THREATQUOTIENT™

# How to Map MITRE ATT&CK Techniques:

## Bridging the Gap between Theory and Implementation

*Steve Rivers, Director, Threat Intelligence Engineering*

# Contents

## MITRE ATT&CK and ThreatQ

The MITRE ATT&CK framework contains a tremendous amount of data that can prove valuable in a range of use cases, including spearphishing, threat hunting, incident response, vulnerability management and alert triage. To make the information contained within the MITRE ATT&CK framework actionable for these use cases, ThreatQuotient integrates components of the framework into the ThreatQ platform to provide the following capabilities:

- Enable investigations that originate with components from the MITRE ATT&CK framework, such as techniques.
- Automatically build relationships between MITRE ATT&CK data and other useful pieces of threat data.
- Automatically map threat data from internal sources (e.g., SIEM, ticketing, email gateway) and external sources (e.g., feeds) with MITRE ATT&CK techniques.
- Store historical threat hunting investigations, data and learnings and automatically associate these with related components of the MITRE ATT&CK framework.

The integration enables security operations teams to take full advantage of the framework, while working within the ThreatQ platform, to proactively and collaboratively accelerate detection and response.

> The integration of MITRE ATT&CK enables security operations teams to take full advantage of the framework while working within the ThreatQ platform.

## MITRE ATT&CK Mapping

The MITRE ATT&CK framework is a huge step forward in creating a knowledgebase of adversaries and associated tactics, techniques and procedures (TTPs). Many vendors are starting to build ATT&CK data into their detection tools which is driving adoption globally of the ATT&CK framework for threat hunting and incident response processes. This is great progress, but unfortunately many organizations still have a gap when trying to apply process to technologies that do not integrate with ATT&CK data. ThreatQuotient has created an integration between the ThreatQ platform and MITRE ATT&CK that helps to bridge this gap.

The ThreatQ platform offers a threat-centric approach to security operations. Purpose-built to accelerate detection, investigation and response, the platform is integrated with a large number of key security systems and is aware of contextually relevant detections or alerts that are threat related. This information is ingested directly into the ThreatQ Threat Library. The ThreatQ MITRE Mapper integration offers a tool to automatically establish relationships between MITRE ATT&CK techniques and threat data that has been ingested from internal and external tools. The functionality is powered by Threat Library searches, which enable users to seamlessly leverage data from technologies that do not support ATT&CK directly out of the box.

The remainder of this document uses a threat hunting use case triggered by a spearphishing incident to demonstrate how the ThreatQ MITRE Mapper integration may be used.

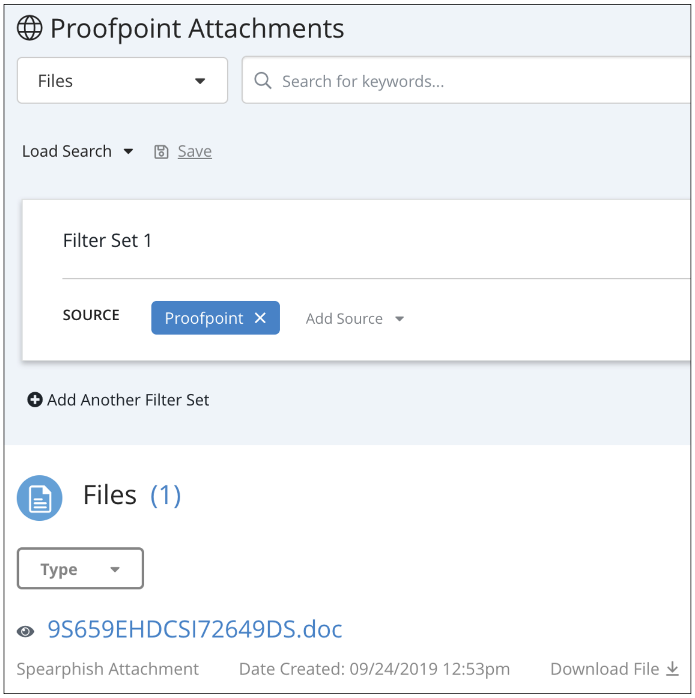
## ThreatQ MITRE Mapper Configuration

This section shows how the integration could be configured using the MITRE ATT&CK technique: T1193 — Spearphishing Attachment.

