Email Risk Assessment Report

Prepared For
Informata College

Prepared By
John Smith
Fortinet

Report Date
May 5, 2021

Executive Summary

We aggregated key findings from our email risk assessment within the Executive Summary below. As represented in the summary, this report is divided into three sections: Security, Productivity, and Utilization. While the highlights are listed below, a more detailed view of each section follows. Be sure to review the Recommended Actions page at the end of this report as well for actionable steps your organization can take to mitigate email borne threats and optimize your overall email experience.

Security

842
Known or Suspected Attachment-based Attacks

52
Known or Suspected URL-based Attacks

4
Known or Suspected Impersonation-based Threats

Note that any threats observed within this report have bypassed your existing email security solution, so they should be considered active and potentially dangerous.

Productivity

415,225
Emails Flagged as Spam

19,925
Suspected Newsletters

1,647
Emails Detected with Adult Content

Although not necessarily malicious, spam, newsletters and/or emails with adult content represent a potential nuisance and/or offense. Organizations should consider whether the current level of unwanted or inappropriate email is acceptable.

Utilization

15,215
Average Emails Processed Per Day

1.6GB
Average Email Bandwidth Per Day

110.6KB
Average Email Size

Although you may have moved to cloud-based email infrastructure, utilization statistics can be valuable in a number of ways, they can be used to compare your email utilization against industry norms. Daily usage numbers can be tracked over time; deviation analysis is also helpful when determining anomalous company-wide behavior.

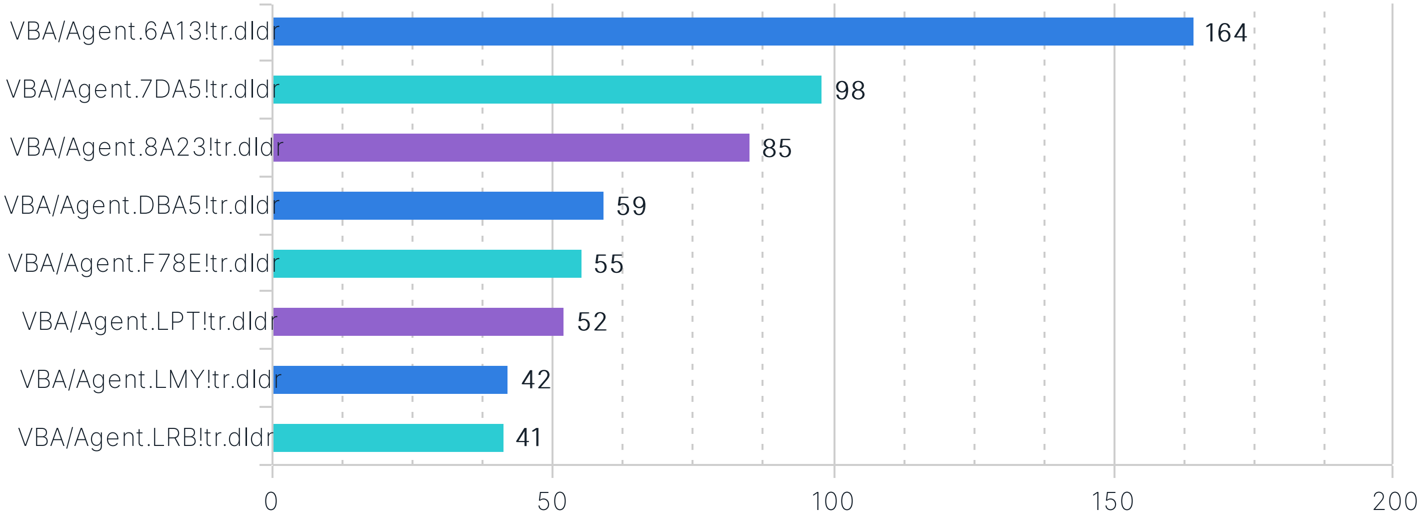
Security

Quick Stats

- **842** known or suspected attachment-based attacks
- **52** known or suspected URL-based attacks
- **4** known or suspected impersonation-based attacks
- **VBA/Agent.6A13!tr.dldr** is the top known malware detected in attachments
- **745** known malware identified
- **mode.us72.reservierian.org** is the top suspicious domain from URL-based attacks

Known Malware Identified

By applying the existing intelligence of FortiGuard Labs to your email traffic, we've identified known malware on their way to your end user inboxes (via attachments). Below you can see the top 8 known malware identified by volume.



