Havtil

Exercise planner

Package 1, exercise 2

‘Cyber incident in the supply chain’

Version 1.0

Table of contents

1 Introduction

1.1 Background and scope

Facilities and installations in the petroleum sector are required to have preparedness plans in place for managing serious incidents. The industry is subject to various scenarios involving ICT incidents, but the Norwegian Ocean Industry Authority (Havtil) has, through audits, noted that little or no training is carried out related ICT security in the industrial control and security systems. Considering this, Havtil has commissioned a set of training and exercise scenarios. These exercises have been prepared by Proactima together with Netsecurity and was adapted by Havtil.

The Activity regulation § 23 stipulates that: «necessary training and necessary drills are conducted, to ensure that the personnel are always able to handle operational disturbances, hazard, and accident situations in an effective manner». The Technical and Operational regulation stipulates the same in § 52. This means that the requirements for training and exercise are the same for onshore and offshore facilities.

Training enhances personal skills and knowledge, while exercises test collaboration and response capabilities during an emergency. In addition, exercises can reveal organisational and structural strengths and weaknesses and prepare management for dealing with various crises.

1.2 Structure of this guide

The exercise planner contains several scenarios. Each scenario includes suggestions on which functions are relevant to the exercise. The scenarios can be used for training, tabletop exercises, or incident response simulation exercises.

Part 3 of the guide contains additional information to aid in preparation and implementation. This includes:

- a possible sequence of events prior to exercise start-up
- a sequential incident flow chart
- relevant technical material

2 Scenario

The scenario in this guide is initiated by a notification from KraftCERT concerning a supply chain attack on systems being utilised by the sector.

2.1 Overview of the scenario

There are different aspects that can impact the industrial ICT systems. This scenario describes four stages of an incident. If required, the scenario can be split up according to the time available.
Table 1 indicates which functions/departments may be appropriate to include in the different stages of the scenario. To scale down the scope of the exercise, it may be appropriate to play out the roles that are not related to ICT.

Table 1. Summary of roles/functions that can usefully be trained using the various modules.

Task	**Stage**	**Personnel responsible for SAS/IACS**	**Local operations managers**	**Personnel responsible for systems operation**	**ICT department**
2.2	Initial events – notification			x	
2.3	Escalation – new information		x	x	x
2.4	Malware			x	x
2.5	Updated software available	x	x	x	

2.2 Initial events – notification

KraftCERT issues a TLP:AMBER+STRICT[1] notification. It notifies that a supply chain attack has been discovered where a threat actor has had access to a software development environment for several years. The threat actor has installed malicious code into the software delivered by the supplier of the central SAS system. The modified code includes control and communications functions in the industrial ICT systems. The notification originates from an international CERT environment.

2.2.1 Advisory questions

Personnel responsible for systems operations

- How are notifications received and managed?
- How do we establish whether installed software versions are affected by the notification?
- What types of network access do the systems have in relation to other networks and units?
- How do we identify signs of irregular activity and traffic?
- Who will be involved?

2.2.2 Additional action points (dependent of the outcome of discussions/decisions)

- Verify notification reception and record internal delays
  - Map the notification management both from relevant suppliers and from KraftCERT
- No indication of misuse is identified
- Unknown DNS traffic from the systems
  - How can this be controlled and managed?

[1] The Traffic Light Protocol (TLP) is an international standard for the classification and sharing of unclassified information. Read more about this at https://www.nsr-org.no/tlp

2.3 Escalation – new information

New information is published by KraftCERT. It has been uncovered that the actor has exploited updates to implement a backdoor. Two different types of backdoors have been observed. These differ depending on when and which updates have been performed.

Backdoor 1:

Monitors TCP/UDP port 1414, where it is possible to establish a command line on the unit by using the password 'ics123' in the initial request.

Backdoor 2:

The same functionality as Backdoor 1, but it also contains a functionality that attempts to achieve contact with the internet (c2). It has been confirmed that the backdoor is attempting to look up the address 'ics-timedate.com'.

