MSIS 512: Spam Email Analysis

Hypothesis:

Focusing attention on the recent annual event of Black Friday, we attempted to determine that the majority of spam messages observed (past 30 days) will be related to shopping, classified as low risk, originating from North America (region), and be sent on a weekday (day of week) as people are likely to check their emails on weekdays while they are working.

Introduction and Methodology:

Methodology - We first created a repository of roughly 100 spam emails, aggregated using 8 personal email accounts. This collection process required manual extraction of artifacts. The reason is several-fold:

- Aggregation between different email accounts (with private passwords/credentials and service providers) makes it difficult to use 1 piece of code to extract the details easily by a single team member
- Despite being marked as 'Spam', roughly 30% of messages we observed were wrongly flagged by service providers (which verges on the safe side). That is, many spam emails were simply advertisements or subscriptions from legitimate shopping websites. We want to filter out, and exclude these messages from the analysis to improve accuracy (which requires human intervention)
- Spam boxes are cleared after 30 days, meaning that a few personal email accounts checked were nearly empty, making it relatively convenient to check by hand. Similarly, a busier email account often had repetition between the spam received (i.e. the same message sent by the same actor several times). For the sake of covering as much diversity as possible, we excluded repeated messages.

Thus, by analyzing the headers of the original messages (HTML) we extracted: subject line, sender's ID (domain), IP address, URLs/clickables, and date/time. This information was collected into an Excel.

Next, we verified the IP addresses (and embedded links), using Brightcloud Threat Intelligence to help determine: the related threat level (IPs, links) and the location of the sender (country and region). This information (checked one by one) for all the spam emails, was added as new columns in our Excel, acting as the information repository. Note that Brightcloud categorizes threat into the following levels: Trustworthy, Benign, Suspicious, Low, Moderate, High.

The final step (prior to analysis), is classifying these emails individually by risk. As defined in lecture:

Risk = Likelihood * Impact
Likelihood = Threat * Vulnerability
∴ Risk = (Threat * Vulnerability) * Impact

Using this general equation, we discussed the relative risk of each spam message, ultimately fitting/assigning them into a classification structure as follows (0-5): Trustworthy risk (0), benign risk (1), low risk (2), suspicious risk (3), moderate risk (4), and high risk (5).

Breaking things down further, vulnerability was determined in our risk equation by looking at the nature of message body. Vulnerability was numerically divided into: Plaintext (0), Disabled pictures (1), Button (2), Links (3).

2 sample calculations of this risk categorization process is as follows:

Description: Spam message containing plaintext ("hi there")

- Threat (intent of the actor) from Brightcloud = "Trustworthy"
- Vulnerability (patching, safety precautions): 0
- Impact (# people using service, affected): relatively high (we may expect this email to have been sent to others, perhaps using the same service provider, Gmail)

Risk = (Threat * Vulnerability) * Impact = Trustworthy * 0 * High = 0
So this spam is classified as "**trustworthy risk**".

Description: Spam message containing UChicago account being flagged

- Threat (intent of the actor) from Brightcloud = "High Risk"
- Vulnerability (patching, safety precautions): 3
- Impact (# people using service, affected): High (the number of people falling victim to this spam will be limited to students/alumni/applicants related to UChicago, as a ballpark. However, this is also the application season when many prospective students are applying to university. This includes the number of high school seniors perhaps within the top 15% of class rank, along with grad students.)

Risk = (Threat * Vulnerability) * Impact = High Risk * 3 * High
Classified as "**high risk**", considering all variables are high across the board.

Examples of Spam in different risk levels:

After initial categorization/processing, we dug deeper into the analysis, examining what relative risk implies, typical behaviour of the actors, and mitigation techniques that can be used to tackle these differing types of spam. In this part, we will pick one representative spam (from each risk category) to explore in greater depth.

[Trustworthy risk, 0] Sample spam content: 'Hi' (untargeted malicious)

1. There is no risk associated with this particular email and reflecting on the nature and type of the email, it is of a random email type and contains simple text. Analysing this content of the email, the likelihood of something unfortunate or risky happening is negligible. Taken along with the impact, which too is nearly negligible, the relative risk involved in the scenario is insignificant.

2. The message was sent from the IP address - 150.36.167.9, coming from United States. It belongs to the direct/random spam category.
3. In order to avoid the inconvenience of spam overload, the user can block this individual, configuring their inbox setting to filter the contents of incoming messages.
4. It can be interpreted from the nature of these emails that certain organisations or domains where a user might have registered their contact information, will be contacted, as a consequence of their email address being easier to obtain.

