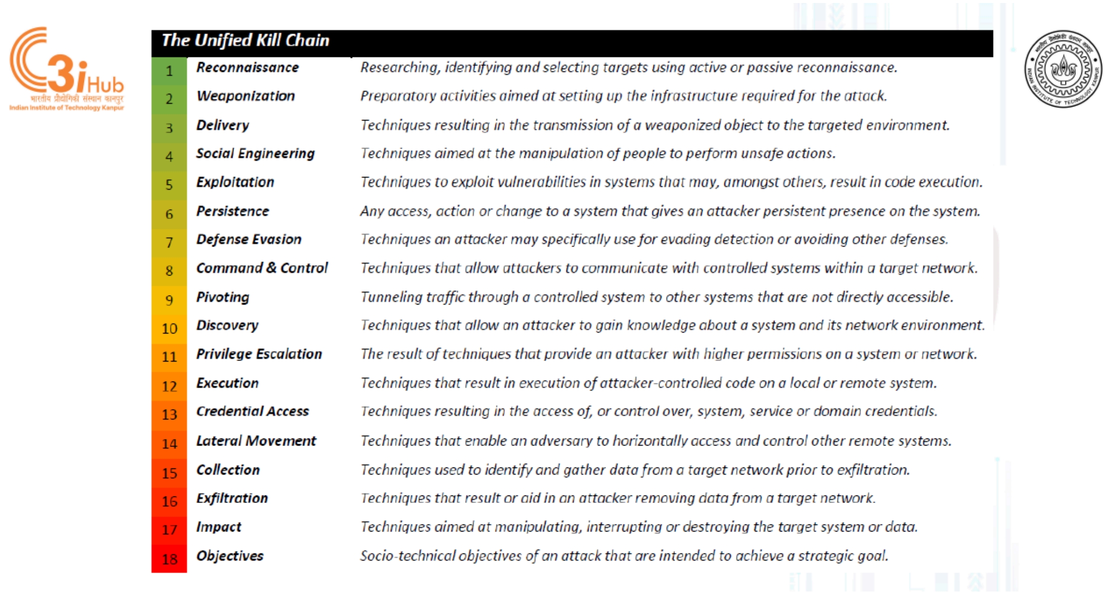
Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

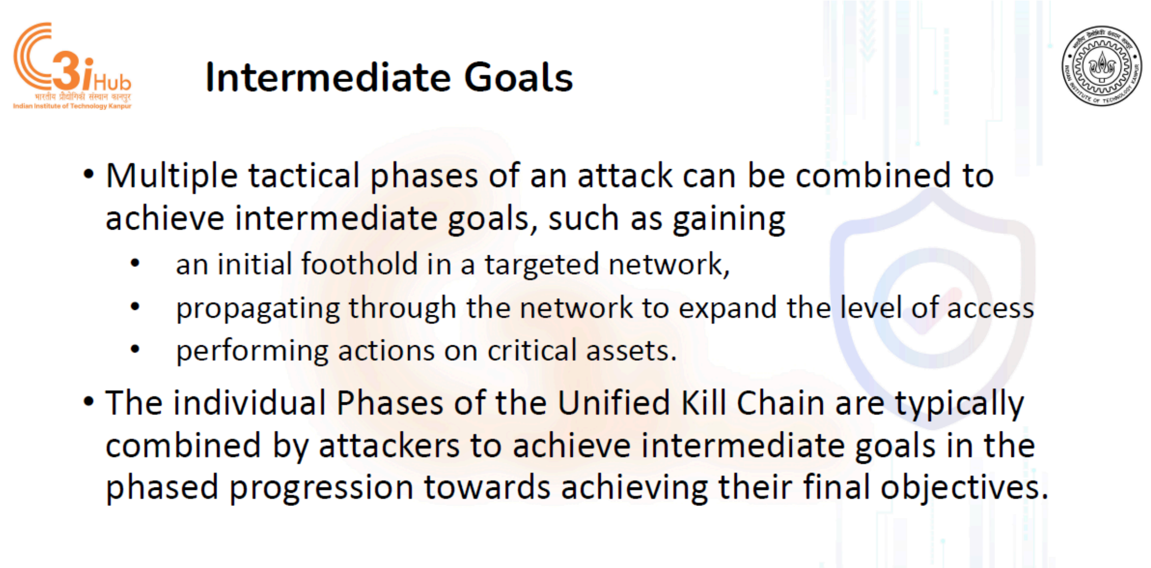
Lecture 14



The Unified Kill Chain		
1	Reconnaissance	Researching, identifying and selecting targets using active or passive reconnaissance.
2	Weaponization	Preparatory activities aimed at setting up the infrastructure required for the attack.
3	Delivery	Techniques resulting in the transmission of a weaponized object to the targeted environment.
4	Social Engineering	Techniques aimed at the manipulation of people to perform unsafe actions.
5	Exploitation	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6	Persistence	Any access, action or change to a system that gives an attacker persistent presence on the system.
7	Defense Evasion	Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8	Command & Control	Techniques that allow attackers to communicate with controlled systems within a target network.
9	Pivoting	Tunneling traffic through a controlled system to other systems that are not directly accessible.
10	Discovery	Techniques that allow an attacker to gain knowledge about a system and its network environment.
11	Privilege Escalation	The result of techniques that provide an attacker with higher permissions on a system or network.
12	Execution	Techniques that result in execution of attacker-controlled code on a local or remote system.
13	Credential Access	Techniques resulting in the access of, or control over, system, service or domain credentials.
14	Lateral Movement	Techniques that enable an adversary to horizontally access and control other remote systems.
15	Collection	Techniques used to identify and gather data from a target network prior to exfiltration.
16	Exfiltration	Techniques that result or aid in an attacker removing data from a target network.
17	Impact	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	Objectives	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

So, how is preparation going on for mid-sem? Hopefully, you are practicing translating TTPs from the threat reports and making the defensive recommendation. Defensive recommendation were there in assignment 2. So, today we will also again see one more example for defensive recommendation once we complete UKC. I will just give a quick revision for the UKC Kill Chain stages which we saw yesterday. So, UKC Kill Chain has it has it merged or extends the capability of LMCKC and MITRE ATT&CK and created 18 different attack phases include starting from reconnaissance first stage of the attack till impact and objective. And also you can see add a new perspective towards seeing the kill chain by adding a concept of sequentially arranging the attack phases.