Known Malware Identified with Details

For the known malware we identified, we have presented more detail about the most persistent messages and malware.

#	Sender	Subject	Malware	Count
1	colin.chen@kh.roohsing.com	External: Invoice Available	VBA/Agent.6A13!tr.dldr	6
2	irazema.vega@trico-group.com	External: Outstanding invoice	VBA/Agent.7DA5!tr.dldr	6
3	esanchez@informata.edu	Cambion de pago de sus servicios	VBA/Agent.LPI!tr.dldr	6
4	err84yanker@mountainmarycoll.com	External: Invoice Query	VBA/Agent.LPT!tr.dldr	5
5	ww88291@mail.shabot.co.mx	External: 29217 - SHABOT INC Invoice # 93855800121 12/07/2018	VBA/Agent.F78E!tr.dldr	4
6	ARDept@glovelane.net	External: Versa Comm / Account 63092	VBA/Agent.LRB!tr.dldr	4
7	moverslogisticintl@gmail.com	External: Purchase Order	RTF/CVE201711882.OIE!exploit	3
8	khurram@loyalbranding.pk	Billing Notification - New Invoice(s)	VBA/Agent.3ABF!tr.dldr	3

Security

Unknown Malware Identified

After inspecting for known malware, attachments can be sent to a sandbox for further inspection. This normally entails detonating the application/macro in a virtual environment and assessing behaviors. For instance, the sandbox may detect malicious attempts to alter registry settings or system files or identify communications to known malicious sites. The top 10 unknown malware identified (ranked by risk rating) are listed below. Note: a rating of 1 = clean and 5 = malicious, with grades of risk in between.

#	Rating	Malware	Count
1	4	hash(59259401da43fb5152df9e6a6355de68e4c47d6583f628bff96e1e311c4d0)	5
2	3	hash(44ada5048a609f6adf619dfb929d0958199fe5a7282e60c9e770fa4bb69300b3)	5
3	3	hash(20ad3cd96e837f7fbd2835f1473116dbe4278f47dde82740092f4c98fe14225a)	1
4	3	hash(9546a2994d62fdd92b699546a2994d62fdd92b699546a2994d62fdd92b6977e2)	1
5	3	hash(b999a5324924b8f82a10be072004e8d678a437f6146ff5df44ab32f10fa8eb7f)	1
6	3	hash(d431846871dd01bd95811e7b9d41fe0face6f05e45a2a5aa063090a3c47e009c)	1
7	3	hash(eedf69e23d3fcf2f498db76ea91f49ccab5e07b64d741dd29abda7df98487c4e)	1

Suspicious URLs Identified

Emails were also scanned for embedded URLs and also followed in the sandbox, with communications, downloads and other system activity analyzed as above. Often, these are attempts to establish an initial foothold within the network via a drive-by download. The top 10 suspicious URLs below are ranked by risk rating.

#	Rating	URL	Count
1	4	http*//bestbnbnepal.com/En_us/Documents/122018	1
2	4	http*//mirabellekruger.com/sryddihn	1
3	4	http*//moder.us13.detailmnt.org/trackinTZ5ktrvoUVZ5v5UNZkk/fr/UCZ/n/SqUi/click?u=8f323da014191e03b8981d530&id=2ed588983e&e=3987288334	1
4	4	http*//moder.us13.embarkon.org/trackin9LXme184_fLXyX_KLmm08C8_bL7g8jQ_i/click?u=8f323da014191e03b8981d530&id=2ed588983e&e=3987288334	1
5	4	http*//moder.us13.heavyhave.org/trackinzlv&H&0sqdlvevqbl&&00ePqElv./dzqi/click?u=8f323da014191e03b8981d530&id=2ed588983e&e=3987288334	1
6	4	http*//moder.us13.heavyhave.org/trackinzlv&H&0sqdlvevqbl&&00ePqElv.pJPqi/click?u=8f323da014191e03b8981d530&id=2ed588983e&e=3987288334	1
7	4	http*//moder.us13.livealways.org/trackinr2/VNYwk=Z2/0/=J2VV_wlw=72/5rnf=i/click?u=8f323da014191e03b8981d530&id=2ed588983e&e=3987288334	1
8	4	http*//moder.us13.livealways.org/trackinr2/VNYwk=Z2/0/=J2VV_wlw=724AWmr=i/click?u=8f323da014191e03b8981d530&id=2ed588983e&e=3987288334	1
9	4	http*//moder.us13.livealways.org/trackinr2/VNYwk=Z2/0/=J2VV_wlw=72_A5nX=i/click?u=8f323da014191e03b8981d530&id=2ed588983e&e=3987288334	1
10	4	http*//moder.us13.noonwith.org/trackinBUn8uL=9YSUnlnYlU88O=f=YPU11DKJYi/click?u=8f323da014191e03b8981d530&id=2ed588983e&e=3987288334	1

Note: URLs within this chart have been changed from “protocol://” to “protocol*//” to prevent clicking on live malicious links.