[Benign risk, 1] Sample spam content: Fake news subscription alerts (untargeted malicious)

1. There is low risk involved, since there are no URLs or executables. Additionally, the likelihood of people clicking on random political news email blasts is rare, as the conventional medium for getting news is by browsing the Internet for interested topics, or watching television/reading a newspaper.
2. The email was sent from the IP address - 199.191.59.67 and was based out of Ukraine.
3. One of the reasons to have been targeted by these news email blast senders is when people give out their emails on less secure websites which do not encrypt the information properly, or share the information with other agencies. The email IDs, among other details are intercepted by groups with tendencies to gather attention and then later probably misuse the individual's details for convoluted purposes. It is advisable to not sign up with any loose websites and reviewing all checkboxes during, say "sign up", to see how their information will be used.
4. From research, many fake news-type spam messages are received from foreign, and largely European/Asian countries. It can be interpreted as a political gimmick for influencing public in either of positive or negative connotation against a government.

[Low risk, 2] Sample spam content: Survey related (untargeted malicious)

1. This type of email asks you to take a survey related to the completion of a shopping trip or appointment, and it contains links redirecting you to such shopping/service websites. The website then typically asks for additional contact information to send you future promotional opportunities. However, the website, in most cases, is legitimately a platform for selling of goods.
2. Majority of the emails which ask for filling out a survey we observed, were coming from legit online retailers or service providers, especially those we had visited before. However, we did notice that some poorly designed messages came with typos and information that did not match our records.
3. In order to mitigate the risks from related survey oriented emails, we need to pay attention to the sender to determine whether we are familiar with the source or not. We should also be aware of the possibility of CSRF (Client Side Request Forgery) attacks.
4. Reporting the low risk emails may be helpful for reminding future recipients to be aware of the potential risk of having personal information be exposed. Also, links included in the survey emails may redirect users to other suspicious websites containing executables (downloading malware/viruses). This is a good reminder to have proper

firefall installed (both on the network and antivirus on the computer) as protection measures.

[Suspicious risk, 3] Sample spam content: Fake eBay Spam (untargeted malicious)

1. In this email, the sender was requesting the receiver's home address under the guise of eBay asking to confirm their address to be entered in a prize giveaway. When a user clicks the link, a response email is generated and the only thing the user needs to do is click reply. This email would not only not be sent to eBay, but to a list of various emails of unknown users (chain email with 5-10 other people).
2. The message using the IP attached of 185.34.216.47 is located in Amsterdam and is claiming to be eBay. Although the sender uses a .br (Brazil) email, they forwarded the message via restojob.ru which is a website with servers in Amsterdam and owned by Russia.
3. To mitigate the risk, we should trust our spam folders as a first layer of protection. Regardless, some spam emails will still get through so if we don't recognize the sender we should probably not open it. Make sure to not download any pictures or files within these suspicious emails.
4. This IP/URL could be reported to sites like Brightcloud, which could be used to help others avoid potential harm and ensure that future email from this domain is confirmed to be a risk, and quarantined to more spam folders. In the case of dangerous URLs, we could also turn to firewalls (i.e. stateful inspection, proxy firewall as examples).

[Moderate risk, 4] Sample spam content: Black Friday Promotion (untargeted malicious)

1. Clicking on the link in the email will lead you to a shopping website that asks you to put in credit card information. Leaking this information may cause monetary theft, which could be worse if it goes undetected by the victim.
2. Belk.com is the particular website domain that sent out this email, which sells cosmetics
3. We can look up the reputation of this shopping website by searching customer reviews on internet. Complaints about shopping experiences on sites like FCC or consumer forums could be a reg flag. Pictures in this email were actually disabled because of Gmail’s Spam security features, although an unprotected email could easily contain executables or click-jacking opportunities.
4. Not all promotion emails on Black Friday are safe to be trusted. Similarly, don’t be tricked by the low prices advertised on the banners, as ridiculously low price points should make you even more skeptical. In case you clicked on link accidently, proceed cautiously if credit card information is requested. We also noticed that emails of this type often have money (or emojis) shown in the subject lines, which could be an identifying attribute.

[High risk, 5] Sample spam content: UChicago Account Flagging (untargeted malicious)

1. The email claims that the student’s UChicago account has been flagged (and reported, ironically, as spam). The recipient is asked to reactivate the account by clicking a link (button), which redirects them to a malicious website classified as “high threat” (10 of 100 on Brightcloud). The site could possibly request information like SSN, birthday,

name, email, and educational history. Identity theft is probably why the given threat score is so high, since the impact for the victim could be very costly. Additional details can be seen in the sample calculation performed for this message in the previous section.

