Practical Cyber Security for Cyber Security Practitioners

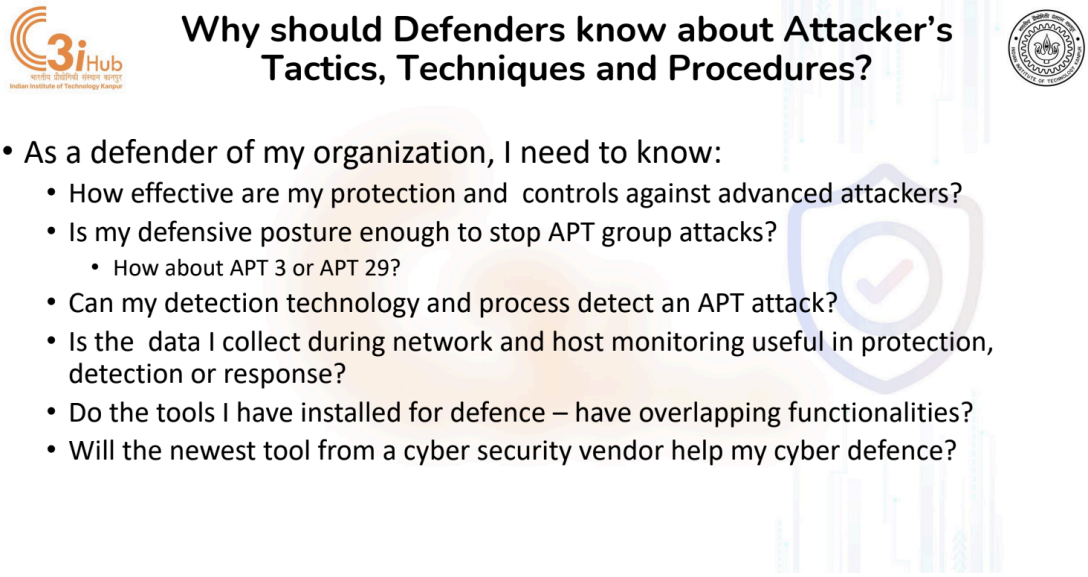
Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 06

Understanding MITRE ATT&CK: A Guide to Cyber Threat Intelligence



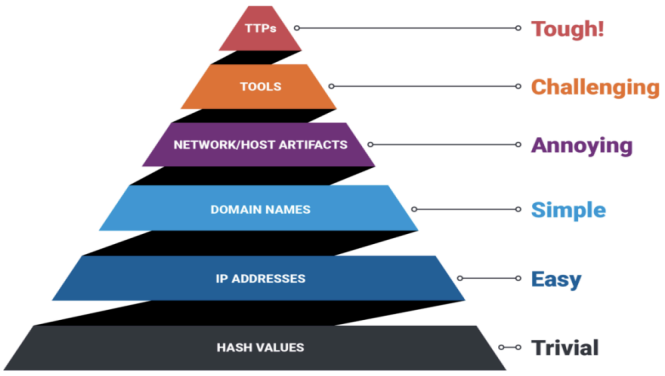
Hello everyone, so we started in the last lecture about MITRE ATT&CK and we discussed about what it is and where we are going with this module 3 so and then we talked about why defenders need to know attackers TTPs or tactics techniques and procedures and I explained that ATT&CK is actually a knowledge base framework, using which you can wrap your head around what the attackers do normally, especially the APT attackers. And we said that unlike CKC, which is a linear sequence of activities that the attackers usually do, here we are actually not giving a sequence. We are saying that these are the tactics or sub goals. that they try to achieve in order to achieve the final goal. And we gave examples of how Stuxnet can be looked at as a set of tactics that were applied against the Iranian nuclear enrichment plant. And each tactic is actually implemented using techniques.

What is ATT & CK?

- A knowledge-base of adversary behaviour
  - Based on real-world incident analysis based on a large number of attacks
  - Organized into tactics, techniques and procedures
  - Developed by the MITRE Corporation, USA
  - Available for anyone to use in developing threat intelligence, post incidence analysis, and developing defence tactics, techniques and procedures
- An attacker uses a series of tactics
  - Each tactic can be realized by some technique from a set of techniques
  - Each technique can be implemented with procedures from a set of possible procedures
- The Knowledge-base is community driven and continuously improved

Now, the first thing that I want to talk about in this lecture is something that you should remember if you are in the cybersecurity space as a career option. This is called the pyramid of pain. So pyramid of pain is basically a way of looking at what kind of threat intelligence, that is intelligence about the adversary that helps defenders, right. So, for example, so many times we say that this I want to detect whether a particular adversary is attacking me by looking at whether the malware they normally use is being used in my system or if there is any sign of that malware in my system, and the way to recognize a malware which has been seen before is to actually take the hash value hash function is applied on the entire binary of the malware that has been found in another system another attacked system people actually make that as a kind of a indicator of compromise that is if you find a binary with the same hash value then it is be that same malware that is in my system.

David Bianco's Pyramid of Pain



However, it is not very difficult for an attacker when he realizes that the targets are aware of the hash value of the malware they are using, they can easily change some values inside their source code and then recompile it and the hash value will be different. So if you have stored the hash value as a defender to actually wait for that particular hash value to appear in any new file that you downloaded. It does not work because what this trivial means in the bottom of this pyramid is that it is trivial for attackers or adversaries to actually change the hash value and therefore depending on hash value to detect a particular adversary is not a very effective approach. The other thing that we often detect. while analyzing an attack or while detecting an attack in the while is IP addresses.

