Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 12

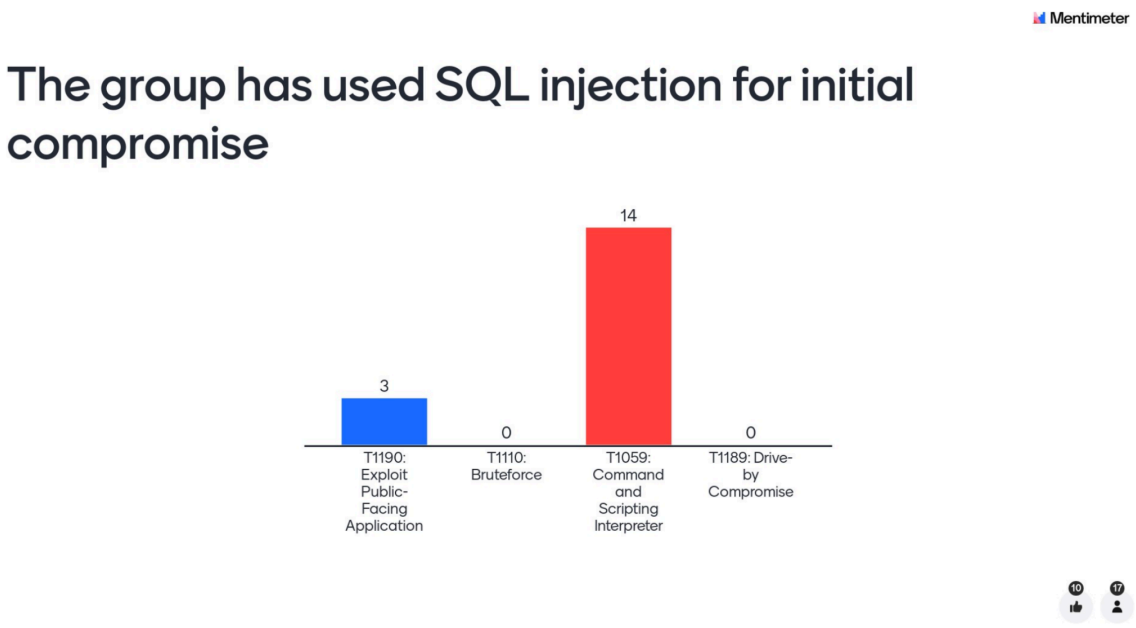
TTP Mapping & Introduction to Unified Kill Chain

NOTE: RESPONSES GIVEN BELOW ARE THE STUDENTS FROM IIT KANPUR WHO ENROLLED FOR THE COURSE. DON'T TAKE THE RESPONSES IN THE COMING SLIDES AS CORRECT. READ THE NOTES BELOW THE FIGURES TO GET BETTER UNDERSTANDING OF THE RESPONSES

So today we will do some practice and see how one can map TTPs from sentences. So this type of question and such practice will help you for exam preparation. So I thought to have some practice with you. So I request everyone to go to menti.com and put that code to enter into the quiz. Go to menti.

com, use this code 12362939. We'll see the first question. The first statement is the group has used SQL injection for initial compromise. So to get into the victim infrastructure, attackers have used SQL injection attacks.

So there are four options. First one is T1190, which stands for Exploit Public facing Application. The second one is brute force attack. The third one is command and scripting interpreter. And the fourth one is driven by compromise.



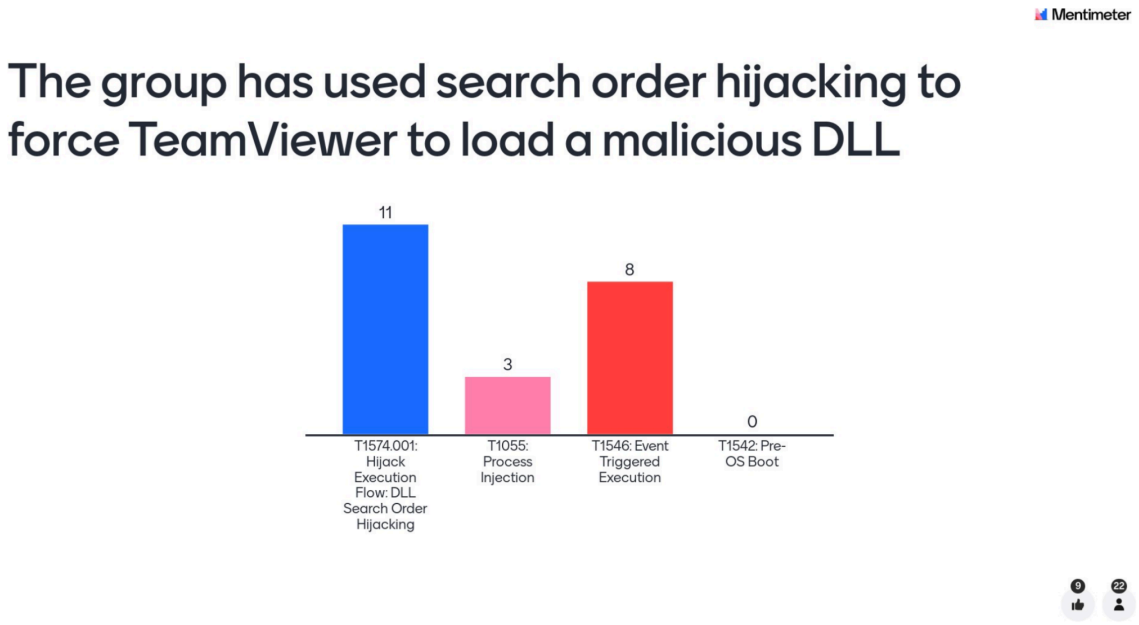
So you have to select one option which reflects behavior or attack patterns present in this sentence. Okay. Unfortunately, the majority is wrong that this is not a command and scripting interpreter. Actually, if you think more about it, there is an attack being performed, which is Sql injection. How does Sql injection one perform? Like there will be one application, a web application, which will be the target for the attacker and entry point.

