

# Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

## Lecture 10

### Storing and Analyzing ATT&CK Mapped Data

So in today's class as we discussed in the last class that will be discussing storing and analyzing attack map data. Means whatever TTP we extracted, how we are going to analyze that further. So the community, the threat intel community is still figuring this out. There is no single way of storing and analyzing for everyone, which can satisfy the requirements of each and everything, such as humans or machines. For humans, they may have different requirements, and the machine may have different requirements, such as a human needs a human-readable format, such as written in English or natural language. Our machine needs to have a machine-readable format, such as JSON.



### Considerations When Storing ATT&CK-Mapped Intel

- **Who's consuming it?**
  - Human or machine?
  - Requirements?
- **How will you provide context?**
  - Include full text?
- **How detailed will it be?**
  - Just a Technique, or a Procedure?
  - How will you capture that detail? (Free text?)
- **How will you link it to other intel?**
  - Incident, group, campaign, indicator...
- **How will you import and export data?**
  - Format?

**The community is still figuring this out!**



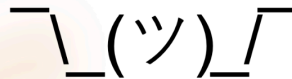
©2019 The MITRE Corporation. ALL RIGHTS RESERVED Approved for public release. Distribution unlimited 19-01075-15.

Also there is, if you are sharing the intel that TTPs with the community, either human or machine, how are you gonna give the context? Like why are you saying that these TTP attackers have been employed in the victim infrastructure? So that is a big question. Then how detailed do you have to explain the TTPs? These things we discussed in the last class. So whether we want to adjust for the technical label details or the procedure label details. Also, there will be multiple intels of the past attacks and the current attacks.

So how you are going to correlate them and connect with the other intel that we have in the community based on things like the incidents which happened in the past, the APT groups which have already been known or the campaigns, APT campaigns and other indicators. Figure out if somehow we figure all these things out, then there is still a question regarding how we are going to import and export this intelligence with the machines or the tools which we have in the victim infrastructure for defensive purposes. So to list out or to save the data, the first step which we all follow and which is universal is the Excel. To list out the information, to store the information, which even the attack navigator started with, firstly it started on the Excel itself only. Now later on they created their own version by improving again and again.



## Ways to Store and Display ATT&CK- Mapped Intel



**Scheduled Task**

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically requires being a member of the Administrators group on the the remote system.<sup>[1]</sup>

An adversary may use task scheduling to execute programs with startup or on a scheduled basis for persistence, to conduct process execution, as part of Lateral Movement, to gain SYSTEM privileges, or to execute processes in the context of a specified account.

**Contents [hide]**

- 1 Examples
- 2 Mitigation
- 3 Detection
- 4 References

**Examples**

• APT18 actors used the native Windows task scheduler tool to use scheduled

Scheduled Task	
<b>ID</b>	T1003
<b>Technique</b>	Execution, Persistence, Privilege Escalation
<b>Platform</b>	Windows
<b>Permissions</b>	User, Administrator, SYSTEM
<b>Required</b>	
<b>Effective</b>	User, Administrator, SYSTEM
<b>Permissions</b>	
<b>Data</b>	File monitoring, Process command-line parameters, Process monitoring, Windows event logs
<b>Sources</b>	
<b>Supports</b>	Yes
<b>Recurse</b>	
<b>CAPEC ID</b>	CAPEC-657/6
<b>Contributors</b>	Tiana Smith, Trupin, Luc Lodeve, Shiroobek, Ashwani Homeoool, Innoova Security

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.

Also there is an open source threat intel platform named MISP. which allows organizations to share threat intel data. So here, if an organization gets attacked, once they understand the intelligence related to the attackers, like they extracted the TTPs and the other attack patterns and indicators, they share this information on this open source platform where multiple organizations of the same community have also joined. So it's kind of social media for sharing the threat intel. Okay, so one if there is a company of a nuclear power plant and there is some other company of the same domain that has got attacked by an APT group, then if that attack company has uploaded the threat interrelated to the attack such as here you have listed a sample.

# Ways to Store and Display ATT&CK-Mapped Intel



Tags	tip:white x Unstructured x osint:source-type="technical-report" x dnc:malware-type="CoinMiner" x
Date	2018-11-13
Threat Level	Undefined
Analysis	Completed
Distribution	All communities
Info	OSINT: WebCobra Malware Uses Victims' Computers to Mine Cryptocurrency
Published	Yes (2019-01-26 14:09:07)
#Attributes	44
First recorded change	2018-11-13 16:10:27
Last change	2018-11-13 16:10:27
Modification map	
Sightings	0 (0)