So the IP address from which the initial emails came phishing emails came or IP address which was trying to scan my system or an IP address that is being contacted by a malware inside my which has been already put into my system, I can try to blacklist those IP addresses in my firewall and thereby not getting contacted by those IP addresses but Attackers who are very clever, so they continue to move the IP addresses, so the IP addresses from which they try to scan your system or IP addresses that they use for sending phishing emails or IP addresses from which control and command communication happens, they can be easily changed, so because you can easily get new IP addresses. So therefore depending on the IP addresses to detect presence of an adversary is also very unlikely to be very effective and it is actually that is why easy here means that the adversary for the adversary it is very easy to change the IP addresses. Similar is domain names, so domain names from which attacks are seen or domain names that are used in command and control server communication, those also can be easily changed, when we talked about this before that there is domain flux, there is that people use to continuously move the domain name and register a new domain name very quickly. Therefore, the domain names are also very simple for the attacker to change, not as easy as changing IP addresses or not as easy as changing the hash value, but it is quite easy. Then the network and host artifacts, Sometimes we actually see some artifacts related to the network.

For example, MAC addresses, it could be certain fingerprints of hosts that we can actually use as a way of detecting some activity of an adversary in my system. But even that can be changed by the adversary. Although acquiring a new host, or acquiring new network connection etc. is slightly more challenging for the adversary because he has to then subscribe to a different cloud, maybe a different cloud service and things like that. So, it is kind of annoying for the adversary, but it is not that difficult.

Now the tools that they use for you know doing the attack like for example in solarwind they use this one particular malware or one particular code that they inserted or in case of

Stuxnet or in case of the Stuxnet they use the Stuxnet worm that is one of the that is a tool for them. or the use of the black energy malware in case of Ukrainian power attack in 2015 those tools are expensive to build and so therefore if you are just going by the tool not by the hash value of the malware but going by the tools. ah like what exactly the functionality of the adversaries unwanted you know program that has been inserted into your system. If you go by that to recognize the adversary you may be more effective and for the adversary to suddenly go and develop new tools they do, but over time not necessarily like very quickly. So, it is kind of challenging for the adversary.

Now if you recognize the adversary by their tactics, techniques and procedures that they are using, then for the adversary to hide that or to change that completely is lot more work, because it takes them a long time to study a target, figuring out all the different sub goals that needs to actually succeed in order for the final goal. has to succeed if you, if they use those tactics techniques and procedures they are likely to use it in other similar targets same tactics technique techniques and procedures because it takes time to actually plan and build that capability so for the adversary that is the toughest challenge to you know do a mutation of their TTPs very quickly adversaries do change their TTPs over time, but at a very close proximity or in time, it is tougher for them to change and that is why this is in the top of the pyramid. So, this is called the pyramid of pain and this pain is with respect to the adversary's pain, not the defender's pain. So, going from bottom to top, So, what we are looking at on the pyramid we see the various artifacts or various evidences that we use for recognizing an adversary and on the right hand side what we see is that the gradual difficulty level for the adversary to change that quickly so that it cannot be discovered. So that is why TTPs are very important and as MITRE has come up with this TTPs, this own entire framework, now everybody uses that and many tools actually will tell you like when they analyze a malware, they can tell you what TTPs this malware is trying to apply.

or if they analyze an attack they can tell you what TTPs actually are being used in that particular attack. So, this is something that we normally use when we talk to other cyber security experts. So that we have a common language to describe what a particular adversary normally does. So ATT&CK matrix, this matrix is basically a way of organizing the various tactics, techniques, and procedures. So what you are seeing here is the 12 tactics that normally we see, actually it is less than 12 here, so initial access, execution, persistence, privilege escalation, so 4, defense evasion, credential access, discovery, lateral movement, 4, 8 and then 3, 11.

ATT & CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Disabling Security Tools	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
		External Remote		Exploitation for Defense		System Network				

So there are 11 tactics that are put in this matrix on the top. And below each of the tactics is a list of techniques that are usually used to apply that tactic right. Now what you are seeing here for example for under initial access you are seeing 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 10 techniques but actually if you drill down then there are sub techniques in each of these. So the number of techniques may look not so many like probably 11 times 13 or so. or 11 times 15 or so but actually there are more because if you actually look at like drive by compromise you will see there are sub techniques within each of these.

So, therefore, whenever we look at an attacker and how he or she worked on our system. we will always find that they have to get initial access. So, initial access would be through maybe a drive-by compromise, that is when you have an user in your system who goes to a website, And while in that website, something gets downloaded onto his system, so that is a drive-by compromise. There may be various ways to actually attract the user to that specific malware laden website, for example, by watering hole attack where the attacker sends very attractive emails saying that if you go to this site then you will get some money or you will get some health related advice or things like that and then when they go there.

they get compromised. Then the other way to do initial access is exploiting a public facing application. You have, for example, a web application which has a command injection vulnerability and attackers can use it. It may have a XSS vulnerability that the attacker may use or you may have a server and service running at a certain port where the service has certain vulnerabilities that the attackers come to know and then they can actually use that. You can also do hardware addition.

So this hardware addition is a very interesting one because recently it actually happened in UP in one of the cooperative banks. Some miscreants actually took a laptop and they came to the bank and at some corner there are ethernet ports on the wall and so they connected their laptop on the ethernet port and this is an area that was not like well lit and usually people do not come to that area. So, they put that laptop and the bank's network was not well protected. So, it was assigning a DHCP IP address to that device, any device that connects to its Ethernet. So, there is no authentication that was required to connect to the network.

So, now the attacker's computer is now on the bank's network. And then the attacker goes home and he turns on RDP or remote desktop on this machine. Attacker goes home and starts using RDP to connect to that machine and that machine being on the same network, then it tries to, it does various kinds of, finds other kinds of vulnerabilities and then moves from that laptop to important servers and eventually manages to siphon off funds from the core banking. So this was a very interesting case of a hardware addition. So similarly, if you are not careful about how you protect your Ethernet ports in a local LAN, you know, through a proper authentication mechanism, you might get hardware added to your system and then that hardware can be controlled by somebody else.

