Impersonation Detection

How The Email Laundry's Impersonation Detection Saves Customers over $107 Million a Month

the email laundry

The Email Laundry is a leading provider of email security as a service to the private sector in the US, UK and Ireland. Having built one of the top performing secure email gateways worldwide, as ranked by Gartner Peer Insights, the company has gone on to provide a full range of cloud based security services through the channel. The Email Laundry suite of products covers all your email security needs, Email Security, Email Continuity, and Email Archiving.

Introduction

To help combat the ever-evolving variations of impersonation attacks, The Email Laundry makes use of machine learning, threat intelligence, and content analysis to identify impersonation attacks before they reach the user's inbox.

Running reports like the one you will see outlined below is just one way The Email Laundry ensures our systems are staying one step ahead of the cyber criminals. Through these reports we are able to identify patterns, problems, and possible improvement areas, which are then acted upon and implemented, creating a more refined and optimized email security service for our customers.

Data Information

The data in this report covers 25 days of inbound email traffic (September 10th – October 4th). For the purpose of this report we will focus on emails that were blocked on the content level of our email security service for hitting our impersonation detection filters.

These include:

- Emails containing URLs from newly registered domains
- Emails originating from a similar domain to the receiver's domain
- Emails originating from a domain that sounds like the receiver's domain
- Emails impersonating a known friendly name or display name

Impersonation Attacks

Coming in various forms and varieties such as CEO Fraud, impersonation attacks have become a major threat to businesses around the world. The Email Laundry is committed to keeping those threats away from our customers and have developed various systems and tactics to protect corporate assets and finances.

What Do They Look Like?

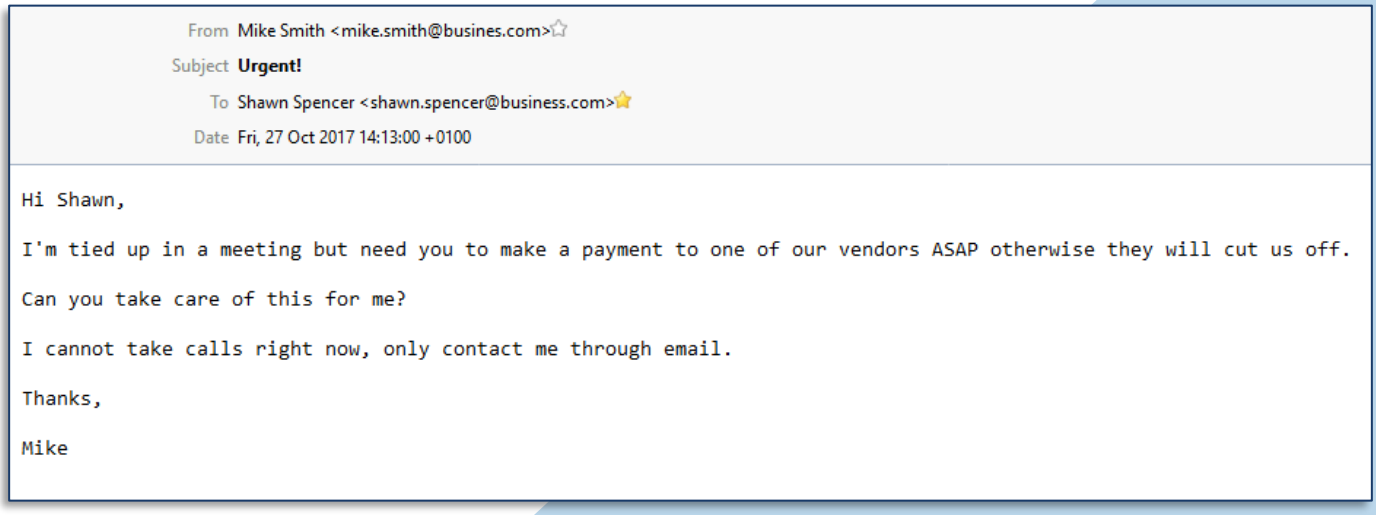
As mentioned above impersonation attacks come in many different variations; they can appear to come from a boss, friend, vendor, government agency, or any other trusted source. These attacks may claim they contain overdue invoices, confirmation links, or just request the receiver complete a task such as wire or file transfers.

Below is an example of an impersonation attack that attempted to be from Mike Smith, the boss of the recipient:

What Can They Lead To?

Impersonation attacks may seem very authentic and can be hard for users to identify as an email attack. If a user completes the requested action in an impersonation attack there can be many consequences including:

- Infection of Company Systems
  - Ransomware, Keylogging, Etc.
- Loss of Corporate Finances
- Breach of Corporate Data
- Breach of Employee Data



From Mike Smith <mike.smith@busines.com>
Subject **Urgent!**
To Shawn Spencer <shawn.spencer@business.com>
Date Fri, 27 Oct 2017 14:13:00 +0100

Hi Shawn,

I'm tied up in a meeting but need you to make a payment to one of our vendors ASAP otherwise they will cut us off.

Can you take care of this for me?

I cannot take calls right now, only contact me through email.

Thanks,

Mike

Impersonation Detection

The Email Laundry's Impersonation Detection was designed to identify and isolate impersonation attacks before they reach a user's inbox. Utilizing a combination of machine learning, advanced threat intelligence, and content analysis, all emails that flow through The Email Laundry's email security service are scanned and assessed for malicious intent.

Machine Learning & Threat Intelligence

A subset of artificial intelligence, machine learning systems are designed to take a large set of data, analyze it, and learn from it. Our machine learning systems work with our industry leading threat intelligence to recognize patterns and make a prediction on whether the email in question is dangerous on the connection level.

