

Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 08

Mapping to ATT&CK from Finished Cyber Incident



Module 3.2 MITRE ATT&CK:

Mapping to ATT&CK from Finished Cyber Incident

Reports

**Sandeep K. Shukla
IIT Kanpur**

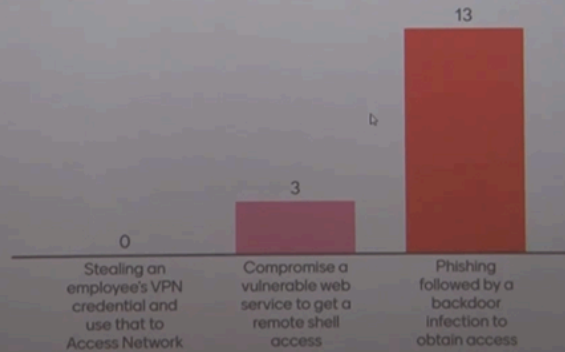
Main thing that we want to do today is learn how to map to the ATT&CK framework from raw data. So, let's first look at a few things. But before that, let's do this: use menti.com with the code number 4597457 and answer the questions.

So, which of the following is not—oh, sorry, it should have been—a procedure for external remote service? We talked about external remote service last time.

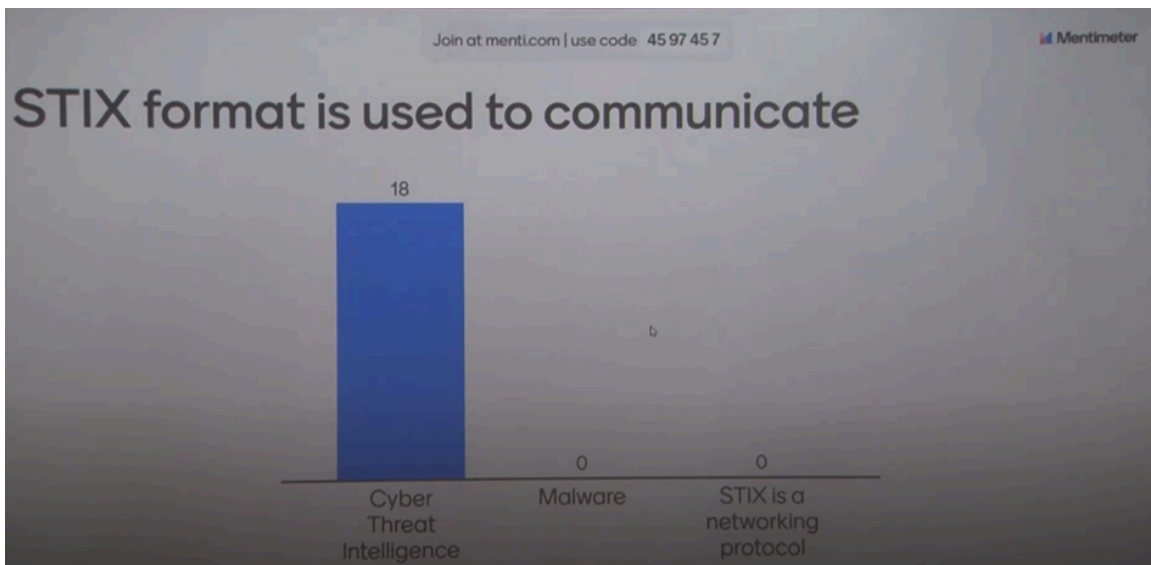
It's technique number 1133, and you have three choices. One is stealing an employee's VPN credential and using that to access the network. The second is compromising a vulnerable web service to get remote shell access. And the third is phishing followed by a backdoor infection to obtain access.

Okay, this is going well. A few more: Stealing an employee's VPN credential and access is an example of external remote service as a technique for initial access, right? So, we are talking about initial access. The second one—compromising a vulnerable web service to get remote shell access—is also like last time when we talked about a payroll service that was used to access the network. So, this is also a type of external remote service.

Which of the following is not an procedure for External Remote Service (T1133)



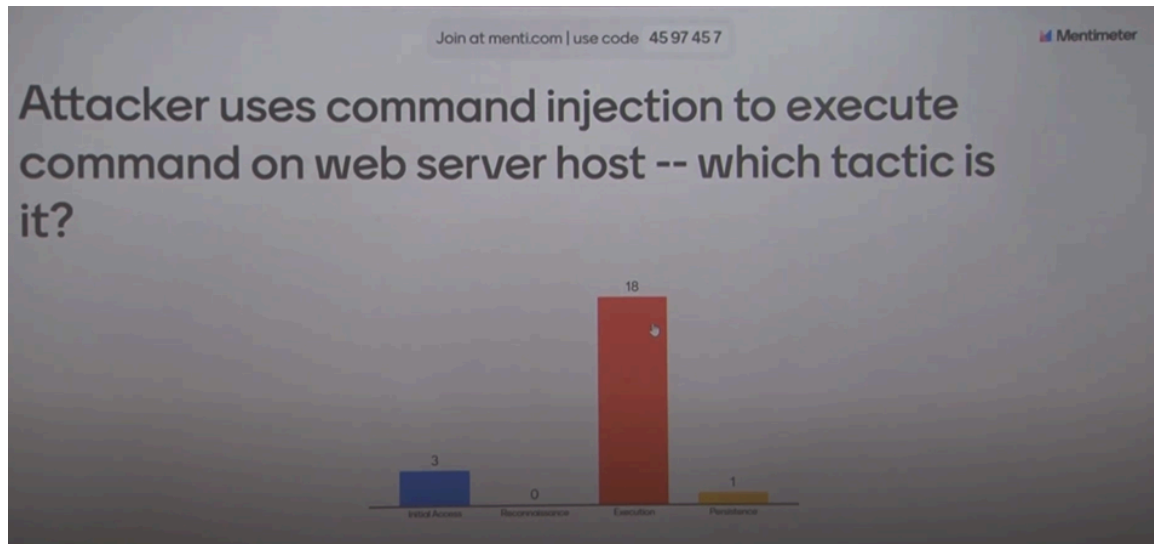
But when you do phishing, your initial access is through phishing, right? So, initial access is not through external remote service. You may use external remote service later for further access, but your initial access is already done. So, that is not an external remote service procedure.