So, that is one way to get into this another case was that the Ethernet that was connected to the door of a bank. There was some kind of a device that was used to control access to the bank and that device was connected to the Ethernet. So some hackers actually went and used that Ethernet connection and connected their own device and that way they would hack into the bank. So this kind of thing can happen. Similarly, replication through removable media, this is the case of Stuxnet where the USB device was removable media is USB, it was used.

Spear phishing attachments, so you can actually know who your targets are inside the organization. Send and malware send a malware filled file like a PDF file or a JPEG file or whatever the word file which can exploit unpatched Acrobat Reader or unpatched Windows Office, etc. Microsoft Office, etc. Similarly, you can send a spear phishing link by which you actually do the drive-by compromise like the user goes to the URL, it has to be the email is made looking attractive. And with chatGPT etc, earlier we used to know that this is a phishing email when we used to see many mistakes, grammatical mistakes, spelling mistakes and so on and inconsistency in the writing style and so on.

But now with ChatGPT, etc, it's very easy for the attackers to actually craft emails that are very believable. So users have to be trained very carefully into recognizing this kind of thing. Spear phishing via service. So you can actually provide a service that the attacker uses. So then that particular service can be compromised.

So, supply chain compromise as we have seen in case of solarwind that the solarwind company was created an update of the solarwind the software this update server was the development servers were compromised and this develop the they added the adversary in this case probably APT28, the Russians they added additional 100 lines of code and this code was actually basically malicious code and then the engineers they did not probably had already done the code review before So, they did not do an again code review and they did not notice this additional 100 lines of code and when that code was compiled into the update and the update was pushed to various users, the users got compromised. So, this is a supply chain compromise. Various cases when you download free software from GitHub or various other places. It has been the case that many times the various GitHub accounts which are not properly protected, the code that is being supplied to users actually has been contaminated with malicious code, so that is another case of supply chain compromise. Trusted relationship, so when you actually have a relationship with a vendor or something, you actually use the vendor as the carrier of your malware.

Because of trusted relationships, people might actually not assume that there might be a danger in using their software or their USB into their trusted machines and that could be a problem. and then sometimes you can actually do enough reconnaissance to actually get the password etc. of a user and thereby you first get into a user's account and then you start downloading payloads into the user's account and from there you do all the other compromises. So, all I am by telling you all these 10 different techniques for initial access. And if you go to MITRE website and open these you will find a lot more information and a lot more different procedures to actually realize these techniques and also there are sub techniques within each of these.

So, similarly to execution like once you have the initial access you have somehow put the payload into one machine at least in that system in that network. Then you have to do execution. You can do various kinds of script based command line executions. You know all kinds of stuff then you have to create a persistence. So, you can write something on the shell, the login shell or or the shell the login script or shell script or you can inject the malicious code into well-known DLLs, all kinds of stuff, browser extension and so on. Similarly, once you have done a persistence but you are still running under the same privilege as the user you actually used as your initial access, so you may have to do a privilege escalation, there are multiple different techniques to do privilege escalation. Now defense evasion you have to hide yourself from, for example, endpoint security agents or from antivirus agents and so on.

So, there are various techniques by which you can do that to evade defense you can even change some of them. binaries you can turn off the antivirus. A very common thing is to

turn off the antivirus and so on because if you escalate your privilege you can do that. Then you can also do credential access. Credential access means that there may be a shadow file or there may be a database of credentials which you can use and send it back to your command and control so that more access can be achieved into the system. You can do discovery of various things including policies and including files and databases and so on and so forth. Then you may also have to do lateral movement because your actual target like in case of this Stuxnet, the actual target was the Windows system, Windows 7 system which actually had the PLC loading capability.

They actually exploited zero-day vulnerabilities in Windows 7 as well as the Siemens PLC program. So all that stuff can be used to do movement inside the network. Then if your final goal is to do exfiltration of personally identifiable data, for example, in that case you would actually So, collect various things for this and then do the exfiltration. So, exfiltration is next and then you also have command and control and then there is one that is not shown here is the impact, so that is where the 12th one, the impact is what we called in the CKC, we had the last one that is to actually do the harm to the target and that is what is called impact tactics here. So, we will see a lot of these many times over you know during this module as well as later on but what you see here is that even though I described them in a kind of a sequence you could see that one could actually do this in a different sequence.

So, as I was describing that privilege escalation and persistence can be in different order. So, similarly, defense evasion can be done in the very beginning or if you are getting into an administrative access account first, you may not do credential access because you already are inside, you may not want to. But in case of the Ukraine attack, if you remember, there was credential access for VPN credentials. which then was used to get into the actual target network. So, you can do credential access, but you may not need to do any discovery because you already have done a lot of research on the structure of this system or if you are actually launching your malware into a system which is not connected to the internet, so you have no command and control.