2.3.1 Advisory questions

Personnel responsible for systems operations

- How do we establish if any affected software versions have been installed?
- How can we detect whether functionality of the control system is being impacted?
  - Which measures are implemented?
- How to detect whether we have systems where the backdoor has been installed?
- How do we issue notifications for such incidents?

ICT department

- How do we identify signs of irregular activity and traffic?
- Where can we find relevant log data?

Local operations managers

- What are the potential operational and contingency impacts of this incident?
- How does such incident affect the daily risk management?

2.3.2 Additional action points (dependent of the outcome of discussions/decisions)

- Logs show queries to 'ics-timedate.com'.
- Attempts to establish HTTPS-connection to public IP address.

2.4 Malware

New information concerning Backdoor 2. The backdoor is integrated into the system's source code and is activated at start-up. It has been confirmed that the threat actor is able to exploit the backdoor by running random commands (RCE). This is confirmed by CERT environments and several users of the software who have reported the following file (IOC):

Filename: C:\Windows\System32\winhostssvc.exe
Sha256: 2a55d47df5b430bb7c74e7092c8a7f34c7801330ffd5177e3227f3c9ba4fae14

2.4.1 Advisory questions

Personnel responsible for systems operation/ICT department

- How can we detect whether this file is on our systems?
- Do similar files exist?
- Do we conduct monitoring that enables us to investigate what may have been run on behalf of the system supplier?
- What functions does the reported file execute?

2.4.2 Additional action points (dependent of the outcome of discussions/decisions)

- The file is detected on C:\Windows\System32\
- Similar sha256sum on another file on c:\Windows\temp\svchost.exe
- No files that have similar sha256 hash or filename.

2.5 Updated software available

Update is available from the supplier. Following installation of the update, the machine must be restarted to remove the backdoor.

2.5.1 Advisory questions

Personnel responsible for SAS/IACS

- What corrective measures must be taken before or during installation of the update?
- How do we coordinate updates of SCADA nodes?
  - Who should be involved?
  - What procedures should be followed?

Local operations managers

- Which mitigating measures must be implemented before or during installation of the update?
- What are the potential operational impacts?

Personnel responsible for systems operations

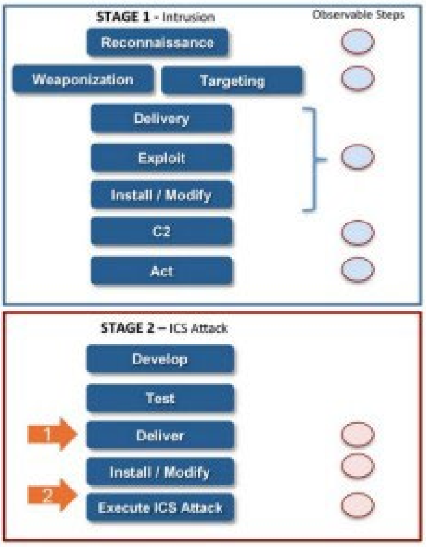
- What systems and services are impacted by the update and restart?
- Which procedures should be followed?
- Who should be involved to execute the update?
- Who will be impacted by the update?

2.5.2 Additional action points (dependent of the outcome of discussions/decisions)

- The update is working as intended and the systems running after a short delay.
- An error (‘missing dependencies’) is discovered during the update.
  - We are not able to contact the supplier.
  - We receive an offer of assistance from the supplier.
  - This requires a comprehensive system update (dependencies).

3 Additional information for preparation and implementation

This chapter contains background information about targeted cyber-attacks against industrial ICT systems. Digital attacks often adhere to fixed patterns, often referred to as ‘kill chains’. Supply chain attacks also follow this pattern but are more challenging as stage 1 is executed in a different organisation. The diagram on the right illustrates the various stages making up this exercise, as well as the exercise items incorporated into the guide.