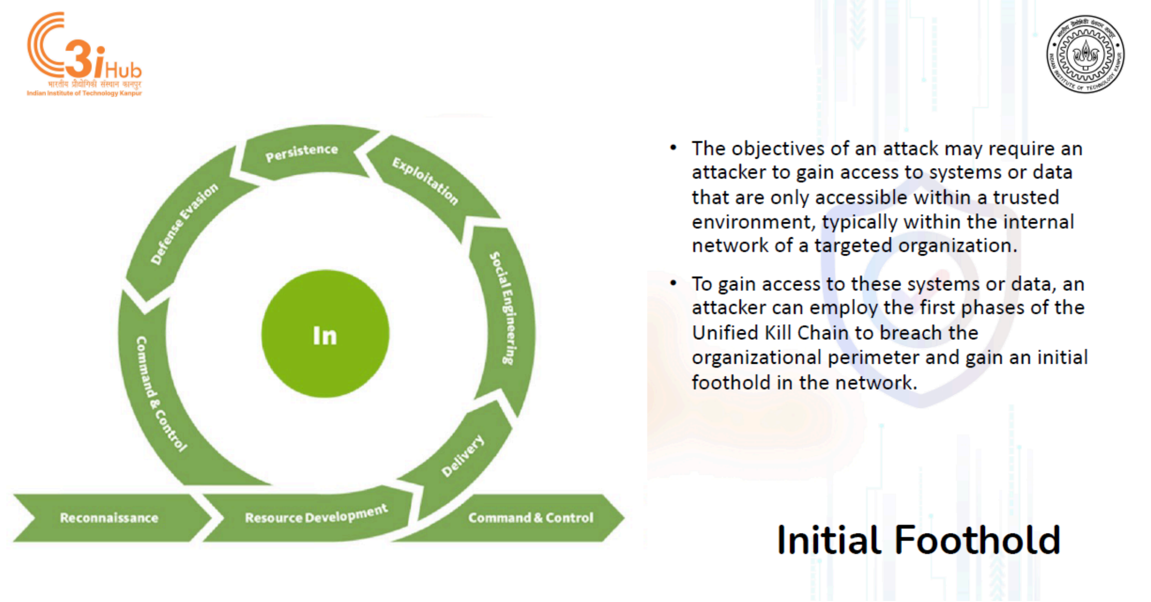
And in addition to this sequentially adding this attack stages, they also emphasize that attackers need not to execute this attack phases deterministically like LMCKC. They may bypass or they may ignore some of these stages in order to achieve their objective. So, we as we discussed this UKC is divided in three different intermediate goals. The initial foothold which is which will also be represented at in like going coming into the victim environment propagating through the network will come under the thorough and the performing action on critical assets will come in an intermediate goal which this authors of UKC has also referred as out in throw out 3 different goals which were listed here.



Intermediate Goals

- Multiple tactical phases of an attack can be combined to achieve intermediate goals, such as gaining
    - an initial foothold in a targeted network,
    - propagating through the network to expand the level of access
    - performing actions on critical assets.
- The individual Phases of the Unified Kill Chain are typically combined by attackers to achieve intermediate goals in the phased progression towards achieving their final objectives.

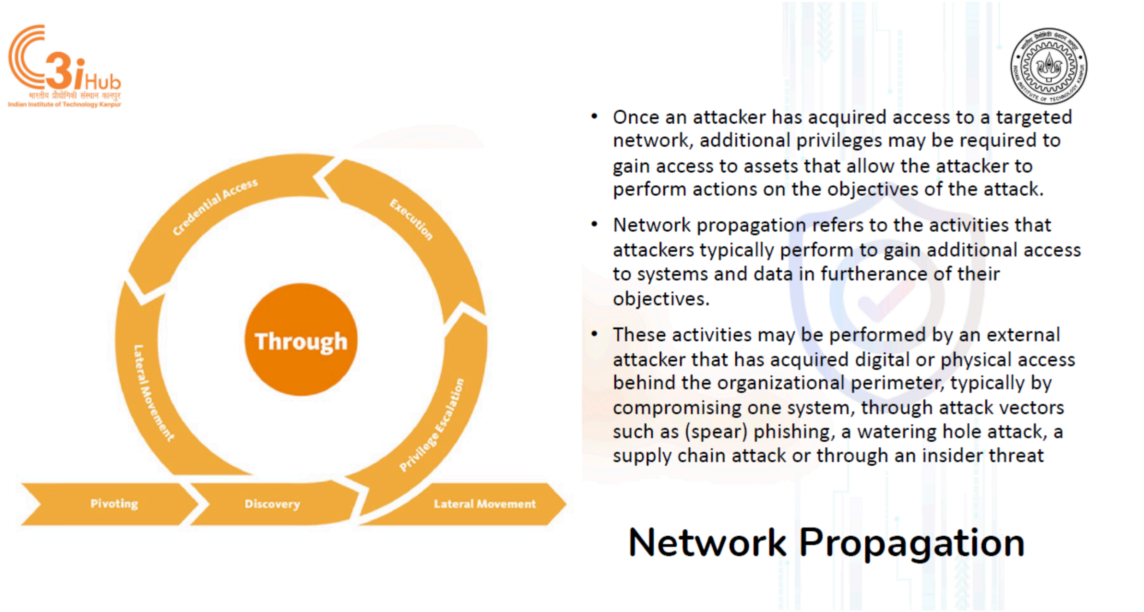
So we discussed there are multiple attack phases sequentially arranged for each of these three intermediate goals. In the first intermediate goals, they focus on how one can get initial foothold in the victim environment, all these attack stages which usually attack as employee to get the foothold, then how it will propagate inside the victim network, all these attack stages which lies in propagating the attack infection, all these stages are sequentially arranged in this second intermediate goal.



- The objectives of an attack may require an attacker to gain access to systems or data that are only accessible within a trusted environment, typically within the internal network of a targeted organization.
- To gain access to these systems or data, an attacker can employ the first phases of the Unified Kill Chain to breach the organizational perimeter and gain an initial foothold in the network.

Initial Foothold

In the third one we had action on objective third goal which authors have also referred as out like after this stage attacker is going to out from the victim network and the attack stages which belongs to this intermediate goals they arrange them sequentially here. So now once we understand whether it's LMCKC, MITRE ATT&CK or UKC, one has to understand that how we are going to use this skill chain concept or the framework in the real time. So we'll discuss for UKC today that this can be, this UKC, once we have attack behavior or attack patterns list, what has been executed in the environment, we can prepare a kill chain like similarly sequential steps which attackers follow and that will give us an insight about what exact set of tactics attackers has followed and which we later on will be representing the whole model separately how attackers follow to perform the attack.