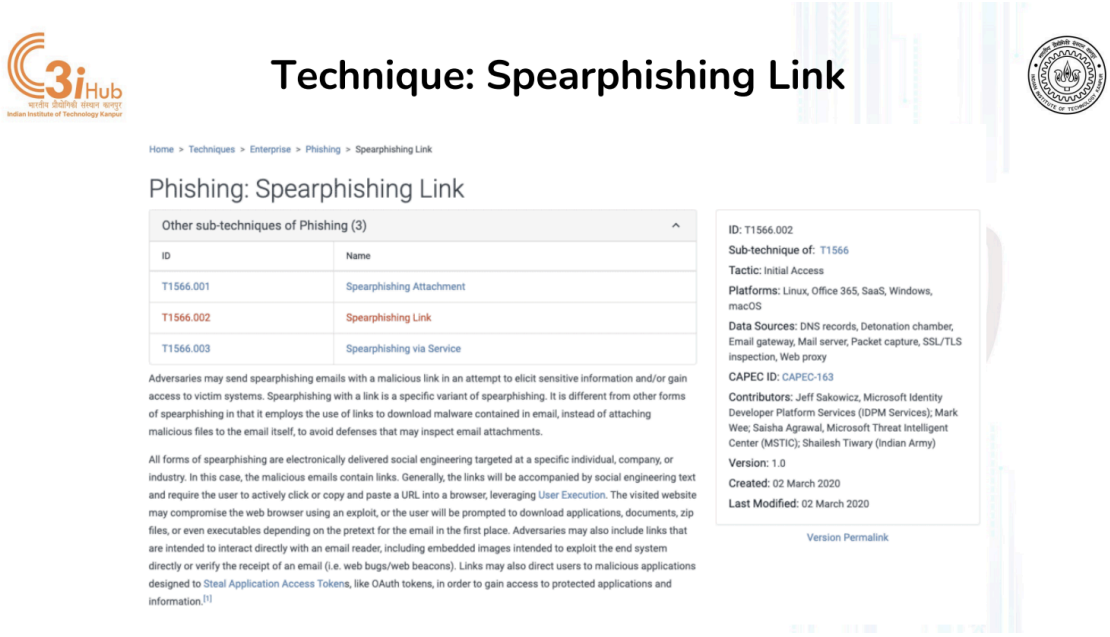
visibility into that network. So discovery will also not be useful because whatever you discover you cannot tell your command and control because your system, the network that you are in is disconnected from the internet. So all these different tactics may not be used. or some tactics may be used in different order or some tactics may be used twice. For example, if you do credential access, then you might do further weaponization and further initial access into other parts of the system.

You may do lateral movement much earlier. You may not do collection if exfiltration is not your goal. Command and control, in some cases command and control is not

required. or the system is not internet denied that you cannot do command and control. So, all these different tactics are not necessarily used in every attack or by every adversary and that is where the way of recognizing or attributing who the attacker is. comes from, because every attacker has you know different sets of tactics, techniques and procedures that they use.

Sometimes they may attack two adversary groups that may have very similar ones because they might have branched out from the same. Sometimes they actually another thing the adversaries very advanced adversaries do is that they do false flag operations. So, they would look like it is coming from another group, but actually it is the group that is already known in that case they actually have changed their TTP very fast. So, even in the pyramid of pain we say that the TTPs are very difficult to actually change. but some very advanced attackers can actually very quickly also change TTP.

So, in that case we have to do further investigation to realize that such a false flag operation has happened. So, these matrix you will see a lot more. We will just show you how you can know more about these techniques and so tactics are only like 12 plus 2 that is not shown here which is reconnaissance and the weaponization so they do not call it weaponization they call it. They call it, I guess, preparation or something.



So there are basically 14 tactics here. So 14 tactics is not difficult to remember. The tactics names are good enough mnemonics for understanding what roughly these tactics are for. But each tactic has this number of techniques, sub-techniques and so on. And actually in order to, sometimes some techniques may be used by two tactics. Like some techniques may actually apply to execution as well as can also apply to, for example,

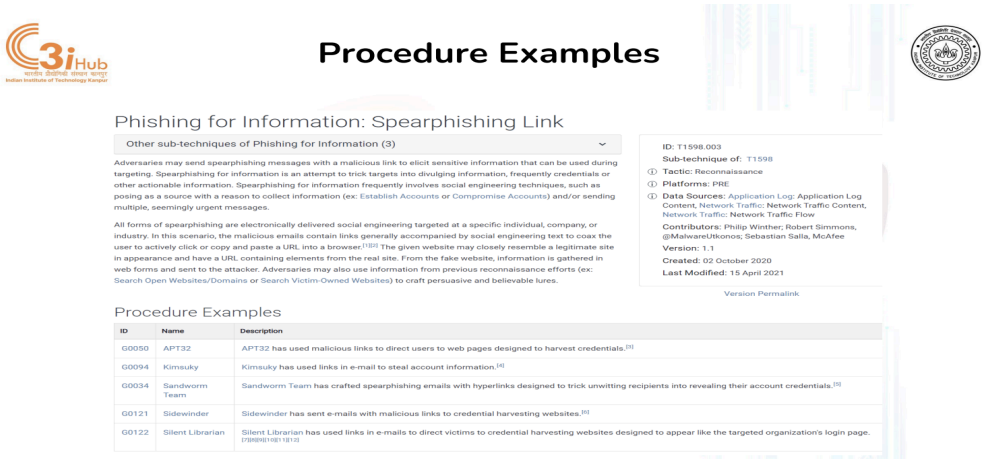
persistence.

So, those are also there. But what you will see in all this is that, you have to drill down to the techniques and procedures to actually understand what the attacker actually does. And so here, what you are seeing here is basically from the attack.mitre.org website. So, these are enterprise TTPs, in this there is phishing as a category and then there are sub categories or sub techniques like spear phishing attachment, spear phishing link or spear phishing via service.

So this as I said that this is a knowledge base so you have all these different things you can actually figure learn more about for each of the techniques. If you become a defender you know as a career option then you probably would have to know all these techniques very well in order to also recognize them as you see them. Now MITRE also has a very good like nomenclature and identifier for each of these, so each tactic and technique and procedure they have a number, so in this case this is T1566 is a, is the number for identifier for fishing and then because of sub techniques you will see 0.