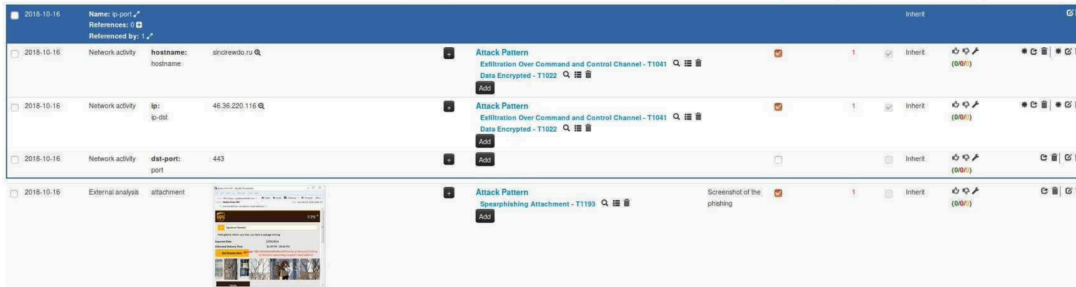


Courtesy of Alexandre Dulaunoy

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.

So, the other company can be aware of the arising attacks and they can implement their mitigation and the defense mechanism accordingly. So, in the MISP they have what is the galaxy where they list tools which have been used in the attack and the attack pattern in terms of TTPs. So, what all attack patterns have been seen in the attack. Also, it allows you to add a snapshot or the images. This is helpful in the case when any spear phishing attack happens.

# Ways to Store and Display ATT&CK-Mapped Intel



Name	References	Referenced by	Incident
2018-10-16	ip:port		
2018-10-16	Network activity	hostname: alibabacloud.ru, ip:dist: 45.95.220.110	Attack Pattern: Exfiltration Over Command and Control Channel - T1041, Data Encrypted - T1022
2018-10-16	Network activity	ip:dist: 45.95.220.110	Attack Pattern: Exfiltration Over Command and Control Channel - T1041, Data Encrypted - T1022
2018-10-16	Network activity	dst-port: 443	Attack Pattern: Exfiltration Over Command and Control Channel - T1041
2018-10-18	External analysis	attachment: screenshot of the phishing	Attack Pattern: Spearphishing Attachment - T1193

**Ability to link to indicators and files**



Courtesy of Alexandre Dulaunoy

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.

So, they can add it to make a more informed post for the other organization. Also, MISP allows to link two incidents and they allow to link and perform analysis about commonality and differences between two attack incidents uploaded on the MISP. And

there are many security firms. One is named as anomaly. They list out the threat analysis reports and in the reports they, as we discussed in the last class, list out the techniques or TTPs extracted at the end of the report. Similarly McAfee also lists out the reports along with TTPs and their procedure level details at the end of their threat analysis report. We'll see several examples of such security firms, CrowdStrike, they add this list, technique list, like techniques observed in the beginning of their report, which one can see and understand the whole attack flow.



## Ways to Express and Store ATT&CK-Mapped Intel



ANOMALI

**Sophisticated New Phishing Campaign Targets the C-Suite** (February 5, 2019)

A new phishing campaign attempting to steal login credentials has been observed to be specifically targeting C-levels and executives in organisations, according to researchers from GreatHorn. ...

[Click here for Anomali recommendation](#)

**MITRE ATT&CK:** [MITRE ATT&CK] Spearphishing Link (T1192) | [MITRE ATT&CK] Trusted Relationship (T1199)

### Techniques at the end of a report

<https://www.anomali.com/blog/weekly-threat-briefing-google-spots-attacks-exploiting-ios-zero-day-flaws>

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.



## Ways to Express and Store ATT&CK-Mapped Intel



### Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide

#### Techniques at the end of a report

MITRE ATT&CK techniques

- Exfiltration over control server channel: data is exfiltrated over the control server channel using a custom protocol
- Commonly used port: the attackers used common ports such as port 443 for control server communications
- Service execution: registers the implant as a service on the victim's machine
- Automated collection: the implant automatically collects data about the victim and sends it to the control server
- Data from local system: local system is discovered and data is gathered
- Process discovery: implants can list processes running on the system
- System time discovery: part of the data reconnaissance method, the system time is also sent to the control server
- File deletion: malware can wipe files indicated by the attacker

<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/>

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.



# Ways to Express and Store ATT&CK-Mapped Intel



## Growing Tensions Between U.S., DPRK Coincide with Higher Rate of CHOLLIMA Activity

### Techniques Observed

- Persistence: New Service
- Defense Evasion: Masquerading
- Discovery: System Information Discovery, System Network Configuration Discovery, File and Directory Discovery
- Command and Control

## CROWDSTRIKE

Consistent with reporting trends across the community, OverWatch saw an increase in threat activity attributed to North Korea in 2017. For example, in mid-May, STARDUST CHOLLIMA actors exploited a web-facing SMB server belonging to a high-profile research institution located in the U.S. They leveraged access to install the following malicious DLL:

## Techniques at the beginning of a report

<https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/>

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.



