

Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

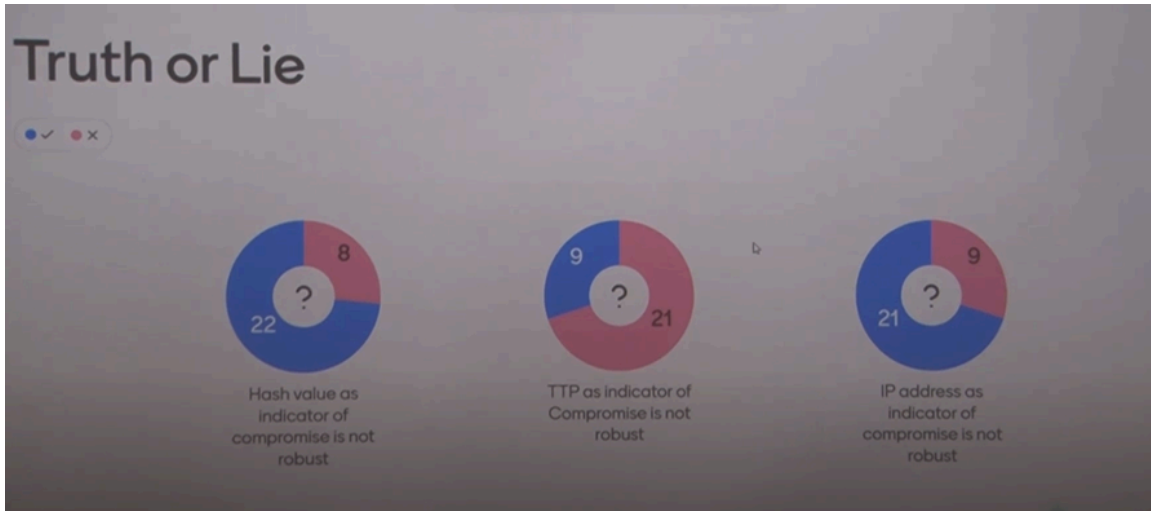
Indian Institute of Technology, Kanpur

Lecture 07

Mapping to ATT&CK from Finished Cyber Incident

Let us see true or false, whether this statement is correct: hash value as an indicator of compromise is not robust, TTP as an indicator of compromise is not robust, and IP address as an indicator of compromise is not robust. Which ones are correct and which ones are incorrect? Okay, so the hash value is basically used for identifying the malware, right? Or a document, right? So when we say something as an indicator of compromise, what we mean is that, let's say somebody gets attacked or some company like Symantec or VirusTotal, they come to know of malware and they tell everybody that, hey, there is a malware going on and this is the hash of that malware. So everybody will then have that, check for that hash, right? So they will always be searching for any file that comes with the same hash and then reject that file, right?

Now, how easy is it for the malware writer? See, when this information is broadcast, the malware authors will also know, the miscreants will also know, that this hash is now commonly known. So how hard is it for the person to change the hash? He has to just change a bit in the malware file.



So, malware file headers will have a lot of space where you can make a small change without altering anything about the malware, and the hash will change. As an indicator of compromise, hash values are not that reliable. An attacker can change the hash value easily, and therefore, if you are just looking for that hash value, you will probably be fooled as a defense. It works sometimes, but it does not necessarily mean that the attacker will sit quietly and let everybody detect them by that hash value. They will change the hash value, right?

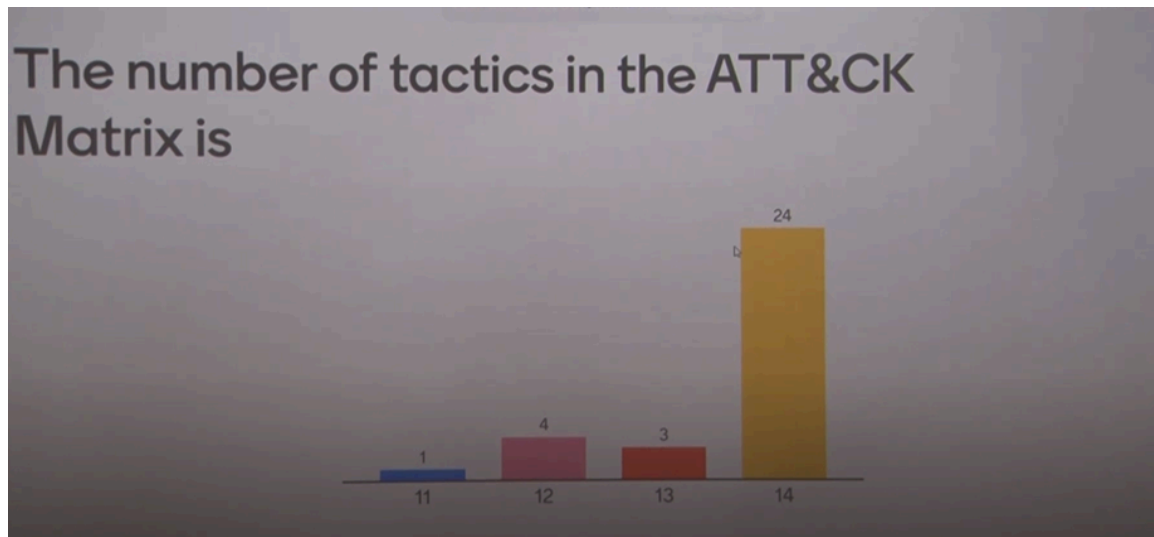
Now, when a threat intelligence company says, "Here is a threat actor that uses these TTPs—tactics, techniques, and procedures," and as a defender, you are detecting what the TTPs are, what kind of activities are happening from outside into your system, and what tactics and techniques are being used, you can see whether the one that the threat intelligence company is talking about is actually attacking your system or not, right?

