other admins. For example:

> "[URL to MS TechCommunity Windows 10 Ask Me Anything]
> IMHO the question really wasn't answered.
> So if you were in charge of patching/servicing and testing at Microsoft, how would you gain back the trust?"

Senders would often point to decisions being made, and often use them to justify their stance on certain patching services, as seen here:

> "Here is a reason to not deploy LTSB:
> [URL to MS TechCommunity Windows 10 Ask Me Anything - LTSB for Pro Users]
> We've recently announced that Office will no longer be supported on LTSC in the future (today, it is still supported on certain LTSC versions). So please keep this in mind. Here's the blog with that announcement:
> [URL to MS Technet Blogs on Windows IT Pro, Changes to Office and Windows]
> ..."

**6.6.2. Windows/Microsoft Query (n=2, 0,6%).** In this code, the sender would reach out to the community for clarification regarding the actions of Microsoft as a company or Windows as a service. These queries would often follow from announcements or observations made regrading adjustments made to update services or related products. More often than not, senders would be angry or upset with the proposed change, often the discontinuation of a product used in patching. Those affected are pushed to reach out the community, to create a discussion as to why Microsoft will have made this decision. For Example:

> "Talking to an engineer about Bitlocker and he asked why I don't have an Azure presence yet? I say I don't need one. He says you do know you will be required to have one in the very near future. I scratch my head. Is this truly the path Microsoft is taking and will I be required to have an AD-Azure presence even if I don't want one?
> I'll sit back and read your replies."

## 6.7. Off-Topic, List Rules, and Community (n=18, 5.0%)

The community is clearly a trove of data on patching related issues. However, we observed examples of emails that were not directly patching related, and were considered off-topic, list information, or community related.

**6.7.1. List Info (n=3, 0.8%) and List Query (n=3, 0.8%).** These two codes captured emails which informed community members of the rules and running of the mailing list, with List Info focused on sharing this information. This could include moderators stating they would be away for a while, or GDPR's affect on the list, as seen here:

> "Since
> a. this list is voluntary
> b. this list is not selling anything
> c. this list is not selling email addresses
> d. it is merely a peer resource
> Therefore this list is not covered by GDPR rules and thus does not need to ask everyone from the EU to re-opt back in."

The opposing code, List Query, captured queries regarding what was appropriate content for the list, such as the example below:

"Am I mistaken to say that this list primarily refers to servers? I work in the desktop environment and follow this list to help determine what to release."

**6.7.2. Off Topic Info (n=5, 1,4%).** Not all emails coded were directly related to patching or the patching cycle, but could still be replated in some way. For example, we saw the list share tools or information regarding sysadmin tasks, such as Amazon Web Services (AWS), seen here:

"For those on AWS – [URL to Github Hammer Project]
[URL to Medium article on Dow Jones Hammer Tool]
Today, Dow Jones Tech is pleased to open source Dow Jones Hammer, a DevSecOps tool that lets you identify and proactively fix misconfigurations in cloud workloads.
..."

Moreover, we saw examples of information source sharing, which took the form of members posting their go-to Twitter followers:

"Hi Folks,
This is me and my Twitter Following List.
**Microsoft People**
[List of 10 Twitter Accounts]
**Microsoft**
docs.microsoft.comVerified $@docsmsft$
The PowerShell Team $@PowerShell_Team$
Windows InsiderVerified $@windowsinsider$
.NET Foundation $@dotnetfdn$
Visual Studio Team ServicesVerified $@VSTS$
.NET TeamVerified $@dotnet$
Windows Defender Security Intelligence $@WDSecurity$
Microsoft SecureVerified $@msftsecurity$
Security ResponseVerified $@msftsecresponse$
Microsoft SupportVerified $MicrosoftHelps$
MicrosoftVerified $@Microsoft$
MS Windows IT ProVerified $@MSWindowsITPro$
Microsoft NewsVerified $@MSFTnews$
WindowsVerified $@Windows$
Microsoft Channel 9Verified $@ch9$
**Media, NetCasters & Others**
[List of 22 Twitter Accounts]
..."

**6.7.3. Community (n=7, 2.0%).** This code captures the camaraderie shown amongst list members, primarily in the form of thanks, or appreciation to the list for its help.

