ThreatQuotient

MITRE ATT&CK

Use Case

August 18, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

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

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

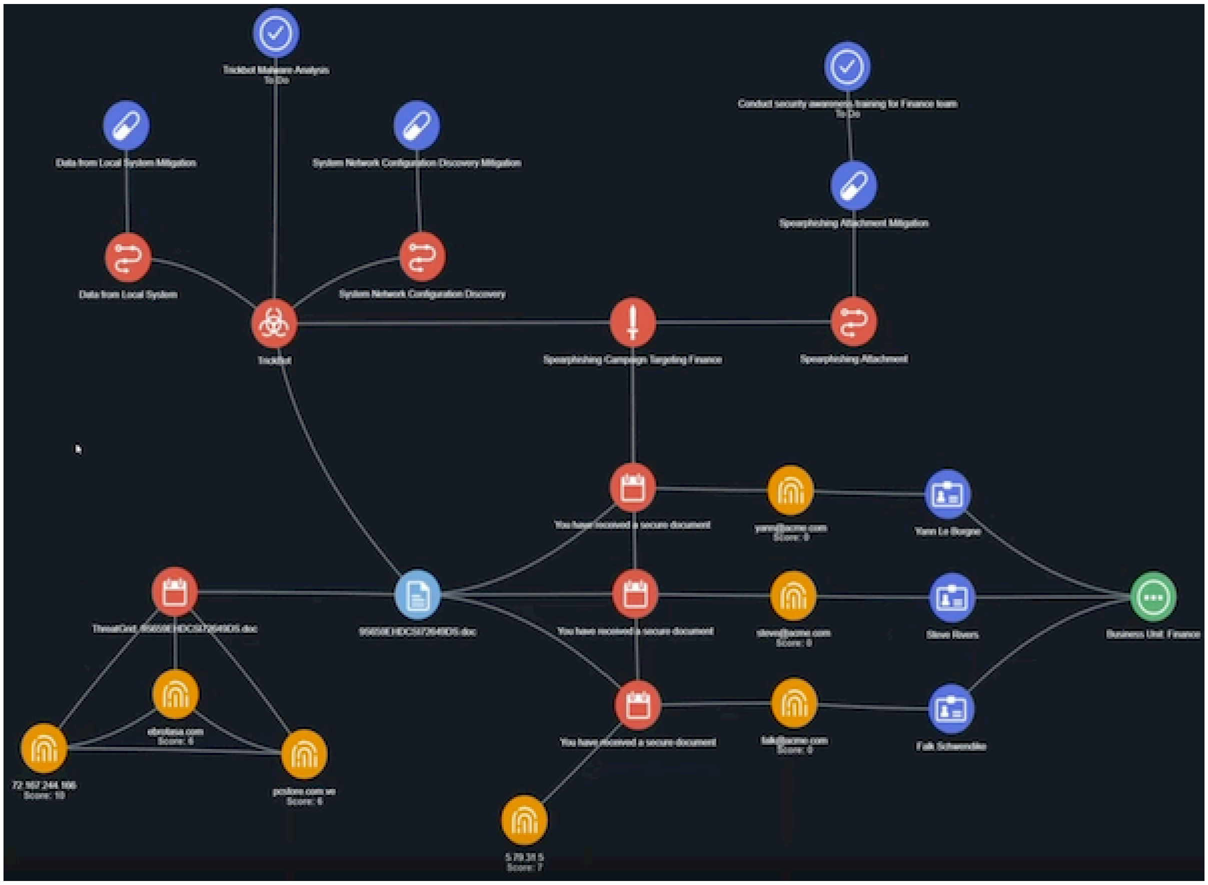
Contents

Use Case - MITRE ATT&CK®

ThreatQ's integration with the MITRE ATT&CK knowledge base of adversary tactics and techniques allows you to add another layer of information to your threat investigations by automating the collection and aggregation of data from MITRE ATT&CK. This use case outlines the steps taken by a company to deepen their knowledge of an attack by leveraging the MITRE ATT&CK feed in ThreatQ to explore the tools and techniques of their adversary.

Backstory

This use case begins after the detection, analysis, and response detailed in the Spearphishing Attack use case. As such, we begin with a fully fleshed-out investigation of a spearphishing attack targeting the Finance department using Trickbot malware.