Impersonation Analysis

Impersonation emails are generally targeted attempts by nefarious actors to emulate an authority within a specific organization rather than using attachments or URLs, they rely solely on communications to establish trust and entice the recipient to take an action. The top 10 impersonation email interactions are listed below based on attempts.

#	From	Subject	Count
1	mcc72ber@gmail.com	Fwd: Current work	1
2	mcc72ber@gmail.com	Fwd: School Registration	1
3	samps@wk-338.com	External: Important: Tax Update	1
4	samps@wk-338.com	External: Fwd: Registration Confirmation - Informata2019 Event	1

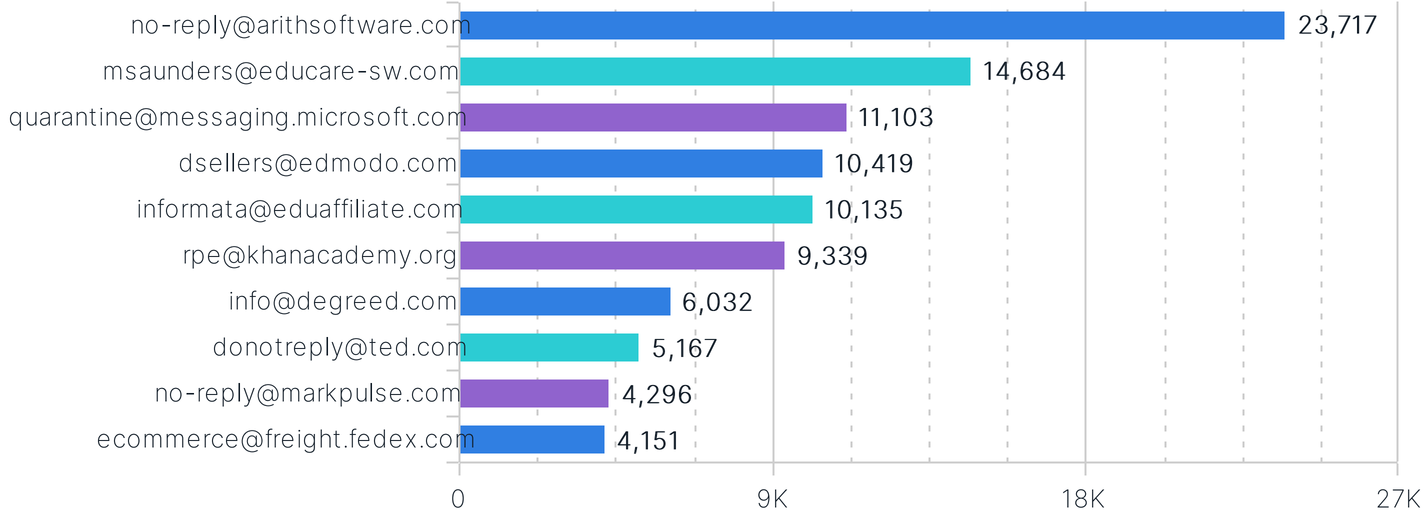
Productivity

Quick Stats

- 415,225 emails flagged as spam
- no-reply@arithsoftware.com is the top spam sender
- arithsoftware.com is the top spam domain
- 91:100 spam versus valid email ratio
- news@edumarketnews.com is the top newsletter sender
- 19,925 suspected newsletters
- 1,647 emails detected with adult content