### Step 1 — Define Mappings

In this step, we determine the type of data that we would like to map to the Spearphishing Attachment technique.

We search for the data that we would like to map to a specific ATT&CK technique and then save the search for use by the MITRE Mapper integration. In Figure 1 we have defined a search that looks for all files that have been sent to us from our Proofpoint system, which is not integrated with the MITRE ATT&CK framework. Crucially, we are only interested in the files and have limited our search to that data.



Proofpoint Attachments

Files

Search for keywords...

Load Search

Save

Filter Set 1

SOURCE: Proofpoint ✕

Add Source

Add Another Filter Set

Files (1)

Type

9S659EHDCSI72649DS.doc

Spearphish Attachment

Date Created: 09/24/2019 12:53pm

Download File

**Figure 1:** Searching for data to map

### Step 2 — Configure the Integration

The integration is configured to map the results from the saved search against the MITRE ATT&CK Spearphishing Attachment technique.

The integration is designed to run on a periodic basis. Each of the saved searches that have been defined will be executed by the integration. The results from each saved search will then be related automatically to their designated MITRE ATT&CK technique. In this example, the integration will map any files that have been sent to ThreatQ by Proofpoint to the record for T1193 — Spearphishing Attachment that exists within the Threat Library.

Once configured, the integration will automatically build any relationships between a designated MITRE ATT&CK technique and the outcome of the saved search every time that it executes. This includes any new data that has arisen.

## A Threat Hunting Example Using MITRE Mapper

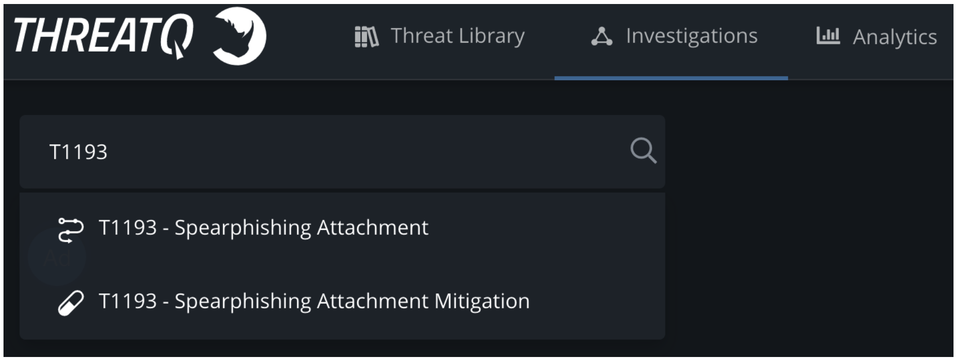
Many users of ATT&CK will build a risk and impact matrix to determine which techniques are most likely to impact their organization.

### Overview

Many users of ATT&CK will build a risk and impact matrix to determine which techniques are most likely to impact their organization. It is common for Threat Hunting teams to then use high risk or high impact ATT&CK techniques as the basis for further investigation. Let's assume that this is the situation now and that a threat hunter is keen to analyze the Spearphishing Attachment technique in more detail.

### Step 1 — Starting the Investigation

A new ThreatQ Investigation is created. The starting point for the investigation then needs to be defined. In this case, we are using the ATT&CK technique: T1193 — Spearphishing Attachment. Figure 2 shows the use of the search feature within ThreatQ Investigations, which is then added to the investigation once clicked.