# Ways to Express and Store ATT&CK-Mapped Intel



## digital shadows \_

## Mitre ATT&CK™ and the Mueller GRU Indictment: Lessons for Organizations

## Adding additional info to an ATT&CK technique

MITRE ATT&CK Stage	GRU Tactics, Techniques and Procedures	Mitigation Advice
 <p>1. Initial Access</p>	<p>Trusted Relationship</p>	<ul style="list-style-type: none"> <li>• 3rd parties, such as suppliers and partner organizations, typically have privileged access via a trusted relationship into certain environments.</li> <li>• These relationships can be abused by attackers to subvert security controls and gain unauthorized access into target environments.</li> <li>• Managing trusted relationships, like supply chains, is an incredibly complex topic. The NCSC (National Cyber Security Center) has an excellent overview of this challenging topic.</li> </ul>

<https://www.digitalshadows.com/blog-and-research/mitre-attck-and-the-mueller-gru-indictment-lessons-for-organizations/>

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.

There is one more security firm, Digital Shadow, who gives the tactics and their TTPs, like trusted relationships, and along with that mitigation advice, which one organization can leverage to apply mitigation methods on their organization. So for this trusted relationship TTP, they have given three different mitigations. So all these things are being done to share the threat intelligence detail, the attack data and the information related to the attack. So there is a recorded future who gives us this wonderful timeline based on the APT groups when they were active and what exactly they were doing in that active period. So there is unit 42, so till now whatever this threat information sharing we saw is

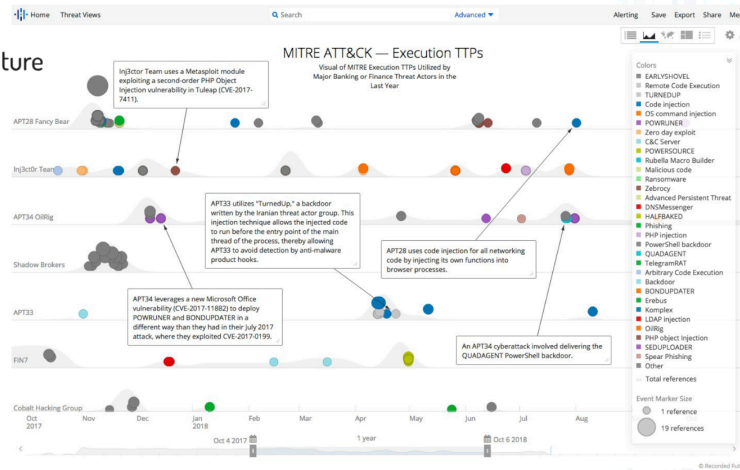
in natural language, so human readable.



## Ways to Express and Store ATT&CK-Mapped Intel



Recorded Future



With timestamps


<https://www.recordedfuture.com/mitre-attack-framework/>

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.



## Ways to Express and Store ATT&CK-Mapped Intel





### PLAYBOOK VIEWER

**Machine readable**

Description	Indicator Pattern
<p><b>Technique:</b> T1064: Scripting</p> <p>Sysget writes a batch script in the %TEMP% folder to clean up the original files and spawning a newly written winlogon.exe executable.</p>	<pre>[process:command_line = 'echo off ;t timeout 1 for /f %*i in (\tasklist /FI "IMAGENAME eq [original_executable_name]" ^) find /v /c ""\') do set YO=%*i if %YO%==4 goto :t del /F "[original_executable_path]" del /F "[tmp_file]" start /B cmd /c "[startup_winlogon.exe]" del /F "[self]" exit']</pre>

### Linking techniques to indicators

Description	Indicator Pattern
<p><b>Technique:</b> T1071: Standard Application Layer Protocol</p> <p>C2 server communicates over HTTP and embeds data within the Cookie HTTP header.</p>	<pre>[domain-name:value = '2014.zzux.com']</pre>

[https://pan-unit42.github.io/playbook\\_viewer/](https://pan-unit42.github.io/playbook_viewer/)

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.

And now unit 48 gives in a format of this, with the name of indicator pattern, which they show as a machine readable like a domain name having some value equal to this. Similarly to the command line process, there is some process in which the command line has been used and this is the command. So, in some structure format they provide the information so that it can be processed easily further.



# Ways to Express and Store ATT&CK-Mapped Intel



Component Object Model Hijacking	APT28 has used COM hijacking for persistence by replacing the legitimate <code>MMDeviceEnumerator</code> object with a payload. <sup>[14]</sup>
----------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------

<https://attack.mitre.org/groups/G0007/>

## What else could we do?

### Full-Text Report

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in the victim's network in the event of

<https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/>

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.