- Once an attacker has acquired access to a targeted network, additional privileges may be required to gain access to assets that allow the attacker to perform actions on the objectives of the attack.
- Network propagation refers to the activities that attackers typically perform to gain additional access to systems and data in furtherance of their objectives.
- These activities may be performed by an external attacker that has acquired digital or physical access behind the organizational perimeter, typically by compromising one system, through attack vectors such as (spear) phishing, a watering hole attack, a supply chain attack or through an insider threat

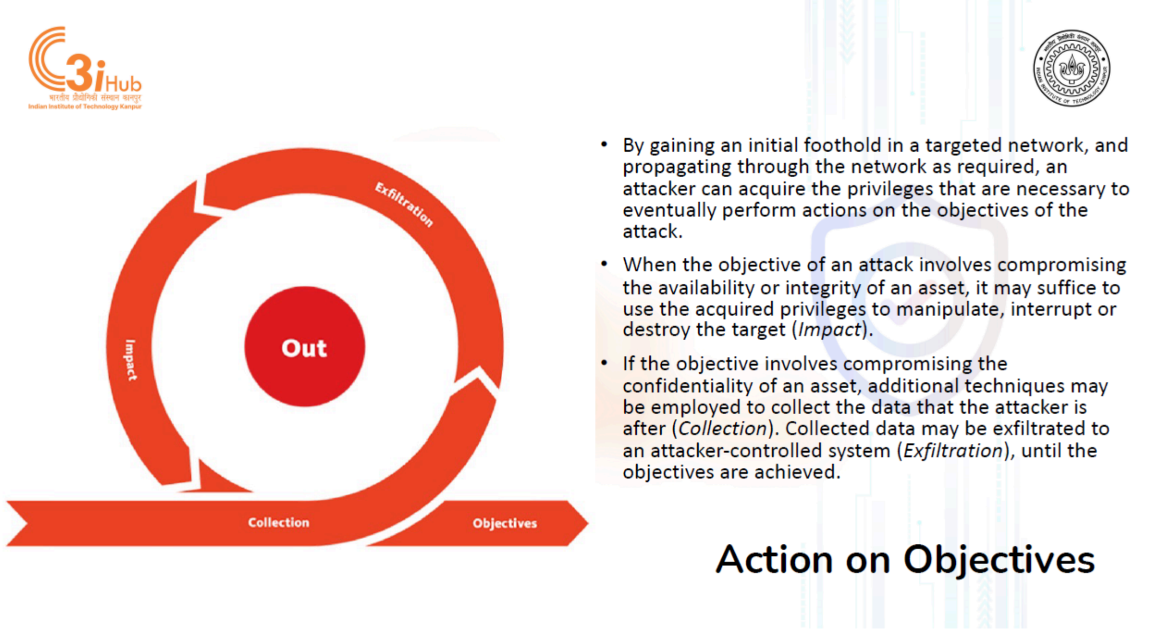
Network Propagation

from starting to ending. So this will give a complete picture. Also, this UKC specific to this UKC, this skill chain will facilitate this to visualize the whole attack scenario from start to end. Specific to this UKC, this kill chain can be used in two ways. First one is one can use this UKC to create attack specific kill chain and the second one is one can use this UKC to create an actor specific kill chain.

So for attack specific kill chain if you have a data or details of past attacks we can create the kill chain stages for each and every attack stages attack past attack data which we have and then one can perform the analysis to understand the correlation between the historical attacks and this may give them a key insights related to the commonalities and differences between the two different attacks campaign. later on in addition to this for attack after specific kill chain this will help a analyst to create this kill chain from starting to kill chain what attackers one specific threat group follows. So, the actor which is performing attack if I want to perform profiling of threat actors or threat groups profiling in that case one can create this kill chain stages specific to the actors like APT 28, APT

29 these are the some of the threat groups. So, one can create this tactical modest operandi one can understand their tactical modest operandi by creating this specific kill chain specific to the different threat groups. So this will give an insight about the what all threat groups have a common or what all threat groups have a common modus operandi which they follow.

Some of them will give the similarity between the threat groups. Even in some sophisticated situations, more than one threat groups collaborate together to perform some highly sophisticated attack with their personal like common interest regarding victim. So, in such cases creating this actor specific kill chain will help them to understand whether the actor behind the any specific sophisticated attack, is there more threat groups modus operandi is being aligned with the current attack or is there different actors modus operandi is overlapping more with the actor specific kill chain. So, this two has a different purpose. And this all this kill chain is one can create by putting them in the right order how it how this attacking attack patterns has been seen in the victim environment ok.



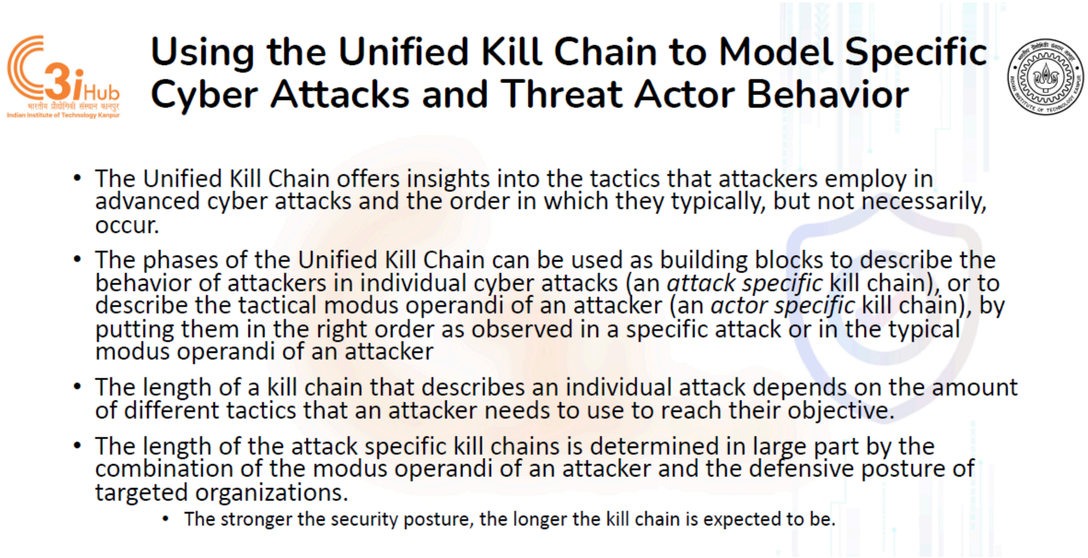
- By gaining an initial foothold in a targeted network, and propagating through the network as required, an attacker can acquire the privileges that are necessary to eventually perform actions on the objectives of the attack.
- When the objective of an attack involves compromising the availability or integrity of an asset, it may suffice to use the acquired privileges to manipulate, interrupt or destroy the target (*Impact*).
- If the objective involves compromising the confidentiality of an asset, additional techniques may be employed to collect the data that the attacker is after (*Collection*). Collected data may be exfiltrated to an attacker-controlled system (*Exfiltration*), until the objectives are achieved.

Action on Objectives

So, now if we creating the kill chain there will be a thought that what will be the this length of kill chain how long it can go. So this length of kill chain like how long this stages a sequential stages will go depends on the sophistication of the threat actor, how sophisticated they are performing the attack, what amount of their different tactics they are going to follow.

In addition to that, what all the defensive mechanism has been employed on the victim machine or victim environment will also affect the skill chain. Like if the victim has a strong countermeasures implemented, so there may be attacker will struggle to evade or invade the infrastructure on the victim side and that will reflect as a result that they may demonstrate more stack stages or the more malicious actions in the environment. This length of the kill chain which depends on the amount of different tactics will belongs to this attack, this actor specific kill chain.