On that web application, the attacker will perform Sql injection to get into the victim infrastructure. So this reflects this TTP exploiting public facing applications. So there is an application on the victim end, which is public facing. And because this is a public facing application, the attacker is able to interact with the application and leveraging this opportunity, the attacker is performing this attack. So, we have no information given in this sentence how they are performing SQL injection.

If they have mentioned that they are using some script or something, then one can go with this and this both, but if nothing is mentioned, we have no idea how they have done, but we have only idea that they have performed SQL injection using some web application. Any doubt? So we have no, this will be a wrong option and this exploiting public facing application will be the correct one. Is it clear? So we'll go to the next question now. One more thing I would like to explain is TTP, drive by compromise. So I will, even though these options are wrong, I'll explain this TTP so that you can get familiar with these things.

So a drive-by compromise happens when the attacker tries to convince the victim to do something. And because of that action, victims may get compromised, such as you see

advertisements, malicious advertisements. Attackers sometimes run malicious advertisements, adding some malicious JavaScript code in the advertisement, which they publish through Google Ad. And through that advertisement, once you click on the ad, link or advertisement picture, that executable JavaScript code will get executed in your browser and it will get into your system. So in the case where the attacker is trying to convince the victim to do something, like the victim is driven by the attacker, then it will come as a drive-by compromise, okay?



So the next question is, the group has used search order hijacking to force teamviewer to load a malicious DLL.

We have multiple options, first one is hijacking execution flow and this technique has a sub technique DLL search order hijacking. The second one is process injection, the third one is event trigger execution and the fourth one is pre OS boot. So, these are the 4 TTPs, one of them represents the sentence you have to choose. You have to read sentences carefully, understand the meaning and connect with the options given. I believe everyone is answered.

So if any of you can explain to me then why we go with this event triggered execution. Anyone out of the seven people? See, we'll be having a discussion, otherwise I'll be explaining the things going forward, and we may not have a fruitful discussion, because understanding the sentence's meaning, understanding TTP's meaning, mapping them, requires brainstorming and discussion. And practice also. Such type of question will come in exam, and then if you don't have practiced much, didn't have discussed much, you may have misunderstood the statement and may go with the wrong answer. Okay, no

idea, event trigger execution.

So let me explain what exactly this TTP is. This behavior is representing a pattern where attackers set some activity based on Windows events. Like they will set the execution of some binary. If an event happens in the WMI, Windows Management Instrumentation, I don't remember exactly the full form, WMI, where we set the events. how events are supposed to execute.

So, one can say that once this screensaver starts, execute this event. So, execution which is driven by some event like triggered by some event will be coming into this T1546. So, while reading this sentence we are not getting any sense that there is any execution being triggered because of any Windows event. Rather than we can see that the execution, the execution flow of the system is being hijacked and even this word, this search order hijacking matches here. So what happened in search order hijacking? Whenever any application is running in the system, they require some supporting DLLs to function.

