Threat Emulation videos and exercises

Objectives:

1. What is threat emulation and why is it needed?

2. Explaining threat emulation and some basics on threat intelligence and how the two work together.

3. You will learn about the Mitre Att&ck framework and you'll have some labs to complete to learn how to use it for your organizational needs.

4. Walk through a threat intelligence report and learn to interpret it to create a threat emulation plan.

5. Create a threat emulation plan based on the threat intelligence report.

6. Perform the threat emulation exercise.

7. Learn to evaluate your current detection mechanisms to determine if those can detect or mitigate attacks that target your specific organization.

# Part I

Introduction to Threat Emulation

<https://watch.screencastify.com/v/wzyiGfzl7jhpVHj6vwGc>

# Part II

1. <https://watch.screencastify.com/v/XLReoYzbwt9wbx5gJHDi>
2. <https://drive.google.com/file/d/1OZN8r4e-bYpxMDkx6oemutyaSS7itMAK/view?usp=sharing>

This week is about the Mitre Att&ck navigator and creating heatmaps. Please let me know if you have any questions. There is an assignment I want you to create a heatmap based on the capabilities of a software program and threat group. Please send me your heatmap and I'll provide some comments back on it and I'll send you my heatmap for comparison, as well.

1. This Github repo has the description of a backdoor program called Jaded Wraith:

<https://github.com/phath0m/JadedWraith>

Map its capabilities to Mitre Att&ck: <https://mitre-attack.github.io/attack-navigator/>

2. Here are some commands from APT34. Create a heatmap based on what these commands are performing:

shell laZagne.exe browsers [-f]

python2 laZagne.py all

grep -ri password /

findstr /si pass \*.xml | \*.doc | \*.txt | \*.xls

ls -R | select-string -Pattern password

type C:\Windows\Panther\unattend.xml > nul 2>&1

type C:\Windows\Panther\Unattend\unattend.xml > nul 2>&1

Download the heatmaps as a json file and send it to me and I'll provide you feedback.

Links from Video:

<https://attack.mitre.org/>

<https://mitre-attack.github.io/attack-navigator/>

<https://www.varonis.com/blog/cryptolocker/>

<https://www.netsurion.com/catches/mitre-attack-enriches-ransomware-detection>

In this video, I discuss some basics of the Threat Emulation Plan, going through a report to plan out the emulation exercise for next week, and a quick intro to Caldera Mitre, the threat emulation program we'll use next week.

<https://watch.screencastify.com/v/vdah0p58pZjRJnT26yLH>

Here is the threat intell report from the video:

[https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020](https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-003.pdf)

If you want to get started on Caldera, here is the link:

<https://github.com/mitre/caldera>

# Part III

Below are the video labs for this workshop. Please complete each one which will prepare you for running the Full Threat Emulation exercise. Please ask questions or let me know if you need assistance with during the process of running any steps.

Testing Windows Connection:

<https://watch.screencastify.com/v/Vbjsr5aUL0i79LutVuoB>

<https://youtu.be/vBwvuf5D01M>

Deploy First Agent:

<https://watch.screencastify.com/v/Izd7K0yGYuvCCFtpVpCh>

<https://youtu.be/kzK_18pR4Pw>

Reviewing the Windows System before the emulation: <https://watch.screencastify.com/v/zgIck3gAqjdMVxtzQ6qB>

<https://youtu.be/gf4EZb11akI>

Testing Custom Legal Warning Banner:

<https://watch.screencastify.com/v/AdQAXuKbN5imTJeefwX1>

<https://youtu.be/kxCBuXF5-Bc>

Create Legal Warning Banner Ability:

<https://watch.screencastify.com/v/A8aRqfYG2bP2aRDkIy9a>

<https://youtu.be/i0OWLgbYc00>

Create Adversary Profile:

<https://watch.screencastify.com/v/NzbQiO4bFqw2F6vQQrHj>

<https://youtu.be/djo__Zv-pLw>

Create Legal Warning Operation:

<https://watch.screencastify.com/v/xffQL7NSk4RovFnUTFkC>

Test File Association for README that the ransom creates:

<https://watch.screencastify.com/v/YpnMLpJrRaRIp5OUq2i1>

<https://youtu.be/HxmGM-f1jXk>

Create File Association README Ability (You are going to run your own Operation with this):  
<https://watch.screencastify.com/v/hk99mpqJkcKPxvORXASP>

<https://youtu.be/6AxKdVFh5Qo>

Testing the Ransomware Simulation on your own

<https://watch.screencastify.com/v/EsCvDq96a52Ue6hzTNrx>

<https://youtu.be/lT-ZCpw4XGQ>

Running the ‘Full’ Threat Operation:

<https://watch.screencastify.com/v/DWHfTDyNCPaa4vCg4bjJ>

<https://youtu.be/tCRV1RIXr7k>

Wrap Up:

<https://watch.screencastify.com/v/5WB5IW05pymwTbhAwv2g>

<https://youtu.be/qKuszwShb3A>

Here are the sample documents I copied to the Windows system for the user to test with too:

<https://drive.google.com/file/d/1oMqttsBOqNP1Rb1q9i41YeChnUKCP827/view?usp=sharing>

Here is the content of the file they were copying and pasting from:

1. Commands to run on Windows to see current settings.

-Open a Powershell prompt.

--View Documents for ransomware test:

dir -Recurse c:\Users\ddunston\Documents

-- View current restore points:

Get-ComputerRestorePoint

2. Setting Legal Warning abilities Text (Note that the commands are separated by a semicolon in order to run multiple commands):

Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "legalnoticetext" -Value "Information is on the Desktop to get your data. We are looking forward to working together." ; Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "legalnoticecaption" -Value "YOUR DATA IS ENCRYPTED !"

3. Creating README.READ on the Desktop and changing file association abilitiy (Note the commands are separated by double ampersands to run multiple commands):

echo Your data is encrypted. Contact us to get your data back! > Desktop\README.READ && assoc .READ=txtfile

4. Simulate Ransomware ability text:

get-childitem C:\Users\ddunston\Documents -Filter "\*docx\*" -Recurse | rename-item -NewName {$\_.name -replace 'docx','pysa' }