T1193

T1193 - Spearphishing Attachment

T1193 - Spearphishing Attachment Mitigation

**Figure 2:** Searching the Threat Library for a starting point

## Step 2 — Identifying Interesting Attachments

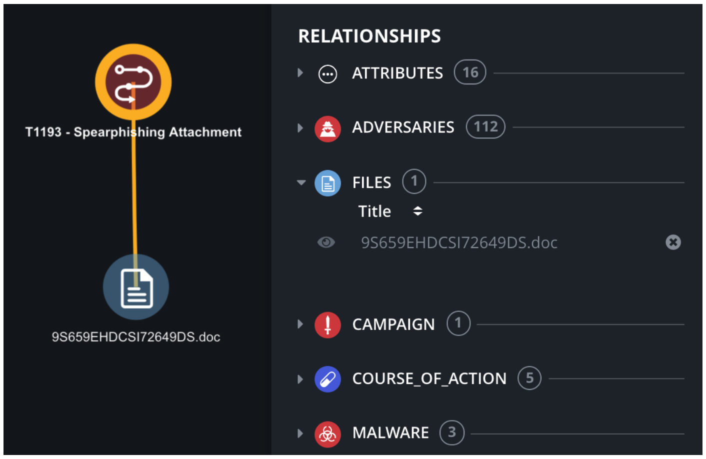


**Figure 3:** Finding related files

Clicking on the Spearphishing Attachment node reveals a set of associated relationships. In this case, there is a large amount as ThreatQ has captured contextually relevant data directly from MITRE and inserted it into the Threat Library. The associated relationships that exist in Files are a great starting point given the type of attack technique that is being investigated. Here we see a single related file. Figure 3 shows the results after this file has been added to the investigation.

## Step 3 — Related Events

The next step is to look for related events that are associated with the file that has been added to the investigation. Relationships are used to identify any associated events and add these and associated contextual data directly into the investigation.

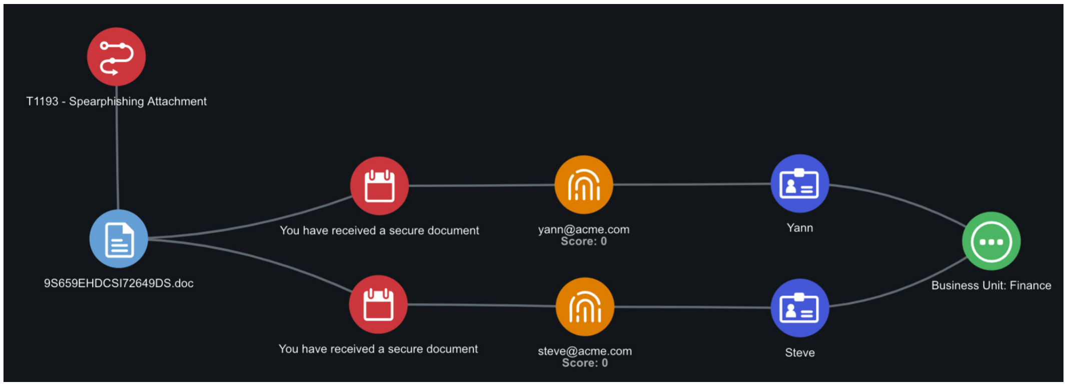

T1193 - Spearphishing Attachment
9S659EHDCSI72649DS.doc
You have received a secure document
yann@acme.com
Score: 0
Yann
You have received a secure document
steve@acme.com
Score: 0
Steve
Business Unit: Finance

**Figure 4:** Additional events

Figure 4 shows the result of this process. In this case, we have identified two separate events tied to this file, which were both forwarded to ThreatQ by another integration. Both events were emails that were sent to two separate recipients. Those recipients have been identified as being associated with the organization's finance department.

## Step 4 — Deeper Analysis

It is clear this file may highlight the existence of a potential threat within the organization and that further analysis may be required. So, the threat hunter chooses to learn a little more about any contextually relevant data that may be associated with the file.

The file is analyzed for any associated indicators that ThreatQ may be aware of. This information is captured from external technologies (such as threat feeds) or internal technologies (such as vulnerability management). Interesting indicators are added to the investigation as per Figure 5.