Under 24 Hour Newly Registered Domains

There is normally a 24-hour delay between the registration of a domain and the publication of the newly registered domain lists that security services use to identify and blacklist malicious domains. The Email Laundry can check these lists before they are published, allowing us to catch the first malicious email sent from a domain without having to wait for an attack to react.

Content Analysis

Evaluating the header, body, as well as links and attachments, our systems are able to catch any harmful emails that have passed through the connection level. We use a variety of filters to help identify these emails such as:

- Newly Registered URLs
- Similar To Domains
- Sounds Like Domains
- Friendly Display Name
- Friendly Name

Results

The following is an analysis of some of The Email Laundry Impersonation Detection filters over 25 days of observation.

Newly Registered URLs

Cyber criminals will register new domains as they will not be on any blacklists, increasing the likelihood that their email will arrive in their target's inbox unimpeded. Since The Email Laundry has access to under 24 hour domain registration lists, our systems are able to check not only the sender domains for malicious activity but also check the domains of URLs contained in the body.

Quick Stats

- 4.54% of all blocked emails were blocked because they contained URLs from hostile domains
- On average 20,592 emails containing newly registered domains were blocked everyday
- 56% of the 25 days, had over 20,000 emails blocked because they contained newly registered URLs
- Tuesday, September 12th had over 40,000 emails with newly registered URLs blocked

Similar-To Domains

In hope of appearing to becoming from an internal source, cyber criminals will spoof the sender domain to a domain similar to the receiver's domain. Some examples of similar to domains are bit-flipped domains, domains that are missing a letter, or domains with letters replaced by a symbol, number, or similar letter (ie. replacing a lowercase L with a capital i).

Quick Stats

- 1,436 emails were blocked every Tuesday because they were sent from a similar-to domain
- Over 547,000 emails hit our similar-to filter
- There was a 650% increase in emails blocked due to the similar-to filter between September 18th and September 19th
- 11,600 emails originating from similar-to domains were blocked in the first week of the data (September 10th to September 16th)

Sounds Like Domains

Sounds like domains are domains that appear to be coming from the receiver's domain by including the receiver's domain in the sender domain. These emails differ from the similar to emails since they actually contain the receiver's domain in the sender address.

Examples of Sound Like Domains

example@**theemaillaundry.marketing**.com

example@**no-reply.theemaillaundry**.com

example@**contact.theemaillaundry.temp**.com

Quick Stats

- 403,254 emails hit our sounds like filter
- 61% of all email that was blocked by the sounds like filter occurred on a weekday
- On average 1,384 emails were blocked every day in the first week due to the sounds like filter

Friendly Display Name

From the evolution of smartphones and mobile email viewing, has come the friendly display name. With limited screen space, these friendly display names have replaced email addresses as the main sender information displayed on mobile email clients. While convenient for the end user, these display names are easy for cybercriminals to spoof, making phishing emails harder than ever to identify.

Quick Stats

- 37,974 emails using a friendly display name were blocked over 25 days
- Emails blocked by the friendly display name filter increased 103% from week 1 to week 2
- On average 10,556 emails were blocked by the friendly display name filter every week
- Tuesdays had the most emails blocked by the friendly display name filter with 8,460 impersonation attacks blocked

Friendly Name

Friendly name attacks spoof the username portion of an email, making it appear to come from a trusted source of the user, usually found through social engineering. Since the email address has the username of someone they know in it, users are more likely to click before thinking, leading to compromised credentials or systems.

Quick Stats

- 26,922 emails containing friendly names were blocked on Wednesdays (the most of any day of the week)
- On average 4,896 emails were blocked every day by the friendly name filter
- Week 3 (September 24th to September 30th) had almost 39,000 emails blocked by the friendly name filter
- 17% of all impersonation attacks blocked were due to the friendly name filter

theemaillaundry

Average Success Rate of Impersonation Attacks

https://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx

0.5%

Average cost of Impersonation Attacks

https://pdf.ic3.gov/2016_IC3Report.pdf

$30,000

Impersonation Attacks Blocked by Impersonation Detection

715,804

Potential Successful Attacks without Impersonation Detection

715,804 * 0.5% = 3,579

Amount Saved from Potential Impersonation Attacks

3,579 * 30,000 =

$107,370,000

Conclusion

Canada's *Get Cyber Safe* reports that 0.5% of phishing attacks like impersonation attacks will be successful (financial or information gain).

To find the number of impersonation attacks that would likely have been successful, the number of impersonation attacks blocked over the 25 days (715,804) is multiplied by the above success rate (0.5%).

The number of potential successful attacks is then multiplied by $30,000 (the average cost of an impersonation attack reported by the Internet Crime Compliant Center (IC3)) to find the total amount of money saved with The Email Laundry's Impersonation Detection ($107,370,000).

Final Thoughts

The Email Laundry is committed to keeping email safe for businesses around the world. Our impersonation detection seen in this report is just one way in which we protect our customers from malicious email attacks. We are consistently innovating and optimizing our services to ensure that we are always one step ahead of the ever-evolving threats.

If you'd like to know more about how we protect email or want to stay up to date on our features and additions, please visit www.TheEmailLaundry.com.

The Email Laundry is a leading provider of email security as a service to the private sector in the US, UK and Ireland. Having built one of the top performing secure email gateways worldwide, as ranked by Gartner Peer Insights, the company has gone on to provide a full range of cloud based security services through the channel. The Email Laundry suite of products covers all your email security needs, Email Security, Email Continuity, and Email Archiving.