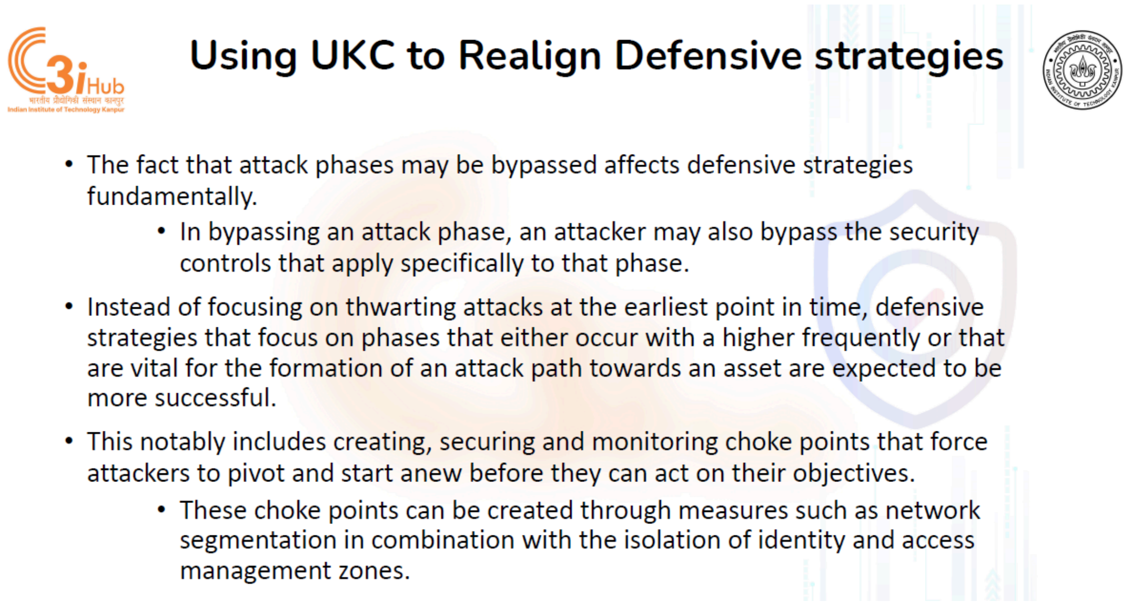
But for attack specific kill chain, this will again, it will be having the similar way that all, what all defensive measures has been employed at the victim side and what all modus operandi attackers has decided to execute in the victim environment. Then we discussed this yesterday that the longer the kill chain is can be not exactly but can give a sign that a victim has a stronger security posture which will reflect that if attackers have struggled to not get directly access to the victim critical assets rather than they perform a series of several actions or several intermediate goals and that led this kill chain to be longer. Okay, once we understand the use cases how one can use this kill chain unified kill chain in the real world. We will be discussing about how we can realign the defensive strategy based on this kill chain. So, basically in the first class we discuss about resilience that this facilitates organizations to be more resilient towards cyber attack sophisticated targeted attacks.



C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

Using the Unified Kill Chain to Model Specific Cyber Attacks and Threat Actor Behavior

- The Unified Kill Chain offers insights into the tactics that attackers employ in advanced cyber attacks and the order in which they typically, but not necessarily, occur.
- The phases of the Unified Kill Chain can be used as building blocks to describe the behavior of attackers in individual cyber attacks (an *attack specific* kill chain), or to describe the tactical modus operandi of an attacker (an *actor specific* kill chain), by putting them in the right order as observed in a specific attack or in the typical modus operandi of an attacker
- The length of a kill chain that describes an individual attack depends on the amount of different tactics that an attacker needs to use to reach their objective.
- The length of the attack specific kill chains is determined in large part by the combination of the modus operandi of an attacker and the defensive posture of targeted organizations.
  - The stronger the security posture, the longer the kill chain is expected to be.



Using UKC to Realign Defensive strategies

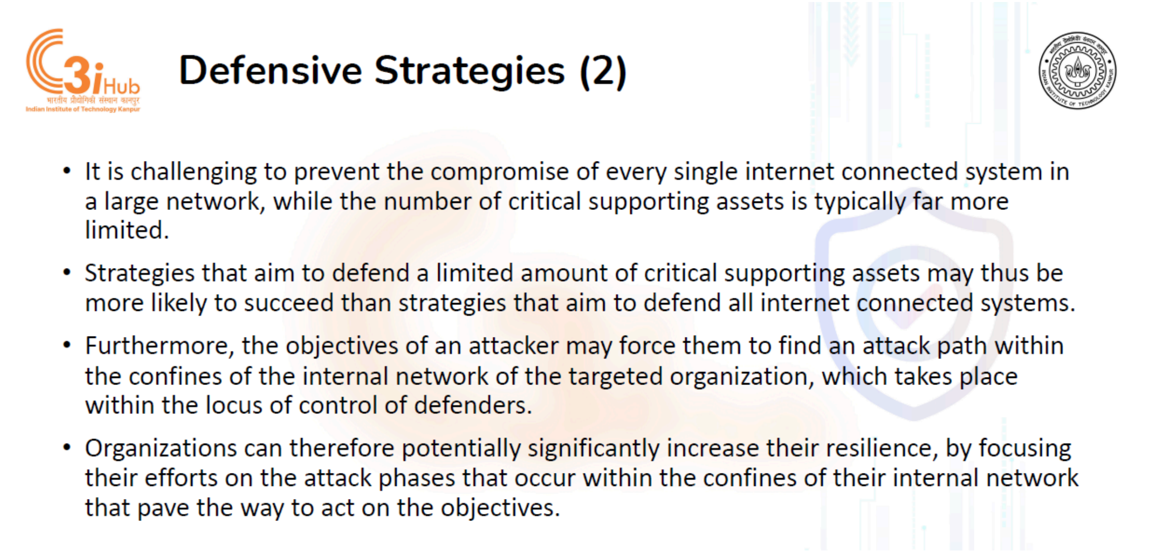
- The fact that attack phases may be bypassed affects defensive strategies fundamentally.
  - In bypassing an attack phase, an attacker may also bypass the security controls that apply specifically to that phase.
- Instead of focusing on thwarting attacks at the earliest point in time, defensive strategies that focus on phases that either occur with a higher frequently or that are vital for the formation of an attack path towards an asset are expected to be more successful.
- This notably includes creating, securing and monitoring choke points that force attackers to pivot and start anew before they can act on their objectives.
  - These choke points can be created through measures such as network segmentation in combination with the isolation of identity and access management zones.