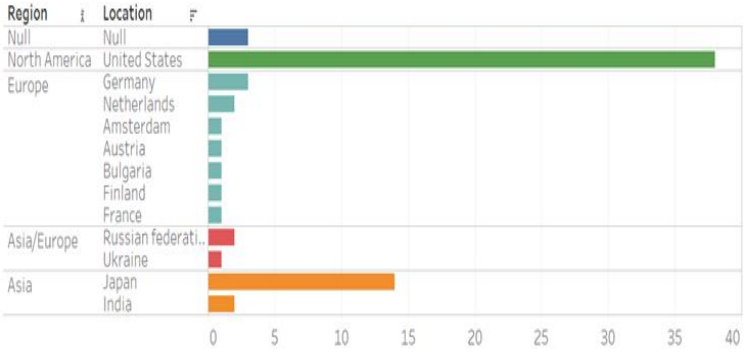
2. Interestingly, the spam was 'supposedly' sent from by the University of Washington (likely a typo, as UChicago would have been a much more convincing name)- although really this is just a name the malicious actor is displaying for the email address (which is @bristol.ac.uk, rather than an .edu source). The traced IP address (128.95.242.222), originated from the United States, and was sent on a Wednesday (weekday). There has been 1 infection (in the past 12 months) by clicking this link.
3. Mitigation includes checking for consistency between names/addresses, catching misspelled words/phrases in the body of the email. The recipient could also 'hover' their cursor on top of a link/button to catch a glimpse of the actual URL they are being directed towards before clicking. In this example, the redirected site also does not come from a trusted .edu source, which becomes a red light.
4. General reporting includes flagging this domain as unsafe, or blocking this website from the router/firewall (i.e. Web Application Firewall, WAP). But more specifically to this example, this website is an example of phishing (fraud). Prevention could come in the form of being aware of modern techniques such as cross site scripting (likely reflected XSS) and click-jacking (along with clever overlapping of transparent links behind images), in such that in this day and age, criminals really don't have to rely on brute force Rubber-hose cryptanalysis to extract personal information anymore. The lesson: tread cautiously.

Aggregated Analysis of the Data:

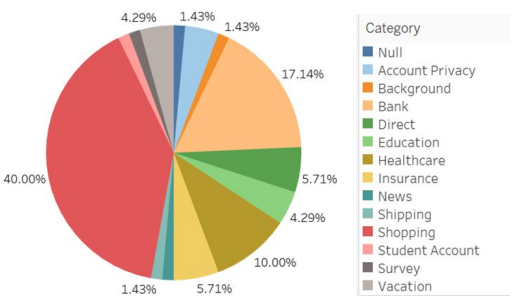
Inspecting the dataset, we attempted to visualise overarching trends to get a vivid understanding of our spam. Focusing on our hypothesis and Black Friday's influence, we explored the following attributes of the dataset:

Spam based on Region

Regional analysis describes the distribution of the email over different geographies and breaks them down in a country-wise manner. Looking here, we saw an unfiltered spike in United States' spam records, showing that most of the spam was sent from within the US.



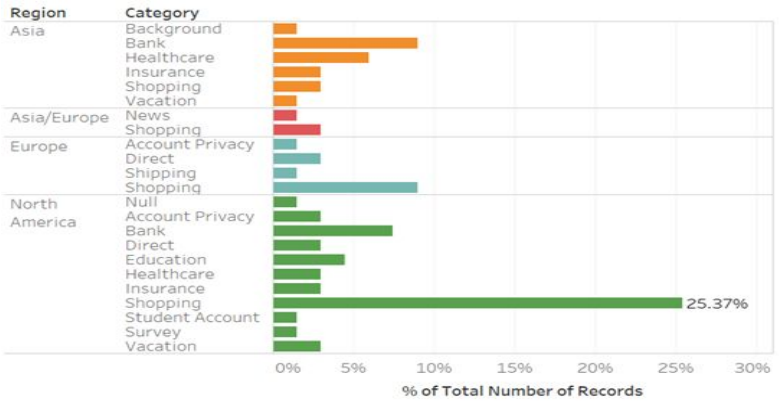
Category of Spam



Analysing the categories, the data reflects that most of the emails sent overall were as lucrative means to entice the user to shop for products listed.