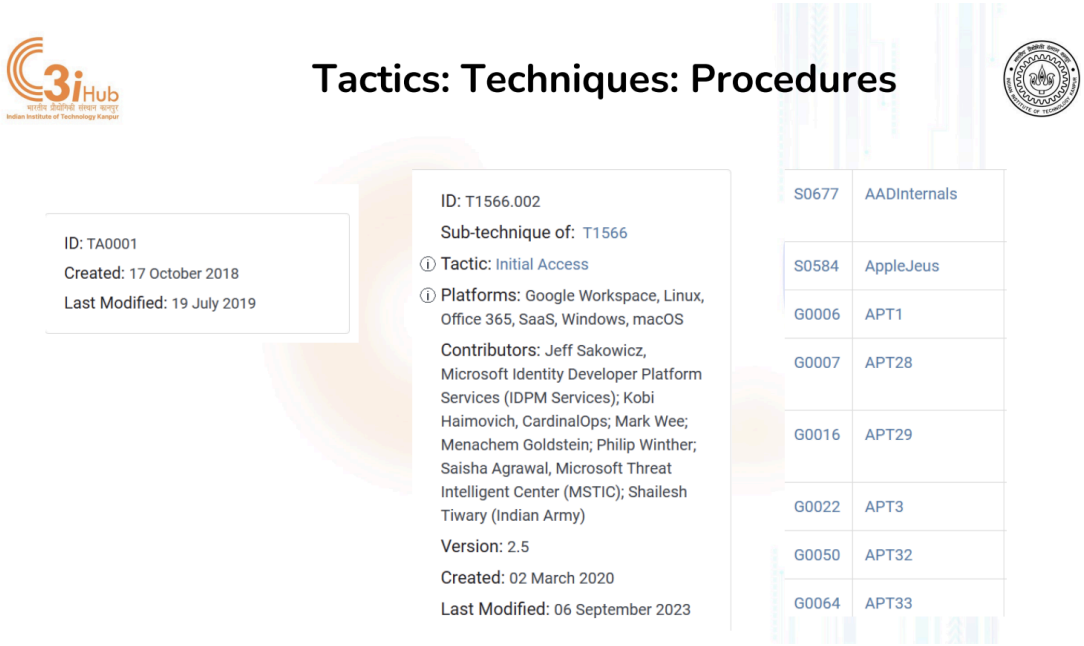
001, 0.002, 0.003 for different sub techniques. So, you see these are all sub techniques of T1566. You can find also this information like spear phishing link in this case is sub technique number 2 of 1566. It will tell you what kind of platforms it works on, what kind of data sources can be used to detect these. There is also a CAPEC ID.

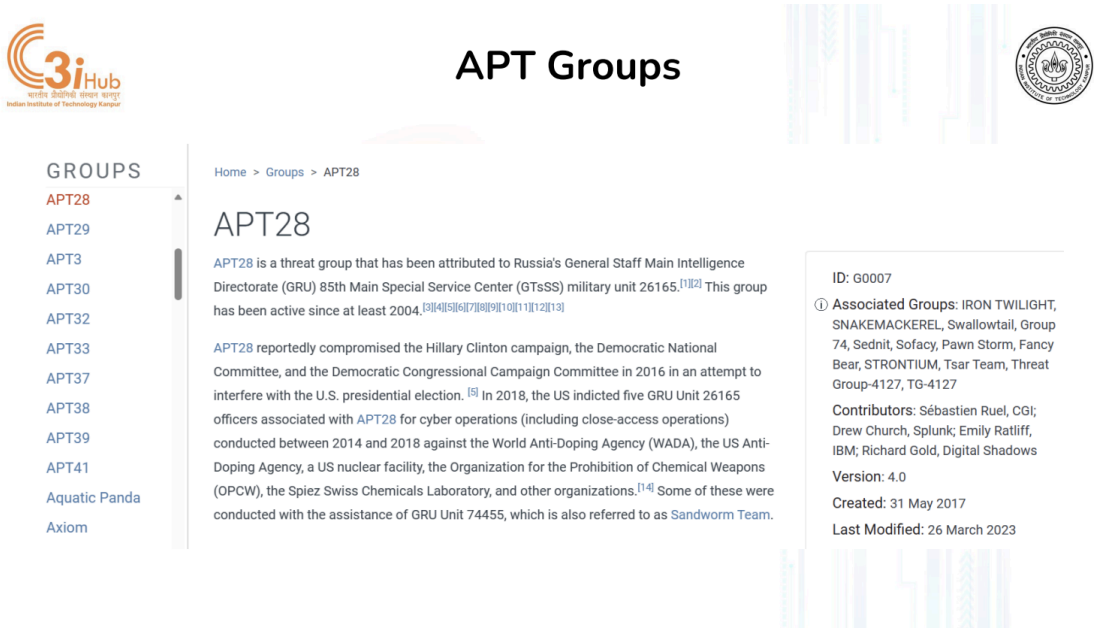
So this is, we will talk about CAPEC later. And this shows who are the contributors of this particular write-up and nomenclature, etc. So, this is a version from 2020, there is also a new version, but the numbers have not changed in the new version. So, for this one at least it does not matter. Now, here is a procedure. Procedure is basically how a sub-technique is actually done.



So, it is a detailed description of how the sub-technique is actually done. And so, here you see that this is part of the reconnaissance tactic. The spear phishing could be a part of a reconnaissance tactic. It could also be part of the initial access tactic. And then here you see application logs or network traffic, these are the places where you may be able to find that spear phishing link is being sent.