- Supply chain attack
  - Stage 1 executed against SW supplier
- Attack:
  1) Stage 2, deliver
  2) Backdoor opens for execute/C2 in the control network
- Exercise points:
  - Information flow from CERT
  - Control over installed SW
  - Uncover traffic to/from backdoor

3.1 Introduction to the incident

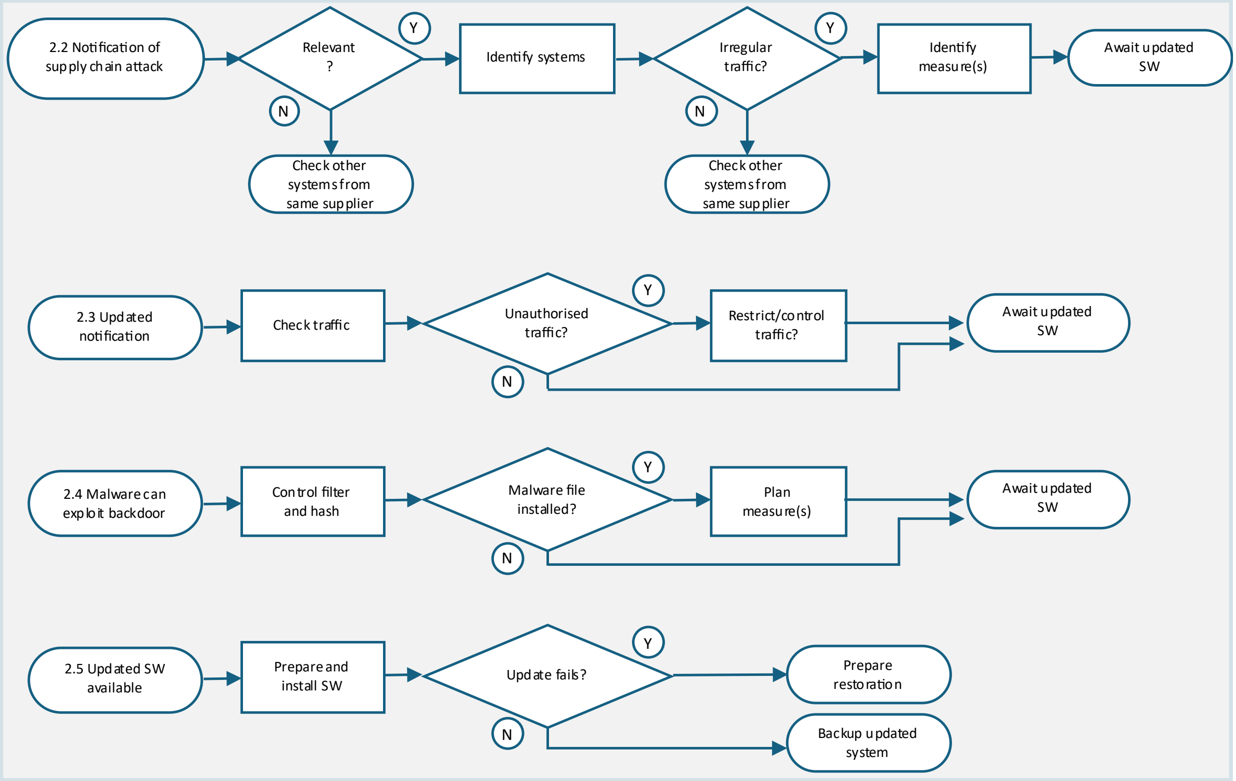
Threat actors do not always attack their primary target directly. Organisations that are know they may be attractive targets often have effective procedures in place and robust systems that can be difficult to penetrate. Subcontractors do not always operate with the same levels of security.

Another approach may be to attack organisations that supply systems to multiple clients. You will find two such examples referred to in Chapter 3.4 of this guide.

This incident describes an attack on a control system manufacturer using software updates containing malware.

3.2 The incident

This scenario has been based on the following sequence of events:



The sequence of events illustrates one potential approach to how industrial ICT systems can be infiltrated. The threat actor ‘APT29’ often targets sectors such as energy and telecom, as well as military and governmental organisations. It is also assumed that this actor may be affiliated with the Russian foreign intelligence services (SVR).[2]

The final page of this guide contains a chart from the global knowledge database MITRE ATT&CK®[3]. It shows an extract from a set of tactics and techniques used by threat actors based on reported observations. MITRE ATT&CK® also contains information about typical tactics and techniques used by a variety of different threat actor groups.