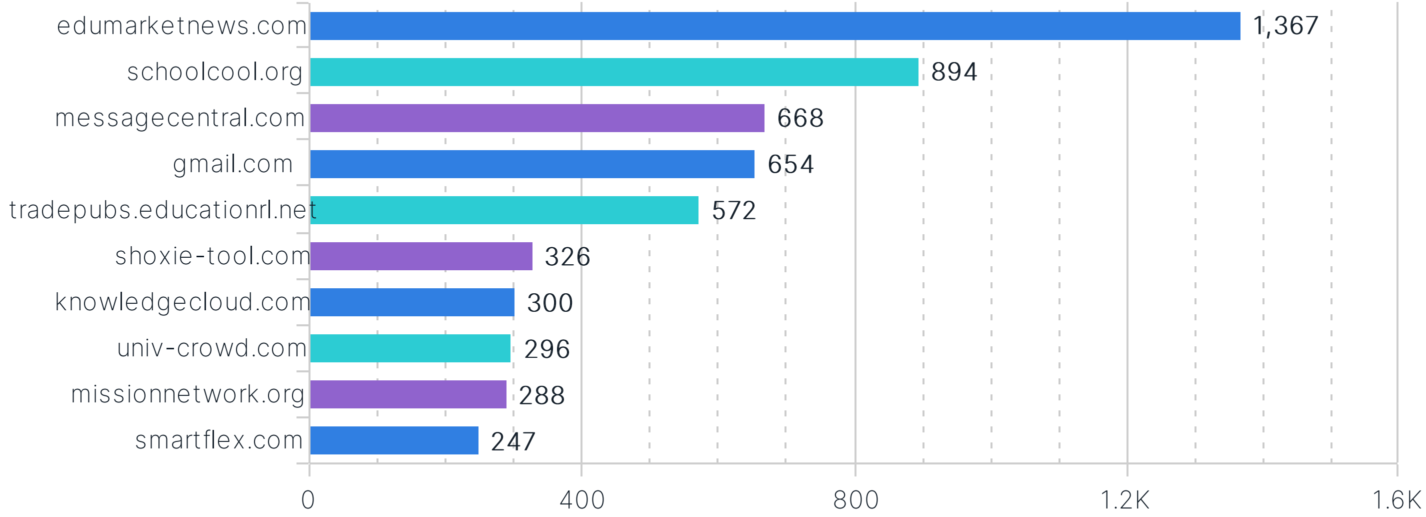
Top Spam Senders

Spam is a persistent annoyance with most organizations. By understanding sources, enterprises can simply blacklist senders. Should they find they are the senders, often in the case of marketing communications sent internally, it is recommended that volume is rate controlled to avoid the organization ending up on blacklists. The top 10 spam senders by volume to your domain are listed below.



Newsletter Domains

Generally not considered spam, but sometimes equally as impactful are newsletters that your email users subscribe to. If newsletters are a burden on your email infrastructure, we recommend modifying or enforcing corporate use policies and asking subscribers to use their personal email addresses for such communications.