And in the procedure examples, so they say that okay this is the procedure ID G0050, it has been observed, this is an example like others might have also used it but APT32 has used malicious links to direct users to web pages designed to harvest credential and there is a link to the actual story from which this has been curated. So it will show you the procedure example. There are too many so they do not have an exhaustive list of procedures but they have example procedures and an example description of who might have which trade group might have used that procedure. So you see that here you have all this you know tactics this is basically a tactic, tactic is numbered by TA some number then you have the techniques and then within techniques there are sub techniques and then there are procedures so these are some of the procedures this is like So, you do not see what is else is in the table it basically has examples of how APT 1 use this procedure or what this G0007 procedure is like and where APT 28 used it, but does not mean that only APT 28 used it just an example. And then you can find also information about so far known APT groups.





So, APT groups like I discussed APT 28 in the past. So, it is a threat group that is from the GRU and it has this attribution is pretty certain. So, here are some examples where they actually have done attacks like Hillary Clinton's campaign Democratic National Committee servers also and US actually attributed and indicted 5 officers of GRU for this operations and so here you will find in the same website when you go to the groups tab and then you go to a particular group you will find all these details you will see the group ID and you will see associated groups. Now remember I already discussed that this APT nomenclature comes from the FireEye or Mandiant they actually call this once they see a lot of attacks then they based on the similarity of the attacks they cluster them then they say okay this attack here and this attack there looks like from the same adversary and because I see a common malware or I see a common C2 the command and control infrastructure or I see the common you know geopolitical reason why such attack happened or I see a common time when they actually do are most active. Or I may see that the command and control systems are located in such and such location or I have seen in another attack this same was used, so they basically clustered them.

When you cluster them, that does not give you the attribution. It only gives you an ability to tell that this attack here, this attack there, and this attack there, they are all from the same adversary with very high probability. As I said, there could be false flag operations and so on. So you may go wrong, but when you become a threat intelligence expert, and there are few famous threat intelligence experts around the world, especially in the US, They are very good at actually looking at this and looking at various attacks and figuring out that they are from the same adversary, so they clustered them. When they cluster, after the cluster becomes big enough, they actually start giving it a name. So Mandiant or FireEye has a tendency to give them names with numbers, so say APT1,

APT2, APT3, etc.

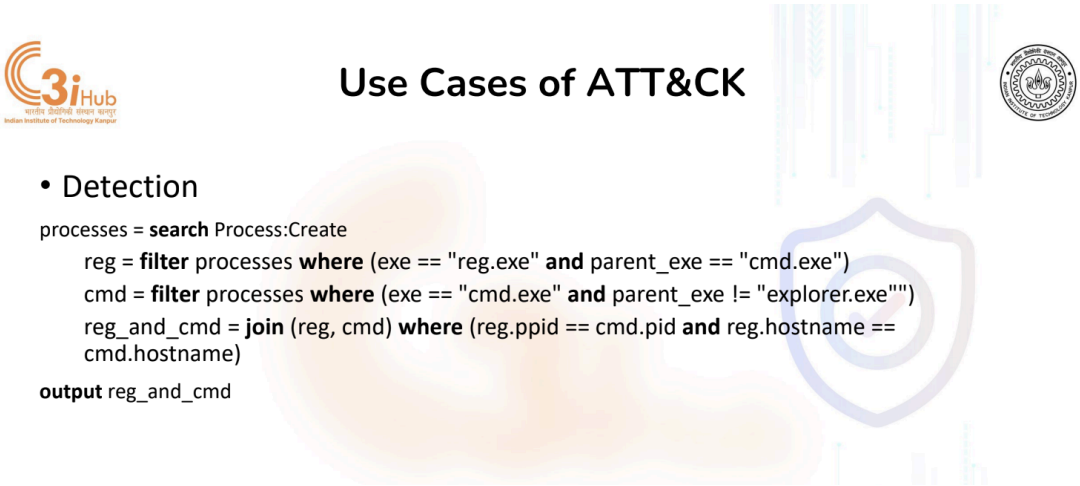
Now when another threat intelligence company they work at they are also looking at multiple different attacks, maybe some other attacks that these guys did not see and clustered them they might call it something else because they do not know in the meantime these guys have called it APT 28. So in this case for example the fancy bear is one of the common names for APT 28 or strontium There are some other names as well Iron Twilight and so on. So many times we do not necessarily say that Fancy Bear and APT 28 are this one and the only one and the same but we say that they seem to share common infrastructure, common malware or style of doing things, TTPs are very common and so on. So in that case you may say well Fancy Bear is APT28 more or less sure or maybe it is slightly branched out of APT28, so we do not know, so they call it associated groups. But when they call it associated groups, it is probably likely that they are the same or they are somehow related in some form.

So, that and so you can find this kind of information like which are the other, what are the other names given to similar clusters by other threat intelligence agencies. Also for each of the techniques there are mitigations that are described in this knowledge base. So, it is a knowledge base. tend to be pretty comprehensive. So it will say okay so you must do an audit to ensure access to data and resources are limited based upon necessity and principle of least privilege and so on.

So restrict web based content. or do the right software configuration like email configurations but this is not your email configuration as much as the email that the

attackers are using spoofing. Their configuration also is important here. It also says how to detect if that technique is being applied. So where the data source would be, where you should look to know that this technique is being applied, what would be the data component and what does it detect. So the mitigation and detection advisors are also in the same knowledge base.