"I just want to give a HUGE **THANK YOU** to everyone in this group for helping me *SO* much over the last years. The information provided here is invaluable, and the time and effort everyone takes to submit and SHARE information is, well breathtaking. I've learned SO much and appreciated folks stepping up and answering my (sometimes neophyte) questions
As it turns out, it's time for me to ride off into the sunset and enjoy retirement. ...
It has truly been my honor being part of such a magnificent group."

Thanks were the most common example, but we also found emails that were part of community wide efforts, such as a list moderator thanking the community for help in the writing of an open letter to Microsoft [67].

"[URL to Computer World article on Open Letter to Microsoft]
My deepest thanks to all who participated.
Bottom line the fight for change has just begun."

## 7. Limitations

In our analysis we look at a single online community focused on the topic of patch management. We selected this community due to its age and popularity; however, it is only one of many similar online communities discussing this topic. Both Reddit's r/sysadmin subreddit and the Microsoft official TechNet forums also contain discussions of patch management. All such communities have their own norms, values, and methods of interaction and may also exhibit different platforms of focus, such as Linux. We believe that many of our findings will generalize to other groups, but without exploring them we cannot know that for certain. Similarly, we only study people who contributed to the list within our time frame. People who are engaged through reading, but not contributing, are not well represented in our work. Additionally, due to the list's focus on Microsoft, we have only been able to analyze the patching information regarding this particular vendor. Although this is a large and important software vendor, the information provided and delivery of patches will differ across other vendors and therefore our results will have limited generalizability

In our analysis we also chose to only focus on the first email in threads. We believe that doing so allowed us to get a good overview of the purposes people have when interacting with the list, a method which has also been successfully used by others [64]. However, it also limited our exploration. It is very possible that some threads contained changes in topic mid-thread.

Finally, our analysis was constrained to a five month period in 2018. The number and type of communications across the list are heavily impacted by the number and severity of patches released in a given month. So it is quite likely that if we selected a different set of months, such as January when Meltdown was announced, we would have found slightly different themes and a different balance of topics. We also have some evidence that the list has several long-running email threads, some of which go back years. By limiting to thread starting emails within these five months we excluded these long running threads from the analysis. Having reviewed several such threads, we feel that the impact was minimal, but it was still present.

## 8. Discussion

### 8.1. Online Community of Practice

The themes uncovered during our analysis suggest that the mailing list PatchManagement.org lends itself well to being studied through the lens of Communities of Practice (CoP). CoP is a concept that emerged from the social theory of learning proposed by Lave and Wenger [68], and

was further developed in 1998 by Wenger [69]. Kandogan et al. [28] have already identified the important role that social learning plays for system administrators.

Essentially, in a COP, a group of people who share a craft or profession build a community where members can share information and experiences as well as learn from each other. CoP's can either form naturally or be explicitly created and grow through the discussions of community members around topics such as best practices. A CoP can also be virtual [70]. A COP has three key characteristics:

**Domain** - a body of knowledge which allows for mutual understanding amongst the members of the community, and guides the learning and goals of the community;

**Community** - a community feeling provides the social framework for learning. A strong and accepting community fosters discussions and encourages further learning opportunities; and

**Practice** - the members of the community are practitioners in the domain, therefore through their social interactions they gain an insight into best practices for their chosen domain.

The **domain** of PatchManagement.org is software patches – release, intended and unintended side effects, and mitigation of problems introduced by the patches. Members are mostly sysadmins, and therefore **practitioners** in the domain – part of their role is to apply patches in a way that is both timely and minimally disruptive. Our qualitative analysis, in particular the smaller themes, clearly demonstrate that the mailing list also has the third element of **community**. There are well enforced rules that allow list members to debate the advantages and disadvantages of each patch openly.

### 8.2. Tasks are Highly Complex and High Risk

Typical of contexts that generate Communities of Practice, patch management is a highly complex task. It requires sysadmins to manage potentially large networks of computers, each of which have a different set of requirements and setups. Then, with the release of each patch, they must balance the risks and benefits of installing it [11], not just globally but on each computer or set of computers. The information that sysadmins have at release is skewed and incomplete. They know what issues the patch is supposed to fix, but not what new issues the patch is likely to cause across the entire network. Therefore, they need a way of monitoring emerging issues for data that they can use in their own decision processes.

The online CoP of PatchManagement.org is a safe space where sysadmins can access up to date information and obtain expert advice on their decisions, as shown in the themes of Errors and Troubleshooting, and How-To and Tools.

