# ThreatQuotient

## Spearphishing Attack

Use Case

February 20, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

# Use Case - Spearphishing Attack

This use case provides a real-life example of a spearphish attack and illustrates how ThreatQ can help you detect, analyze, and respond to the attack.

## Detecting the Attack

Your organization received a set of spearphish emails. The emails were detected by filters on your email gateway and automatically added into the ThreatQ platform. In addition, you received a separate spearphish email to your email account.

Before you begin to analyze the spearphish attack, you need to upload the email to the TQ platform:

1. From the Investigations page, click the Create button.
2. Click the Spearphish Parser option.
3. From the Add Event window, click the Source field and select the email account that received the spearphish email.
4. Enter a status and point of contact for the event.

   > The Event Status field is displayed only if an administrator has configured Event Statuses in the Object Management page.

5. Use one of the following methods to upload the email:
   - Drag the email to the window.
   - Click the click to browse link to access your File Finder/File Explorer and select the file.
   - Paste the email content into the text box on the right.
6. Click the Add Event button.
   The Spearphish Parser page displays the initial process information from the ingestion. From this page you can:
   - Set additional parameters such as the status to be applied to all extracted indicators.
   - Establish a relationship between this spearphish attack and another object such as an indicator, event, or adversary.
7. Click the Next Step button.
   The second Spearphish Parser page displays any attachments associated with the imported email and gives you the option to import these attachments.

   > If the imported email did not include attachments, ThreatQ bypasses this page and takes you directly to the third Spearphish Parser page.

8. Click the Next Step button.
   The left side of the third Spearphish Parser page displays the email content.  The right side displays the following tabs:
   - Spearphish Attributes - Lists the email's metadata such as the email recipient (To) and subject line (Subject).

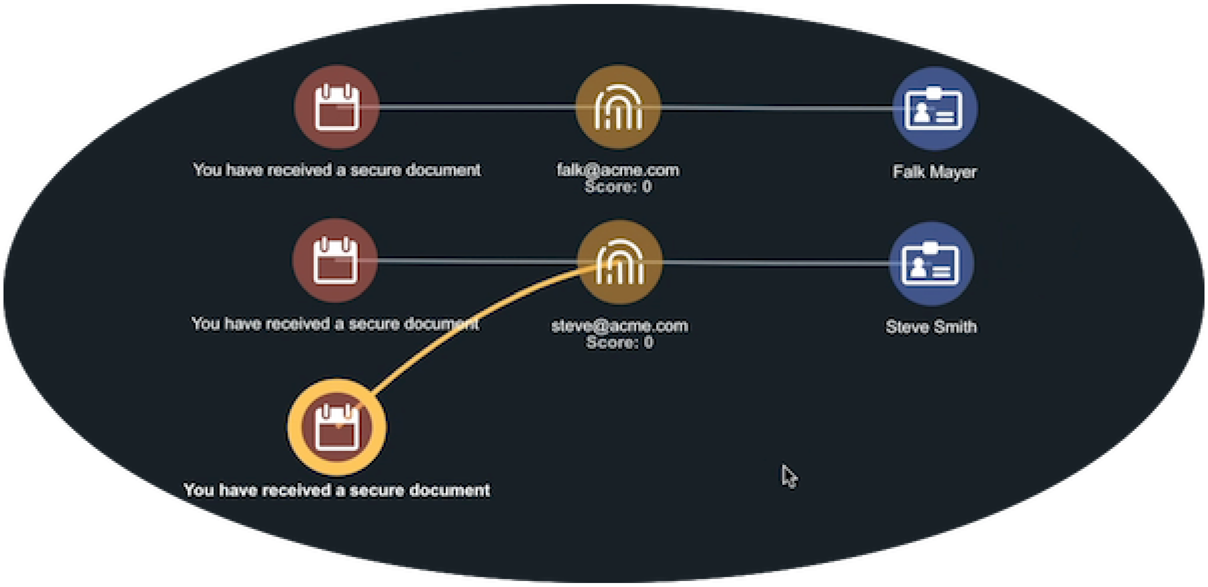
    - Extracted Indicators - Lists information extracted from the email body that correlates to indicators already defined in TQ. These indicators are labelled as Pre-Existing.
9. Click the Create Spearphish button.
   The spearphish record is ingested into the Threat Library.
10. To add your new spearphish record to your spearphish investigation, access the Investigations page and select your spearphish investigation.
11. Use the search field to locate and select the spearphish record you just created.
    The new spearphish record is displayed in your Evidence Board. This visualization allows you to identify the targets of the spearphish campaign based on which users received the spearphish emails.