### ATT&CK Technique

Credential Dumping (T1003)

Similarly, this is the example which you already discussed like MITRE ATT&CK list out the techniques and their corresponding procedure level details and how we map TTPs from the full text report is like in this sentence represents that attackers have used Mimikatz to dump credential and use Kerberos golden tickets for authentication and this sentence while reading is going to map to a technique which is named as credential dumping. So to understand the, to get the idea of techniques, you need to go through the ATT&CK matrix techniques details, like their details is available on their website, and the different examples in terms of procedure, so that after reading about the techniques, you can, and after that reading the sentences, you can connect the techniques and the sentences in a better way.

# APT28 Techniques\*



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
File Compression	Apple origi	bash profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Recovery	Apple origi	Audio Capture	Automated exfiltration	Commonly used on
File Compressio	Apple origi	bash profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Recovery	Apple origi	Audio Capture	Automated exfiltration	Commonly used on
File Compression	Apple origi	bash profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Recovery	Apple origi	Audio Capture	Automated exfiltration	Commonly used on

**\*from open source reporting we've mapped**

So this is a glimpse, this is a very old version of ATT&CK Navigator, so in which this yellow highlighted, TTPs are techniques used by APT28 which have been mapped by using open source threat intel reports.

# APT29 Techniques



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
File Compression	Apple origi	bash profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Recovery	Apple origi	Audio Capture	Automated exfiltration	Commonly used on
File Compression	Apple origi	bash profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Recovery	Apple origi	Audio Capture	Automated exfiltration	Commonly used on
File Compression	Apple origi	bash profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Recovery	Apple origi	Audio Capture	Automated exfiltration	Commonly used on

So this is another example of APT29 where blue marked TTPs have been used by the APT29 group. It is again mapped using the threat intel reports. Now, if one had these two APT28, APT29 details in a MITRE ATT&CK navigator form, they can merge both and see what all the common techniques these both groups employ and what are the distinguished techniques they have. So you can see yellow represents the APT28 group,



blue represents APT29 group and the green technique represents the common techniques between both APT groups.



## Comparing APT28 and APT29



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Apple Compromise	Apple exploit	Dark profile and beacons	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Recovery	Apple exploit	Android Capture	Advanced Attribution	Command and Control
Apple iMessage	Apple exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control
Browser Exploitation	Browser exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control
Cloud Service Exploitation	Cloud Service exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control
Hardware Exploitation	Hardware exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control
Mobile Device Exploitation	Mobile Device exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control
Network Exploitation	Network exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control
Service Exploitation	Service exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control
Supply Chain Compromise	Supply Chain exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control
Trusted Relationship	Trusted Relationship exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control
Web Application	Web Application exploit	Accessibility features	Accessibility features	Accessibility features	Account Recovery	Account Recovery	Apple exploit	Automated Collection	Automated Attribution	Command and Control

Overlay known gaps

APT28

APT29

Both groups

So, once you understand this an organization can use this information to see how robust their defensive mechanism is against these APT groups, these APT groups attack methods. Assume our organization sees these three methods, for these three methods our organization, these five sorry, these five methods our organization is lacking, there is a gap and there is a possibility to execute, being executed in our environment. So they may focus on these five techniques, how they can implement defensive mechanisms specific to these techniques. Okay, so this attack navigator facilitates storing and analyzing this extracted TTPs or threat intel using this navigator tool which is open source. You can also host this navigator locally on your machine and there is an online hosted version which I showed you last class.



## ATT&CK Navigator



- One option for getting started with storing and analyzing in a simple way
- Open source (JSON), so you can customize it
- Allows you you visualize data

Then you can export this mapped TTPs in JSON format, which is in machine-readable format, which can be further ingested in other tools, which supports these patterns. Also, it will allow you to visualize the data. So now we'll see a demo of ATT&CK Navigator. So this is the Navigator tool. So in the header side, there are all 14 different tactics here and there's a number of techniques listed inside each tactic.

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

Then there are lists of techniques which have been listed inside every tactic. Let me rephrase it. So now let me create it again. Yes, so we will see the functionality of this navigator tool one by one. So there are several functions.

If you notice that there are some techniques which have been listed in multiple tactics. So this boot or logon's auto start execution technique lies inside persistence and privilege escalation because one can use this method to achieve both persistence and privilege escalation. And for our case, like if we are analyzing, the attackers have used this method to only make the persistent connection, not the privilege escalation. So if I want to map this technique on this navigator, I need to choose only this tab. If I selected this, you can see there is a rectangle over this technique.