Once that information is known, it is still very difficult—though not impossible—for the attacker to change its TTP overnight. Because you have to hone the skills for attacking a system using certain techniques and certain types of tactics, you do not want to give up on all the research that you have done to develop a TTP to attack. So, you will eventually change, but you will not change overnight. Therefore, it is rather robust as an indicator of compromise.

Now, the IP address is again similar to the hash value. If the threat intelligence company tells you, "Hey, here is an IP address that is being used by threat actors as a command and control or as an originator of spam," you will block it in your firewall, right? But the attacker can easily change that IP address. They will just change the server from which they are doing the activity, or they will change the DNS resolution from one IP address to another. Therefore, it is not very robust, but it is more robust than the hash value.

So those of you who have watched the previous lecture, the last pre-recorded lecture, will recognize this as the Pyramid of Pain. This is from the Pyramid of Pain. So, go and look for that part of the lecture: Pyramid of Pain.

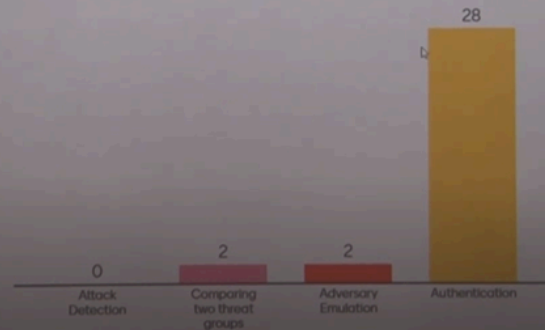
Now here is an easier question. How many tactics are there in the ATT and CK matrix? So, I would have taken both 12 and 14 as answers.



ATT&CK has two pre-attack tactics: reconnaissance and development of the payload. Then there are 12 others, starting from initial access, execution, privilege escalation, persistence, lateral movement, etc. So, 14 altogether, but usually in the matrix, they show 12 from the initial access tactics. But there are two pre-attack tactics, which are reconnaissance and development of the payload. So that's why it's 14.

So, 14 is correct. 12 is also sort of correct. 11 and 13 are probably just random choices. I don't see where you got that. So, which of the following is not a use of ATT&CK? Remember, we are asking about what is not a usage. Okay, so it is going in the right direction.

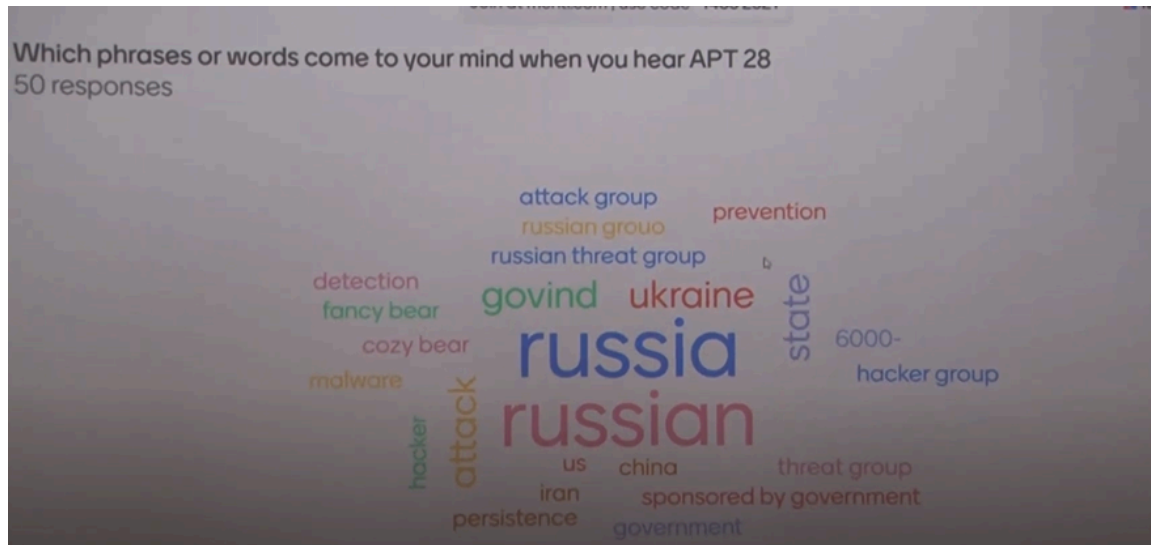
Which of the following is not a usage of ATT &CK