So, we will understand how this resilience is aligning with this kill chain. So, for each kill chain stage what defenders do that they implement a different defensive strategies how I have to defend if attacker is going to execute this stage. So for all like even for the LMCKC, for MITRE attack, even also for UKC, there are different attack stages and defender is responsible to implement defensive strategies for each of these attack phases. So as we saw in LMCKC that they were more focused towards the starting of the attack. If we can disturb this execution in the starting of the attack itself, then there can be a chance that I can save more destruction in the victim environment.

But here in this you can see the authors are emphasizing towards that attackers may bypass some of the attack phases. So assume in the starting some of the attack phases attackers did not even follow and the defensive strategy which has been placed on for those specific attack phases will be also attackers is going to bypass those security controls which has been implemented. So, in that case it will be difficult for an attack to restrict their infection in the starting if we go with that mindset that I have to start attack in early phase rather than you can see authors have more emphasized towards rather than focusing on stopping attack or detecting attack in the earliest point we will focus on the attack phases which has a higher frequency. Like which has a tendency that attackers is going to perform this specific attack stage at any cost or which has a more probability that attacker is going through this attack phase. So we discussed command and control stage in the last class.

So command and control stage is kind of a critical stage where attackers is expected to perform that stage to make a communication with the victim with their C2C server. So, one can focus a defender analyst can focus on CNC it can prioritize to focus command

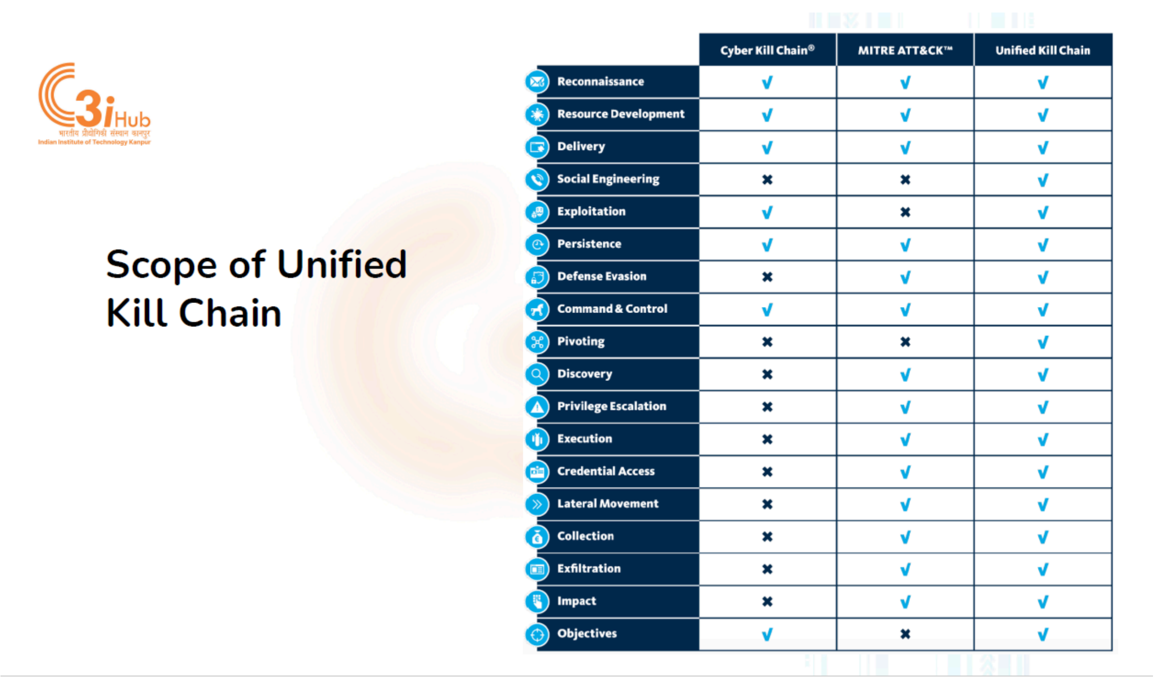
and control because that has a high tendency and the probability that attacker is going is not going to bypass that attack stage. So, the instead of that focusing this earliest point, earliest attack stages in a kill chain, this authors have more emphasized towards focusing on higher frequency or the those stages which are attackers are kind of bound not exactly, but kind of bound or the more intended to perform the action. So, this creating this defensive Strategy includes the creating secure a securing and monitoring choke points. So, how we will understand where we have to focus on to implement the defensive strategies.



Defensive Strategies (2)

- It is challenging to prevent the compromise of every single internet connected system in a large network, while the number of critical supporting assets is typically far more limited.
- Strategies that aim to defend a limited amount of critical supporting assets may thus be more likely to succeed than strategies that aim to defend all internet connected systems.
- Furthermore, the objectives of an attacker may force them to find an attack path within the confines of the internal network of the targeted organization, which takes place within the locus of control of defenders.
- Organizations can therefore potentially significantly increase their resilience, by focusing their efforts on the attack phases that occur within the confines of their internal network that pave the way to act on the objectives.

So, the analyst job is to understand the whole victim infrastructure how it has been set up and find out the choke points where attackers are kind of forced to go through it. So, that attackers behavior comes under the locus of control of the defender and then the defensive strategy which defender has implemented for that specific choke point will get activated or it will reflect in detecting the attacks okay. So these choke points can be created by having a thorough measure of total network segmentation we have and what all the combinations of critical assets, how difficult for attacker to get the access of the critical assets in the victim infrastructure and based on all these things and the victim infrastructure setup altogether, analyst has to understand the all choke points. Is it clear? So now authors have also shed light on that it is really challenging to preventing each and every single machine or single asset which has been connected with the internet in the environment if the victim has large network. So, in that case rather than protecting each and every assets of the victim infrastructure, they focused on to implement the strategies for the limited or more critical assets rather than covering each and every machine in the present in the victim infrastructure.



Scope of Unified Kill Chain

	Cyber Kill Chain®	MITRE ATT&CK™	Unified Kill Chain
Reconnaissance	✓	✓	✓
Resource Development	✓	✓	✓
Delivery	✓	✓	✓
Social Engineering	✖	✖	✓
Exploitation	✓	✖	✓
Persistence	✓	✓	✓
Defense Evasion	✖	✓	✓
Command & Control	✓	✓	✓
Pivoting	✖	✖	✓
Discovery	✖	✓	✓
Privilege Escalation	✖	✓	✓
Execution	✖	✓	✓
Credential Access	✖	✓	✓
Lateral Movement	✖	✓	✓
Collection	✖	✓	✓
Exfiltration	✖	✓	✓
Impact	✖	✓	✓
Objectives	✓	✖	✓

So, they emphasizes that that defending a limited amount of critical supporting assets may more likely to succeed than strategy which is going to cover each and every single critical assets and the machine present in the victim environment okay. So, the objective as we discussed in the previous slide the attackers the objective of the defender has to make attackers force to go within the confines of the internal network of the victim organization and in the locus of control of the defender like identifying the choke points. Therefore, organizations, therefore the organization may have a potentially increase in their resilience if they follow such a strategies to implement the defensive strategy in their environment in which they have to focus on their efforts on attack phases that occur within the confines of internal network rather than the earlier stages of the attack. Okay, so we understand we saw this unified kill chain, now we will see the scope of this unified kill chain over this cyber kill chain LMCKC and MITRE ATT&CK. So, this is we discussed yesterday that what all the stages are there in a cyber kill chain and what are there in the MITRE ATT&CK and what all not there out of this you can see 18 attack stages.