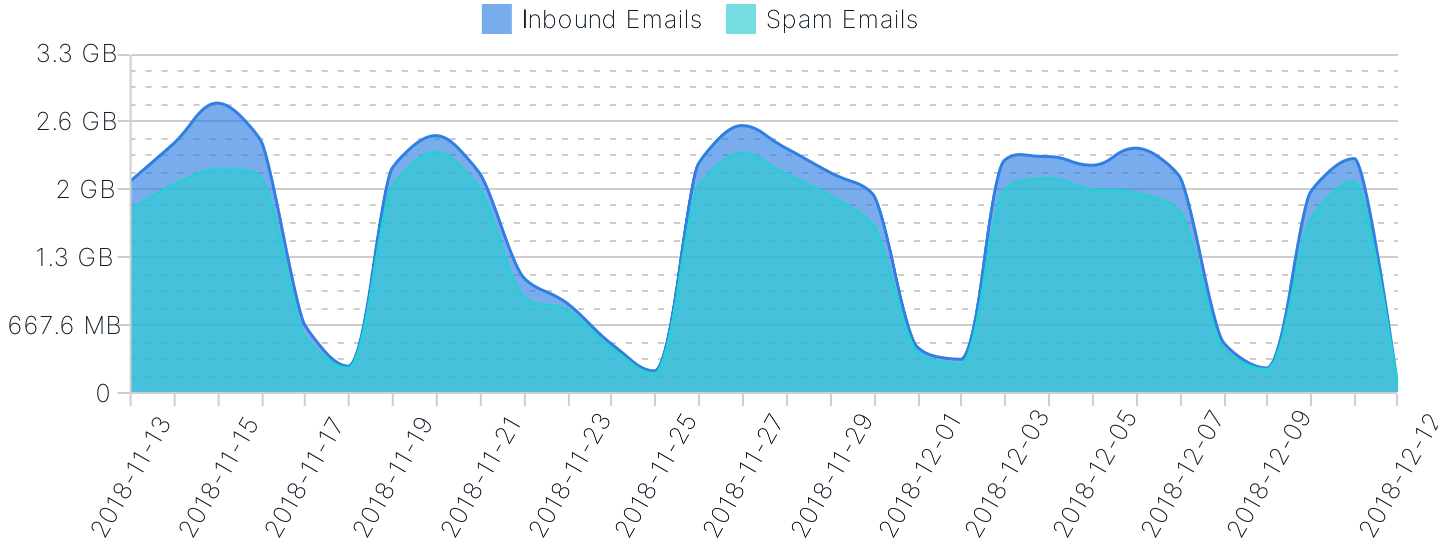
Utilization

Quick Stats

- 15,215 average emails processed per day
- 1.6GB average email bandwidth per day
- 110.6KB average email size
- 28,263 peak number of emails processed per day
- 456,451 total emails processed
- 8.8MB largest size emails on average per day
- 2.8GB peak email bandwidth per day

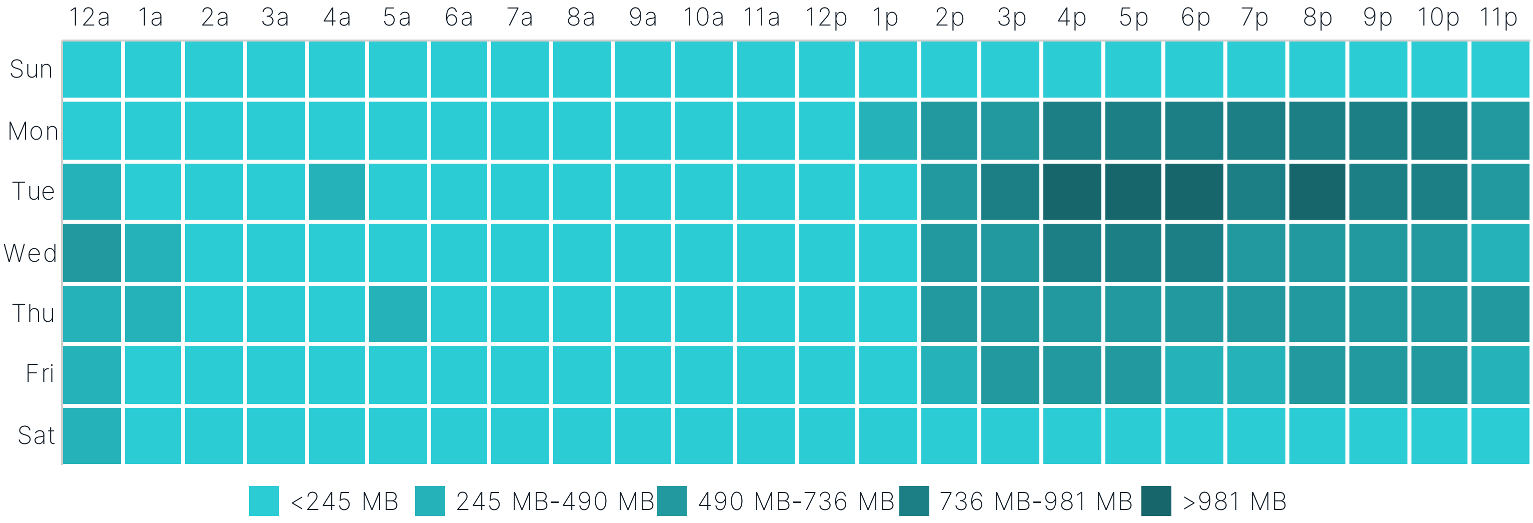
Email Bandwidth per Day

The chart below details the amount of inbound traffic relative to spam received during the length of the email assessment. There is typically a dip during non-work hours (usually resulting in a decline in email activity over the weekend).