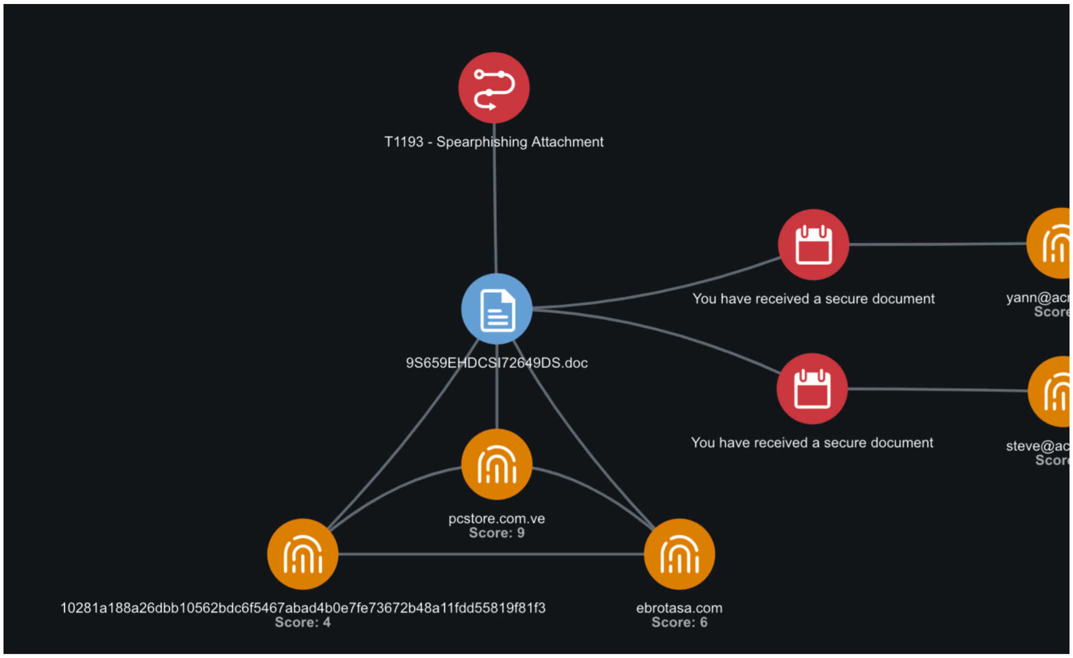
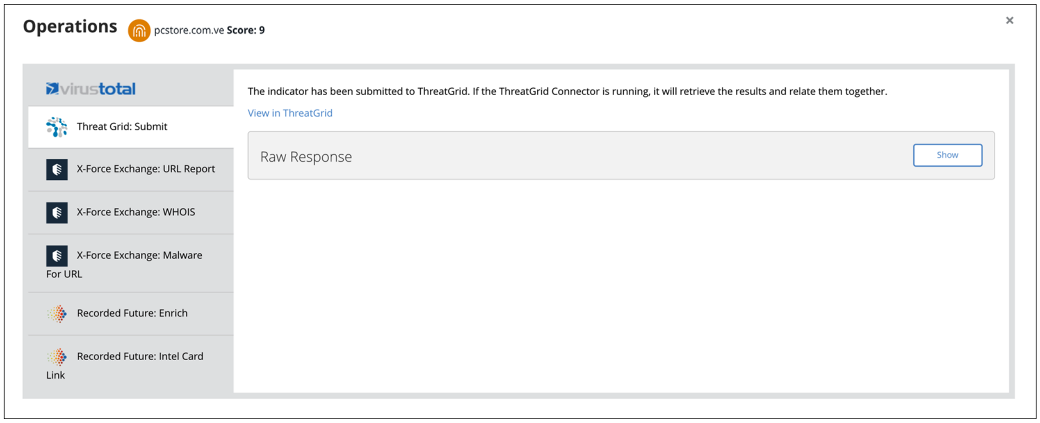

T1193 - Spearphishing Attachment
You have received a secure document
yann@acı
Score
9S659EHDCSI72649DS.doc
You have received a secure document
steve@ac
Score
pcstore.com.ve
Score: 9
10281a188a26dbb10562bdc6f5467abad4b0e7fe73672b48a11fdd55819f81f3
Score: 4
ebrotasa.com
Score: 6

**Figure 5:** Adding context

The threat hunter may also choose to use additional enrichment tools to capture more data about any potential threats. This is accomplished using ThreatQ's Operations feature, which allows users to execute enrichments against specific pieces of data. Figure 6 shows an example of a URL being sent to Cisco ThreatGrid for further analysis. The results will be automatically captured by ThreatQ and made available to further the investigation if required.



The indicator has been submitted to ThreatGrid. If the ThreatGrid Connector is running, it will retrieve the results and relate them together.

**Figure 6:** Submitting a URL for further analysis

Further analysis using MITRE ATT&CK and sandbox data reveals that the attachment has an association with the TrickBot malware. This is also added into the investigation (Figure 7) for further analysis by Incident Response teams at a later stage.