Since sysadmins may be isolated in their own companies or work in very small teams, it is invaluable to have access to the "wisdom of the crowd" when it comes to a high risk activity such as patch management. Errors, such as installing a buggy patch, or not installing a patch for a security vulnerability that is then exploited, can take large numbers of computers that are vital to the functioning of an organization offline very quickly [12]. Often it is not possible to mitigate all the associated risks, so instead sysadmins must manage their risk appetite and decide how much and what type of risks they will take. The open discussion of questions such as how quickly a patch should be deployed, or whether difficult-to-patch computers should be protected behind a firewall, help the community come to a consensus on what best practice mitigations are "enough".

### 8.3. Time Pressures Require Prioritisation of Work

Looking more specifically at the monthly patch cycle, one large source of complexity is the time pressure to get patches installed quickly [11], [14]. Most official guidance on patching, such as the UK's Cyber Essentials [7], recommends installing patches as soon as possible to avoid potential compromise. Practically, however, installing all patches at once is not possible as each patch should be tested and then deployed. Some months as many as 60+ patches can be released by Microsoft alone in one day. To handle the overload, sysadmins use available information to prioritize patches that have serious security implications over those that do not [17].

We saw evidence of the PatchManagement.org community openly discussing what patches needed to be prioritised and which could or should be delayed. The community's wisdom was drawn upon to prioritise not only the patches themselves, but how severe the vulnerabilities they impacted were and what systems would be impacted.

### 8.4. Verification is Hard to Impossible

Verifying that a patch is "safe" or "working" is a challenging (and occasionally impossible) problem partially because there is no good definition of "safe" or "working" [71]. After installation, sysadmins "test" the patch by doing everything from observing a lack of errors, conducting basic actions like opening email, deploying it to beta testers, or running a full battery of automated tests on a dedicated testing environment. However, these activities do not produce definitive proof that the patch is good, just that no errors have been found, therefore the decision to move to production systems is always a gamble.

Patch failures can also have several sources beyond the patch itself. The purpose of a patch is to change how software works, that change can then have side effects for other software or react badly to specific configurations [28, ch3]. As a result, when a patch is seen to fail, the first question is what and/or who is the cause rather than assuming the patch itself is problematic.

The PatchManagement.org community actively shared information about observed and potential patch problems. The list allowed members to collect together information they found across the Internet to bring together a picture of what patches were causing issues drawn not only from their local experience, but also from those of other related communities. For members who were currently struggling

with post-patch issues, the list offered a place to openly discuss the problem and gain not only solutions but also learning about how systems like Windows work.

### 8.5. Fixing Requires Evidence

Getting problematic patches fixed can also be difficult. There are many possible sources of issues beyond the patch itself. So getting a vendor, such as Microsoft, to fix the patch requires providing evidence that the problem being observed is really caused by the patch and not something else.

In this regard, the list served as a collective method of contacting vendors and a source of multiple cases to provide to the vendors as evidence. When a problem was identified, list members would comment that they "had a ticket with Microsoft" and promised to report back to the list with the response. Some members had elevated Microsoft Support contracts and could use them to get better support which was then passed on to the list.

## 9. Conclusion

We conducted a qualitative analysis of 356 emails shared on the patch orientated mailing list PatchManagement.org with a focus on Windows Update. We found that the list is used for sharing information critical to the patching process such as identifying critical patches, and also for help seeking when in a troubleshooting state following patch application. Moreover, we found that this list also deals with queries related to the practice of patching, and allows for clarification on inconsistent documentation and terminologies. We believe that this Online Community of Practice alleviates the difficulties found when dealing with the uncertainties of patching, by providing the expertise of others it can direct sysadmins towards best practices, or tools. Furthermore, we argue that these communities of practice provide a source for learning the best practices in an uncertain patching landscape.

## 10. Acknowledgements

We want to thank the members of the TULiPS lab for their feedback throughout the work. We also thank our anonymous reviewers for their insightful comments. This research is funded in part by a Google Research Award. Maria Wolters acknowledges the Alan Turing Institute (EPSRC, EP/N510129/1).

## References

[1] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg, "Meltdown: Reading kernel memory from user space," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018.

[2] P. Kocher, J. Horn, A. Fogh, , D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre attacks: Exploiting speculative execution," in *40th IEEE Symposium on Security and Privacy (S&P'19)*, 2019.