Email Bandwidth by Hour

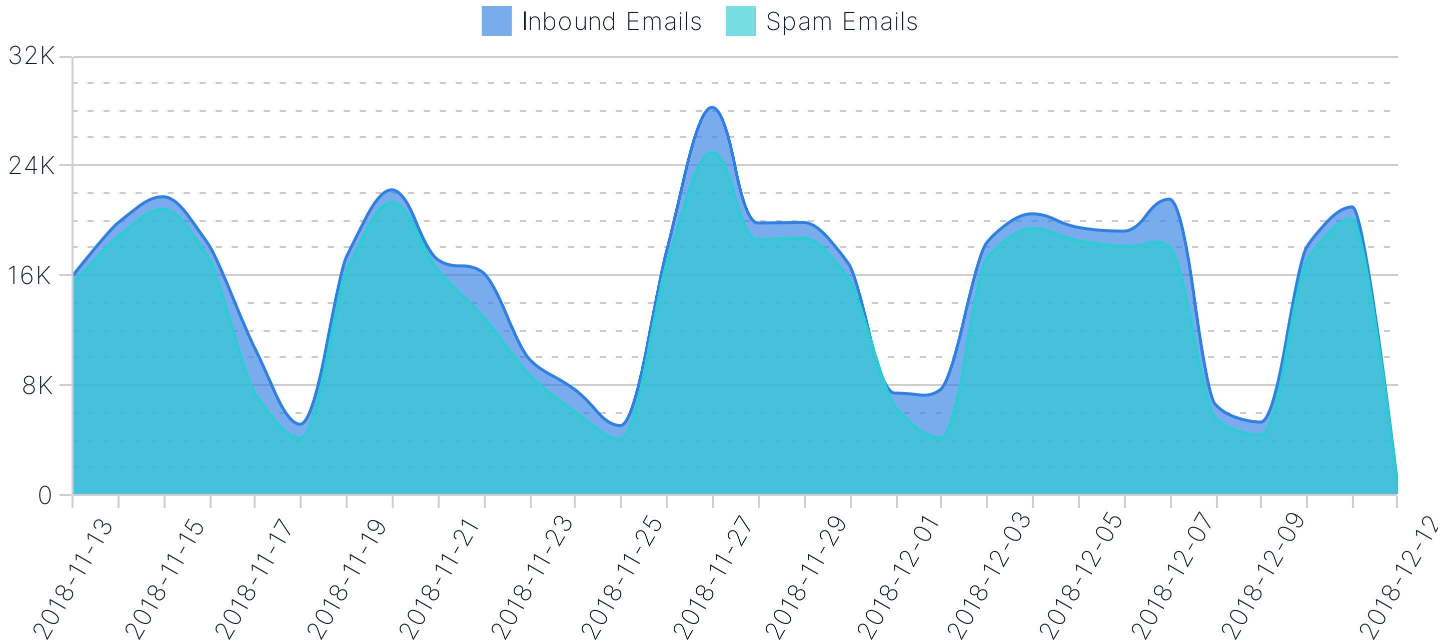
The intent of this chart is to visualize peak usage for bandwidth related to email. Keep in mind that the legend is based on a sliding scale which illustrates bandwidth segmented into five equal distributions. It's typical for this chart to display heavy bandwidth usage during work hours. However, heavy activity outside of normal work hours could be indicative of issues worth further investigation.