So both these techniques have been selected. If you want to go with only one technique, this is the selection behavior lock and unlock button. You can click here and see how you want to select the techniques, whether it should be across the tactics or only the tactics which you are clicking on. So we'll just disable this. And now if we'll choose this, we are going to only choose one technique.

Further, there is a search option where one can search about the techniques about the thread group. Let me show you. This is a technique listed here. There are a total of 625 techniques, including enterprise and the other ICS and mobile. There are 141 thread group details.

There are 648 softwares. and mitigation methods, campaign and data sources. So if I want to see APT29 group's TTP, which they have used till now and there is also a search setting where you can filter the things, what exactly you want to search. So assume we want to go with a name and an attack ID. So we'll write here APT29. So you can see there is no technique which consists of this APT29, but there is a threat group.

APT 29 so on the select button you can select all techniques which APT 29 has used till now and deselect, you can deselect them. Similarly, if you want to see only techniques related to registry, techniques which involve registry, so you can find there are techniques listed here which involve registry information. So assume you got some behavior where

you are suspecting that there has been a registry used in that operation. So you can directly search here and see what all techniques we have which utilize the registry and one by one you can go and see the techniques and understand which techniques lie to that behavior. Now as I selected APT 29 TTPs, now I assume I selected this TTP and now I want to deselect it.

There is one option here: cross sign from where you can deselect all the selected techniques. You might be seeing the difference now. This was related to the selection control. Now we have this layer control where we will be controlling layers. So this is called one layer in ATT&CK Navigator.

Here you can rename this layer by a name like APT29. You can give a description which can help your team to understand what exactly you are mapping to. And then you can add the domain details like we are going with the IT, I opened IT enterprise navigator only. So this is disabled right now.

So this is enterprise. You can add some metadata, the analysis which you are performing if there is something related to them. this layers and this Intel, you can add here as a metadata. Also you add a link which can give some contextual information for the other analyst. Okay, assume once we mapped it, okay, now you can export this in the form of JSON by clicking here, in the form of Excel by clicking here and also in the form of SVG format like this which helps us to use these mapped techniques in an image form on the presentation. As we just saw in our presentation, we had APT 28, 29, TTPs mapped images.

So you can use the SVG format for that. Now here you can filter out the platform, which platforms related techniques you want to see. You might be seeing a number of techniques being changed when I am filtering out these platforms. So now my navigator is only for techniques which are related to the windows platform. You can shorten these techniques inside each tactic based on this alphabetic number and the score.

We'll discuss what a score is. Then there is a color setup. You can set different colors for the different selections. This is to show and hide the disabled. If you have disabled any techniques, you can click and you can hide those disabled techniques or you can see all the techniques by clicking here. Now, as we discuss, Each TTP has sub-technique, not each, some of the TTPs have sub-technique.

So you can see there is this boot or logon auto start execution having sub-technique, many sub-techniques. Once you click here, you can see all these sub-techniques lies in this technique. If you want to see techniques along with the whole sub-techniques present

in this attack navigator, you can directly click here. This will get expanded and you can see each technique along with their sub-technique.

You can collapse using this. Also if I assume I mapped this LSASS driver technique, I selected this by coloring this and we can go to system services and this service execution I selected. These two sub techniques I selected. Okay now I want to see only sub techniques which we have selected in our analysis. So you can click here to expand annotated sub techniques you can see only these two sub techniques will get expanded in that case. Also you can change the layout. There are various different layouts to see these layers.

There is a button to show IDs like till now we are just seeing technique names along with their ID. If you want to see we can click here and also the aggregated score. What aggregated score is we will be discussing further. Also if you want to disable this technique you can toggle this by clicking here. So you can see this has been disabled. Once you want to enable it again, you can again click here. This is to select colors for the techniques which you are selecting.

As we saw in the PPT, there was yellow and blue. Here, if you select this technique, If you select this technique and you want to add contextual information, which may lie that why you are saying that these techniques attackers have used. So those contextual information you can add here in the comment section. You have a link here to add the link. You have different metadata if you want to add for each and every technique, you can add it.

This is to, if you want to clear all annotations, you can click, let me show you. And this is for the sticky toolbar. So there is, you might be seeing once I'm enabling it, this is disabled mode, when I'm enabling it, there is a kind of note where you can click on here and get all the information about this MITRE Attack Navigator, which you can see. So this was all the detail of the Attack Navigator. Now we'll see how those APT28 and 29 details which we saw just have been mapped.

So we will name this layer as we will compare APT3 and APT29 for this comparison. So I will name it as APT3, I will search here APT3. So APT3 is the group, I can select every technique that has been seen in the past which APT3 has used and can be selected now okay. There was a scoring option, but I missed it. This score, there is a scoring option where you can give a score to the techniques in between 0 to 100, what kind of rating, what, how, in terms of different perspectives like how important it is and how different it is based on your analysis, what you are doing.