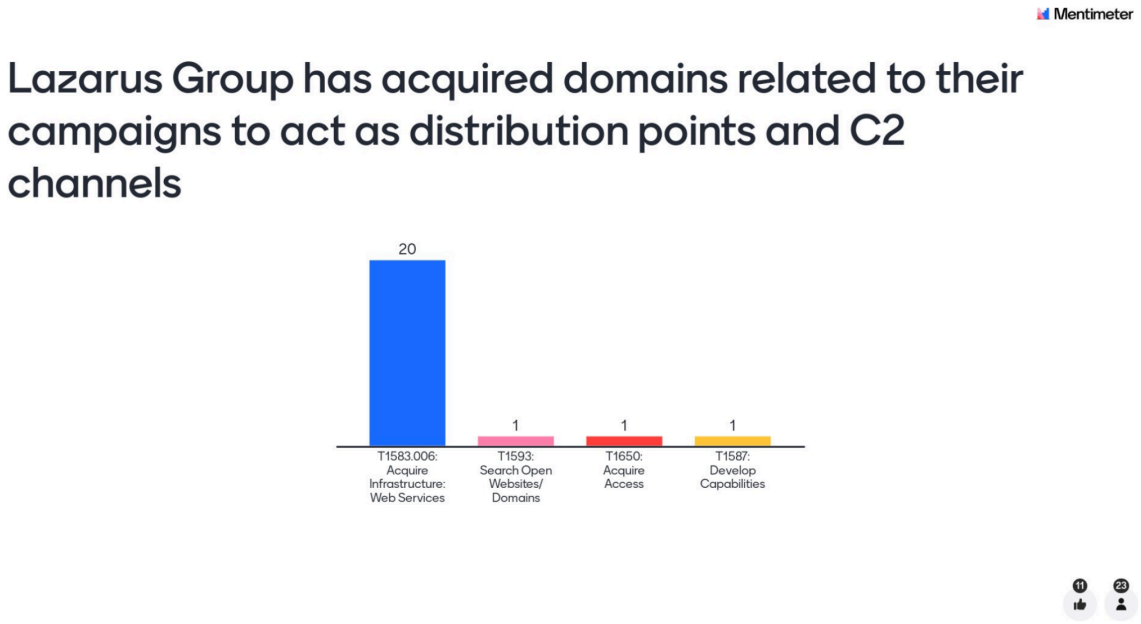
So what Windows does, they search this DLL on the legitimate path where this attacker supporting materials has been placed in the machine. What attackers do is, they place their own DLL with their own name, such as assume for team viewer, there is one DLL named as teamviewer.dll, just for example. So what an attacker does is create their own malicious DLL, the name is as a teamviewer.dll, they will remove that original legitimate DLL and place their malicious DLL on the same folder, the path where this OS is going to search for.

Okay. So in that case, they are trying to hijack the search order of the OS window machine. And this is a specific case for TeamViewer. In this case, they are using TeamViewer supporting DLL. They are replacing TeamViewer supporting DLL with their malicious one. Is it clear? If you have any doubt, you can ask me in between.

Okay. This is this, T1574, stands for hijacking execution flow. There are several sub-techniques in this technique. The first one is DLL search order hijacking, which aligns with this sentence, okay? This process injection, this usually occurs when attackers place their malicious code in a memory of a process. See, any process, if it is running in the system, they acquire some set of memory. So if there is some memory blank, like the whole block is not captured, then they place their own malicious code in that set of memory blocks where when this process will execute along with their own execution code, they will add those malicious code also in their execution.

An attacker will let that legitimate process do malicious things for them. Okay? And the fourth one is pre OS boot. In this TTP, attackers place their malicious code or malicious

executable in the boot section. So whenever this machine starts booting, that malicious code will get active. This is all kind of making a persistent connection with the victim machine.

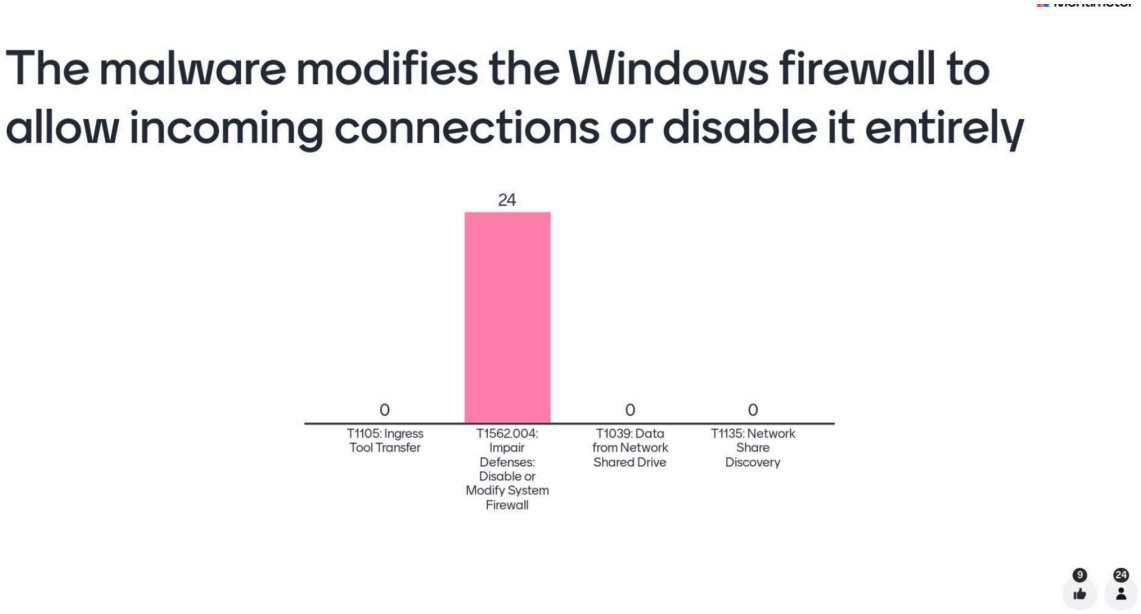


Is it clear? So the next question is the Lazarus group has acquired domains related to their campaign to act as a distribution point and C2 channel. So you have to select one possible TTP which is reflected in this sentence or this behavior. I'm assuming that people have practiced this, mapping sentences to TTPs. You have done your assignment too, because these things will be having a major part in the midsem. It would be a really fruitful discussion if you have, why you are choosing these options, if you can explain and justify your point.