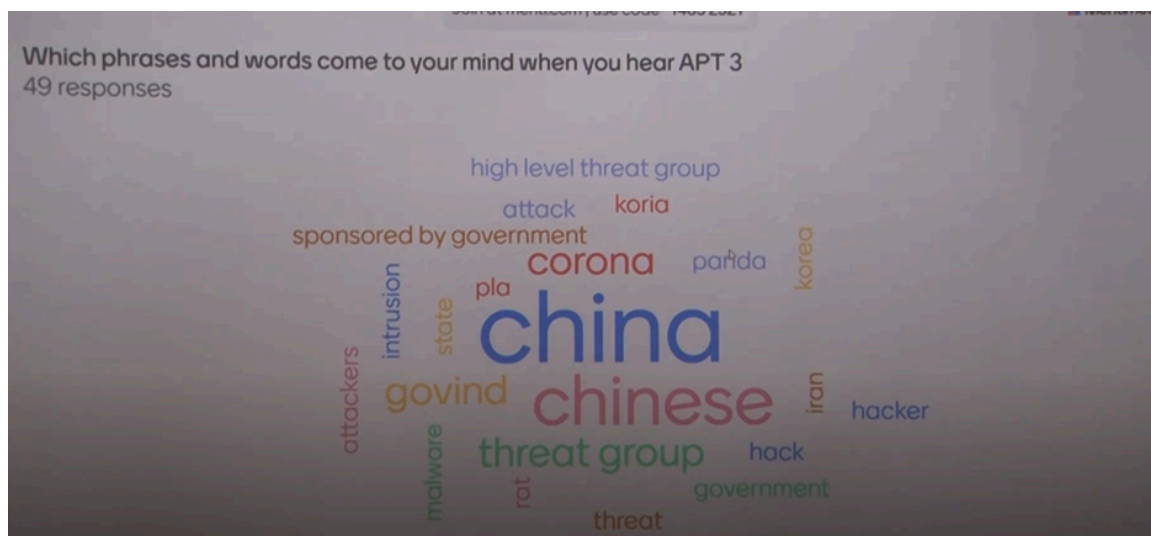
So in the pre-recorded lecture, we discussed the different uses of ATT&CK. Of course, authentication has nothing to do with tactics, techniques, and procedures, so this is an obvious answer. When you hear about APT 28, we have mentioned APT 28 many times. So, I want to know how much you remember. What comes to your mind when you think about APT 28? It's like Donald Trump, Russia, right? It's a Russian threat group, and you know it's state-sponsored or government-sponsored. It has been used against the US government, things like that.

Which phrases or words come to your mind when you hear APT 28

Waiting for responses ...



It's not Chinese or Iranian. APT 28 is a very well-known threat group from Russia. Okay, so last one: what comes to your mind when you hear APT 3? Govind, Corona, Korea... Yeah, so APT 3 is a Chinese threat group.



So most of you seem to know that. Some of you think it's Iranian and some think it is Korean. Now, first of all, you know that there are two Koreas, right? Korea is not a single country. There is South Korea and North Korea, right? North Korea has very well-known threat groups like the Lazarus Group or APT 37, but this is not one of them. That doesn't mean South Korea does not have threat groups, or the US doesn't have threat groups, or India does not have threat groups.

There are threat groups associated with every government. However, because most of our threat intelligence companies are US-based, we normally talk about Chinese threat groups, North Korean threat groups, Iranian threat groups, and so on. If you go to

attack.mitre.org and look through the threat groups, you will find Pakistani threat groups, Indian threat groups, and many others.

APT 28 is also called Fancy Bear. Can you imagine what the Indian threat group is named after? Which animal? No? What? No. Well, there may be one, but the well-known one is associated with an elephant.

So, let us go back to the second part of the submodule of ATT&CK.



Module 3.2

MITRE ATT&CK:

Mapping to ATT&CK from Finished Cyber Incident Reports

Sandeep K. Shukla
IIT Kanpur

So in the previous classes, we talked about what ATT&CK is all about, what tactics are, and what techniques are. Tactics and techniques can be found on the ATT&CK knowledge base, which is a very well-documented knowledge base at attack.mitre.org.

Now, the question is, what is it good for, right? We said it is good for several things. It helps us identify threats or threat groups. It helps us compare two threat groups. It helps us emulate adversaries to see what an adversary does by going through the various tactics and so on. In general, it helps us understand what an attack is. It gives you a frame of mind through which you look at an attack, like a lens.