For now, we will just give a random number for scoring. So, I am giving a similar score for all selected TTPs, score 1. Okay so you can see there are several techniques which have been selected now. Okay, I'll just rename it again.

Okay, so we are done now. Now we'll add one more layer here and we'll again similarly map APT29 group details. So APT29 is a Russian group and APT3 is a Chinese group. We selected and now I'll give a score. So I'll give it a score of 2. So this score can have different meanings based on what we are trying to do.

For here I am just distinguishing between APT29 group TTP and APT3 TTPs by seeing this score. Okay, now there are two different layers. Now I have information about APT3, TTP, APT29, and how I'll club both of them. So for that, I'll create one another layer. So there we can see in the starting page, we have a different option like creating a new layer, opening an existing layer, creating a layer from another layer and creating a customized navigator.

So the third option, creating layers from other layers will help in this case. So we'll click here. We will see which navigator we want to load.

So it is an enterprise. The latest one is version 14. Now you must be seeing that this APT3 and APT29 has been labeled as A and B to help them to understand how I should express the score which I have given to the TTPs. So A represents APT3 TTPs, B represents APT29 TTPs. So I will just give an expression as A plus B. It means the score given to the TOP of APT3 having 1 score and APT29 having 2 score. So wherever this technique presents both in the group should have a score 3 now, 1 plus 2.

And now there is some customization related to this. Colors and all, we can leave everything as it is. Or if you want to add something, you can add here. We'll click on the create layer. So now you can see there are three colors, yellow, red and green. If you hover mouse on the yellow one, you can see this is score two.

You might be seeing score two. So this yellow color mark TTPs are of APT 29. The red one is score 1 which is used by APT28 and this green one is score 3 which has been used by both of the groups okay. Also if you want to change this based on your interest you can click and change any color with this you can select anything randomly. Based on your choice, so now you can see we have changed the color. Is it clear? So for assignment two, I missed to announce that assignment two has been released now, last night.

So you have to do this, such mapping, like this APT3 and APT29 we mapped. So you have to extract TTPs from the given threat report. You have to map it here. For each TTP,

assume for this, for this, if they have exploited the web server which was phased towards the public domain, This case, if you selected this, you have to go to the comment section and add that exploit. Okay, so this will give contextual information why you selected this technique.

So once we add any comment here, you might be seeing that there is a yellow underline with the techniques which represents that this technique has some contextual information. If you hover mouse here, you can see comments along with the score. Okay.

## Exercise : Comparing Layers in ATT&CK Navigator



■ Docs you will need are at [attack.mitre.org/training/cti](http://attack.mitre.org/training/cti) under Exercise 4

- Step-by-step instructions are in the “Comparing layers in Navigator”
- Techniques are listed in the “APT 9 and Cobalt Kitty techniques”

1. Open ATT&CK Navigator: <http://bit.ly/attacknav>
2. Enter techniques from APT39 and Cobalt Kitty/OceanLotus into separate Navigator layers with a unique score for each layer's techniques
3. Combine the layers in Navigator to create a third layer
4. Make your third layer look pretty
5. Make a list of the techniques that overlap between the two groups

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.

Now we will see another exercise which is present in this MITRE CTI training under exercise 4 where you have been given 2 APT groups techniques to tell APT 9 and cobalt kitty and you have to perform the same experiment by yourself. You have to open the attack navigator, you have to enter the techniques used by APT 39 and cobalt kitty group.

And by giving them a unique score for each group, then you have to combine both layers in the navigator. Then you have to create another layer which consists of both groups' techniques and their common and distinguished techniques. And once you are done with this, you can make a list of overlap techniques between the groups. I missed to show you how you can export this.

So I showed the button but I will just show you how you can export here. So you can download it directly here. You can see JSON downloaded. We can open this JSON. So here you can see JSON.

This JSON also you are supposed to give in the assignment. So this is, sorry, not JSON, XLS. So the versions and other details related to the navigator which we used. So there is domain information, description, what are the platforms we use to map the TTPs, whether we followed sorting methods or not. Then there's layout information, exactly what we selected from the layout.

Then there is technique details stats. So here T1027 execution tactics having two scores has been enabled through. Similarly, there will be various techniques for the persistence, for the previous connection, You can see there are various techniques which were listed there, and have been listed here. So this is a kind of machine readable format which can be used further to ingest it for the other tools which support MITRE, this threatening Intel in terms of TTPs. So these are the other metadata grade and color information which we selected.