Trickbot Malware Analysis
To Do
Data from Local System Mitigation
System Network Configuration Discovery Mitigation
Conduct security awareness training for Finance team
To Do
Spearphishing Attachment Mitigation
Data from Local System
System Network Configuration Discovery
Trickbot
Spearphishing Campaign Targeting Finance
Spearphishing Attachment
You have received a secure document
yann@acme.com
Score: 0
Yann Le Borgne
ThreatGrid_95659EHDCSI72649DS.doc
95659EHDCSI72649DS.doc
You have received a secure document
steve@acme.com
Score: 0
Steve Rivers
Business Unit: Finance
ebrofasa.com
Score: 6
72.167.244.106
Score: 10
poslore.com.ve
Score: 6
You have received a secure document
falk@acme.com
Score: 0
Falk Schwendke
5.79.31.5
Score: 7

Pro Tips

- As you add nodes to your investigation, you can drag them to new locations on the screen for easier reference. For instance, you might choose to group your adversary nodes in the upper right corner.

- When you click a node, the right side of the screen displays a scrollable list of information on the node.

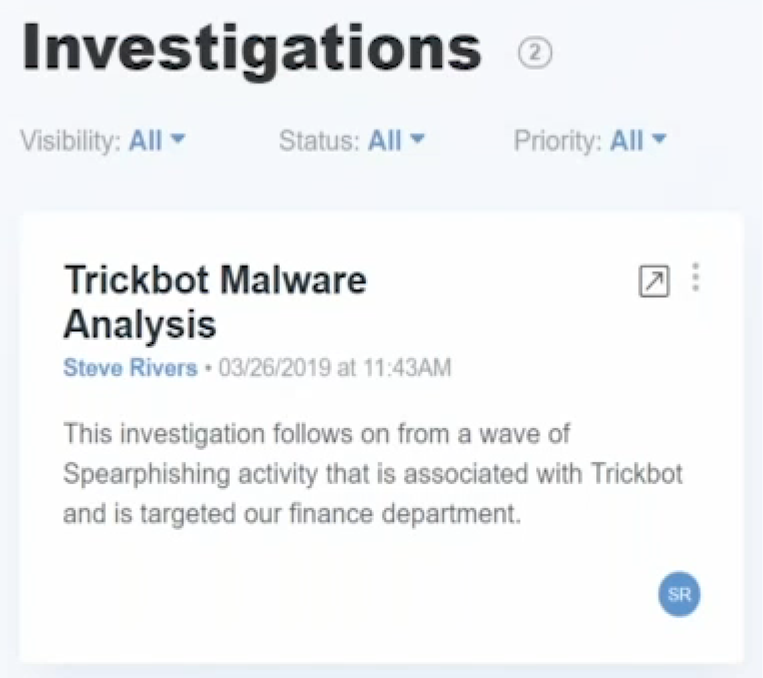
Know Your Adversary - Malware Analysis

One of the tasks created during the spear phishing investigation was to find out more information on the adversary behind the attack.

Digging into the Details

ThreatQ allows you to leverage MITRE ATT&CK as an information reference or to map events to the MITRE ATT&CK framework. Digging into the details on Trickbot provided by MITRE ATT&CK allows us to take advantage of MITRE ATT&CK as a reference.

1. From the Investigations screen, click the Trickbot Malware Analysis task.



Investigations 2

Visibility: All Status: All Priority: All

Trickbot Malware Analysis

Steve Rivers • 03/26/2019 at 11:43AM

This investigation follows on from a wave of Spearphishing activity that is associated with Trickbot and is targeted our finance department.

2. From the evidence board, click the Trickbot icon.
   The right side of the screen displays information on Trickbot derived from the MITRE ATT&CK feed.
3. Click the arrow ↗ next to the investigation name to view more details.
   The details screen lists data on Trickbot received from the MITRE ATT&CK feed.

Expanding Your Investigation

To find out more about instances of Trickbot in our system, we add related events, attachments, and indicators to the evidence board.

Add Events

1. From the evidence board, right-click the Trickbot icon.
2. Click the Expand option.
3. Click the Events option.
4. The evidence board now displays two additional Trickbot events. This highlights additional events involving Falk in the Finance group.

Add Attachments

1. Click one of the new events to view additional information on the right side of the screen.
2. Right-click the new event.
3. Click the Expand option.
4. Click the Attachments option.
5. This adds two new attachments, a .doc and a .pdf, to the evidence board. These attachments were pulled in from Proofpoint.
6. Click an attachment to access the details.

Add Indicators

1. Click one of the new events to view additional information on the right side of the screen.
2. Click the arrow next to the Indicators section to view a list of indicators and their scores.
3. We are looking for an indicator with a high score that indicates it is relevant to our investigation.
4. Click the plus next to the indicator with the high score to add it to the evidence board.
5. Click the indicator to view its details on the right side of the screen.
6. Click the Run Operations button to get more information about the IP.
7. In the Relationships section, click the arrow next to the Events option to expand the list of events.