Utilization

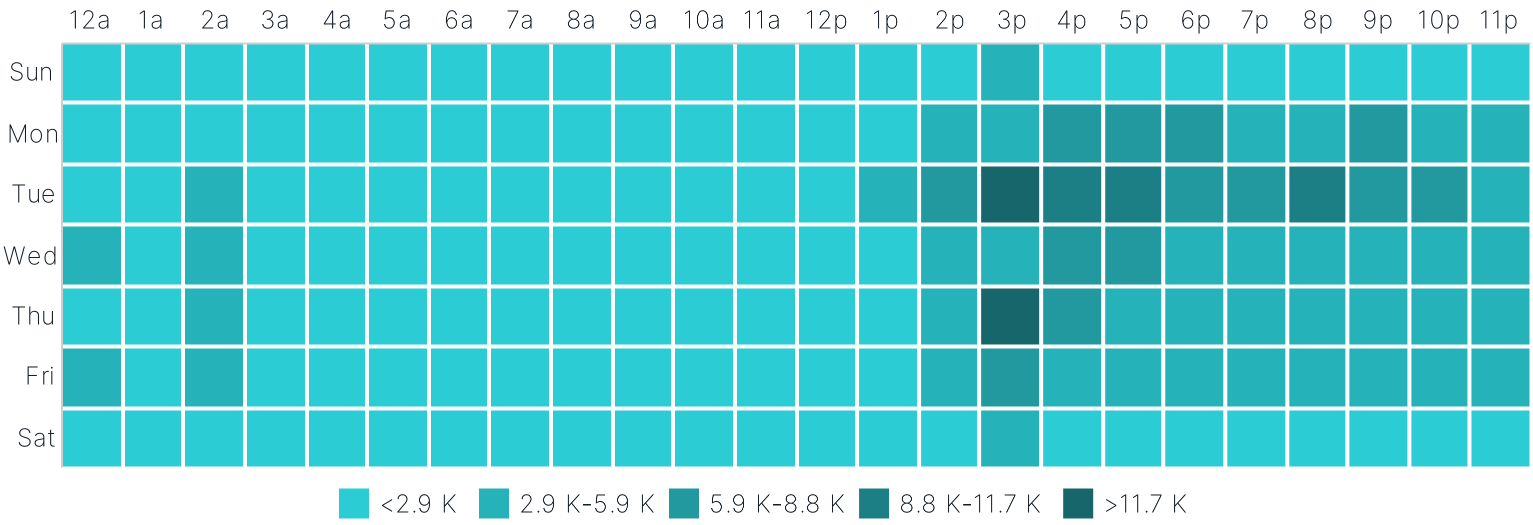
Email Count per Day

As opposed to Email Bandwidth Per Day, this visualization represents the sheer number of emails (total count) moving through your email infrastructure. As with the bandwidth chart, this will typically fluctuate from highs (during the work week) to lows (during weekends).



Email Count by Hour

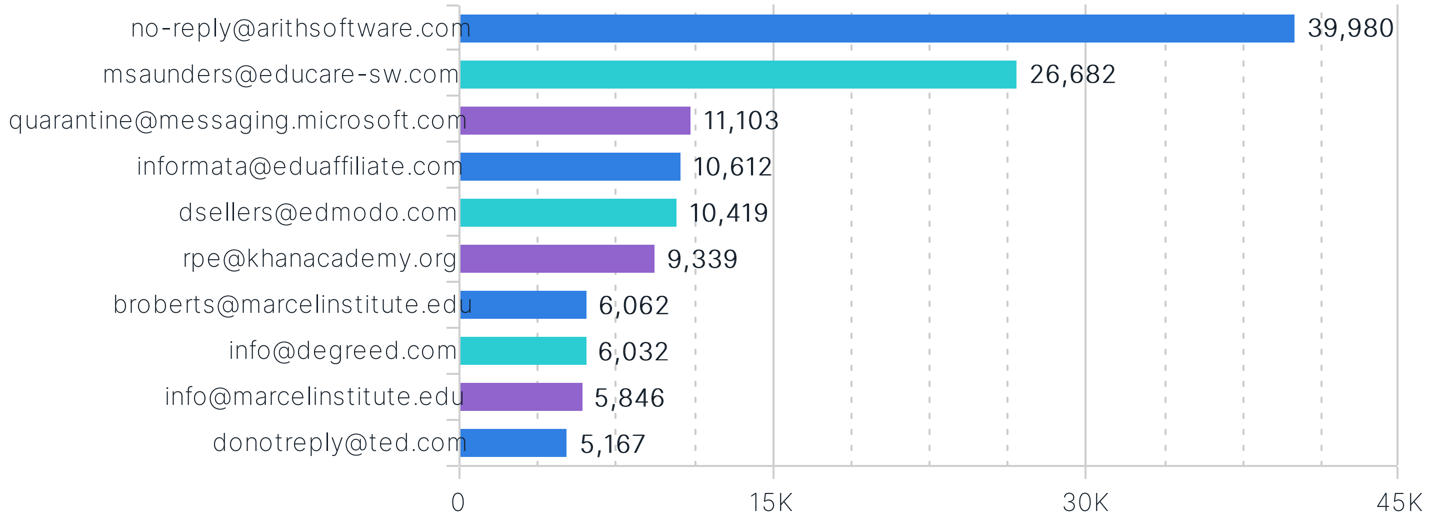
Similar to Email Bandwidth by Hour, this heat map renders a count of emails across five evenly spaced (dynamically generated) distributions. Any peak email counts outside of normal work hours may be worth investigating. If your email system applies to a global organization, this can help identify regions which may need increased email capacity.