So before we go into use cases, I want to summarize. So attack.mitre.org is a treasure trove of information about how to recognize adversary behaviors in terms of a framework that is the ATT & CK framework. So that when you analyze an adversary's activity in your system very clearly, then you actually can see that to achieve their final goal and you may not know their final goal if you have already stopped it in the middle of achieving that goal. But in some cases it usually achieves the goal like in case of a solar wind attack for example. So in such cases what you would see is that you will with the knowledge of ATT & CK tactics techniques and procedures you will start seeing that I can describe what they did over let us say 10 days or 10 months whatever into achieving that that they actually went on by achieving sub goals and so those are the tactics then you will see if how did they did achieve that sub goal so you look at the techniques and that way you can actually discover the TTPs of of this not only that this knowledge base also gives you a very good curation of which adversary groups use which kind of techniques and procedures so that you can also try to not only recognize what tactics and procedures have been used but you may also try to guess at least if not you know finalize that which attack group might be doing this and also the same knowledge base also tells you what are the mitigations and detection process for each of the techniques so that you can if you see that that technique is not being detected in your system your SOC or security operation center did not detect that some technique is being used next time you have to look at a different data source probably continuously in real time so that you can quickly and early detect that a particular technique is being used And mitigation tells you like how to even avoid it right, so one is to mitigate that is you stop it or you can also see how it can be detected you know from the logs and you know network packet streams and all these places how I can detect that some technique is being applied.



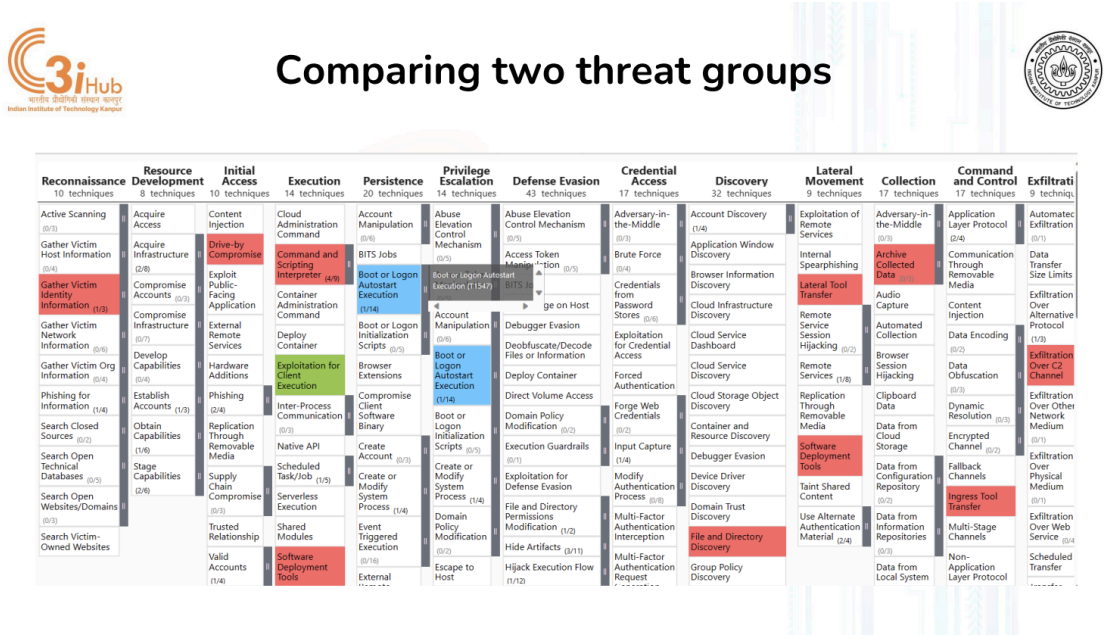
This knowledge base is about. Now, just to quickly go through the various use cases of this framework. What you see here is basically a script or query in Splunk. Splunk is a tool that often is used as a security and incident management tool. tool, so what this Splunk does is that it collects logs, it collects the network traces, it collects various information that is sent by the endpoint agents or network monitoring agents, it may collect the firewall rules and so on, firewall logs etc. And then it tries to put them in a database so that you can run queries on this to do whatever you want to do, like you may want to visualize the trend of various things like how often you get a spam email or how often you are getting scanned, all this kind of information you can visualize, can query this database with the specific query language to know various things. Now, Splunk itself cannot tell you what queries to make. So it is your idea of threat intelligence that will make you decide what query you will make. For example, here basically they are trying to detect if there is a process which is writing on the registry, and whose parent process is the command line. And it is trying to then get that information about this child and parent process.

So this is a query that can give you information about whether some process is writing onto the registry. So, this is what you may want to know, it is a little more complex than what I just described, but this is the query that can be automatically fired. So, you can write these queries and then automatically fire so that every time this query gets a hit, it will show you on the screen or may generate alerts and so on. But the idea here is that how do you know what queries to make? So if you understand the tactics and techniques that the attackers use, then in order to detect those, you can formulate your queries to see whether a particular technique is being used and so on. So knowing the tactics and remember the knowledge base also tells you that for a particular technique, what are the data sources that you should look at that would give you that will indicate that will have a some indication that this particular technique is being used or you can actually it also tells you you know what is the detection process.

So using that you can create this kind of a query so data is only as good as you make use of it right. So if you do not know what to look for in this huge amount of data that you collect in real-time from your network, from your endpoints, and from various logs that are being generated, then that data is useless. So to make use of the data, understanding ATT&CK can actually help quite a bit. You can also do what is called a comparison of two thread groups.

So this is actually we will come to that later. This is a tool called ATT&CK Navigator. In this tool you can actually say you can actually select the various techniques that a particular case used like so you analyze you do forensics afterwards and after an incident you then use this tool to click and select which techniques you saw in that particular

attack. Then you see another attack and this is the blue one, so you can color the ones that you have selected, so you coloured the first one with red, you coloured the second one with blue and then anything that is common for both, you will see the color will be a mix of the two colors, so blue and red, this became green. Now why is this useful because I told you about clustering right, so I see an attack here, I see another attack there, another attack there, I want to know if their TTPs match right. So if I capture their TTPs in this tool and color them in different colors and then put them together, then I will see like for example this one here and this red one here, clearly are not the same TTPs right I mean only one place they match right.