We talked about STIX. So, what is the STIX format used to communicate? Okay, this is going well.

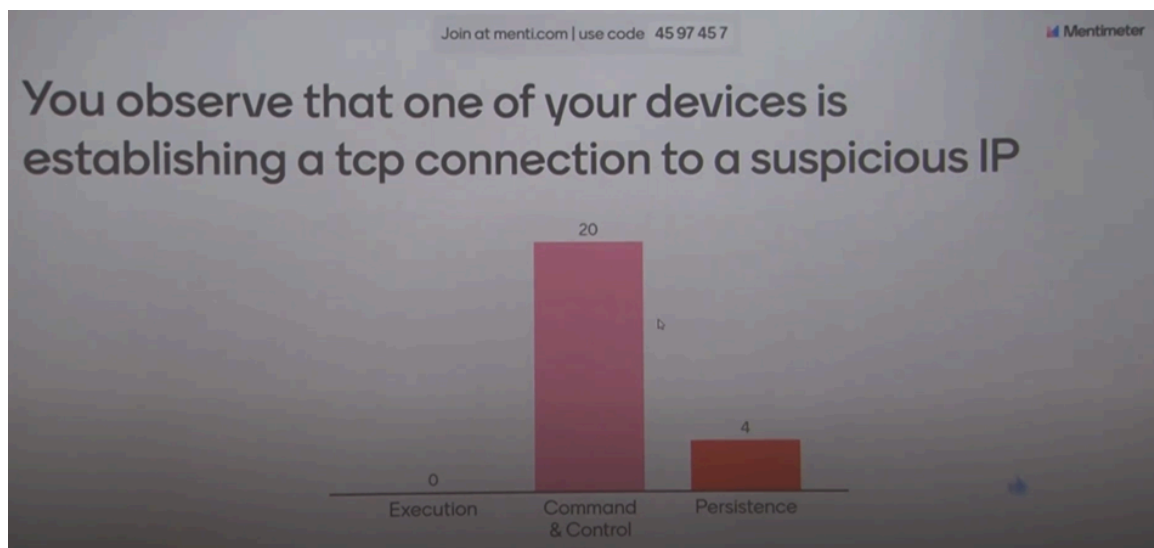
All right, STIX is for cyber threat intelligence, and later in the course, we'll look at the STIX format in detail. You'll learn how STIX files are created for cyber threat intelligence.

Now, an attacker uses command injection to execute a command on a web server host. Which tactic is it? Is it initial access, reconnaissance, execution, or persistence?



So, in this case, it is executing a command, so it is execution, but it may also be initial access because that is probably how the attacker got into the system. But execution is certainly the tactic.

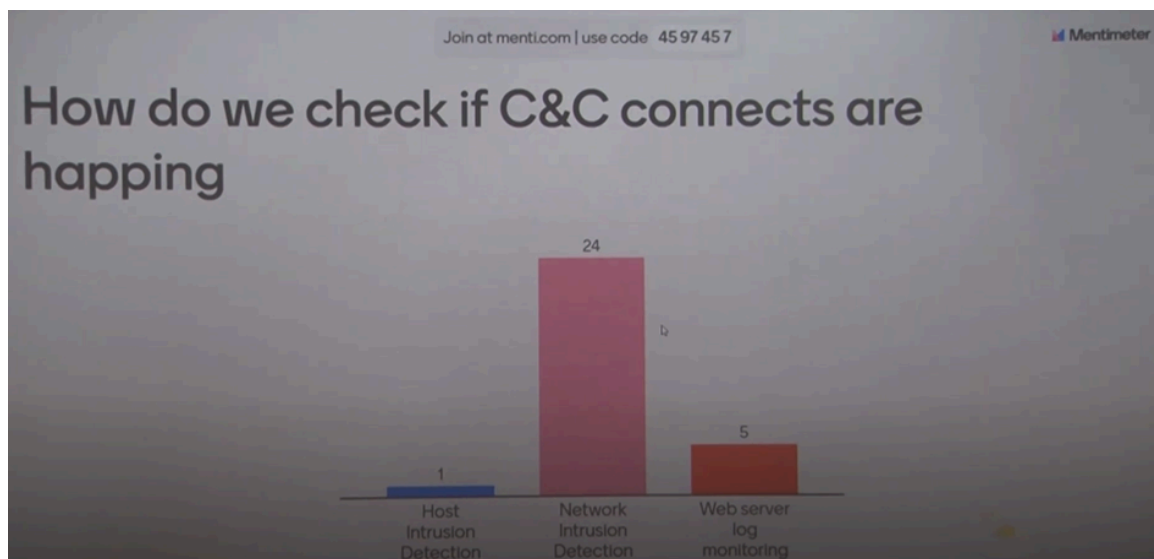
Certain behaviors can actually have multiple tactics. That's something you have to consider. They might combine two tactics in one action, right?