I might be wrong, you might be wrong, we can discuss and we can come to the same conclusion. If you think that this option is correct and if you are marking any option, it means you have some logic or reasoning behind that. So, if you put that logic behind in front of us, then either you may get a clarity or I may get a clarity. Okay, so majority have answered correctly that this behavior represents acquiring infrastructure techniques for preparing for attack and inside this technique there are sub-technique web services to be very specific that they are acquiring a set of domains or domains for either distribution and creating the multiple C2 servers. But some people have chosen this search open website or domains, T1593.

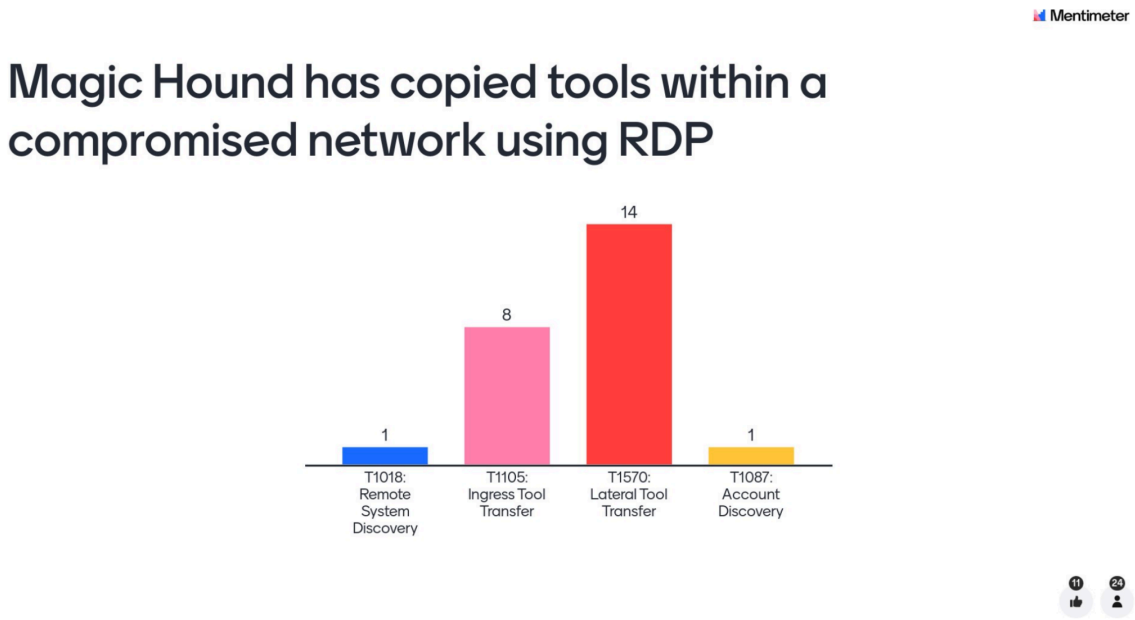
These techniques attackers use to gather information about victims. So they see some open websites or domains, if there is something like matching with their victim's domain,

they can get that or they can acquire access if there is a third way, if they can acquire access to the victim's infrastructure from a third party or from some, not a direct access kind of. And the fourth one is developing capabilities. In this technique, attackers try to develop capabilities to perform the attack. So like developing malwares or some zero-day vulnerability exploit can come into this technique, TTP.



So the next question is that the malware modifies the Windows firewall to allow incoming connection or disable it entirely. We have four options, you have to choose one. So for today's quiz, I'm going with easy sentences. So everyone has answered correctly that this comes under impaired defenses. And within this technique, we have a sub-technique, disable or modify system firewall.

This name suggests only. But if this sub-technique has not been given, then also you have to understand that there is a defense mechanism which is a firewall and which is being impaired by these attackers or the malware. Along with this, we have different options which I'll explain just to have an idea that another TTP was ingress tool transfer. In the ingress tool transfer, attackers download subsequent malwares from their C2 server through C2 channel in the data from network shared drive, in this technique T1039, attackers collect data from all shared drives in the victim infrastructure. Then in T1135 network shared discovery, attackers or malware discover what all shared networks drive or the network files or folders victim has.



So the next question is, Magic Hound, which is an APT group, has copied tools within a compromised network using RDP.