[2] https://attack.mitre.org/groups/G0016/

[3] https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0016%2FG0016-enterprise-layer.json

3.3 Lessons learned

Review of procedures, clarification of areas of responsibility, and systems improvements.

- How are the participants involved to provide feedback to the final report from the exercise?

Personnel responsible for systems operations

- Are roles and areas of responsibility adequately described?
- How do existing procedures support incident management?
- Were the procedures adhered to? What modifications should be made?

Personnel responsible for SAS/IACS

- Are roles and areas of responsibility adequately described?
- How do existing procedures support incident management?
- Were the procedures adhered to? What modifications should be made?
- How do we ensure learning across all shifts?

Local operations managers

- How do existing procedures support incident management?
- How do we ensure learning across all shifts?

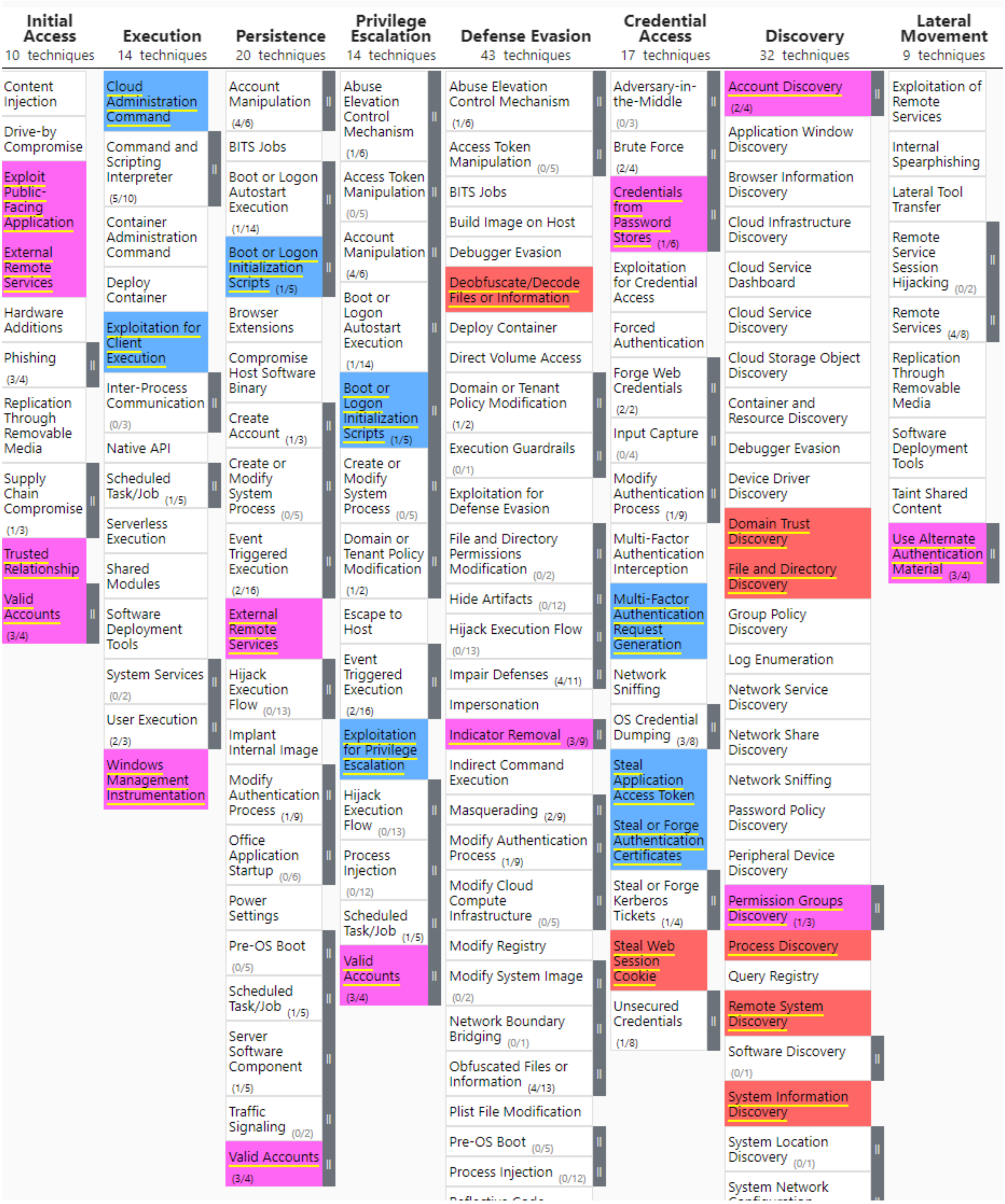
3.4 Relevant reference material relating to supply chain attacks