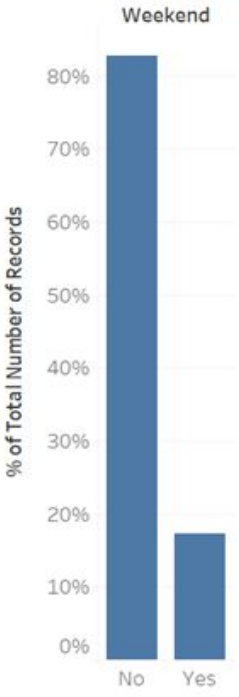
Spam based on Region and Category

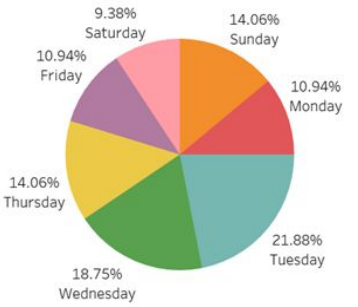
Drilling down further, we found that of all the spams received, the ones in the category of shopping was the highest from the whole set, alone in the US; going as high as 25.37%. This is likely because we are in the U.S market. So, it makes sense that we receive most of the emails from North America since we are their target customers.

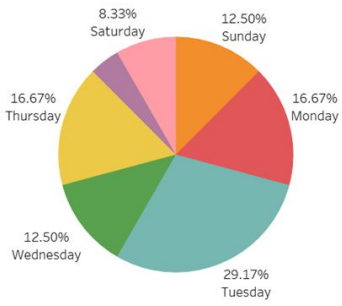


Spam relative to Day of Week

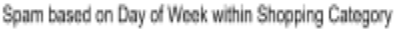
From this bar chart, we can easily tell that there were more spam emails during the weekdays, although it's unclear if the actor could set-up messages to deploy at scheduled times. We further plotted a pie chart to see whether the specific work days will have a higher chance of collecting incoming spam. From both charts, we can determine that Tuesday (21.88%) and Wednesday (18.75%) are the days that most spam emails are received.







As shopping related content is the most popular spam emails, so we did a separate analysis for it. Consistently for general spam emails, Tuesday (29.17%) has the highest percentage compared to other days of the week. Monday is another big day for shopping category spam emails.



Text Mining of Spam

We analysed the most common words on the subject lines of emails, picked the top 25 words in terms of frequency, and built a word cloud using R text mining techniques. This word cloud further strengthens our hypothesis of Black Friday shopping related emails being circulated widely at this particular point in time.

Observations and General Insights

False positives are higher for spam inboxes (by email service design). A decent percentage of spam emails were classified as “From a trusted sender” while being in the spam folder. The algorithm sorting the mails has to be more sophisticated to accommodate this anomalous behavior and users have to be more careful while traversing their mails. Titles containing monetary and Emojis incentives to attract attention are usually a spam email. Moreover, it can be observed that spam emails tend to have incomplete sentences with noticeable grammatical mistakes, allowing for easier identification of potentially fraudulent emails. Afterall, human intelligence and gut feelings about an email being spam is comparable to any filtering algorithm.

Additionally, higher risk spam is less common, but the effects could be much more pronounced using methods such as phishing and other forms of fraud. Spam messages are deleted after 30 days, and it is one of the most popular default settings for many email service providers’ to free up the storage for their users. However, the email service providers are trying to filter incoming emails by comparing emails that users marked as spam, so the more emails marked, the better their automatic filter work. In this case, users need to put some effort in this process to help the email service provider to more accurately filter the spam emails to protect their users.

Findings

In regards to our hypothesis, we have discovered through our observations that the majority of the spam messages we receive where shopping related (around 40%). What we were not expecting is that most of the spam we received was not classified as low-risk like we had imagined. Instead we found that a larger portion of our emails were suspicious (28.6%) followed by benign (22.9%) and finally low-risk (20%). We had hypothesized that low risk spam would have been the most common because we did not expect so much spam to have a threat level high enough to push it into the realm of suspicion through our Threat Intelligence software. In this regard, we also found a relatively low level of trustworthy (7.1%) and high risk (2.9%) spam emails which was surprising. We were however, correct in our hypothesis about the region most of the spam was coming from. It comes at no surprise that most of the spam was originating from North America (specifically the U.S) due the the holiday season. From our results, we also found that most spam is sent on the weekdays between Tuesdays and Thursdays, in general, but if we dig deeper into categories and isolate shopping, we find that most spam is sent on the weekdays and comes even more in line with our hypothesis. Shopping season means the frequency of emails sent on Tuesday, Wednesday and Thursday (before Black Friday) is higher. This could impact the results we are observing for day of the week for emails.

Works Cited

"BrightCloud Threat Intelligence." *URL/IP Lookup* www.brightcloud.com/tools/url-ip-lookup.php#.