> Takeaways:
> The first thing you notice is that this email was sent to the one the email addresses already associated with your investigation.

## Analyzing the Attack

Now that TQ has information on the spearphishing emails, the Evidence Board allows you to work with a visual representation of the emails and users involved in the spearphish attack.

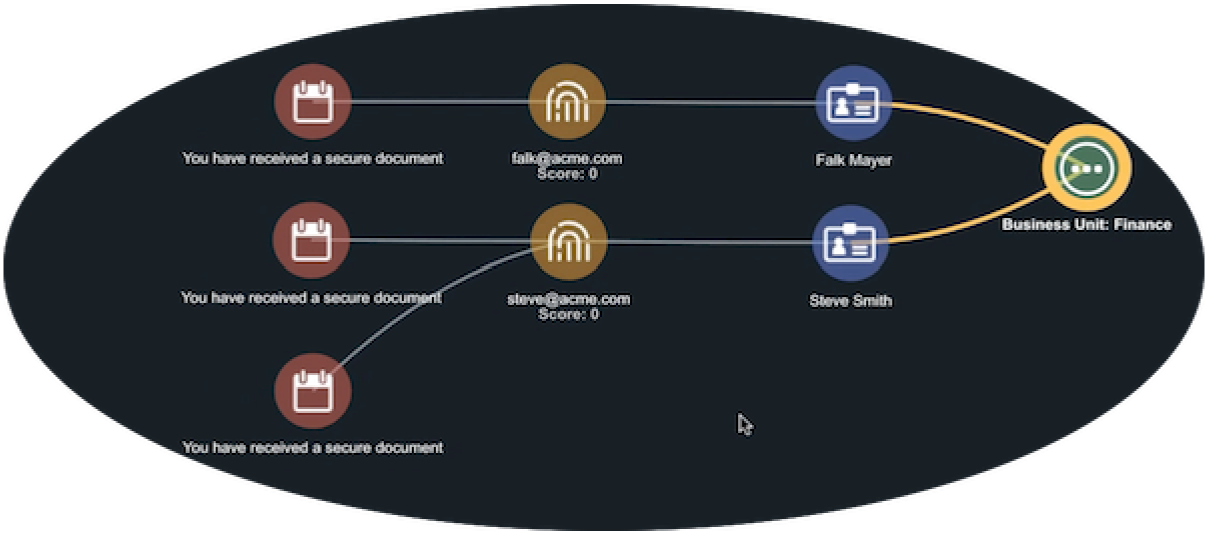
> Takeaways:
> Take advantage of ThreatQ's drag and drop options to organize the nodes on your Evidence Board to suit your preferences. The lines connecting the nodes will adjust to accommodate your changes


You have received a secure document
falk@acme.com
Score: 0
Falk Mayer
You have received a secure document
steve@acme.com
Score: 0
Steve Smith
You have received a secure document

### Step 1: Finding Relationships

In this case, the spearphish campaign seems focused on two people, Steve and Falk. So let's take a closer look at their relationships:

1. In the Evidence Board, click Falk.
   The right side of the page displays additional information on Falk.
2. In the Relationships section, click the arrow next to Attributes to view more information.
3. Falk has a business unit attribute of Finance. Click the plus sign next to Finance to add this attribute to the Evidence Board.
   When you do this, you notice that both targeted users are members of the Finance team. This lets you know that the attack is focused on your Finance group.


You have received a secure document
falk@acme.com
Score: 0
Falk Mayer
Business Unit: Finance
You have received a secure document
steve@acme.com
Score: 0
Steve Smith
You have received a secure document

## Step 2: Email Attachments

The next step of your analysis is to take a closer look at the email you added to the investigation to answer the following questions:

*Did the emails in this attack have the same attachment file?*

1. In the Evidence Board, click the email record.
   The right side of the page displays additional information on the spearphish email.
2. In this case, we want to focus on the email attachment. So, scroll down to the Files section.
3. Click the arrow next to Files to view the email's attachments.
4. Click the plus sign next to the attachment file to add it to the Evidence Board.
   When you do this you notice that all the spearphish emails in this attack had the same attachment.

*Have we received other emails with the same attachment?*

1. In the Evidence Board, click the attachment record.
   The right side of the page displays additional information on the email attachment.
2. Click the arrow next to Events to view a list of other emails, outside of the current investigation, that had the same attachment.
3. Click the plus next to the email to add it to the Evidence Board.

*Are there any relationships between the other emails and the emails in my investigation?*

1. Click the new email record.
   The right side of the page displays additional information on the email.
2. In this case, we want to focus on the email recipient. So, scroll down to the Relationships section.