So, we can see that social engineering this MITRE has a social engineering as a technique not a stage or the attack phase. Then exploitation, CKC has, but MITRE doesn't. Defensivization, CKC doesn't have, but MITRE has. For again, this from pivoting to discovery, escalation, execution, credential access, lateral movement, collection, infiltration, impact. All these attack phases are not there in cyber kill chain, but these are in MITRE attack.

But there are some of the stages which unified kill chain has introduced, which has not been either in CKC and MITRE. such as this social engineering, exploitation, pivoting and the objective. So one can think, we discussed this yesterday, but I'll just repeat the same here, that social engineering, why they put the social engineering out of the initial access attack phase, Because these author believe that counter measures which one has to implement for the social engineering is more crucial and totally different what we follow for the initial access like exploiting any zero-day vulnerability or exploiting any public facing application. And this can be a kind of social engineering is more driven, more kind of being frequently used and highly used by the attackers. So they believe to give a special face for the social engineering as it is being highly used in the current scenario.

And also with the perspective of countermeasure and raising the resilience, they realize that social engineering needs to be given a separate identity from the initial access. So now if we have unified kill chain and even though we are comparing LM CKC and MITRE attack and comparing advantage pros and cons over all of them, we cannot say that this once we have a unified kill chain, we do not need this LM CKC and MITRE attack. So all these three having the different identity, different contribution and one analyst can implement either one of them or blend of them or more than one they can combine and create their own customized kill chain or method for their specific victim organization or involvement, okay. So, after merging all these intermediate goals which we discussed in the class, this was the final kill chain framework. So this first one is initial foothold in which attacker will try to get in, in the victim environment.

Then once they have performed this initial foothold actions, then it will proceed towards the network propagation. And once they execute the steps to propagate and propagate it completely in the victim network, then they can go towards the action on objective. So this is the whole picture of the unified kill chain. So it's we are not creating any choke points for implementing the defensive strategy rather than we are identifying what all choke points we have in our infrastructure.

So the failure which you are talking about it is already there like obviously if a choke point fails this even the normal operations in the organization will fail but here our focus is not to keep developing a special choke points for defensive strategy.

Sorry. One second. Okay, the creating securing no, but I believe it is identifying the choke and it is not going to affect our system because let's say a fireball, a fireball allowing all kind of packets flowing from outside world to our network and vice versa has to become a choke point for all the packets from outside. Yes, but in that case his concern is if I. Understandable, but then we have to allow only those items which we release are, you know, belong to let's say our friends. Obviously, it can become. And how does UTC address denial of service? See this kill chain is not to addressing or detecting the attack, it is all the kill chains are to facilitating a way to how one can analyze and implement the strategies.

LMC case is focused on malware. LMC case is focused. Yes, in that case we can see our goal is not to even address any attack rather than how one can perform analysis and how one can place the counter measures. So, we are aiding in that aspect rather than addressing any attack. Which technique or technique is used in that? That will come under that probably in initial access where the first communication is being made with the machine. See in DOS what will happen, there will be multiple bots or there will be multiple requests on a specific machine, right.

So there must be some communication which was being done between that C2 server or the attacker machine to or bot to the victim machine. So hardly either they will be giving some kind of connection request like request to three-way handshake in which they may do, they may request for a kind of ARP, like they may do ARP resolution request. In that case, DOS will execute, but in the terms of techniques, what techniques is going to map, which I am also not clear with in the initial access, there should be some technique which will reflect the connection, active connection between victim machine and the attacker machine. No, no. So, these are mostly towards the targeted attacks not this kind of non-targeted.

So, DOS mostly comes under non-targeted attacks. So, in targeted or sophisticated attacks what happen, they follow a sequence of steps from starting to ending. So, DOS is like I just want to disrupt the victim infrastructure, I do not want to espionage, I do not want to exfiltrate something from there. I believe in my knowledge there is no such framework to address this untargeted attacks. So this No, I believe exploitation part is kind of Once we have the access, one can go with the exploitation.

So there is one TTP, exploiting public facing application in initial access. So I believe for DOS, that TTP can be get mapped. In which attackers is trying to exploit an application which is publicly phased towards the internet. and create a single point of failure of stroke points. Actually, here in this instance, the network segmentation, isolation of identity, access management bugs, these things actually do not create specific failure points.

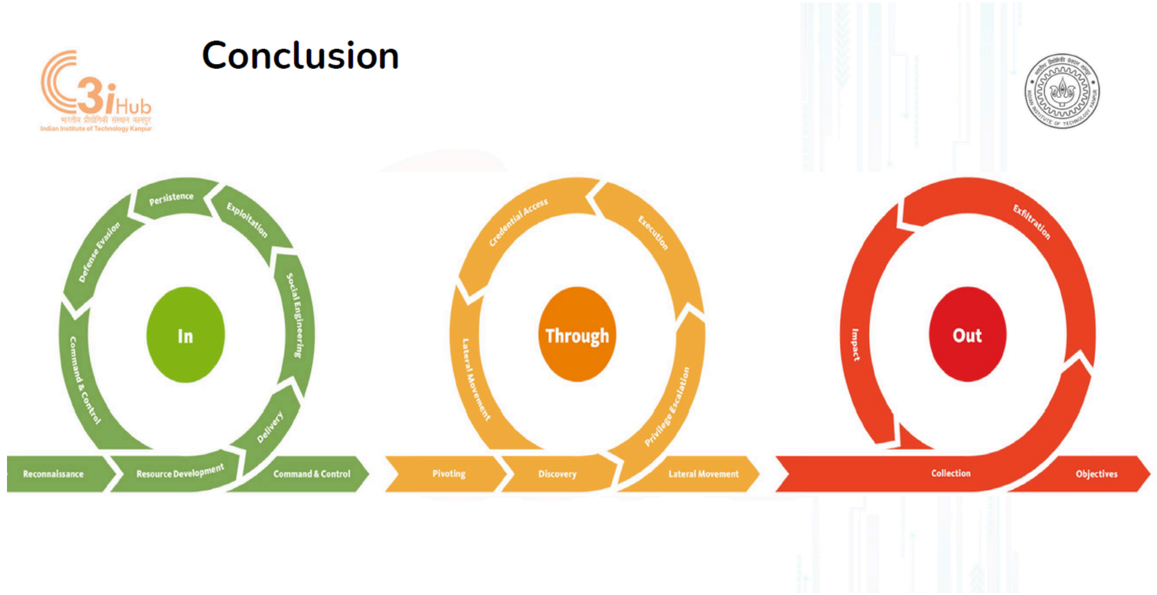
It is a strategy to make Yes, that is what we discussed. This, we are not creating any choke points here, rather than we are identifying and arranging our network in such a way as either segmenting and the isolation. So how we can make attackers to follow our path or our locus of control. So I believe this network segmentation and for isolation, this creating choke points comes, coming to.