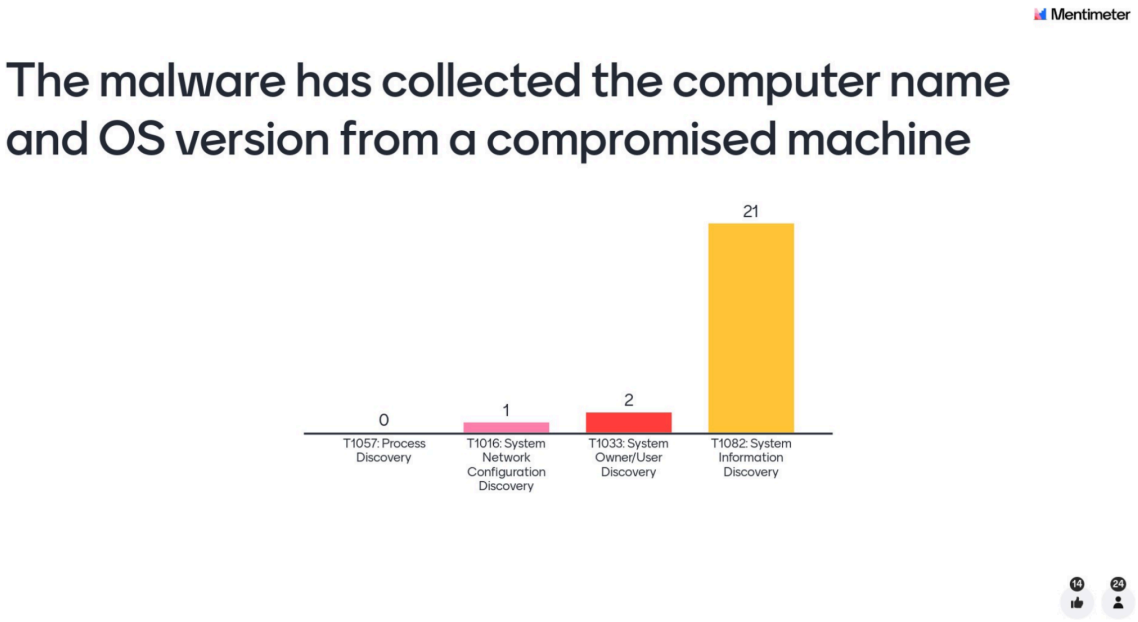
Please see this sentence carefully. Choose one option which belongs more, which represents more of this attacking behavior. You can discuss with each other if you have any doubt, or you can discuss with me if you have any concerns. Okay, so if someone can explain to me then why we go with this lateral tool transfer? Anyone? Please, yes. Okay, anyone, why do I import tool transfers? Just now I explained why ingress tool transfer, okay. So, just now I explained that ingress tool transfer is a behavior in which attackers download or capture subsequent malwares from the C2 server.

As your friend said, you can see here that the tools have been copied within compromised network infrastructure within the victim system. It means that tool is already placed on one of the victim infrastructure machines and from that machine they are using RDP connection to transfer tools within that same network. So in this attack pattern, they are not communicating with this external network to get the tool. And for this type of behavior, there is a specific technique named lateral tool transfer. So the correct answer is lateral tool transfer.

You have to understand the difference between ingress tool transfer and lateral tool transfer. So similarly, there are some techniques which are close to each other and might be confusing for you during exams if you have not seen and understand the differences between these techniques. Is it clear? So they are transferring laterally within the network only. That is why the name itself represents it. Then remote system discovery is a TTP

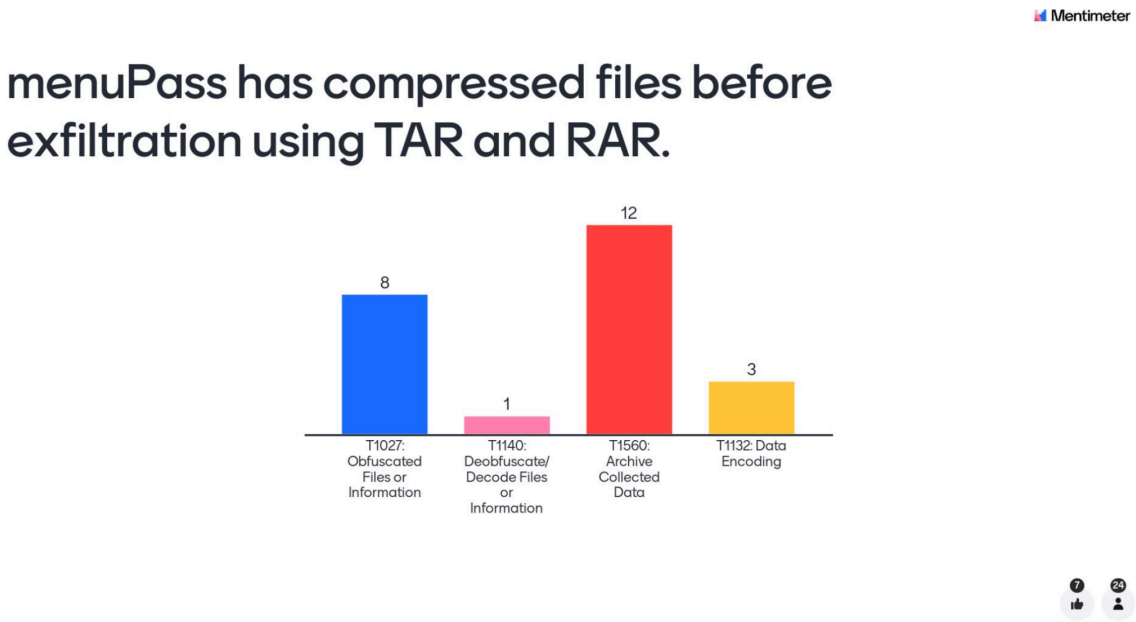
when attackers try to discover what all remote systems victim infrastructure is connected with.