3. Click the arrow next to Indicators.
4. Click the plus sign next to the email address to add it to the Evidence Board.
5. Then, click on the new email address.
   The right side of the page displays additional information on the email address.
6. In this case, let's take a look at the identity or person associated with the email address.
7. In the Relationships section, click the arrow next to Identity to view more information.
8. The email address belongs to User 3. Click the plus sign next to User 3 to add this attribute to the Evidence Board. Once you add, User 3 to the Evidence Board, you immediately see that User 3 also belongs to the Finance team. This points to a spearphish attack targeting your Finance team.

## Step 3: Recording Your Findings

Now, it's time to log your findings to share them with your team:

1. On the right side of the page, scroll to the Comments section.
2. Click the Arrow next to Comments.
3. Type a brief synopsis of your finds, such as:
4. This is targeting the Finance team.
5. Click the Add Comment button.

> Takeaways:
> So far, TQ has allowed you to identify emails not captured by your email gateway filters, the email address/user targets, and determine that the spearphish attack is a pointed assault on your Financials team.

## Step 4: Digging Deeper

The next step is to send the email attachment to a sandbox for malware analysis. We can then bring that analysis into our investigation:

1. From the Evidence Board, click the attachment file.
2. On the right side of the page, scroll to the Relationships section.
3. Click the arrow next to Events.
4. Click the plus sign next to the Malware Analysis record to add it to the Evidence Board.
5. Click the malware analysis record to view more information in the right panel.
6. Scroll to the Indicators section and review the scores assigned to each indicator. Scores are assigned on a scale of 1 - 10 with 10 being the most critical indicator.
7. Click the plus sign next to each indicator you want to add to the Evidence Board.
8. Click an indicator to view its details.

> The Run Operations button allows you to run processes that provide additional information on an indicator.

9. Click an indicator.
10. Scroll to the Relationships section.
11. Click the arrow next to Malware.

12. Click the plus sign next to the malware name to add it to your Evidence Board.
    This allows you to view any additional relationships between the malware and the other elements of your investigation. In addition, the information panel on the right gives you a description of the malware and other details captured by multiple sources.

Takeaways:
If your users had opened or executed the email attachments on the spearphish emails, TrickBot malware would have been deployed on your network. You now have information on adversaries, attack patterns, and tasks (within your organization) associated with Trickbot.

# Responding to the Attack

Armed with information, you can now begin responding to the spearphish attack by deploying mitigations. ThreatQ allows you to focus on three primary levels of response to attack:

- Direct response.
- Data capture and additional actions/tasks.
- Education and protection moving forward.

## Direct Response - Deploy Signatures

Create a task to deploy signatures to your Intrusion Prevention System (IPS).

1. From the Evidence Board, right-click the malware name.
2. Click the Expand option.
3. Click Signatures to add all the signatures associated with the malware to your Evidence Board.
4. From the Evidence Board, select all of the signatures and right-click on them.
5. Click the New Task option.
   The Add Task window is displayed.
6. Create a task to deploy the signatures to your IPS as a proactive measure to defend against a potential threat.
7. Click the Save button to save the task and add it to your Evidence Board.

## Data Capture and Additional Actions - Attack Patterns

Attack patterns are the techniques used to attack a particular organization. Reviewing the attack patterns associated with TrickBot and adding it to your Evidence Board will give you more information and allow you to formulate a course of action such as deploying user training.

### Review and Add Attack Patterns

1. From the Evidence Board, click the malware name, such as TrickBot.
2. The right-side of the page displays additional information on the malware.
3. Scroll to the Relationships section.
4. Click the arrow next to Attack_Pattern.

5. Review the list for attack patterns similar to your current investigation, such as the spearphishing Attachment attack pattern.
6. Click the plus sign next to this attack pattern to add it to the Evidence Board.