### Exercise: Comparing Layers in ATT&CK Navigator

**APT39**  
**OceanLotus**  
**Both groups**

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution is unlimited. AT&CK Navigator v19-10-075-15.

Okay. Now I'll just show you this format. You can see you can directly download this and see a nice picture which you have mapped right now okay. So this was all about the attack navigator demo. So, the same similar experiment you have to perform by using these materials listed here in exercise 4. So, once you mapped it this you will be getting a similar kind of interface where this yellow one is for APT 39, blue one is ocean lotus and green one is has been used by both groups. So these are the overlap techniques which have been used in this practice exercise in which spear phishing attachment and link were common in both groups.

## Exercise: Comparing Layers in ATT&CK Navigator



- Here are the overlapping techniques:
  1. Spearphishing Attachment
  2. Spearphishing Link
  3. Scheduled Task
  4. Scripting
  5. User Execution
  6. Registry Run Keys/Startup Folder
  7. Network Service Scanning



©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-15.

Scheduling tasks to automatically execute the executables has been used by both groups. Scripting which is obvious in any attack that attacker will use scripting. User execution, as there is a spear phishing attachment and link, the user is expected to execute or either click on the link or they click on the attachment. So this is also obvious if there is a spear phishing attachment.

So there will be TTPs which are correlated. So if one TTP is occurring, there is a high chance that other TTPs are also occurring. So while we are extracting the TTPs from the report, you have to see that if you are getting this, you have to see how this attachment, image were executed. So if it is downloaded and auto run, then it's okay. But if it is supposed to get clicked by the user, then this technique will get mapped. So there are some attachments in terms of PDFs or the Word, Microsoft Word, where in the macro section, attackers added JavaScript code.

So in such cases, users are expected to open the Microsoft Word document. Once they open that document in the machine, the script placed in the macro section, it gets executed automatically. Similarly registry run keys were common in both the groups activity and the network service scanning. So now there is a quick question answer quiz.

So please go to menti.com and use this code. In this quiz, there are a few sentences I just wrote and you have to read the sentence and understand what exactly it is doing and you have to select the techniques based on your understanding. So if anyone has any doubt, you can ask. Related to the navigator, have you checked the assignment? Anyone checked the assignment? So before starting this, let me show you the assignment first



then. But you can, anyway you can go to this and click for the quiz.

Link to the report:

<https://www.microsoft.com/en-us/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/>

So now we will go to, so now this is a report, this is an analysis report published by Microsoft which is talking about the latest early stage tool set which has been used by the Nobelian APT group. Okay, so you can start reading from here, but you can see that recently Nobelium have used email based attacks in which they are targeting, sending spear phishing emails to the victim. So you can see what all how they attack let me open that section. Okay, so you can see here they have used this different kind of malicious softwares, EnvyScout, Boombox, NativeZone and VaporRage. So this report talks about all the softwares which they have used or the malicious files which they have used.

So for EnvyScout, they found this HTML as a malicious file of type HTML, Envy.html, which describes the malicious dropper. Like this HTML is kind of capable of dropping the malicious executable and which has been, you can read the sentence, like can be best described as a malicious dropper capable of deobfuscating and writing a malicious ISO file to disk. It means this HTML file is capable of dropping malicious executables on the machine, then deobfuscating them. It means the executable which has been being dropped is obfuscated.

So there is one more technique to obfuscate and there is another technique for deobfuscating. So you can choose those techniques also. Again this is delivered to targets nobilium by way of an attachment to spear phishing email. So this HTML is being delivered using a spear phishing email.

So there is a technique named as phishing in the navigator tool. Let me show you. So, there should be obfuscation. You can go in the search section, disable all these, not required, only name and obfuscation. So you can see in this technique, you can get in two techniques, obfuscated file or information or deobfuscated decode file or information. So whatever obfuscated files are being delivered on the victim machine, they are supposed to deobfuscate before executing.

So you can select this technique and color it. Also select this, color this. We can see deobfuscated and obfuscated ones. So this both lies in defense evasion tactics like when attackers try to evade defensive mechanisms deployed on the victim machine these two techniques are usually performed. Then now you can see in the HTML body section that

they observed that there is image information which is hosted on an unknown IP and one of the websites. So what it means is that this img\_lk and img\_tst images will be getting downloaded once you run this HTML object.

okay and which will be downloaded from this IP and this web address. So these two can be extracted in the list of IOCs indicator of compromise which can be a CNC server IP address and the web address. So there is one more tool for downloading these files from the CNC server and we see it Ingress tool transfer. So this technique represents when attackers try to download subsequent dropouts or subsequent malicious files once they are into the victim machine, ingress tool transfer.

So you can see this TTP ID T1105. I will just show you the details of this TTP. So you can see they may, adversaries may transfer tools and other files from the external machine to the victim machine. So you can select this tool, this TTPs again.