The last one, account discovery, when they discover what all accounts, user accounts present on the machine, when they list such total user accounts on the machine, then this TTP reflects.



So now the next question is the malware has collected the computer name and OS version from a compromised machine. Okay. So if someone can explain to me then why this system owner or user discovery reflects this attack pattern which is mentioned in this sentence? Is there any user discovery at what users are present on the machine and who is the owner, who is the admin is being represented in this sentence? No, right? So this option will be incorrect. So we can see that they are collecting information related to the system: what the computer name is, what OS version has been installed on the machine.

So there is no discovery related to the network configuration or neither network configuration nor system owner or user discovery, okay. So the correct option is the system information discovery. Also sometimes attackers list what all processes are running. So like before masquerading their malicious executable with the legitimate process name, they do this discovery thing to understand what name you can go with. Also like before doing process injection, they do this discovery to understand what process they can target to exploit, okay.



Now the next question is menuPass who is an APT group that has compressed files before exfiltration using tar and rar. The attacker has compressed all collected files before exfiltration. You have to map the corresponding TTP. Done? Okay. Now you have to explain to me why data encoding? Please.

I'm expecting any answer, whatever you're thinking you can discuss. Otherwise you'll not get clarity. Why data encoding? Okay. We have to understand the difference between encryption, compression and encoding. Before going with the options which include these terms, encoding in which we transform the look, you can say, I'm not getting the correct word, but the way it looks, if it's changing, that comes into the encoding.

When we do encryption using some key and there are some decryption techniques, also even encoding, we have decoding techniques. So that will come under encryption. But when we are keeping data as it is, just removing the metadata, not removing, compressing it in some smaller size, then it will come in the compression. Okay, so encoding means if we have data and we transformed its look, how it looks. So this option is standalone, we have to discard that this does not come under the compression.

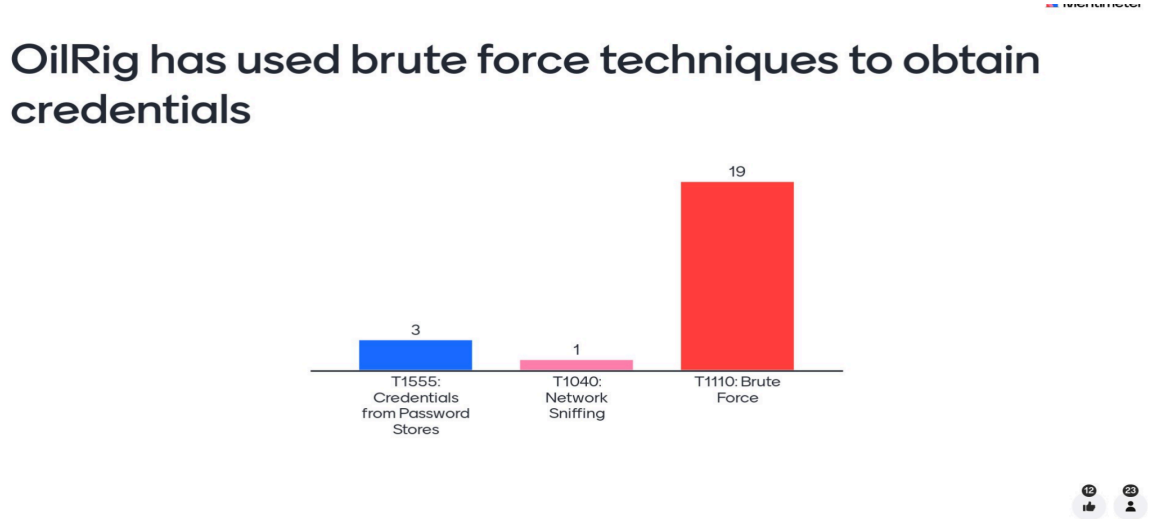
But there is a confusion between obfuscated files or information and archive collected data which you have to answer. Anyone can explain why this and others can explain this, please. Any insights, whatever you are thinking, why you chose this option, why you chose this option, just explain. Okay, if there is, because they are using tar and rar to compression, that is why you went with archiving collected data, right, okay. What about obfuscation then? Doesn't this compression also come in this obfuscation category? Sorry? Okay, any other option? Yes, but that compression also comes under this

obfuscation.

So we have to understand which tactics it belongs to. This obfuscation comes under defense evasion and this archive collected data comes under exfiltration. This obfuscation file and information represents that obfuscating the files by having an aim or the goal to evade the defense mechanism. Also even in this they are trying to evade, they do not want to get seen as a that we are said exfiltrating this data, but this comes this represents that if some malicious files or payloads is coming and they are trying to evade and this comes if some data is going outside the network and they are compressing.

So, the. Can be, can be, can be. That can be larger also. So they compress and send the payloads on the victim machine. So if they are doing that behavior then it will comes under this, obfuscation file and information because they have obfuscated some file or information to hide defense, hide from defense mechanism and here they are doing compression for the purpose of exfiltrating the data because here the archiving and compression is being done on collected data like victim's data. And here in the obfuscation, the obfuscation methods will be performed on the attackers payload or exploit. Sorry. Defense evasion and obfuscation, yes, exfiltration can go in parallel, yes.