### Select a Course of Action

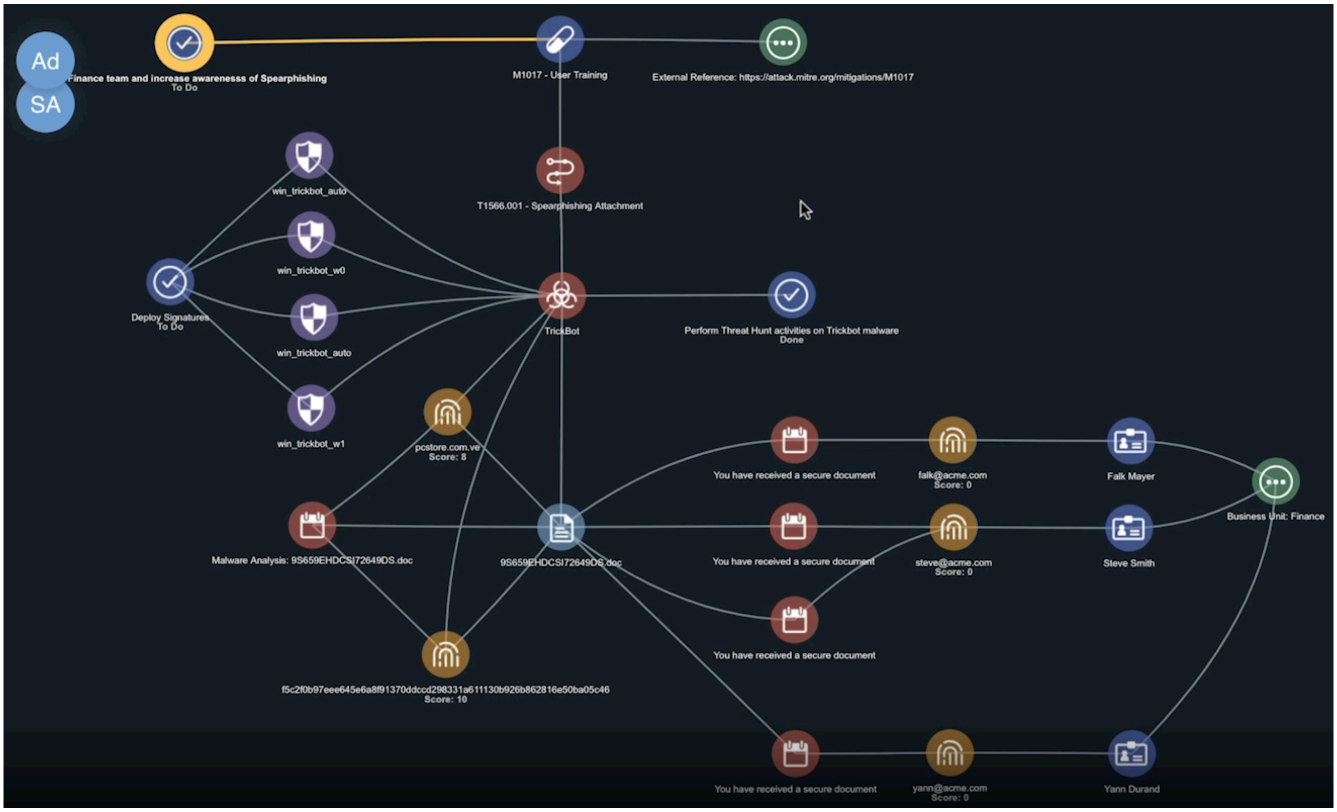
1. From the Evidence Board, click the attack pattern.
2. The right-side of the page, displays additional information on the attack pattern.
3. Scroll to the Relationships section.
4. Click the arrow next to Course_Of_Action.
5. In this case, let select User Training as our course of action by clicking the plus sign next to User Training to add it to the Evidence Board.
6. With User Training still selected, you can also scroll to the Relationships section, click the arrow next to Attributes and add reference material to the Evidence Board by clicking the corresponding plus sign.

### Create a User Training Task

1. From the Evidence Board, right-click User Training.
2. Click the New Task option.
   The Add Task window is displayed.
3. Create a task for training of your Finance team as well as to increase organizational awareness.
4. Click the Save button to save the task and add it to your Evidence Board.

## Wrapping Up the Investigation and Moving Forward

You've used ThreatQ to move from "Yikes!  What is that email?" to a comprehensive assessment of the spearphish attack as well as long and short-term plans to address the threat.  Your customized and expanded Evidence Board is now a hub for tracking the attack as well a reference point for handling future attacks.


Ad
SA
Finance team and increase awarenesss of Spearphishing
To Do
M1017 - User Training
External Reference: https://attack.mitre.org/mitigations/M1017
win_trickbot_auto
T1566.001 - Spearphishing Attachment
win_trickbot_w0
Deploy Signatures
To Do
TrickBot
Perform Threat Hunt activities on Trickbot malware
Done
win_trickbot_auto
win_trickbot_w1
pcstore.com.ve
Score: 8
You have received a secure document
falk@acme.com
Score: 0
Falk Mayer
Business Unit: Finance
Malware Analysis: 9S659EHDCSI72649DS.doc
9S659EHDCSI72649DS.doc
You have received a secure document
steve@acme.com
Score: 0
Steve Smith
You have received a secure document
f5c2f0b97eee645e6a8f91370ddccd298331a611130b926b862816e50ba05c46
Score: 10
You have received a secure document
yann@acme.com
Score: 0
Yann Durand