[3] T. Warren, "Microsoft halts amd meltdown and spectre patches after reports of unbootable pcs," Jan 2018. [Online]. Available: https://www.theverge.com/2018/1/9/16867068/microsoft-meltdown-spectre-security-updates-amd-pcs-issues

[4] J. Segura, "Fake spectre and meltdown patch pushes smoke loader malware," Jan 2018. [Online]. Available: https://blog.malwarebytes.com/cybercrime/2018/01/fake-spectre-and-meltdown-patch-pushes-smoke-loader/

[5] Microsoft, "Microsoft security intelligence report, volumne 13," January – June 2012.

[6] Symantec Corporation, "Internet Security Threat Report, Volume 18," 2013.

[7] "Cyber essentials," Nov 2017. [Online]. Available: https://www.cyberessentials.ncsc.gov.uk/

[8] N. A. Office, *Investigation: WannaCry cyber attack and the NHS*. National Audit Office, Oct 2017.

[9] E. Kovacs, "Heartbleed still affects 200,000 devices: Shodan," Jan. 2017. [Online]. Available: https://www.securityweek.com/heartbleed-still-affects-200000-devices-shodan

[10] G. Maayan, "Five years later, heartbleed vulnerability still unpatched," Malwarebytes Labs, Sep. 2019. [Online]. Available: https://blog.malwarebytes.com/exploits-and-vulnerabilities/2019/09/everything-you-need-to-know-about-the-heartbleed-vulnerability/

[11] S. Beattie, S. Arnold, C. Cowan, P. Wagle, C. Wright, and A. Shostack, "Timing the application of security patches for optimal uptime." in *LISA*, vol. 2, 2002, pp. 233–242. [Online]. Available: http://static.usenix.org/legacy/events/lisa02/tech/full_papers/beattie/beattie_html/

[12] D. Moore, C. Shannon *et al.*, "Code-red: a case study on the spread and victims of an internet worm," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. ACM, 2002, pp. 273–284.

[13] P. Bright, "Data-deletion bug forces microsoft to suspend rollout of windows 10 update," Oct 2018. [Online]. Available: https://arstechnica.com/gadgets/2018/10/microsoft-suspends-distribution-of-latest-windows-10-update-over-data-loss-bug/

[14] L. Bilge and T. Dumitraş, "Before we knew it: an empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 833–844.

[15] "Update inertia:the psychology behind patching and updating software," Jun 2019. [Online]. Available: https://press.avast.com/hubfs/media-materials/kits/AvastBusinessPatchManagement/PatchInertiaReport-SMBs.pdf?hsLang=en

[16] S. Furnell, "Vulnerability management: not a patch on where we should be?" *Network Security*, vol. 2016, no. 4, pp. 5–9, 2016.

[17] F. Li, L. Rogers, A. Mathur, N. Malkin, and M. Chetty, "Keepers of the machines: Examining how system administrators manage software updates for multiple machines," in *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[18] P. P. Maglio, E. Kandogan, and E. Haber, "Distributed cognition and joint activity in collaborative problem solving," in *Proceedings of the Annual Meeting of the Cognitive Science Society*, vol. 25, no. 25, 2003.

[19] R. Barrett, Y.-Y. M. Chen, and P. P. Maglio, "System administrators are users, too: designing workspaces for managing internet-scale systems," in *CHI'03 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2003, pp. 1068–1069.

[20] R. Barrett, E. Kandogan, P. P. Maglio, E. M. Haber, L. A. Takayama, and M. Prabaker, "Field studies of computer system administrators: analysis of system management tools and practices," in *Proceedings of the 2004 ACM conference on Computer supported cooperative work*. ACM, 2004, pp. 388–395.

[21] R. Barrett, "People and policies: Transforming the human-computer partnership," in *null*. IEEE, 2004, p. 111.

[22] R. Barrett, P. P. Maglio, E. Kandogan, and J. Bailey, "Usable autonomic computing systems: The system administrators' perspective," *Advanced Engineering Informatics*, vol. 19, no. 3, pp. 213–221, 2005.

[23] E. Kandogan and E. M. Haber, "Security administration tools and practices," *Security and Usability: Designing Secure Systems that People Can Use*, pp. 357–378, 2005.

[24] E. M. Haber and J. Bailey, "Design guidelines for system administration tools developed through ethnographic field studies," in *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*. ACM, 2007, p. 1.