Yeah, but you have to understand this, this obfuscation being done on what? So this is mostly being done on the exploits which they send and this is being done on the victim data which is being, which is about to get exfiltrated to this attacker server. Sorry, sorry, can you please repeat? Yes. Yes, so these two behaviors can go together, but here the sentences which we have given, here we are not talking about anything evading the defenses. Like here this menuPass is not trying to hide itself by using any method. So these two things can go parallel. But the methods which are being used to evade the defense mechanism and for this exfiltration will be two different.

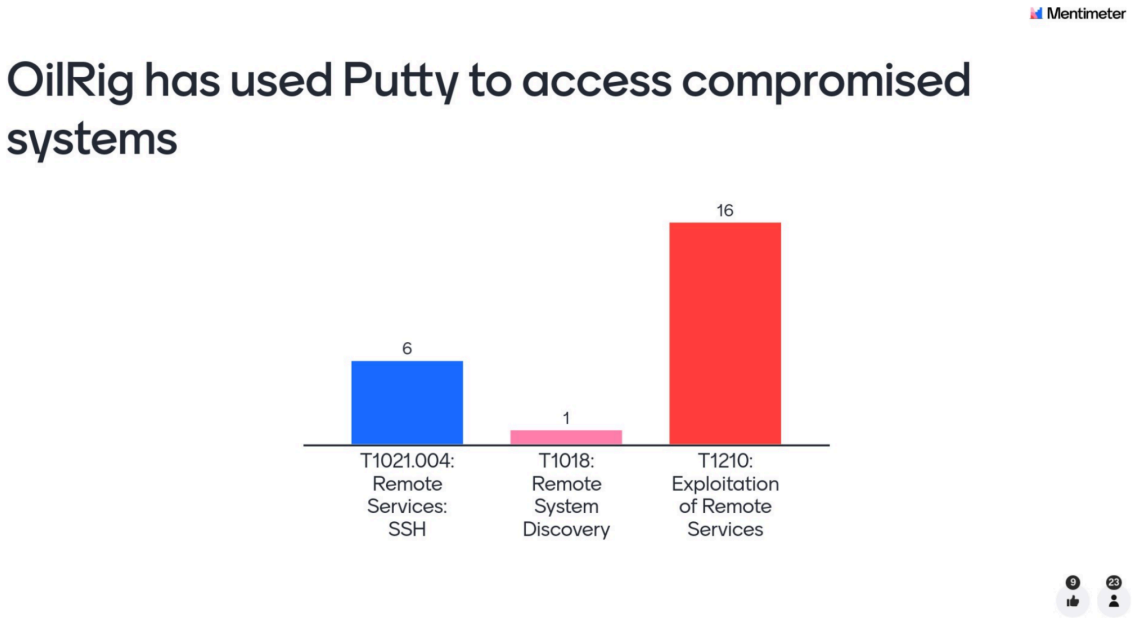


Now the next question is OilRig which is also an APT group that has used brute force technique which is too obvious for these options to obtain credentials. So this comes under credential access tactic. Attacker is trying to access credentials using some method mentioned in this statement.

So the majority are correct that these options represent this brute forcing method, brute force. This is the correct option. There is no network sniffing. Network sniffing means when attackers try to capture traffic, network traffic of the victim infrastructure to understand and to see what all things are being communicated and being in transit in the network.

So that comes when in network sniffing. Credentials from password stores. So there are some password managers or there are some application who saves your password. Like many people, there's a password saved in the browser. So such stores may be helpful for attackers to collect the credential, to get access to the credential.

So this T1555 represents this technique. So there is no such method being represented in the sentence. Rather than the attacker is brute forcing the credential, then this brute force option will be correct. Mostly techniques, they explain themselves by the name itself. If you understand the name, you can go with it.



Now, the next question is OilRig has used Putty to access a compromise system. Putty is to get remote access using SSH in the windows machine. It is a software.

Okay, so the majority have answered this T1210 exploitation of remote services. You

have to explain to me why. Anyone? Why this option? Please explain. There are 16 people who are going with this option. So please let me know, please explain why you think that getting access to the compromised machine using PuTTY represents this exploitation of remote services.

Come on. No idea? Did you choose randomly? Do you like this option? Okay. Exploitation of remote services represents when attackers exploit or they find any vulnerability, they use that remote services to either invade or get access or do some malicious action. So when, is there any remote services present on the victim machine and they are exploiting that remote service, like they're finding any vulnerabilities or any zero days or this DLLs one which we saw, they were using TeamViewer, they were remote service. So they were exploiting in some way that remote service to do some malicious action. But if you see in this sentence, they're just using PuTTY to get the access.

They're not exploiting it. who is giving the remote access, they are using that with some credential which they found in some other space. So rather than going with this option, this option seems to be more feasible than remote services, this technique remote services T1021 represents that attackers leverage remote services to use or access the system. And in these remote services, we have various options to get that remote access.