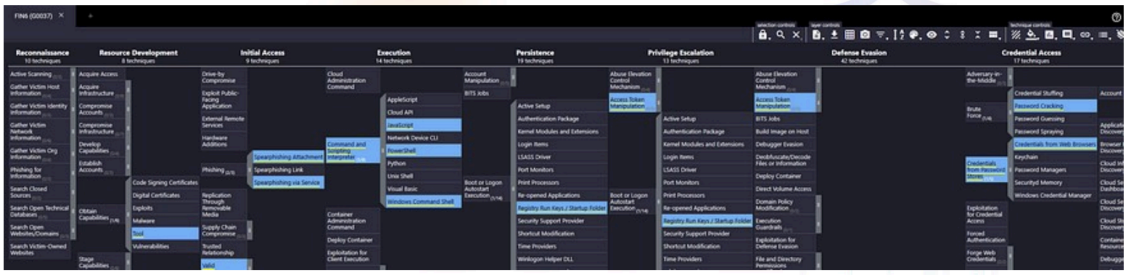


So therefore it is not like the same thread group so this is what the use of this TTP is to know whether at least TTP wise two particular attacks are similar or same. you can also do gap analysis and engineering defense. So like we discussed in case of CKC like when an attack actually happens then you want to use the you want to know you know which stages where the attacker was able to compromise or use and then you see how you could have stopped those stages to be successful. So here is the same thing for every tactic. So, you do not want that tactic to be successful in your organizational network. So, that is your goal and to do that you have to basically exhaustively look at all the techniques that are known for that particular tactic and you have to check whether you have adequate measures to stop all of them.

Now when you do that you will see that oh there are certain things for which I have no check, I am not doing any check, I am not doing any blacklisting or I am not doing any blocking or I am not doing any way to detect it, then you have to go back and do those things, do the mitigations, do the detection techniques, implement them and then re-discuss this again and then again look at all the techniques and tactics and see whether

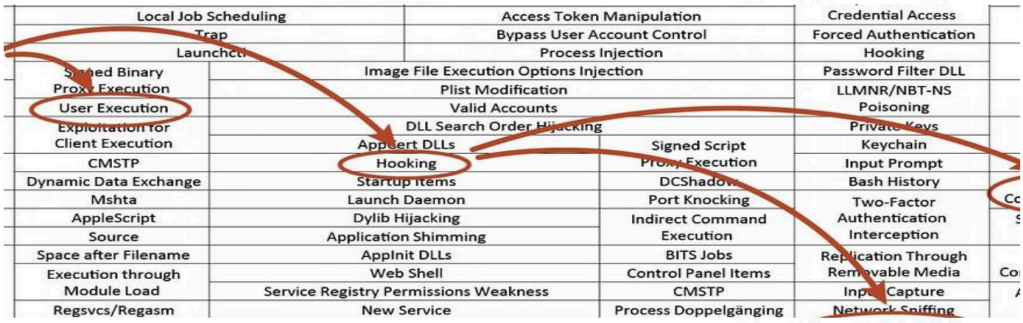
your enhanced defense actually can take care of all of them. Once you have done that, you have a good posture. Doesn't mean that you won't get attacked because this list is not necessarily all the techniques. As I said, this list of techniques that they list here in the knowledge base is a growing list. So if an attacker finds a new way of doing things that may not be stoppable by having the ability to stop all the techniques that are here, And also there are ways to actually circumvent if the adversary is too clever.

Gap Analysis and Engineering Defence



So therefore, it is not a 100% guarantee that if you do all this gap analysis and redo the defense mechanisms, you will actually get fully secure because there is nothing fully secure. But at least you are doing your due diligence and you are getting better. And then adversary emulation, so this is actually by looking at this ATT & CK navigator, you can actually point out that this is what the user did, this is how the persistence happened and this is how the They got the reconnaissance information. So you can actually draw this on this matrix to actually figure out what an adversary did.

Adversary Emulation



And then red teamers can actually use this. Let us say I have an organizational network. I want to know whether I am safe against APT 28. So there is some method called attack bridge simulation, so in attack bridge simulation you want to know that with how what are the techniques and tactics the adversary uses like in this case APT28 and then actually make those try to you know red teamers basically try to break your system, red teamers are your people but they try to break your system exactly following the path that APT 28 usually does. If they are successful, then that means you are not safe against APT 28. If they are not successful or partially successful, then you have to see where your defense failed.

That is the blue team's job. So there is a red team, blue team duality here. Red team is asked to emulate an attack. and the blue team's job is to actually if not stop, detect the attack. If they cannot even detect the attack while the red team is doing it, then you know that there is a problem with your detection also. So not only you cannot prevent, you cannot even detect. So that is something that also this ATT & CK framework allows you to, you know kind of frame the attack simulation for various groups in the form of these techniques right so that gives you a good way of otherwise you know if you tell the red team just try to break my system right so they will try various things but it is not it will not be very systematic.

So, but if you ask them to actually emulate a particular adversary they will go through this attack simulate okay. So, I think I am done for this lecture. So, next time we will go into looking at how to use this ATT & CK matrix to analyze the past attacks and come up with the TTPs that were used. So this is very important because remember we discussed that when an incident happens either to you or to another organization similar to you. then it is highly likely that same attack will happen to you as well, so therefore you have to analyze either the attack that happened to you or your similar organization and figure out what TTPs were used and then use those TTPs to do gap analysis to see whether you are ready to stop or at least detect those things, so we will go into that in the next lecture.