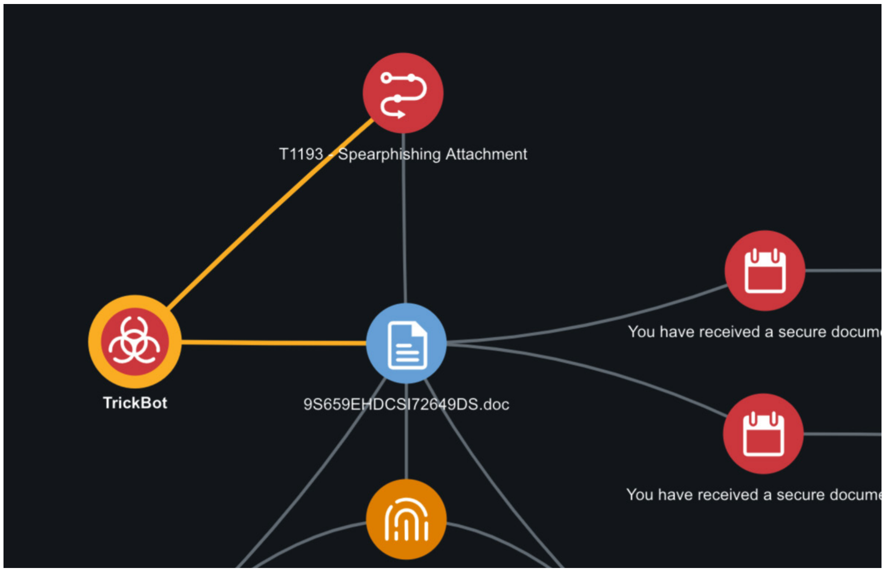

T1193 - Spearphishing Attachment
TrickBot
9S659EHDCSI72649DS.doc
You have received a secure docum
You have received a secure docume

**Figure 7:** Associated TrickBot Malware

There are several additional steps that the threat hunter could choose to undertake at this stage. These include deeper analysis into indicators and associated relationships or looking for TTP-related outcomes such as adversary relationships.

## Step 4 — Mitigation and Response

The final step is to identify mitigation and response actions. Initially, the threat hunter looks for signatures that could be useful in managing any threat from TrickBot. There are several sources for these signatures, but in this case, they have been imported automatically using ThreatQ's Malpedia feed.

In Figure 8 the threat hunter has identified three signatures that may be used to detect TrickBot. Each signature is a complete YARA rule, which may be deployed to an IPS or other network or host-based detection system. A task has been assigned ('Deploy Signature to IPS') to the Security team to deploy the signatures.