But again failure will happen. If there is single point dependency and it fails then operation and everything will get disrupted. Yes. Can become. Yes, it will become, but because of. So, we have to make sure that all the vehicles come to the same point.

Yeah, that will happen like if you have only a single way to get into and it is. So there is that is why we are implementing this defensive strategy on the choke points we are discussing which we are discussing right now. So we are identifying or creating those choke points which we are talking about and we are implementing defensive strategy. So we can rely on those strategy which we are implementing to defending against such attack but yes if any for any reason that defensive mechanism fails so there can be failure on the choke points. And again, we are not detecting on preventing any attack.

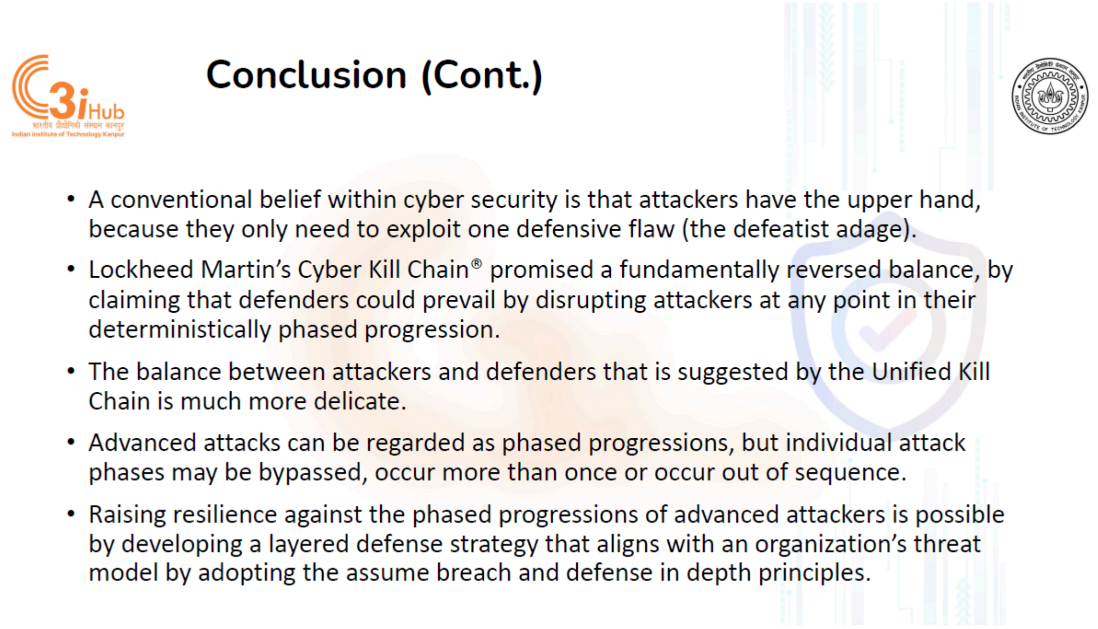
I have no idea of it right now. Yes. So, we discussed this the whole UKC framework. Yes, it was not additional it was there I guess. . It was there once they propagated towards the victim network, then now they have access of everything, now they will go towards their objective, final objective. there is no initial access is different credential is this one second let me go through that there is a credential access already.

So I believe they have not given specific stages and here this access is representing that they have access of network propagation. Should be there. No, it is not there. So this has been taken from their white paper which is present on their website. So we need to look into this why this access stage is not there but this access stage represents that they have access of their critical assets present in the machine in the environment and now they will go to perform their action okay.



Conclusion

As we discussed this as a conclusion that LMCKC is focusing towards deterministically progress towards all the phases rather than it creates a balance between the attackers and defender to chain each and every attack phases present in the which attackers is going to follow. In a conclusion like we concluded that this advanced attacks which has a phase progression, but the individual attack phases may be bypassed which we already discussed. So, also this one stage can occur more than one times like the credential access they can collect credential access from the multi for the victim for the multiple machine. So one phase one attack can occur one or more than one time on even that may not occur like attacker can bypass and the main idea of this UKC is to raising resilience against the phase this sophisticated attacks. by making a layered defense strategy based on these choke points and the other details which we summarize for the victim environment.



Conclusion (Cont.)

- A conventional belief within cyber security is that attackers have the upper hand, because they only need to exploit one defensive flaw (the defeatist adage).
- Lockheed Martin’s Cyber Kill Chain® promised a fundamentally reversed balance, by claiming that defenders could prevail by disrupting attackers at any point in their deterministically phased progression.
- The balance between attackers and defenders that is suggested by the Unified Kill Chain is much more delicate.
- Advanced attacks can be regarded as phased progressions, but individual attack phases may be bypassed, occur more than once or occur out of sequence.
- Raising resilience against the phased progressions of advanced attackers is possible by developing a layered defense strategy that aligns with an organization’s threat model by adopting the assume breach and defense in depth principles.

We will be going with two principle like assuming the bridge that bridge will happen and then following the layered defense inside defense in depth strategy. So now we are done with the UKC. If you have any doubt you can ask, yes.

Let me open that website. Access is not given on that. Where? On the website no? So their snapshot was also taken from their white paper only. It is not there no? That is what I guess he pointed out. Yeah, the axis one is not the… this lateral movement only. So I believe this all snapshot has taken from this there he is the author his master thesis and the you can see white paper only there is a white paper. So yes on the website on the white paper we can see that this lateral movement only gets extended towards the this there is no such stage named axis.

But that meaning of that access was, so I believe it might contain in their master thesis. His thesis is also up on his website. We need to look into that.

But this was the whole picture if you can see. Sorry. This is the final one. So here I reference that the initial getting initial foothold comes under intermediate goal in then throw and then out. You can access white paper present here and all these details are all these things in a more detailed way you can see here in this white paper. They have also given some what all additional improvements they have made over all present Kilchen framework. They have compared with the stages what all different stages they have included and the even therefore, you can see they followed several iterations to do the study and finalize the one this one last one.

You can go through it for the more detail ok. Organizational? Okay. Yes. Okay, yeah. Sorry, do we learn? Yes, no, in this course I cannot, I have no idea and that sir can only clear that whether we are going to cover threat modeling aspect or not. But yes, we have to create the defensive strategies which aligns with this organization's threat modeling by assuming that on these two principles, assume breach and defense in depth.