An attack does not happen by just sending a phishing email and compromising a computer; that's not the end of it. Threat groups want to do a lot more. Once they compromise your computer, they want to create persistence, create lateral movements, move to other machines, try to do data collection, data exfiltration, credential access, and all kinds of stuff. It gives you a handle on how to describe an attack. Most attacks can be

described as a sequence of tactics, identifying which techniques were used to implement those tactics.

What happens is that companies like Recorded Future, FireEye, Mandiant, Microsoft, and Google Security Labs have sensors all around the world. They collect data from various locations, like internet traffic, and try to figure out what is happening. They not only try to understand an attack that has already been reported and maybe analyzed post-mortem by Mandiant, but they also observe the internet for various types of traffic and activities, the malwares that are discovered, and all that, and they try to make sense of it to create threat reports.

These threat reports are often published as part of their free service to the community. You will find that Recorded Future publishes threat reports, Mandiant publishes threat reports, Microsoft publishes threat reports, and so on. These threat reports contain all the descriptions, like how the initial access happened—whether it came through a Log4j vulnerability or spear phishing, and so on. Then they will explain that the first payload that came in exploited a specific vulnerability to perform privilege escalation.

Then they will say that after the privilege escalation, they actually went for the file that contains the hashes of passwords. They then sent it to their command and control server at a specific IP address, where they attempted a dictionary attack or rainbow attack on these hashes, discovered some credentials, and used these credentials to get into the system and so on. They will provide a very elaborate description of what all happened.

Now, as a defender, what good is it, right? I subscribe to a number of different cybersecurity news sources, and every day I read about 5, 6, 7, or 8 such threat reports. So, what do I do with that information? I can talk about it to others, saying, "Hey, did you know that this happened or that happened?" It may give me an idea that, "Oh, this also can happen," and so on. It can also give me an idea that this particular vulnerability is in Windows Office, so I better think about patching it. This kind of knowledge is useful.

But as a defender, I have to get more out of this. To do that, I need to figure out how to use this information to actually defend my infrastructure. There could be many ways to do it. One way is to take bits and pieces of indicators that are in that report. For example, there are some IP addresses in the report, so I collect those IP addresses and tell my firewall guy to make sure these are blocked. If I see that certain versions of Windows are exploited, I tell my system administrator or asset manager to ensure that none of our machines have that version of Windows and that it should be patched immediately.

I can use bits and pieces of that information or indicators for doing some security, but that's not very systematic. So, what is the way to systematically utilize such reports? You

have to extract this information in a way that allows you to design your defense systematically or check your defense systematically to see whether your current defense will be able to stop or detect if these things happen in your system.

There is also a threat intelligence exchange format called STIX. Sometimes I can put it into this STIX format. It is like a meta programming language in which I can put all this information, and many modern tools like firewalls, intrusion detection systems, and endpoint detection systems understand STIX. If you give a new STIX file to them, they will make sure that those indicators are actually used for blacklisting or whitelisting or whatever they need to do.



Outline



- What is ATT&CK? (Module 3.1)
- Mapping to ATT&CK from Finished Cyber Incident Reports (Module 3.2)
- Mapping to ATT&CK from Raw Data from Cyber Incident (Module 3.2)
- ATT&CK Navigator (Module 3.3)
- From ATT&CK Mapping to Defence Recommendation (Module 3.4)

So, therefore, what we want to learn in this sub-module is how to take a finished report—a report that has been published about a threat activity by a well-known threat intelligence company—and how to map it to ATT&CK. That is the first thing we want to do. To remind you, we started with understanding what ATT&CK is. Now, we are going to learn how to use the finished cyber incident report to map to ATT&CK.

Then we'll see how to map raw data when there is no finished report of an incident. This may have happened to your organization, so you have various kinds of raw evidence, such as logs, malware samples, extra files created inside your system, or contact with unfamiliar IP addresses. You use that information and map it to ATT&CK. This is harder, but it is what you will most probably do most of the time since you will not always get a completely finished report.

We will cover this in the next sub-module. Then, we'll show you the tool that MITRE designed called ATT&CK Navigator. After that, we'll see how defense recommendations are made based on the mapping we have created.

The basic idea is cyber threat intelligence. To defend your organization's cyber infrastructure, you need to know many things. Who is attacking us? Not every kind of organization is attacked by every threat group. There are certain threat groups focused on certain sectors, certain geopolitical regions, and so on. Knowing who might be attacking you and what their motivations are will give you an idea of what they might be after. Is it data, is it to extract money from you through ransomware, or is it just to create disturbance or denial of service? You need to understand what they might be wanting.



Cyber Threat Intelligence (CTI)



- To defend an organizational cyber infrastructure, you need to know
 - Who might be attacking you and their motivations
 - Frequency and volume of the attacks
 - The various attack surfaces they tend to exploit
 - The tactics used by different groups of attackers
 - The techniques they use to implement their tactics
 - The procedures they use to make the technique work
 - What kind of malware they use
 - Their Command-and-Control Infrastructure
 - Indicators of compromise
 - Artifacts – e.g. IP addresses, URLs, Malware, credentials, files. Certificates etc.