Okay, so you observe that one of your devices is establishing a TCP connection to a suspicious IP. What is the tactic? If your device is establishing a TCP connection to a suspicious IP, that means some unwanted executable is already executing inside your device, right? So that executable has executed, but we do not know whether it has

established persistence. Persistence means that you establish yourself in such a way that the binary will be executed no matter whether you reboot your system or not.

So, if it just executes once, it doesn't mean that it is persistent. If you shut down your machine and restart, it may be gone, right? So, from this information, we do not know whether persistence has been established, but we do know that it is communicating with some service somewhere, which is a suspicious IP. Probably there is a list in the Abuse IPDB database where we can look and see whether this IP has been listed as suspicious by someone. Then I would say that it is command and control.



Okay, this should be happening, but how do we check if command and control connections are occurring? Command and control communication may use various types of protocols, right? If it is using an HTTP protocol, then it is possible that the communication will be mediated by your web server, and maybe it will be in the web server log. However, it is not necessarily in the web server log because you can have an application-level protocol specifically designed to communicate with the command and control server. It could be DNS, it could be some other direct TCP connection, and all kinds of stuff. So, network intrusion detection is probably your best bet to actually check whether command and control is happening.

If you are going to do host intrusion detection on every host, then there is a likelihood that you will also see it in the collected logs of all hosts' intrusion information at the host intrusion detection manager. But your best bet is certainly network intrusion detection. By monitoring all the network traffic, whenever you see an IP address you do not recognize, you can automatically look it up in an abuse IP database. That way, you can actually identify suspicious IP addresses or URLs. So, network intrusion detection is probably the most likely place where you will find this.

The word 'persistence' in general might mean many things. For example, persistence might refer to someone like Virat, who, after facing setbacks, comes back strong—though I don't particularly like him, so I can't say much about his persistence. In real life, persistence would mean someone who is not easily stopped, someone who remains persistent. It's like when we give grades, and people are very persistent about getting a higher grade. That is a real-world use of the word persistence. However, as a cybersecurity professional, your view of persistence would usually involve unwanted executables making themselves persistent on a system so that they remain there.

Sometimes it also evades defense, so it may turn off antivirus software. It may actually hide itself inside a DLL or some executable by injecting itself into the executable. There are many ways that this kind of persistence is achieved by unwanted executables. The idea is that most nation-state attackers aim not to make a spectacular attack, like the Russians did in the case of the power cut in Ukraine. Such attacks become immediately noticeable, and people will start removing all the malware, blocking all the IPs, and doing their best to prevent it from happening again. Nation-state attackers don't do that very often.

They usually resort to that if there is a war or something, but in general, they want to remain persistent. You'll find that most critical infrastructure in India probably has persistent executables from various countries. Unless these are detected properly—like in our seaports, power system operators, telecom operators, and so on—if they're not doing their cybersecurity properly, they're probably hosting persistent agents who are very stealthy. These agents communicate with their command and control very obscurely through obscure protocols. Without network monitoring or endpoint monitoring, most people wouldn't know that this is happening. And if it is happening, the reason is that, at some point, the command and control will instruct the agents that are sitting in various places to actually take some action.

That's the whole idea—to position yourself so that you can execute a command or a series of commands when required. This usually happens during real conflicts or wars, like between Ukraine and Russia or what is happening between Hamas and Israel. That's when these things occur. You might have read that Iranian gas stations were attacked in large numbers recently, likely by Israel, because Iran was giving implicit support to their opponents. They probably had agents sitting in those facilities who executed some commands. This is the idea of persistence.

could be a vulnerable web server, or another service running on a particular port that we've identified as running an unpatched version, making it susceptible to remote code execution, so that's what I'm going to exploit.

But to do all this, I have to develop an exploit, right? For phishing, I have to write an email that looks believable, and then either create a link that leads to a malware-infested website, or I have to actually attach a malware-infested Word file or JPEG file, and so on. This whole process of creating these resources, which we'll use for the initial access, is called resource development. Or, in the case of exploiting an internet-facing service, I have to design the payload, I have to design the exploit, right? So, all these things, which in CKC we call weaponization, are called resource development here. That's a terminology difference. So, the right answer here would have been weaponization, but you're still thinking from the defender's point of view.

All these answers here are actually from a defender's point of view. The defender is doing hardening, sustenance, creating reliability, upgrading the system, and taking backups. So, you're thinking in terms of the defender. But ATT&CK is about the offender, right? We're trying to understand what the attacker does, so we have to adjust our mindset accordingly and think from an attacker's perspective. That's why most cybersecurity professionals are, in some sense, schizophrenic.