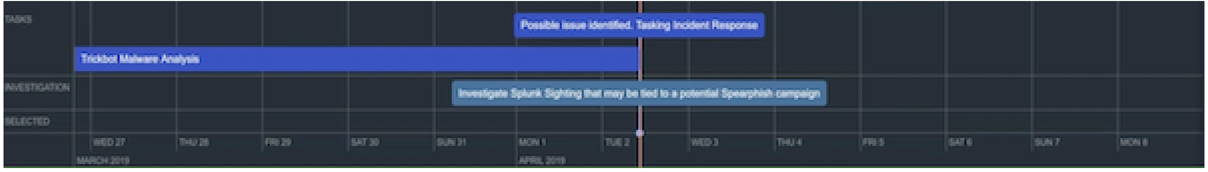
8. Click the plus sign next to an event to add it to the evidence board. In this case, we can add a SIEM Sighting event to the board.

Taking Action

Now, it's time to translate all the data we have gathered into action to ensure that we address the threat and log our activities.

Assign a Task to Your Incident Response Team

1. Right-click the SIEM Sighting event and select the New Task option.
2. Populate the Add Task window with the task details. You will notice that the event and investigation associated with the task are pre-populated.
3. Click the Save button.
4. The new task is added to your evidence board and added to the queue of the Incident Response team.
5. Create a Timeline Entry
6. After you create the SIEM Sighting task, you can highlight the issue further by creating a timeline entry for both the event and the task.
7. Click the arrow in the bottom left corner of the evidence board to view the timeline.
8. Select the SIEM Sighting event and the associated task.
9. Right-click the selected items and select the New timeline entry option.
10. Populate the Add Timeline Entry window.
11. Click the Save button.
12. The investigation timeline now displays an entry for the SIEM Sighting.


TASKS
Possible issue identified. Tasking Incident Response
Trickbot Malware Analysis
INVESTIGATION
Investigate Splunk Sighting that may be tied to a potential Spearphish campaign
SELECTED
WED 27
THU 28
FRI 29
SAT 30
SUN 31
MON 1
TUE 2
WED 3
THU 4
FRI 5
SAT 6
SUN 7
MON 8
MARCH 2019
APRIL 2019

Add a Campaign to the Investigation

1. Click the Create button and select the Campaign option.
2. From the Add Campaign window, click the Add Campaign button.
3. Populate the second Add Campaign window with the details of the newly identified Trickbot incursion.

4. Click the Add Campaign button to save the new campaign.
   Now that you have created the new campaign, you need to add it to the evidence board.
5. Click the magnifying glass icon in the upper left corner.
6. Enter the campaign name in the search field.
7. Click the magnifying glass icon 🔍 to begin the search.
8. Select your campaign from the drop down results list.
   The system returns a message confirming the addition of the campaign to your evidence board.
9. You can then link the new campaign to Trickbot events by right-clicking the event, selecting the link option, and then clicking the campaign icon to establish the link. The evidence board displays a line connecting the campaign and the linked events.

Alert the Targets

Create a new task to alert the Finance team about the Trickbot threat.

1. Right-click the new Trickbot campaign icon.
2. Click the New task option.
3. Populate the Add Task window.
4. Click the Save button.

Update Your Investigation

Adding the Trickbot task and events you created/identified to the investigation allows you to share your analysis with others within your team and organization. To do this, select all the new information points (tasks and events) you created, right-click, and select the **Commit to Investigation** option.

Leverage MITRE ATT&CK

At this stage you are ready to pull in more information from MITRE ATT&CK on the spear phishing attachment sent to your Finance team. This information gives you a more complete picture of potential adversaries associated with this type of attack and the techniques they use.

Add Information on the Spear Phishing Attachment

1. Click the magnifying glass icon 🔍 in the upper left corner of the Investigations screen.
2. Enter Spear Phishing Attachment.
3. Click the Spear Phishing Attachment entry to add it to your investigation.
4. Click the new Spear Phishing Attachment node to view a full description of the attack type as well as a list of adversaries, attributes, and courses of action.
5. Link the Spear Phishing Attachment node to other elements in your investigation, such as the new campaign and the Trickbot malware.
6. Click the Spear Phishing Attachment node.
7. Right-click the node you want to link to, such as Trickbot and select the Link option.

Add Techniques and Adversaries

At this point we are ready to pull in MITRE ATT&CK resources that provide insight into techniques and adversary associations.