Then you have to understand what is the frequency and volume of the attack. What are the attack surfaces that they actually exploit, right? Is it internet-facing services that they're exploiting? Are they doing a supply chain compromise? Are they stealing credentials of legitimate users to get into your system? What surface are they attaching themselves to for the first access?

Next, you need to understand the tactics they are using and the techniques they are using to implement those tactics. What procedures are they following to actually implement those tactics? What kind of malware are they using? What is their command and control infrastructure? Additionally, you need to identify any other indicators of compromise like hashes, other artifacts, URLs, files, and digital certificates.

ATT&CK and CTI



- Knowledge of Adversary behaviour is helpful in planning defence
- Structuring CTI with ATT&CT TTPs help us:
 - Compare behaviours
 - Between threat groups
 - Same group over time
 - Groups to defences
 - Communicate in a common language for sharing CTI across organizations

Communicating to defenders



- APT 18 used legitimate credentials to log into external remote services
- APT 29 used compromised identities to access networks via VPNs and Citrix
- APT 41 compromised an online billing/payment service using VPN access between a 3rd party service provider and the targeted payment service
- All are using T1133 (External Remote Services) technique

So if you have all this information, it's easier for you to actually defend against at least that adversary. It doesn't mean you are going to defend against every adversary, but if you have so much information, then you can do better against that specific adversary for sure.

ATT&CK and threat intelligence: ATT&CK is actually about adversary behavior, right? A sequence of tactics is basically their behavior unfolding—what they do first, second, third, and so on. Structuring the threat intelligence can be done in many different ways. You can present it as text, in the form of a STIX file, or in terms of TTPs (tactics, techniques, and procedures).

Structuring the CTI (Cyber Threat Intelligence) with respect to tactics, techniques, and procedures allows you to compare different threat groups, check your defenses, and understand which defenses work against which groups. When talking to fellow security

professionals, if you describe something in natural language, it may be interpreted differently by different people. But if you use common vocabulary in terms of tactics and techniques, there is no space for ambiguity.

For example, let's say APT 18 steals credentials from various places and then logs into external remote services. If a threat actor remotely logs into a system after compromising your credentials and impersonates you, a common understanding can be achieved using specific terminologies. APT 29 also uses compromised identities to access networks through VPN and Citrix, and APT 41 compromises billing or payment services using VPN access between a third party and the main targeted payment service.

In all these cases, you can describe the scenarios in detail, but one thing that security professionals familiar with ATT&CK will understand is that they are all using T1133—using external remote services to penetrate your system and make the initial access. This use of a common vocabulary eliminates ambiguity. You can define your own vocabulary, but it may not be known to your colleague or another security expert in the same sector with whom you are exchanging information. Using a common vocabulary ensures clarity and effective communication.

Mapping from a finished report to ATT&CK: Many people think of threat intelligence as just indicators of compromise. Indicators of compromise can be many types, such as hashes, IP addresses, and malware samples.



CTI and ATT&CK



- To a lot of defenders CTI = IOC (Indicators of Compromise)
- Threat Intelligence is often shared as STIX format
- STIX = Structured Threat Information Expression
- To map to ATT&CK you need to consider a threat or attack in terms of behaviours of the attacker
- The tactics are the self-contained goals set by the attacker to make progress
- Subsequent tactics build on successes of previous tactics
- There are 14 tactics, and over 300 techniques

URLs are indicators of compromise. Certificates can be indicators of compromise. So, what is an indicator of compromise? If there is a compromise in one place and you collect various artifacts from that place and make it known to everybody, you can say, 'If you see

this hash, if you see a file with this hash, if you see a malware fragment like this, or if you see communication going to this URL or this IP address, then you know that you are also compromised by the same threat actor.' These digital artifacts are called indicators of compromise.

Indicators of compromise, when given in terms of digital artifacts, are relatively easy for an attacker to change. If you've seen the pyramid of pain, you'll know that most of these indicators are not that difficult for the attacker to modify. But if you share threat intelligence in terms of TTPs, the TTPs don't change overnight because it requires a lot of time and investment to develop the techniques and tactics that work on a particular target. You cannot change a TTP overnight without investing more time and money into it.

Therefore, TTP-based sharing of intelligence is beneficial. STIX, as I mentioned, is a format by which you can share threat intelligence, and it is being used more and more. Our Indian Computer Emergency Response Team (CERT-IN) and NCIIPC also share threat intelligence in STIX format. If you have the right tools, like your firewall, that can ingest the STIX format and automatically configure itself to stop those indicators, that's great. STIX is something we'll be discussing a lot more later in the class.