One is SSH. They are not doing anything with that remote service. It is as it is, as we do access, they are doing just the same. And the third option is remote system discovery in which this, I guess we discussed this, they list out and see what all remote systems are connected with in the victim. So this will not be the option. Is there a clear difference between this and this? So there will be some confusing TTPs which you need to get. Once you understand, do practice, you'll get to know which TTP is conflicting with which and for which set of TTPs you have to be more careful while choosing the option.

The next question is Turla, which is also a APT group, has exfiltrated stolen files to OneDrive and 4Shared. Please choose the correct option given here. There are four options we have. Okay. So majority have answered correctly that the exfiltration over web services, this cloud and this OneDrive is nothing but a web service.

So in this behavior the attacker is exfiltrating or sending victim data on one of the web services. So we can go with this exfiltration over web services. This exfiltration over physical medium, this happens when attackers are physically connected with the victim infrastructure and they are transferring data like transferring data into USB or any hard drive. So if there is an insider threat in the organization, this may happen. But if an attacker is sitting remotely somewhere and they're exfiltrating data, so in this, for this statement, there is a web service being used, so we'll go with this option.

So there is no physical medium between attacker and victim in this case, okay, clear? So we have another one is schedule transfer in which attackers schedule transferring data like in the infrastructure. If there is an organization, there's a high chance that there will be no or less communication in the non-office hours. So mostly attackers schedule their transfer for some unusual time when there is not much activity in the network. Or even sometimes when there is a lot of activity that there is a busy network and in that busy network they may do this transferring thing. So once they schedule transfer based on the victim and the scenario that behavior comes under this scheduling the transfer and the automated exploitation when they use any automated tool or any automated scripts to automatically transfer whatever files they are discovering just transfer it to the C2 server.

Okay. Yes. So there will be insights and the context of how they are exfiltrating the data. So here there is no insight. This is just a statement that they are using some cloud service to exfiltrate the data. So there is no insight regarding how exactly they are transferring.

This is just because they are transferring to some destination. So tomorrow we will see some sentences in which more than one TTP is mapped and in such cases you have to choose multiple options, all TTPs which belong and be represented in the sentences, okay. Also if you have time, yeah we have 5, 4 minutes. So we can just see the UKC introduction. So how are you guys preparing for MED-SEM? How are you doing practice? Are you going through the MITRE knowledge base website? Why? Why? That is the only resource you have.

You should go. My suggestion is just, this is just a random suggestion, but if you wish you can take, you should go to, where is this group? Yeah, this attackers groups list. These are all APT groups. You can go randomly with any group like APT 19.

This is a Chinese group. You see what they have done till yet. So there is one option. This technique is used. You see that this technique, why this technique is represented, what exactly they did. There is a list of behaviors which these groups have performed in the past. They are corresponding TTPs.

If you're not understanding, go to this TTP webpage and see what exactly this represents. Go back, see what exactly this sentence represents, match both and understand why this sentence and this behavior has been mapped to this TTP. There are around, I believe, more than 150 groups, 143, sorry. There are a total of 143 groups. If you do this exercise with all groups, you will be good to go. For Midsem and even doing this practice you will get to understand which techniques are being used frequently because all these 200 like 190 plus techniques are not being used like with the same pattern with the same frequency no.

The popular techniques you will get to know once you do this exercise are okay. Now I'll just introduce UKC in today's class and then we'll see details in tomorrow's class. Also we'll do some little bit of practice in the next class because today we spent the whole time getting into the practices only. Yes, UKC stands for unified kill chain. This is also a kill chain version in which all attackers behavior and steps has been listed and framework.

So, this UKC is towards raising resilience against cyber attack. Before we go with the UKC, we have to understand what this resilience comes for. What is cyber resilience? How do we say that one organization is resilient towards any cyber attack? Any ideas? This is just a common word, resilience. Okay. So resilience represents, The capability or ability to protect the infrastructure, which is obvious in defense, plus no infrastructure can be 100% secure.

So that will be attacked. Infrastructure will get attacked for sure. But what ability does the victim have to get back, to resume their operations? So the critical infrastructures, they need to have high resilience and to any kind of cyber attack because they are people and the humans and the majority populations dependent on that and these services cannot get hold for the long, like the power plant or the water treatment plant. So this resilience comes in the cyber, cyber resilience represents the organization's ability to come back. First one is obvious protection and what ability they have to defend and detect or protect from any cyber attack. But once the attack happens, what ability do they have to get back on the system, okay. So, this is what cyber resilience is, what I believe that you need to be aware of before understanding this unified kill chain.

So a unified kill chain, similar to the Lockheed Martin cyber kill chain and the MITRE ATT&CK, has several stages. Here all, there are all 18. 18, we had, I guess, 14 tactics in

MITRE ATT&CK, 7 in CKC, LM CKC. For UKC, we have 18. And we will see why it comes what was the pros and cons of the CKC and the MITRE ATT&CK in next class and we will discuss how this is leveraging over these two and why UKC is important and what about if UKC comes whether this MITRE ATT&CK and LM CKC importance get reduced or not which answer is obvious no.

All these things are used in different cases and different scenarios. It is just because LMCC represents something else on the table. MITRE ATT&CK represents something else on the table. And there is something else which the UKC framework takes on the table.