1. Click the Trickbot node.
2. From the details pane, expand the Attack_Pattern section.
3. Click the plus sign next to each attack pattern you want to add to the investigation.
   In this case, let's focus on attack patterns that center on user account discovery and data from the local system.
4. Click the Account Discovery node.
5. From the details pane, expand the Relationships section.
6. Click the plus sign next to each attribute you want to add to the investigation In this case, let's add the MITRE ATT&CK reference and technique ID for the Account Discovery technique.

Select Mitigation Strategies

The next MITRE ATT&CK asset we want to reference is the recommended actions to mitigate the risks/damage associated with this type of attack.

1. Click the Account Discovery node.
2. Expand the Course_Of_Action section.
3. Click the plus sign next to the mitigation to add it to the investigation.

4. Click the Account Discover Mitigation node and review the details displayed in the action panel on the right side of the screen. In this case, the recommended mitigation is to disable various information through GPO.
5. Right-click the Account Discovery node and select the New Task option to create a task to deploy the GPO mitigation.
   The Add Task window is displayed.
6. Populate the Add Task window with task details and the person assigned to complete the task.
7. Click the Save button.
8. At this point, take a moment to add these techniques, adversaries, and mitigations to the investigation by selecting each, right-clicking, and selecting the **Commit to Investigation** option.
9. Click the Trickbot Malware Analysis node.
10. From the action panel, expand the Comments section.
11. Click the Add a Comment link to add an update on your activities.
12. Click the Add Comment button to save your entry.

Review Your Data - Identifying Key Adversaries

Now that we have leveraged MITRE ATT&CK to gain a deeper understanding of the attack techniques, we need to take a closer look at adversaries. The idea is to narrow down the scope of our investigation to adversaries that pose a particular threat to our organization.

1. Right-click the Data from Local System nodes and select Expand.
2. Click the Adversaries option.
3. Review the evidence board to identify adversaries with relationships to the primary techniques applied in the attack.
4. After you identify your key adversaries, select the remaining adversaries, right-click, and select the Remove option.
   This de-clutters the evidence board so that you can focus on key adversaries.

Run MITRE ATT&CK Tools

Now that we know which adversaries we want to focus on, we can run MITRE ATT&CK tools to look up each adversary and determine if they tend to focus on organizations similar to ours.

1. From the evidence board, click an adversary node.
2. From the action panel, click Expand the Operation section.

3. Click the Run Operations button to access the Operations screen.
4. From the Operations window, click the **ATT&CK Tools: Lookup Adversary** option.
   This generates the MITRE ATT&CK Overview which includes the following sections:
   - **Description** - Provides information on the adversary’s probable country of origin and the organizations they tend to attack.
   - **Aliases** - If an adversary’s alias exists in ThreatQ, you can click the link to view the adversary’s information within ThreatQ.
   - **Associated Techniques** - Lists techniques associated with the adversary and provides a link to the MITRE ATT&CK page for each technique. Also, provides information on how the adversary uses the technique.
   - **External References** - List references to the adversary on sites other than MITRE ATT&CK as well as links to the referenced pages. Gives you the option to pull information on related indicators from associated techniques.
5. Be sure to add a Comment about your findings to the investigation and create a task to do additional research on any adversary you identified as a significant threat.
6. To add the new adversary research task and the primary adversary nodes to your investigation, select them in the evidence board, right-click, and select the **Commit to Investigation** option.

Wrap Up and Close Your Investigation

To wrap up our investigation, we need to revisit the original Trickbot Malware Analysis task and complete the following steps:

- Review the information we added to the task.
- Add a closing comment.
- Set the task to Done status.
- Generate a PDF.

Review Task Updates

1. From the Investigations screen, click the Trickbot Malware Analysis task.
   The right side of the screen displays the task summary.
2. Click the arrow button ↗ next to the task name to expand the task.
3. Review the data you have gathered and added to the investigation by clicking the report name in the Name column.

Add a Closing Comment

1. Expand the Comments section.
2. Click the + Add Comment option.
3. Enter a summary of your findings and recommendations.
4. Click the Add Comment button.

Set the Task to Done

1. Click the arrow next to the current task status.
2. Select Done.
   This updates ThreatQ as well as any linked third-party tool, such as your ticketing system.

Generate a PDF

1. Expand the Related Objects section.
2. Click the task report.
3. Click the expand icon ↗ in the upper right corner to view a full-screen version of the report.
4. Click the Actions button.
5. Select the Generate PDF option. You can share this PDF with others in your organization and/or store it for future reference.