Despite all these methods, we can still use ATT&CK mapping of threat incidents to disseminate information to others, who can then use it to ensure they are protected against these techniques and tactics. There are 14 tactics, as you saw, and more than 300 techniques, and the techniques database keeps increasing.



Mapping Adversary Behaviour to ATT&CK



- Understand ATT &CK
 - Find the adversary behaviour rather than IOCs
 - Do your own research on the behaviour
 - Translate the behaviour into one or more tactics
 - Figure out the technique(s) applied to play the tactics
 - Compare your mapping to other analysts
- Sources of Adversary Behaviour Data
 - Finished Reports from Threat Intelligence Agencies
 - Raw Data from Forensic Analysis

So now the question is, how do you go about doing this? How do you map the incident report to ATT&CK tactics and techniques? First of all, you have to read the report and figure out all the things the adversary did—what they did first, what they did next, and

what they did after that, and so on. This helps you understand the behavior of the adversary.

Some behaviors you may not immediately recognize as a specific tactic or technique. In the beginning, it will take some time to reach a level where you can immediately identify a tactic or technique. So, you have to do some research. Go to the ATT&CK website, do a search for the behavior, and it will give you all kinds of tactics and techniques that might be relevant to that behavior.

Then, you have to figure out which one is a good fit. Translate the behavior into one or more tactics and then identify which techniques have been applied to achieve that tactic. Once you have completed the mapping, ask another analyst to do the same and compare the results, as everyone has a different understanding. This is not an exact science but more of an expertise-based mapping.

This mapping can be done from a finished report or from raw data. In this sub-module, we are focusing on finished reports. To understand the behavior of the adversary, first focus on the verbs. The verbs will tell you what the adversary is doing.

What did the adversary do on the system once it was compromised? How did it gain initial access? How did it find the vulnerability that it exploited? How did it create persistence? How did it perform privilege escalation? How did it become the root user? Did it exfiltrate data or change any settings? Did it use malware? What kind of information did it look for or exfiltrate?

This is the kind of stuff you have to ask yourself while reading the report. Here is a fragment of a report. This report is actually available through this [hyperlink](#). When you get the slides, you will find this [hyperlink](#) and access the report from Mandiant. This example shows how to identify the behavior of the adversary.

In this fragment, you see that a particular CVE was exploited. It's a kernel vulnerability, and exploiting it will give root access. This is the middle part of the report, so we're not starting from the beginning. This is just to show you how to identify adversary behavior. You can see that the adversary is exploiting a particular vulnerability to gain root access.

Finding the adversary behaviour

- Focus on the verbs
 - What did the adversary do on the systems it compromised
 - How did it get its initial access
 - How did it find the vulnerability
 - How did it create persistence in the system
 - Did it attempt to become root user
 - Did it compromise multiple devices via vulnerable protocols
 - Did it exfiltrate any data
 - Did it change any settings
 - Did it use any malware
 - What kind of information did they look for
 - What kind of systems or information it attempted or succeeded to access

Now, it then says that there is a malware component which uses a certain command.exe with the command 'whoami' to figure out whether it is running as root or not. 'whoami' will tell you if it is root, and if it finds that it is running as the system, it creates a scheduled task. So, a scheduled task is being created.

This scheduled task will run the test.exe malware. This describes how persistence is being created. Here, we saw how privilege escalation was performed. Now, we see how persistence was established.

The report then states that when this malware is executed, it first establishes a SOCKS5 connection to a particular IP address outside using TCP port 1913. It then sends a connection request with a specific code and ensures that the server responds with a specific code.

This is essentially a handshake. This malware is trying to establish its connection with command and control.

In this little fragment of the report, we find privilege escalation, persistence, and command and control. Three tactics are easily visible, though there may be more. This is where you find the behavior. We are showing you one snippet here.

If you do not know this behavior, let's say you see it connecting using SOCKS5 to an unknown IP address, and you do not know that this is the command and control tactic.

Finding behaviour of adversary

The most interesting PDB string is the "4113.pdb," which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that, with successful exploitation, would give any user SYSTEM access on the machine.

The malware component, test.exe, uses the Windows command "cmd.exe" /C whoami to verify it is running with the elevated privileges of "System" and creates persistence by creating the following scheduled task:

```
schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"
```

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "05 01 00" and verifies the server response starts with "05 00".

[Operation Double Tap | Mandiant](#)

Tactic and Technique

Research the behaviour

- If you are not familiar with the behaviour described
 - Research which tactics and techniques may have been used in the behaviour
 - Discuss with the red-team members in your organization
 - Refer to the attack.mitre.org website
- Give enough time to the research
- Understanding the behaviour will help with the next steps in mapping to the correct tactics/techniques/procedures

Then you have to do research, right? You need to go to the ATT&CK database and search for this behavior. It will probably give you a number of choices, and you will have to pick which one is the right behavior and the correct tactic describing that behavior.