Utilization

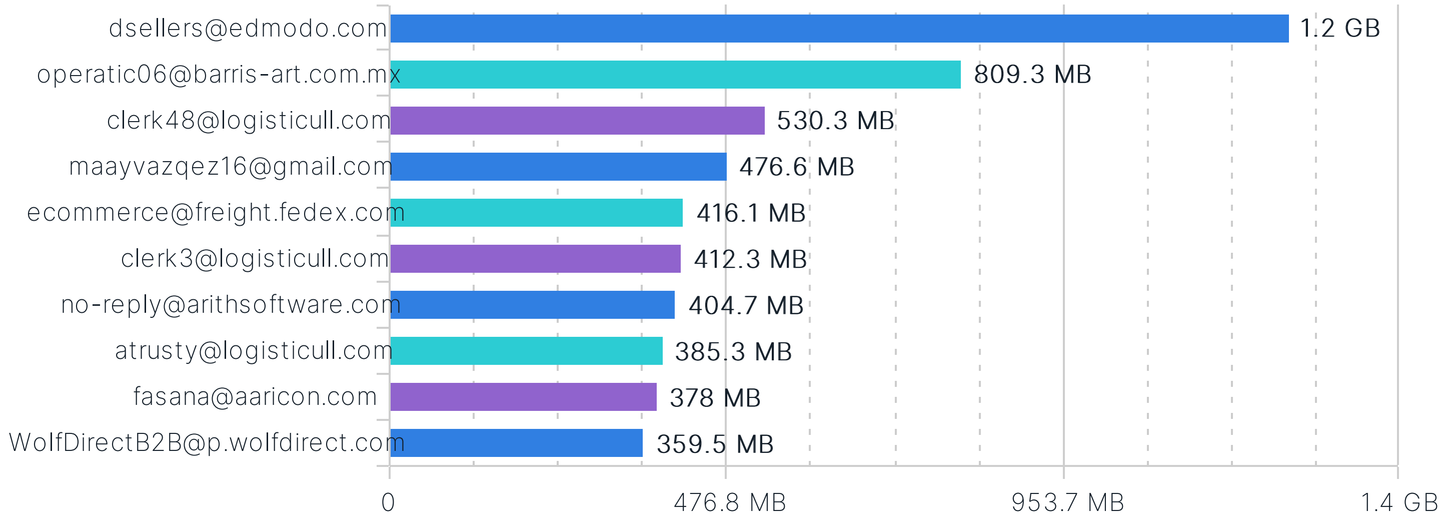
Top Senders by Count

Identifying external senders who are generating large amounts of email can be useful to reduce the load on your messaging infrastructure. This could include working with partners to reduce the amount of automated emails, changing corporate use guidelines regarding newsletters, or even potentially blacklisting certain email addresses.



Top Senders by Bandwidth

Similar to Top Senders by Count, this chart represents external email users who utilize the most bandwidth. This generally means these users consistently include multiple or large attachments within their emails. It can be especially useful in identifying partner processes which may be better served utilizing a different method of data exchange.



Recommendations

☑ 1. Augment Your Email Security to Protect Against Known Malware

Known malware is currently bypassing your existing email gateway. We recommend that you verify the malware signatures on your existing email gateway are up to date. If those signatures are already current, consider augmenting your security with a secondary email gateway.

☑ 2. Add Sandboxing Technology to Detect Unknown Malware

Emails containing suspicious attachments (potentially unknown malware) were detected. Consider implementing sandboxing technology to supplement your email security solution.

☑ 3. Improve Malicious URL Detection and Training

Emails containing known malicious URLs are being sent to your organization and circumventing your existing email gateway. We suggest two courses of action: 1) add an additional layer of security to detect known bad URLs 2) train your email users to never click on unknown URLs.

☑ 4. Educate and Protect Email Users from Impersonation Attempts

We detected emails which were an attempt to impersonate legitimate internal user(s); a type of spear phishing. Ensure that you have: 1) trained your email users how to determine legitimate senders 2) implemented an email gateway which can quantify and root out impersonation email attempts 3) have properly implemented and are managing your DMARC records.

☑ 5. Implement Stronger Controls over Adult Content

Some email users are receiving explicit adult materials via email. This can create an uncomfortable and even unsafe work environment. Consider implementing stronger email security controls over this category of email.

☑ 6. Remind Email Users About Proper Newsletter Use

We detected an inordinate amount (19,925) of inbound newsletters utilizing your email systems. Depending on your corporate use policies, you can use this to remind email users 1) to please use personal emails to subscribe to non-work newsletters 2) to unsubscribe to any opt-in, non-work newsletters 3) to ignore newsletters that were not opt-in, but use this time to minimize their email footprint on the Internet (some non-consentual newsletters are sent to email addresses found via screen scraping).

☑ 7. Contemplate Reducing Your Spam to Valid Email Ratio

Your current spam to valid email ratio is significantly higher than most organizations. With persistent anti-spam optimizations, most organizations can bring this ratio down to something more manageable.

☑ 8. Add Isolation Technology to Address Zero-day Attacks & Suspicious Emails

Emails containing suspicious URLs (potentially phishing or advanced threats) were detected. Consider implementing isolation technology to bolster your email defense so content from the web is accessed in a secure, remote container and risk is eliminated.