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)**

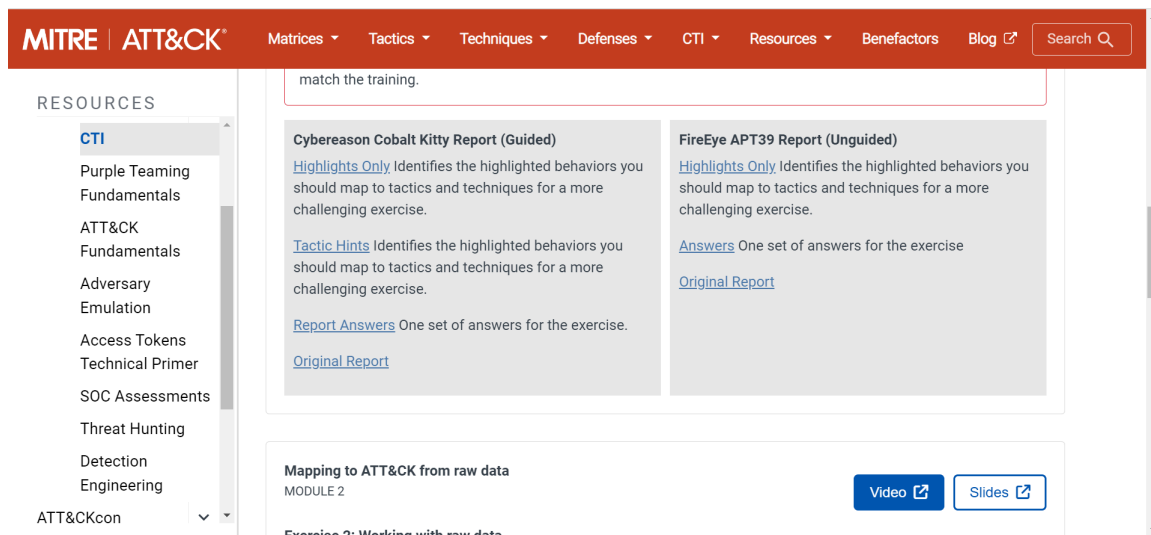
When executed, the malware first **establishes a SOCKS5 connection** to 192.157.198.103 using **TCP port 1913**. The malware sends the SOCKS5 connection request "05 01 00" and verifies the server response starts with "05 00".

They have to always think in terms of the attacker, and then they have to think, 'How can I defend against that attack?' If you cannot imagine what the attacker would do, then you cannot defend yourself, right? So that's the basic idea.

Okay, so that's about these questions. Now, before I go into the raw data aspects, I want to just go back and see where we left off. We actually figured out the verbs in the report, then we tried to identify the behavior. We researched the behavior from the ATT&CK

website and maybe other resources on the internet or in books—whatever your preference. Then, we assigned each behavior to a tactic, and if I can figure out the tactic, I can also try to determine what technique is being used.

Once I have a complete mapping of the tactics and techniques, the question is, 'What does this accomplish?' Then we said that there is an exercise here called the Cobalt Kitty report, and you can go to this place. So, let me show you where it is. If you go to the ATT&CK training and then go to the 'Mapping from Finished Reporting' section, you'll find the Cobalt Kitty report, right?



And this is a highlights-only version of the report, which basically has all the key points, but you have to go through this to figure out what tactics and techniques are being used. So, in this case, you don't have to say, 'Okay, what am I looking for? Am I looking for the verbs and all that stuff?' This report is already pre-filled with the places where you need to identify the tactics and techniques, right?

Link: <https://attack.mitre.org/docs/training-cti/Cybereason%20Cobalt%20Kitty%20-%20highlights%20only.pdf>

This will help you go through this much faster than if you had to go through the entire report by yourself, figuring out where the behavior fragments are and what to do with each behavior, and so on. This report already explains many things in terms of what you want to find. For example, there is a section called 'C2 Communication.' So you can figure out that most of the tactics here would be about command and control (C2) communication, right? It might also include internal reconnaissance.

Now, what is internal reconnaissance? From the Lockheed Martin kill chain, you might get the idea that reconnaissance happens first. Then, once you find where to attack, you

proceed to weaponization. After that, you gain initial access, etc. But many times, once the malware is inside, it will scan again. It has the code for scanning the network, figuring out which internal network is running, which open ports are available, and so on, right? So there could be reconnaissance again, right? And that is the reason why ATT&CK is not a sequence like CKC. CKC is a sequence, but ATT&CK is a set of tactics that can occur multiple times in a kill chain during an attack analysis.

So, internal reconnaissance is being discussed here. This will also give you additional hints as to what the different tactics and techniques could be because of the headings, like 'lateral movement,' right? It's already telling you that here we are discussing how the malware moved laterally. They used Mimikatz for this; they probably did credential dumping, right? These are the kinds of things that happened here. But the point is that if you do this at home, you'll gain some understanding of how this is done, right?

Now, there is another version here. Let me go back. There is another version of the same thing, which is called 'Tactic Hints.' So it's the same document, but now the tactics are already given.

Link:

<https://attack.mitre.org/docs/training-cti/Cybereason%20Cobalt%20Kitty%20-%20tactic%20hints.pdf>

You have to just find the techniques. So you might first try the one without any hints, only highlights. If you do well in that, then you've already gained a good understanding. If not, then you can use the one with the tactic hints already provided.

So, try these exercises. And here are the answers—but do not look at the answers yet. You'll see that not only the tactics but the techniques are also listed.

Link:<https://attack.mitre.org/docs/training-cti/Cybereason%20Cobalt%20Kitty%20-%20answers.pdf>

So this is the answer for this one. Now you can also look at the original report.

Link:<https://attack.mitre.org/docs/training-cti/Cybereason%20Cobalt%20Kitty%20-%20original%20report.pdf>

So, if you want to take a challenge, do not use either the highlights or the tactic hints, and do not look at the answers. Instead, try this on the raw report. If you can do it on the raw report and then match it against the answer key, you will probably feel much more confident that you can handle this in the exam or in the homework, right?