You can also do external searches to understand the context. For example, what is SOCKS? SOCKS is basically a proxy server. If any of you have used a web proxy, like Burp Suite, you know that Burp Suite is a tool for creating a web proxy so that all web traffic from your browser goes to the proxy. External entities can only see the proxy, not your browser.



WIKIPEDIA
The Free Encyclopedia

- Main page
- Contents
- Featured content
- Current events
- Random article
- Donate to Wikipedia
- Wikipedia store

Article [Talk](#)

[Read](#) [Edit](#) [View history](#)

SOCKS

From Wikipedia, the free encyclopedia

This article is about the internet protocol. For other uses, see [Socks \(disambiguation\)](#).

SOCKS is an [Internet protocol](#) that exchanges [network packets](#) between a [client](#) and [server](#) through a [proxy server](#). **SOCKS5** additionally provides [authentication](#) so only authorized users may access a server. Practically, a SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded.

SOCKS performs at [Layer 5 of the OSI model](#) (the [session layer](#), an intermediate layer between the [presentation layer](#) and the [transport layer](#)). SOCKS server accepts incoming client connection on TCP port 1080.^{[1][2]}

So all the encryption, SSL, and TLS terminate at the proxy. Therefore, you can see the traffic between the proxy and your browser in plain text. That's how we actually debug web applications and so on, right? SOCKS5 is the protocol used for that kind of proxy.

Different malware uses different protocols for connecting to the command and control. Some may use HTTP protocols, some may use DNS protocols, and some may use application-level protocols. In this case, it is using the SOCKS5 protocol and a rather non-standard port, 1913. You might need to look for more details about this. There is a website called SG Security where you can find information about all the ports and what services typically use those ports.

[Home](#) » [Ports Database](#) » [Port Details](#)

Port 1913 Details

threat/application/port search:
 [SEARCH](#)

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
1913	tcp,udp	armadp armadp		IANA

1 records found

[SG security scan: port 1913](#)

[« back to SG Ports](#)

jump to: [GO](#) [PREV](#) [NEXT](#)

Now remember that port numbers 1-1024 are standard ports, used for specific services in most cases. But 1913 is outside that range, so it is a custom port. Whoever wrote that test.exe malware decided to use this port. Now, if this malware was inside IIT Kanpur on your machine or on the IIT Kanpur network, would this work? Is port 1913 open or closed? Actually, it doesn't matter because, unless explicitly blocked by our firewall, outgoing connections will typically go through.



Translate the behaviour into a tactic



- Try to understand what the adversary might be trying to accomplish (subgoal)
- May require domain expertise
 - For example, the port number may indicate the protocol being used
- To map to a tactic, you have only 14 choices
 - reconnaissance, weaponization (preparation), initial access, execution, persistence, privilege escalation, defence evasion, credential access, discovery, lateral movement, collection, command & control, exfiltration, impact



Translate the behaviour into a tactic



- “When executed, the malware first establishes a **SOCKS5 connection** to 192.157.198.103 using TCP port 1913. ... Once the connection to the server is established, the malware expects a message containing at least three bytes from the server. These first three bytes are the command identifier. The **following commands** are supported by the malware ... “
 - A connection in order to command the malware to do something
 - **Command and Control**

Anyway, now you have to translate the behavior into tactics. The good thing about translating behavior to tactic is that you have only 14 choices, so you cannot go very wrong. For example, nobody will confuse initial access with privilege escalation. It's not easy to make such a mistake. So, finding the correct tactic is not that difficult.

For example, in this snippet from the previous example, you can see that the behavior can easily be attributed to the command and control tactic. So, this was easy. The harder part comes when finding the techniques because there are 300 plus techniques. The good thing is that not all techniques relate to all tactics. Every tactic has a set of techniques, and some techniques are common between multiple tactics, but only a few. If you know what tactic you have identified, then finding the technique means not searching through all 300 but the subset that applies to that particular tactic.



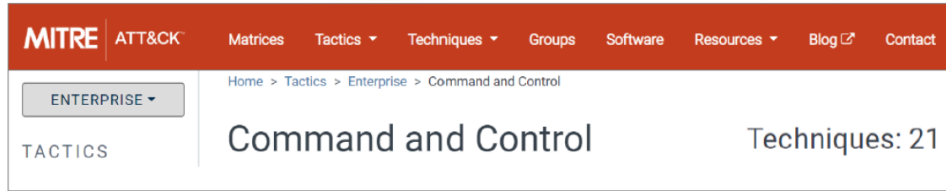
Figure out what techniques apply



- This is harder than finding tactics as there are over 300 choices
- Look at the techniques identified in the ATT&CK matrix for identified tactics
- Search the attack.mitre.org website for technique details and figure out matches with the behaviour
- Some behaviours may not have an existing technique
 - You may consider reporting to the attack.mitre.org

So you have to look at the techniques identified in the ATT&CK matrix for the identified tactics. If you have done the tactics correctly, you have narrowed your possibilities. Then, you do a website search and all that stuff. Some behaviors may not have an existing technique, and in that case, you may report a particular new technique that you have discovered to ATT&CK.