Okay, we are not adding any context here. So let's add context here. Give IP name. give the website name. So it will reflect how and why you have reasoning behind choosing this TTP. Similarly goes for deobfuscation and obfuscation. Again we'll go ahead and we'll see what exactly these things are doing. So the first prefix with the file protocol, yes, here also you can see this.

This is exactly downloading this file from this IP. File protocol is being used. In an indicative attempt to coax the operating system, send sensitive NTLMv2 material to specified attacker's control IP address over port 445. So now you can see whether this port 445 comes under these commonly used ports or not and accordingly you can add. Then again, it is likely that the attacker is running a credential capturing service such as a responder at the other end of this transaction.

So here credential is being captured. So there might be a technique related to credential capturing. Let me see. Okay, so this credential capturing is kind of broad. There is no such technique named it, but there are various techniques which can be used to access the credential or capture the credential. So we need to see further details if there is any to map the exact TTP inside the credential access tactic.

Later, brute forcing of this credential may result in the exposure. So I guess there is brute force, if I remember correctly. Yes there is brute force technique in the credential access section. So you can go and select this, mark it based on your color choice okay, add a comment here okay. Now we'll see the other helper code which is present in this malices file component two.

You have to go to the second portion of this in this cart and see what they're doing there. Oh, the second part is the modified version of open source tool file saver, which is intended to assist in writing of files and disk via JavaScript. So here you are getting a sense that scripting is being used for this purpose. So you can go here. In the script, you can search for this one.

In this technique, you can see we'll directly map to sub technique. There should be JavaScript. Oh, here it is. So we can click on directly sub techniques. So whatever techniques, if they have sub techniques, try to get this as specific a detail as you can. So select JavaScript rather than technique here.

Select sub technique. The code is borrowed directly from publicly available variants with minor alteration. So sometimes attackers use open source tools, they might tweak them based on their interest and objective, and then they use that to deploy the attack. So their alteration includes white space removal, conversion of hex parameter to decimal. So there was very minor conversion that I can see, very minor alteration I can see, renaming the variables which cannot be much differentiating with what they have. The method which they have implemented is circumvent for a static analysis. If someone is performing static analysis on the malicious file which has been captured Now we will see this component 3 which has obfuscated ISO file.

So we already guessed obfuscation techniques by saying deobfuscation but here also you can get evidence that the ISO file which was dropped was obfuscated. Obfuscated means either encoded or encrypted or compressed like they have changed the state or the view of that malicious file. So you can see that it contains a payload stored as an encoded block. So I believe, and this payload is decoded.

So this obfuscation deobfuscation also contains these decoding and encoding methods. So we'll not mark again. Then again see, they're using base 64 payload to encode and for encoding and decoding purposes. So yesterday we saw that base 64s, we mapped it to the, No, I don't remember if we can map it. No, base 64, one second. Okay, there is data encoding having sub-technique standard encodings.

If they are using any standard methods to encode which is already known to the public, you can choose this technique. If they're using some non-standard method like custom methods to encoding their payload, then you can choose this non-standard encoding method. Similarly, you can see this deobfuscating dropper script, you have to read one by one each sentence and understand the TTPs which are being represented by that sentence. Phishing we already mapped I guess, no. I believe no, we didn't map.

So you can see, you can read here in some iteration of the attacker's phishing campaign, they did this, which is explained here. So from here, we can get a sense of what the attacker has sent. We read it earlier, I guess, they send spear phishing emails. So we can map this spear phishing email here. Add contextual information again. And similarly, you have to complete the whole report which has been given to you.

So you can extract details from images too, if you can find any. So here, ADB packs a DLL. So if there is, I believe there is a direct sub technique for running DLL, but for ADB pack, I need to see. No, there is nothing, but for running a DLL, there should be something. Yeah, there is a DLL. So if you are seeing any information in snapshots, don't only see sentences of the reports, see the snapshots also.

So you may get some fruitful information from snaps, from the pictures placed in the report. These are the static analysis is being performed, reverse engineering is being performed on the dropper, drop malices file. So you can see if you can find any information from here.

Yes, so that's it. This is for today's class. You expected to do this practice for your assignment 2. You just focus on these names and the paths if you can find anything related to the behavior so that you can map that. That's it. So you can see there is a link of IOCs.

What all IOCs have seen in this attack? Microsoft has given their GitHub repo a mistake. You can go and see. This is something different. Okay so in next class we will see defensive recommendation, we will see one case study how we are making assumption of the organization and how we are give extracting TTPs, extracting TTPs will go a bit fast then how for extracted TTPs what all assumptions we can give for such scenario okay and that is only your assignment 2, is it clear any doubt? Thank you.