[25] J. Bailey, E. Kandogan, E. Haber, and P. P. Maglio, "Activity-based management of it service delivery," in *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*. ACM, 2007, p. 5.

[26] E. Haber and E. Kandogan, "Security administrators: A breed apart," *SOUPS USM*, pp. 3–6, 2007.

[27] E. M. Haber, E. Kandogan, and P. P. Maglio, "Collaboration in system administration," *Communications of the ACM*, vol. 54, no. 1, pp. 46–53, 2011.

[28] E. Kandogan, P. Maglio, and E. Haber, *Taming information technology: Lessons from studies of system administrators*. Oxford University Press, 2012.

[29] H. H. Clark, "Arranging to do things with others," in *Conference Companion on Human Factors in Computing Systems*. ACM, 1996, pp. 165–167.

[30] S. E. Brennan, "The grounding problem in conversations with and through computers," *Social and cognitive approaches to interpersonal communication*, pp. 201–225, 1998.

[31] G. Klein, P. J. Feltovich, J. M. Bradshaw, and D. D. Woods, "Common ground and coordination in joint activity," *W.R. Rouse & K.B. Boff (eds), Organizational Simulation*, pp. 139–184.

[32] E. Hutchins, "How a cockpit remembers its speeds," *Cognitive science*, vol. 19, no. 3, pp. 265–288, 1995.

[33] N. F. Velasquez, S. P. Weisband, and A. Durcikova, "Designing tools for system administrators: An empirical test of the integrated user satisfaction model." in *LISA*, 2008, pp. 1–8.

[34] N. F. Velasquez and S. P. Weisband, "Work practices of system administrators: implications for tool design," in *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology*. ACM, 2008, p. 1.

[35] D. G. Hrebec and M. Stiber, "A survey of system administrator mental models and situation awareness," in *Proceedings of the 2001 ACM SIGCPR conference on Computer personnel research*. ACM, 2001, pp. 166–172.

[36] N. F. Velasquez and S. P. Weisband, "System administrators as broker technicians," in *Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology*. ACM, 2009, p. 1.

[37] C. R. De Souza, C. S. Pinhanez, and V. Cavalcante, "Knowledge and information and needs of system administrators in it service factories," in *Proceedings of the 10th Brazilian Symposium on Human Factors in Computing Systems and the 5th Latin American Conference on Human-Computer Interaction*. Brazilian Computer Society, 2011, pp. 81–90.

[38] C. R. de Souza, C. S. Pinhanez, and V. F. Cavalcante, "Information needs of system administrators in information technology service factories," in *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*. ACM, 2011, p. 3.

[39] S. Kraemer and P. Carayon, "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists," *Applied Ergonomics*, vol. 38, no. 2, pp. 143 – 154, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S000368700600041X

[40] T. Xu, V. Pandey, and S. Klemmer, "An hci view of configuration problems," *arXiv preprint arXiv:1601.01747*, 2016.

[41] T. Xu and Y. Zhou, "Systems approaches to tackling configuration errors: A survey," *ACM Computing Surveys (CSUR)*, vol. 47, no. 4, p. 70, 2015.

[42] C. Dietrich, K. Krombholz, K. Borgolte, and T. Fiebig, "Investigating system operators' perspective on security misconfigurations," in *The 25th ACM Conference on Computer and Communications Security (CCS'18)*. ACM, 2018.

[43] K. Krombholz, W. Mayer, M. Schmiedecker, and E. Weippl, "" i have no idea what i'm doing"-on the usability of deploying https," in *Proc. of the 26th USENIX Security Symposium, ser. USENIX Security*, vol. 17, 2017, pp. 1339–1356.

[44] S. Chiasson, P. van Oorschot, and R. Biddle, "Even experts deserve usable security: Design guidelines for security management systems," in *SOUPS Workshop on Usable IT Security Management (USM)*. Citeseer, 2007, pp. 1–4.

[45] O. Crameri, N. Knezevic, D. Kostic, R. Bianchini, and W. Zwaenepoel, "Staged deployment in mirage, an integrated software upgrade testing and distribution system," in *ACM SIGOPS Operating Systems Review*, vol. 41, no. 6. ACM, 2007, pp. 221–236.

[46] M. Fagan and M. M. H. Khan, "Why do they do what they do?: A study of what motivates users to (not) follow computer security advice," in *Twelfth symposium on usable privacy and security (SOUPS 2016)*, 2016, pp. 59–75.