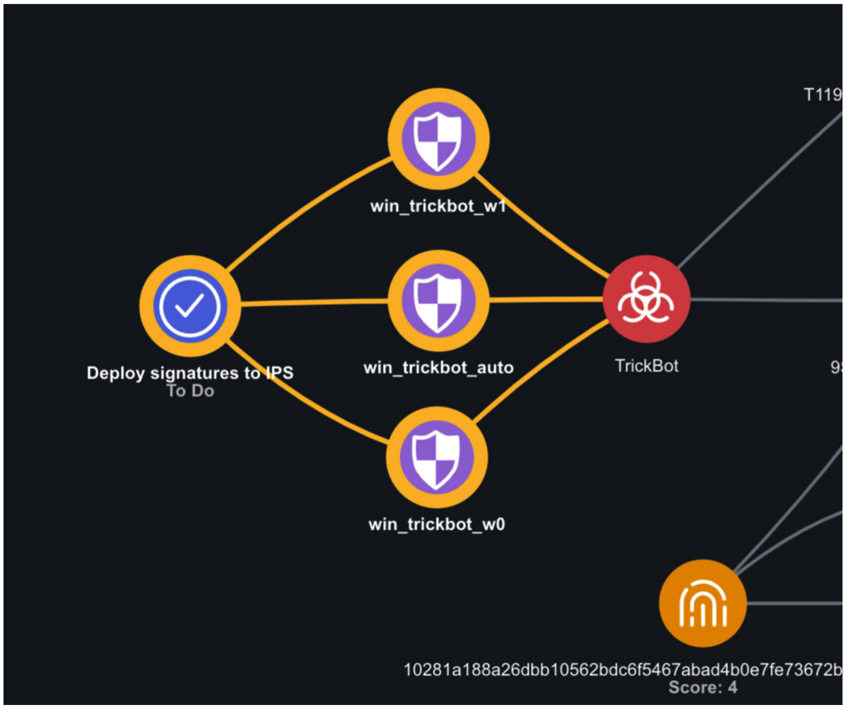


**Figure 8:** Identifying signatures to respond to TrickBot

The Threat Library also contains some information on mitigations that may be deployed to defend against the TrickBot Malware. These are added to the investigation and assigned to the Security team for action (Figure 9).

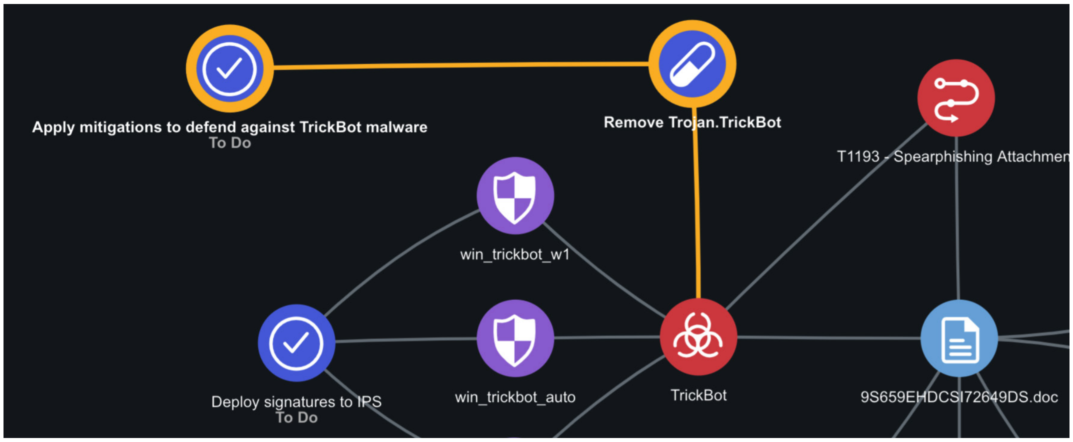


**Figure 9:** Additional mitigations

The investigation has been updated with mitigations and responses to the immediate perceived threat from TrickBot. The final step is to look for longer term steps to help mitigate any additional risks that may be associated with the Spearphishing Attachment technique.

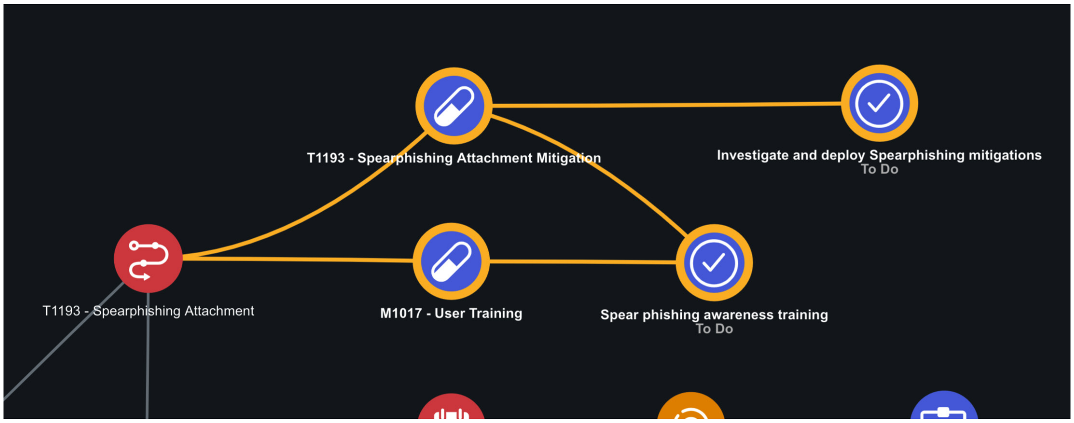

T1193 - Spearphishing Attachment Mitigation
Investigate and deploy Spearphishing mitigations
To Do
T1193 - Spearphishing Attachment
M1017 - User Training
Spear phishing awareness training
To Do

**Figure 10:** Longer term mitigations

The MITRE ATT&CK data that resides within the Threat Library is used to identify a set of mitigations that may be applied to manage the risk associated with the T1193 — Spearphishing Attachment technique. These have been added to the investigation and tasks assigned to the appropriate teams within the organization (Figure 10).