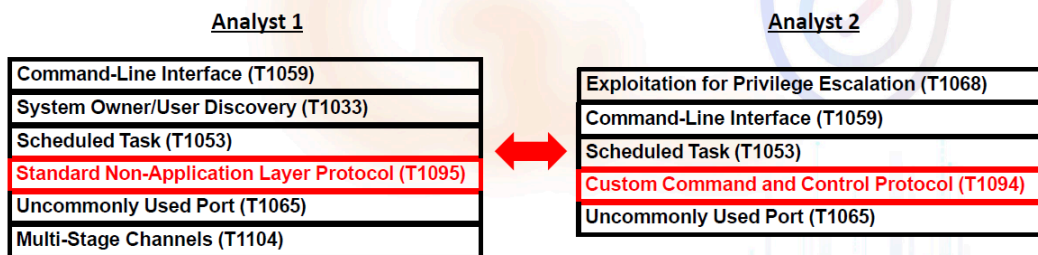
That's the reason why I want you to do this. It's not a formal homework assignment, but if you don't practice this now, you might have trouble later when you need to do it in your homework. Some fragments of this could also appear in the exam.



Compare with the results of other analysts



- Compare your results to other analysts
- Helps hedge against analyst biases
 - More likely to identify techniques you've previously identified



Discuss why it's different

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

And then... If you try to learn this, understand that these things require time. They don't happen instantly. Some people might be very good at this, while others might need to struggle a bit, look up the website, and figure out what techniques correspond to the tactics they identify. It might take some time, but eventually, if you try hard, you will get there.

Now, that's something I wanted you to do. Once you complete the Cobalt-Kitty report, you have your groups, and within the group, you do this exercise, then discuss and see what differences emerge. Someone came to me and said they want to have their wingmates in the group. I have intentionally asked students not to choose their own groups because, in group projects, what often happens is that if there are three people, one or two will work, and the other will be a freeloader. But if they are wingmates, they will never say that this person is a freeloader. However, if they don't know the person very well, they will come and tell us if someone is not contributing, and we can differentiate between them.

This is done intentionally. The other thing is that when you go out into the real world, you won't always find your wingmates in your projects. It's highly unlikely. You have to learn to diversify and work with people you know only professionally. These are some of the things to keep in mind.

Now, comparison-wise, if you do it from the hinted report, it's unlikely that your results will differ much because you're filling in the same boxes. If you do it from the raw report, two of you might come up with very different sets of findings. It's not necessarily that either of you is wrong; you might be mistaken about something, or you might have missed some behavior. That can happen, but it's worth the try. If you don't try and end up doing it for the first time in the exam, it's unlikely you'll do very well.

In the Cobalt-Kitty report, there are, I would say, around 22 techniques that have been used, at least according to their analysis. So, you need to identify 22 techniques from that report. If you do that, you'll be in better shape. Also, on the same website, you'll find more such reports to practice with.



Cybereason Cobalt Kitty Report



- 1. Two types of payloads were found in the spear-phishing emails ... link to a malicious site**
 - Initial Access - Spearphishing Link (T1192)
 - 2. Two types of payloads were found in the spear-phishing emails ... Word documents**
 - Initial Access - Spearphishing Attachment (T1193)
 - 3. Two types of payloads were found in the spear-phishing emails ... Word documents with malicious macros**
 - Defense Evasion/Execution – Scripting (T1064)
 - 4. Two types of payloads were found in the spear-phishing emails**
 - Execution – User Execution (T1204)
- <https://cybr.ly/cobaltkitty>

Cybereason Cobalt Kitty Report



5.  cmd.exe
Parent process

- Execution - Command-Line Interface (T1059)

6. The two **scheduled tasks** are created on infected Windows

- Execution/Persistence - Scheduled Task (T1053)

7. **schtasks /create /sc MINUTE /tn "Windows Error Reporting" /tr "mshta.exe about:<script language=\\\"vbscript\\\"...**

- Execution/Defense Evasion - Mshta (T1170)

8. That **downloads** and **executes an additional payload** from the same server

- Command and Control - Remote File Copy (T1105)

<https://cybr.ly/cobaltkitty>

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

Cybereason Cobalt Kitty Report



9.  powershell.exe  
Parent process

- Execution - PowerShell (T1086)

10. it will pass an **obfuscated and XOR'ed PowerShell payload** to cmd.exe

- Defense Evasion - Obfuscated Files or Information (T1027)

11. The attackers used trivial but effective persistence techniques .. Those techniques consist of: **Windows Registry Autorun**

- Persistence - Registry Run Keys / Startup Folder (T1060)

12. the attackers used **NTFS Alternate Data Stream** to hide their payloads

- Defense Evasion - NTFS File Attributes (T1096)

<https://cybr.ly/cobaltkitty>

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



Cyberreason Cobalt Kitty Report



13 & 14. The attackers **created and/or modified Windows Services**

- Persistence – New Service (T1050)
- Persistence – Modify Existing Service (T1031)

15 & 16. The attackers **used a malicious Outlook backdoor macro ... edited a specific registry value to create persistence**

- Persistence – Office Application Startup (T1137)
- Defense Evasion – Modify Registry (T1112)

17. The attackers used different techniques and protocols to **communicate with the C&C servers ... HTTP**

- Command and Control - Standard Application Layer Protocol (T1071)

<https://cybr.ly/cobaltkitty>

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



Cyberreason Cobalt Kitty Report



18. **:80 (in traffic from compromised machine to C&C server)**

- Command and Control - Commonly Used Port (T1043)

19 & 20. The attackers **downloaded COM scriptlets using regsvr32.exe**

- Command and Control - Remote File Copy (T1105)
- Execution - Regsvr32 (T1117)

21. **binary was renamed “kb-10233.exe”, masquerading as a Windows update**

- Defense Evasion - Masquerading (T1036)

22. **network scanning against entire ranges...looking for open ports...**

- Discovery - Network Service Scanning (T1046)

<https://cybr.ly/cobaltkitty>

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

And in the next homework, what we'll do is give you 31 reports. Each group will have one report, and each group has to do the mapping. There will be no highlights or hints, and our TAs are pretty ruthless, so you'd better put in the work. I think I've given enough hints about the next homework. Now, let's move on to the next sub-module, which is mapping ATT&CK from raw data.