So threat modeling, I have not idea much right now that whether this is there in the syllabus or not. That sir can answer. Okay. So if you have any doubts, you can ask otherwise we'll go with a demo of defensive defensive recommendation we already saw one case study in previous class.

Now today we'll go with some different one. Any doubt? So this is the analysis and defensive recommendation for a attack performed by Lazarus APT group in which they have this report published by Malwarebytes. Let me show you report. This is the whole attack analysis what exactly happened you can see that there are some malices files were delivered on the victim side and which might have get executed and started the infection. So, you one can read this reports and see how we can extract TTPs from these reports, analyze the behaviors attacking patterns. Once we have a TTP, how we can see, we can see how this TTP executed and then we can make a defensive recommendation.

We will go with one or two. So, there is one sentence which says that two macro enabled documents document file in docx format has delivered on the victim machine named as Lockheed Martin. or this salary Lockheed Martin job opportunity, it is look like a job advertisement. Email, this attack starts by executing this malicious macros, if user executed this malicious macro embedded in this word document, then the malware will perform a series of injection and achieves the startup persistence which were explained in the report for the in the target system. So after reading this, one can conclude with this set of TTP, which is user execution, phising, and the command and scripting interpreter, process discovery and process injection.

So this set of TTP were mapped for this part of the threat report. Then we can see how this user execution happened, where the target or user can only initialize the execution by downloading and opening the malicious document. Similarly, this peer-facing attachment, it is being delivered through the email and looking like a job opportunity. Then there is a command and control in which they were using some WB enables document where the micros has, they have used visual basic code to place the malicious shellcode. Then they perform, they list out the, whether this process, trying to get the information about specific process in which they are discovering a process.

This comes under process discovery. then they were performing process injection in which adversary is overwriting this function in the memory with their own cell code. Further, for the other parts of this report, similarly, we can map, we have mapped it for each subparts of the reports. There is a text present in the report and their corresponding TTP here and the details of how this TTP were executed in the victim environment. Once we are done with the all set of techniques here, till here, we identify total 34 TTP and which some of them might be kind of duplicating or repeating with the earlier part of the report. Once we understand this set of TTP techniques is being implemented by the attacker, we can go.

There are 19 techniques which we tested for this specific attack. Then in this above list, these techniques were identified from the document which explains the attack performed by a Lazarus scope. Then we will go one by one for each technique, see the detection and mitigation methods and see how one can suggest or give the recommendation, defensive recommendation. DLL injection from where the attack started. So, first we have to understand the process of the technique is being used. These steps were discussed in the previous classes in which we have to understand how this technique were processed during the attack.

So, the adversary here uses the created remote thread to start the thread inside the target process and inject a DLL file into the allocated space. Similarly, there are various DLL injection happens. So, we have explained each and every injections how it happens. Then we can see that all portal defensive options we have for this DLL injection. So on the website, on the technique webpage of this DLL injection, we can find set of detection and mitigation steps.

So we find these are the all set of detection one can implement on the infrastructure to detect the DLL injection. And this is the one of the mitigation which one can implement to mitigate such injection in the future attacks. And then we, after seeing this, what all these process access, process modification, behavior prevention on the endpoint implementation. So these things comes under detection and mitigation. And based on this, we made two recommendation that user must make sure that their access privilege must not be the same as the .

Like one needs to follow the list privilege principle that the user must should have only privilege which what they require for rather than giving admin to everyone and the user must protect their password with the administrator account. Further, there is more TTP named as native API. This TTP we discussed in the last class in which the malicious payload or the attacker is trying to leverage the legitimate API to execute the malicious actions. We can see set of defensive options present on the native API technique page. And on the set of mitigation we can refer to we can understand how what exactly is this test like implementing the behavior prevention on the each and every endpoint and the execution prevention in which we have to identify and block potential malicious software executed that may be executed through this technique by using application control tools like there are different tools which can help you to understand how this has been executed and for what purpose it has been executed.

And based on this detection and mitigation, we made two recommendations that if the user has a Windows 10 system or higher, then it can use the mitigation method described above to implement the countermeasure or the... mechanism, the user can use different tools mentioned above the to identify and block the potential malicious software. So, basically this you need not to remember this mitigation and detection techniques rather than you have to go and understand how action or a pattern is being detected, what all possible methods we have and based on you have to perform reasoning and suggest the recommendation.

Similar goes for this process discovery, we look for the how this process executed, this techniques executed, then what all the defense mechanism we have and then based on that we can make recommendation for each and every attack pattern seen in the attack, we have to make the recommendation similarly okay. And to making this recommendation, we need to have at least the idea of the victim environment. So if we go down, after reading the report, at least you will get some sense of how victim environment or the infrastructure were set up. But there will be some part which there will be not much clarity in the report. So for such cases, you have to assume a specific scenario that we are assuming that this scenario was present in the victim, and based on that scenario, you have to give the recommendation.

Like for some of the recommendation, we may give the recommendation that implementing SIM tool or the endpoint monitoring system. So for such cases, you can make an assumption that they already have a SIM, but their SIM fails to detect the attack, and this happens. In that case, you can suggest them to either like they can develop their own SIM with their R&D team or they can switch to the better SIM tool or the better vendor which provides to detect the sophisticated attacks or even the advanced attacks, similar kind of things you can give the recommendation. So this recommendation depends on the technique, what exactly technique we are talking about, what all the detection and mitigation steps we have.

plus what all assumptions we are meeting. So, if the same for the same attack 2 person is making 2 different assumptions because we do not have a ground knowledge of the victim environment. So, the recommendation can be different for both of them and in for both of their both of their recommendation will be correct based on if the recommendation aligning with the their assumption and the detection and the mitigation methods of that specific technique okay. So for this case, so just to remind you that we mapped it masquerading because they masqueraded it as a that this attachment is a job advertisement from Lockheed Martin company. So there are several techniques and we made Yes, so for assumption you can see we listed out assumption related to the victim organization capability and what all constant they have. So we assume that they already have antivirus, they have ability to see and change users, user have ability to see and change their own privilege.

They, we may, user may be using some email gateway to filter out spam email. Similarly, we can make this assume the constraint about the victim environment, like user does not have enough resources to monitor each and every execution or function call at the process label. So in that case, if we have this assumption, what exactly we are going to recommend them? Similarly, users here can be a developer, so running arbitrary binary might be a part of work which this constant we already discussed during the class that there may be an environment where the arbitrary binaries are mandatory to get executed for the normal operations of the victim organization. So in that case, how we will deal with any arbitrary or the new or the unknown binaries, how we are going to see their behaviors before it gets executed in the user environment. Like we can create a sandbox, sandbox or isolated environments to get it executed first, get it analyzed, then only it can get executed in the user environment.

Something like that we can recommend. okay so this is all and till today's class the syllabus will be for the midterm exam if you have any doubt we can discuss okay so we can wrap up now Thank you for your time.