Figure 11 shows the completed investigation.

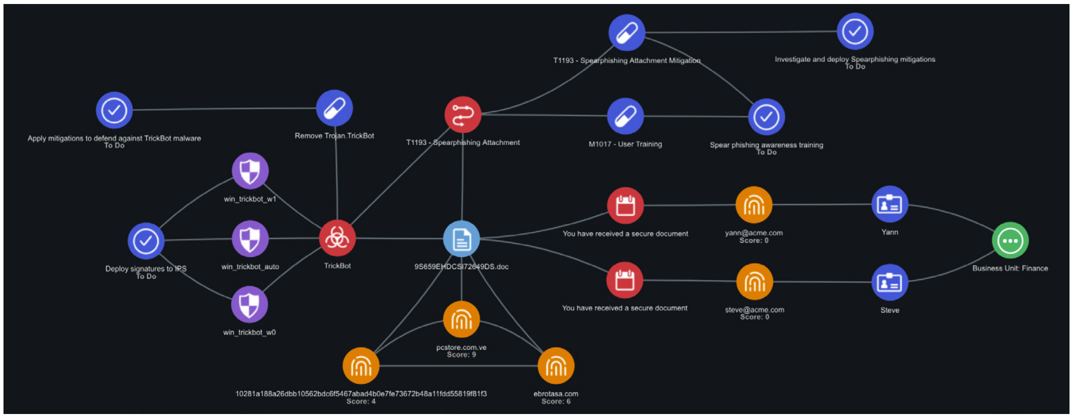

T1193 - Spearphishing Attachment Mitigation
Investigate and deploy Spearphishing mitigations
To Do
Apply mitigations to defend against TrickBot malware
To Do
Remove Trojan.TrickBot
T1193 - Spearphishing Attachment
M1017 - User Training
Spear phishing awareness training
To Do
win_trickbot_w1
You have received a secure document
yann@acme.com
Score: 0
Yann
Deploy signatures to IPS
To Do
win_trickbot_auto
TrickBot
9S659EHDCSI72649DS.doc
Business Unit: Finance
You have received a secure document
steve@acme.com
Score: 0
Steve
win_trickbot_w0
pcstore.com.ve
Score: 9
10281a188a26dbb10562bdc6f5467abad4b0e7fe73672b48a11fdd55819f81f3
Score: 4
ebrotasa.com
Score: 6

**Figure 11:** The completed investigation

## Conclusion

The sample investigation in this paper, started with a MITRE ATT&CK technique but centred around an attachment that originated from a third-party system. This attachment did not originally have a relationship to the Spearphishing Attachment technique from MITRE. Establishing the relationship enabled a threat hunter to utilize the ATT&CK technique as the starting point for a hunt which, in turn, yielded information on a potential active threat and other avenues of investigation.

One of the key advantages of the ThreatQ platform is its open, extensible architecture that allows for strong integration and interoperability with the tools organizations use today.

One of the key advantages of the ThreatQ platform is its open, extensible architecture that allows for strong integration and interoperability with the tools organizations use today, and the tools they may be considering across a broad spectrum of services. The ThreatQ MITRE Mapper allows security teams to use MITRE ATT&CK to its fullest extent, even when their technologies do not support ATT&CK directly out of the box. Users can define searches within the Threat Library and map them to one or many MITRE ATT&CK techniques. The integration automatically builds relationships between the outcome of these searches and the associated techniques over time.

Nearly every organization is interested in using the MITRE ATT&CK framework. The ThreatQ platform can serve as the glue to integrate disparate technologies into a single security architecture, sharing the right intelligence with the right tools at the right time. With ThreatQ, organizations can easily implement the framework and benefit from the significant value it brings to threat hunting and other use cases.