CS668

Module 3.3:

Mapping to ATT&CK from Raw Data

If you are a threat intel analyst in a company, it is likely that nobody is going to give you a finished report when an incident happens, right? When an incident occurs, you perform forensics. You go and look at various places, like logs, network packet traces at the time of the incident, firewall logs, web server logs, newly created binaries at the endpoints, and so on. You collect all this information, and then you are asked to do a root cause analysis, explaining it in terms of ATT&CK.

Now, you might ask, 'Why are you teaching us how to map from a finished report if, in my job, I may not get a finished report because I am the one who will actually create it?' The reason is that you do not become a threat intel analyst overnight. You have to understand what the attackers do. Reading about the 14 tactics and various techniques in theory is one thing, but actually reading a well-done threat intel report from FireEye, Mandiant, Microsoft, etc., is another thing entirely. These reports offer thorough analysis. By learning how to convert this information, you gain valuable insight into how tactics and techniques are applied in real attacks.

But there's another reason. Suppose you have thousands of these kinds of reports, and you want to create a database of tactics and techniques used by various APT groups. Now, why would you want to create such a database? What good is it? Let's say I take 20 attacks from APT28 and map them to tactics, techniques, and procedures. Then I take 15 attacks from APT3 and do the same. Now I have a database that shows what attacks different APT groups use, in what manner, in what sequence, and so on. What can I do with such data? I can try to learn, with machine learning, how to distinguish between various attack groups.

Eventually, I want to know whether the attack I just experienced is from a nation-state actor or a hobby hacker. If it's a nation-state actor, I want to identify which one. This process is called APT attribution. You want to know which APT group is responsible. Creating this database can be useful for learning this.

One of my PhD students has done this. What accuracy are we getting? In her work, she also used natural language processing to extract the mapping automatically from these reports, so you don't have to manually read everything. Does it work for all reports? Yes, these are the kinds of advancements happening. But coming back to the raw data, most of the time, you will be dealing with raw data.



Mapping to ATT&CK from Raw Data



- **So far, working from intel where activity has already been analyzed**
- **Analysis of techniques/behaviors directly from source data**
 - Likely more information available at the procedure level
 - Not reinterpreting another analyst's prose
 - Greater knowledge/expertise required to interpret intent/tactic
- **Broad set of possible data can contain behaviors**
 - Shell commands, malware, forensic disk images, packets

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

So now, this data requires you to understand some technology, commands, and so on, right? You need much more knowledge and expertise to interpret raw data as behavior compared to finished reports.

You'll see that what you are given might include shell commands that have been used, the type of malware involved, forensic disk images that you have to analyze using forensic tools to reconstruct the sequence of events, packet information, and so on. The process of mapping here involves understanding, of course, ATT&CK. From whatever you are given or whatever your forensic team provides, you need to identify the behavior. Then, you have to research the behavior, translate it into a tactic, figure out what technique was used, and compare your results with those of other analysts, just as you would with finished reports.

Here's an example of what the forensic team found after an attack.

Process of Mapping to ATT&CK



1. Understand ATT&CK
2. Find the behavior
3. Research the behavior
4. Translate the behavior into a tactic
5. Figure out what technique applies to the behavior
6. Compare your results to other analysts

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



1. Find the Behavior



ipconfig /all

sc.exe \\1n334656-pc create
.\recycler.exe a -hpfGzq5yKw C:\\$Recycle.Bin\old
C:\\$Recycle.Bin\Shockwave network.vsd

Commands captured by Sysmon being run interactively via cmd.exe

10.2.13.44:32123 -> 128.29.32.4:443

128.29.32.4:443 -> 10.2.13.44:32123

Flows from malware in a sandbox

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Netsh

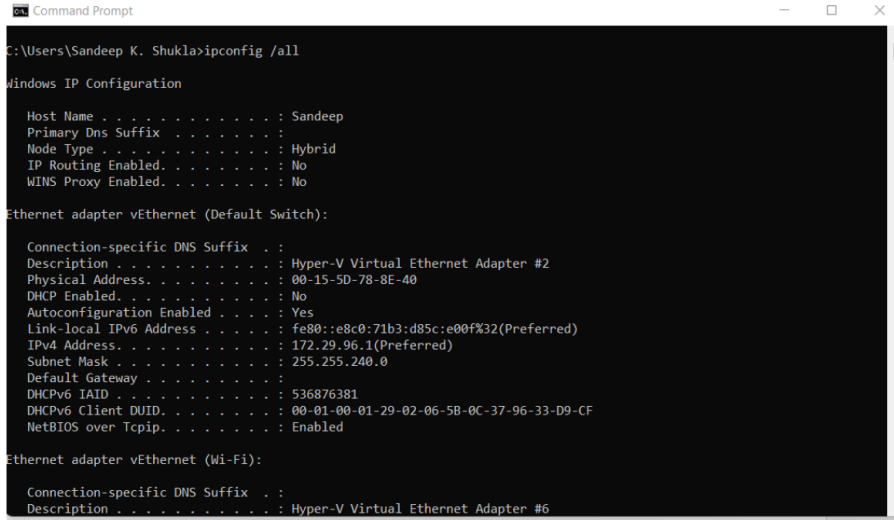
New reg keys during an incident

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

So, they found that the attacker used these commands. First, they used the 'ipconfig' command. Then they used the **sc** command in Windows. Next, they found that there was some two-way interaction between an external IP address and an internal IP address, like 10.2.13.44 and 128.29.32.4. In this machine, like 128.29.x.x, you notice access to port 443, which is the port for the HTTPS protocol, right? Additionally, when you take a registry dump in Windows, you find some new entries in the registry.