[47] A. Mathur, N. Malkin, M. Harbach, E. Peer, and S. Egelman, "Quantifying users' beliefs about software updates," *arXiv preprint arXiv:1805.04594*, 2018.

[48] K. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: How negative experience affect future security," in *CHI 2014: Conference on Human Factors in Computing Systems*, April 2014.

[49] R. Wash, E. Rader, K. Vaniea, and M. Rizor, "Out of the loop: How automated software updates cause unintended security consequences," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014, pp. 89–104.

[50] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How i learned to be secure: a census-representative survey of security advice sources and behavior," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 666–677.

[51] I. Ion, R. Reeder, and S. Consolvo, ""... no one can hack my mind": Comparing expert and non-expert security practices." in *SOUPS*, vol. 15, 2015, pp. 1–20.

[52] R. Reeder, I. Ion, and S. Consolvo, "152 simple steps to stay safe online: Security advice for non-tech-savvy users," *IEEE Security & Privacy*, 2017.

[53] M. Khan, Z. Bi, and J. A. Copeland, "Software updates as a security metric: Passive identification of update trends and effect on machine infection," in *MILCOM 2012-2012 IEEE Military Communications Conference*. IEEE, 2012, pp. 1–6.

[54] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang, "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)*, 2016, pp. 97–111.

[55] F. Vitale, J. Mcgrenere, A. Tabard, M. Beaudouin-Lafon, and W. E. Mackay, "High costs and small benefits: A field study of how users experience operating system upgrades," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 4242–4253.

[56] O. Bergman and S. Whittaker, "The cognitive costs of upgrades," *Interacting with Computers*, vol. 30, no. 1, pp. 46–52, 2017.

[57] K. Vaniea and Y. Rashidi, "Tales of software updates: The process of updating software," in *CHI 2016: Conference on Human Factors In Computing Systems*, 2016.

[58] M. Parmar, "Windows continues to be the dominant operating system on the desktop," Apr 2018. [Online]. Available: https://www.windowslatest.com/2018/04/03/windows-continues-to-be-the-dominant-operating-system-on-the-desktop/

[59] Microsoft, "Description of the windows critical update notification utility," https://support.microsoft.com/en-us/help/224420/description-of-the-windows-critical-update-notification-utility, 2007.

[60] C. Gkantsidis, T. Karagiannis, and M. VojnoviC, "Planet scale software updates," in *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, ser. SIGCOMM '06. New York, NY, USA: ACM, 2006, p. 423–434. [Online]. Available: http://doi.acm.org/10.1145/1159913.1159961

[61] P.-L. Chao, "Windows update and its derivatives - with a focus on sus," Tech. Rep., Apr. 2003.

[62] L. Richardson, "Beautiful soup documentation," *April*, 2007.

[63] "Web filter categories," 2019. [Online]. Available: https://fortiguard.com/webfilter/categories

[64] R. Jones, L. Colusso, K. Reinecke, and G. Hsieh, "r/science: Challenges and opportunities in online science communication," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 2019, p. 153.

[65] J. Saldaña, *The coding manual for qualitative researchers*. Sage, 2015.

[66] M. McHugh, "Interrater reliability: The kappa statistic," *Biochemia medica : časopis Hrvatskoga društva medicinskih biokemičara / HDMB*, vol. 22, pp. 276–82, 10 2012.

[67] W. Leonhard, "An open letter to Microsoft management re: Windows updating," https://www.computerworld.com/article/3293440/microsoft-windows/an-open-letter-to-microsoft-management-re-windows-updating.html, July 2018.

[68] J. Lave, E. Wenger *et al.*, *Situated learning: Legitimate peripheral participation*. Cambridge university press, 1991.

[69] E. Wenger, *Communities of practice: Learning, meaning, and identity*. Cambridge university press, 1999.

[70] M. Barrett, S. Cappleman, G. Shoib, and G. Walsham, "Learning in knowledge communities:: Managing technology and context," *European Management Journal*, vol. 22, no. 1, pp. 1–11, 2004.

[71] P. K. Kapur, A. K. Shrivastava, and O. Singh, "When to release and stop testing of a software," *Journal of the Indian Society for Probability and Statistics*, vol. 18, no. 1, pp. 19–37, Jun 2017. [Online]. Available: https://doi.org/10.1007/s41096-016-0012-6