Supply chain attacks are not merely theoretical. The following paragraphs illustrates two examples:

> In December 2020, it was discovered that the Russian foreign intelligence services (SVR) had obtained access to the internal networks of the company SolarWind. The attack involved the distribution of malware as part of standard program code. The American authorities have published a description of this incident, among others, in the document ‘SolarWinds and Related Supply Chain Compromise’.[4]
>
> In April 2024, *Securityweek.com* published an article describing how a threat actor from North Korea had for at least five years been exploiting a vulnerability in an update of the antivirus software eScan. This vulnerability had enabled a so-called ‘man-in-the-middle’ attack by which malicious code had been connected to the regular updates.[5]

[4] https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds%20and%20Related%20Supply%20Chain%20Compromise%20White%20Paper.pdf

[5] https://www.securityweek.com/north-korean-hackers-hijack-antivirus-updates-for-malware-delivery/?is=152b81581ed4086dca174884e2d1b3dd849835878ef11af1c750fefad5244aa6



Initial Access 10 techniques
- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3/4)
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
- Trusted Relationship
- Valid Accounts (3/4)

Execution 14 techniques
- Cloud Administration Command
- Command and Scripting Interpreter (5/10)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (1/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (2/3)
- Windows Management Instrumentation

Persistence 20 techniques
- Account Manipulation (4/6)
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (1/5)
- Browser Extensions
- Compromise Host Software Binary
- Create Account (1/3)
- Create or Modify System Process (0/5)
- Event Triggered Execution (2/16)
- External Remote Services
- Hijack Execution Flow (0/13)
- Implant Internal Image
- Modify Authentication Process (1/9)
- Office Application Startup (0/6)
- Power Settings
- Pre-OS Boot (0/5)
- Scheduled Task/Job (1/5)
- Server Software Component (1/5)
- Traffic Signaling (0/2)
- Valid Accounts (3/4)

Privilege Escalation 14 techniques
- Abuse Elevation Control Mechanism (1/6)
- Access Token Manipulation (0/5)
- Account Manipulation (4/6)
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (1/5)
- Create or Modify System Process (0/5)
- Domain or Tenant Policy Modification (1/2)
- Escape to Host
- Event Triggered Execution (2/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/13)
- Process Injection (0/12)
- Scheduled Task/Job (1/5)
- Valid Accounts (3/4)

Defense Evasion 43 techniques
- Abuse Elevation Control Mechanism (1/6)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification (1/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/12)
- Hijack Execution Flow (0/13)
- Impair Defenses (4/11)
- Impersonation
- Indicator Removal (3/9)
- Indirect Command Execution
- Masquerading (2/9)
- Modify Authentication Process (1/9)
- Modify Cloud Compute Infrastructure (0/5)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (4/13)
- Plist File Modification
- Pre-OS Boot (0/5)
- Process Injection (0/12)

Credential Access 17 techniques
- Adversary-in-the-Middle (0/3)
- Brute Force (2/4)
- Credentials from Password Stores (1/6)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2/2)
- Input Capture (0/4)
- Modify Authentication Process (1/9)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (3/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (1/4)
- Steal Web Session Cookie
- Unsecured Credentials (1/8)

Discovery 32 techniques
- Account Discovery (2/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (1/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (4/8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (3/4)

Extract of tactics and techniques used by threat actors in attacks against industrial ICT systems. «MITRE ATT&CK®», https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0016%2FG0016-enterprise-layer.json