So, these are the kinds of things given to you as a threat intel analyst by the forensic team. This may not be all the information, but we're showing a fragment of what's provided to you just to illustrate the kind of work you have to do to interpret this data.

ipconfig /all



```
C:\Users\Sandeep K. Shukla>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Sandeep
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter #2
Physical Address. . . . . : 00-15-5D-78-8E-40
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e8c0:71b3:d85c:e00f%32(Preferred)
IPv4 Address. . . . . : 172.29.96.1(Preferred)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 536876381
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-02-06-5B-0C-37-96-33-D9-CF
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter vEthernet (Wi-Fi):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter #6
```

So, ‘ipconfig’—you’re all familiar with it, right? It’s used to look at MAC addresses, IP addresses, and other network information. But in this case, someone is doing it from inside the network, not from outside. You can’t run ‘ipconfig’ from outside the system; you need to be inside the network, either as malware or through a remote shell. It might be a remote shell, or it could be malware. Someone is using ‘ipconfig’ to figure out the various network interfaces.

‘sc’ is a command for creating services, the Service Control (sc) command in Windows. You can also use it to query other things, but in what we saw, it was trying to create a service. So, we now need to figure out what service it was trying to create, but we’ll get there. The ‘sc’ command is what was used.

As a threat intel analyst, you need to know this, or you need to research what the ‘sc’ command does. Here’s how the ‘sc’ command is used: You basically specify a particular computer name, then use the ‘create’ option, and then you specify which binary should run when the service is created. For example, if you try ‘sc <your computer name> create’, it will prompt you to provide the binary path and other necessary details to complete the service creation.

Command sc query



```

Command Prompt

this case. If the query command is followed by nothing or one of
the options listed below, the services are enumerated.
type= Type of services to enumerate (driver, service, userservice, all)
      (default = service)
state= State of services to enumerate (inactive, all)
      (default = active)
bufsize= The size (in bytes) of the enumeration buffer
         (default = 4096)
ri= The resume index number at which to begin the enumeration
    (default = 0)
group= Service group to enumerate
      (default = all groups)

SYNTAX EXAMPLES
sc query - Enumerates status for active services & drivers
sc query eventlog - Displays status for the eventlog service
sc queryex eventlog - Displays extended status for the eventlog service
sc query type= driver - Enumerates only active drivers
sc query type= service - Enumerates only Win32 services
sc query state= all - Enumerates all services & drivers
sc query bufsize= 50 - Enumerates with a 50 byte buffer
sc query ri= 14 - Enumerates with resume index = 14
sc queryex group= "" - Enumerates active services not in a group
sc query type= interact - Enumerates all interactive services
sc query type= driver group= NDIS - Enumerates all NDIS drivers

C:\Users\Sandeep K. Shukla>

```

Command sc <server> create



```

Command Prompt

Link-local IPv6 Address . . . . . : fe80::45c7:c497:dfe6:8f71%61
IPv4 Address. . . . . : 172.20.64.1
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :

C:\Users\Sandeep K. Shukla>sc \\\SANDEEP create
DESCRIPTION:
    Creates a service entry in the registry and Service Database.
USAGE:
    sc <server> create [service name] [binPath= ] <option1> <option2>...

OPTIONS:
NOTE: The option name includes the equal sign.
    A space is required between the equal sign and the value.
type= <own|share|interact|kernel|filesystem|rec|userown|usershare>
      (default = own)
start= <boot|system|auto|demand|disabled|delayed-auto>
      (default = demand)
error= <normal|severe|critical|ignore>
      (default = normal)
binPath= <BinaryPathName to the .exe file>
group= <LoadOrderGroup>
tag= <yes|no>
depend= <Dependencies(separated by / (forward slash))>
obj= <AccountName|ObjectName>
      (default = LocalSystem)
DisplayName= <display name>
password= <password>

C:\Users\Sandeep K. Shukla>

```

As a threat analyst, you need to develop expertise in various areas, such as interpreting network packet traces, understanding forensics, knowing about malware and how it works, analyzing malware, and understanding command line commands and executables in Windows or whatever system you're working with.

You may have to deal with multiple data sources to figure things out. For instance, if you don't know what 'ipconfig /all' does or want to see if there's a tactic related to this command, you can go to ATT&CK and search for 'ipconfig /all'.



2. Research the Behavior



```
.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old  
C:\$Recycle.Bin\Shockwave_network.vsdX
```

- Can make some educated guesses, but not enough context

File analysis:

When recycler.exe is executed, it gives the following output:

```
C:\recycler.exe  
RAR 3.70 Copyright (c) 1993-2007 Alexander 22 May 2007  
Roshal Shareware versionType RAR -? for  
help
```

- Aha! Based on the analysis we can Google the flags to RAR and determine that it is being used to compress and encrypt the file

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

You'll find that it's related to the 'System Network Configuration Discovery' technique. This technique will also show you examples of various attack groups that have used this command, as they are trying to discover the network configuration of the system they've compromised.

But why do they want to know the system configuration?

Because they want to know which interfaces are connected to, say, a WLAN, a wired LAN, or a Wi-Fi LAN, and they might want to use this information for lateral movement, etc.

Next, we saw that in the 'sc' command, they provided a path to a binary. This binary is named 'recycler.exe'. The command also included flags and inputs, such as directory or input files, and mentioned something about a VSDX file. This might leave you confused—'recycler.exe' is supposed to be a benign program, right? So why would someone want to create a 'recycler' service if they are malicious?