Figure out what techniques apply



MITRE ATT&CK Matrices Tactics Techniques Groups Software Resources Blog Contact

Home > Tactics > Enterprise > Command and Control

ENTERPRISE

TACTICS Command and Control Techniques: 21

T1094	Custom Command and Control Protocol
-------	-------------------------------------

Protocol vs. Port
→ 2 techniques?

T1043	Commonly Used Port
-------	--------------------

Submit your findings to mitre.org, and if they accept your submission, your name will eventually be displayed on that page as a contributor to that technique.

In this case, you have identified the command and control tactic. There are two techniques that seem to be relevant here: custom command and control protocol.

Figure out what techniques apply

“the malware first establishes a SOCKS5 connection”

SOCKS
Techniques
Term found on page
Standard Non-Application Layer Protocol (ID: T1095)
Connection Proxy (ID: T1090)

Standard Non-Application Layer Protocol

Use of a standard non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. [1] Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

They are using a custom command and control protocol and an uncommonly used port, 1913. So, it is a standard non-application layer protocol.

Figure out what techniques apply

“establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913”

No results found.

MITRE ATT&CK Matrices Tactics Techniques Groups Software Resources Blog Contact

ENTERPRISE

Home > Tactics > Enterprise > Command and Control

TACTICS Command and Control

T1043	Commonly Used Port	T1065	Uncommonly Used Port	T1205	Port Knocking
-------	--------------------	-------	----------------------	-------	---------------

“CTRL+ F” FTW

So that is T1075. When you say SOCKS5 connection, it's not a non-standard protocol; it's a well-known protocol, but it is not at the application layer. Many times, we design an application layer protocol that eventually uses lower levels like TCP/IP, etc. In that case, we would say it's a custom protocol. However, SOCKS5 is a standard non-application layer protocol. It also uses a connection proxy, so that is T1090. There are two alternatives: commonly used port or uncommonly used port.

Repeat the process

The most interesting PDB string is **Privilege Escalation | 3. Exploitation for Privilege Escalation (T1068)**. E is a local kernel vulnerability that, **with successful exploitation**, **Execution | 4. Command-Line Interface (T1059)**.

The malware component, test.exe, uses the Windows **Discovery | 5. System Owner/User Discovery (T1033)** to verify it is running with the elevated privileges of “System” and **Persistence – | 6. Scheduled Task (T1053)** creates persistence by creating the following scheduled task:

Command and Control | 1. Standard Non-Application Layer Protocol (T1095) **Command and Control | 2. Uncommonly Used Port (T1065)**

When executed, the malware first **establishes a SOCKS5 connection** to 192.157.198.103 using **TCP port 1913**. The malware sends the SOCKS5 connection request "05 01 00" and verifies the server response starts with "05 00".

So here, T1065 will be more appropriate because this is not a commonly used port. Port knocking is not relevant here. When you search for 'port' on the ATT&CK website, it will give you a number of techniques, some of which may be totally unrelated, like port knocking in this case. You have to be aware of that to avoid confusion. Then, you repeat this procedure for all the verbs in the report.

You go through this process again and again. After you finish, you will recognize that privilege escalation was the tactic, and exploitation for privilege escalation was the technique. Additionally, the malware executed commands, which is another technique.

It uses 'exe', so it's a command line interface. It also does discovery by using 'whoami', which is the system owner user discovery technique. It also creates persistence by scheduling tasks, so 'scheduled task' is the technique. Command and control was used here with a standard non-application layer protocol and an uncommonly used port. After examining these six lines, you find three tactics and at least six or seven different techniques being used.

So, this is how you do it. Now, we do not have time to do this exercise in class, so I will ask you to do this on your own and we will discuss it tomorrow. There is a particular finished report by Cyber Reason called the Cobalt Kitty Report.

There are two PDF files here. One already highlights the verbs and the other has tactic hints. One version of the PDF has tactic hints to help you, while the other one only highlights the verbs. You need to identify the tactics and find the techniques for each of these. Once you have done that, you can compare the results with your friends. We will discuss this in the next class and see how you did, okay? A similar problem will be your second homework, so you better try to do it, right? Okay.



Exercise: Cybereason Cobalt Kitty Report



- **Analyze a threat report to find the Enterprise ATT&CK techniques**
 - 22 highlighted techniques in the Cybereason Cobalt Kitty report
- **Choose a PDF from attack.mitre.org/training/cti under Exercise 2**
 - Choose your own adventure: start with “highlights only” or “tactic hints”
- **Use the PDF or a text document/piece of paper to record your results**
- **Write down the ATT&CK tactic and technique you think applies to each highlight**
- **Tips:**
 - Do keyword searches of the website: <https://attack.mitre.org>
 - Remember that you don't have to be perfect
 - Use this as a chance to dive into ATT&CK