You then decide to check if this 'recycler.exe' binary is already on the compromised machine, and you run it. When you do, you discover that it's not the original 'recycler.exe'; it's a renamed executable. It turns out to be the RAR binary. RAR is used for compression and encryption of files. So, to avoid suspicion, someone has renamed

this executable for obfuscation purposes. Now that you've figured this out, you can Google the flags for RAR, not for 'recycler'.

The screenshot shows the MITRE ATT&CK framework page for 'System Network Configuration Discovery'. The page includes a navigation bar with categories like Matrices, Tactics, Techniques, Groups, Software, Resources, Blog, and Contact. A search bar contains 'ipconfig /all'. The main content area features the title 'System Network Configuration Discovery' and a description: 'Adversaries will likely look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.' Below this is an 'Examples' section with a table:

Name	Description
admin@338	admin@338 actors used the following command after exploiting a machine with LOWBALL malware to acquire information about local networks: <code>ipconfig /all >> %temp%\download^[1]</code>

At the bottom of the screenshot, there is a copyright notice: '©2019 The MITRE Corporation. ALL RIGHTS RESERVED Approved for public release. Distribution unlimited 19-01075-15.' and the MITRE logo.

These flags are for RAR, and you determine that it is being used to compress and encrypt the file. So whatever this input file is, it's being compressed and encrypted. Now, you need to figure out what this file is. When you do a Google search, you find that a VSDX file is actually a Microsoft Visio file. However, this doesn't necessarily mean it's a Visio file. You can rename any file with any kind of suffix. It's just that if you try to load it in Visio, you might get an error indicating that the file doesn't match the expected format. You can take an executable file and rename it as a PDF, right? So, it's obvious that the file extension alone doesn't guarantee the file's true nature. From this, we're figuring out that a file is being compressed and encrypted. It might appear to be a Visio diagram, but it's likely that it's just named as such to disguise its real content. It's probably exfiltrating some data. When do you compress and encrypt files? You do it because you want to do something with the file, right? I mean, you're not just encrypting and compressing files unless you're a ransomware attacker, in which case you would encrypt everything. But here, they're encrypting and compressing one file, which means this file probably contains some intelligence or information that they want to send to the command and control server. Compression is necessary because they want to stay under the radar. If they start sending gigabytes of data, someone will notice, right? A firewall alarm might go off, or an intrusion detection system might be triggered.

2. Research the Behavior



```
.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old  
C:\$Recycle.Bin\Shockwave_network.vsdX
```



vsdX



People also ask

What can open a VSDX file?

A **VSDX file** is a drawing saved in the **VSDX file** format introduced with Visio 2013, a program used for making drawings and technical illustrations.

And the file being compressed/encrypted is a Visio diagram, probably exfiltration

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

But if it's a small file, just a few kilobytes or a low megabyte-sized file, it can go out like a regular email without raising suspicion. It won't be considered an anomaly. So, through 'ipconfig', we find that they were trying to perform system network configuration discovery. This falls under the discovery tactic.

One of the 14 tactics in the ATT&CK framework is called 'discovery.' Most attackers, when they first gain a foothold in a system or device, try to do internal reconnaissance to figure out where they are, what the network structure is, what the machine is connected to, and whether they are running as root. All of this falls under discovery, right? So, one tactic here is discovery, and because 'ipconfig' was run, it also falls under execution. Although 'ipconfig' is a benign program, it's being executed on behalf of a malicious actor, making it part of an attack tactic. So, it will also fall under the execution tactic. We found that in this larger 'sc' service create command, the VSDX file is a Visio file.

So, with moderate confidence, we can infer that this is likely exfiltration because they are compressing and encrypting the file. It's likely intended for exfiltration. And then it's being seen as executed by Sysmon, which indicates execution. This is how we are mapping the tactics.

So here, you see that we are actually going more from technique to tactic, rather than from tactic to technique. In the previous example, we went from tactic to technique. But here, since we are looking at the commands, it's likely that we will identify the technique first and then determine the tactic.

Now

here

we



3. Translate the Behavior into a Tactic



```
ipconfig /all
```

- Specific procedure only mapped to System Network Configuration Discovery
- System Network Configuration Discovery -> **Discovery** ✓
- Seen being run via Sysmon -> **Execution**

```
.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old  
C:\$Recycle.Bin\Shockwave_network.vsdX
```

- We figured out researching this that “**vsdx**” is Visio data
- Moderate confidence **Exfiltration**, commands around this could make clearer
- Seen being run via Sysmon -> **Execution**

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



4. Figure Out What Technique Applies



- **Similar to working with finished reporting we may jump straight here**
 - Procedure may map directly to Technique/Tactic
 - May have enough experience to compress steps

```
ipconfig /all
```

- Specific procedure in **System Network Configuration Discovery (T1016)**
- Also **Command-Line Interface (T1059)**

```
.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old  
C:\$Recycle.Bin\Shockwave_network.vsdX
```

- We figured out researching this that “**a -hp**” compresses/encrypts
- Appears to be **Data Compressed (T1002)** and **Data Encrypted (T1022)**
- Also **Command-Line Interface (T1059)**

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

Okay, so it's time to wrap up for today. We'll continue from here in the next class because discussing techniques and concurrent techniques will take some time.

You're starting to get the idea, right? By now, you should have a good understanding of how to do this with finished reports, and you're starting to get a sense of how to approach it with raw data. By the time we meet next week, we'll dive deeper into working with raw data, okay?