Script Functions	**Script Actions**
Preparation	Attacker decided to target the TU/e and hold it's data for ransom (unclear exactly why TU/e was targeted, probably for financial gains).
Entry Gaining access to the crime location.	Gains access to legitimate TU/e VPN accounts through leaked credentials (maybe on the dark web).
Pre-condition Establishing the conditions for the crime.	Using multiple accounts to login to the network without triggering suspicion of the SOC, ensuring MFA is not asked by the VPN. Identify the high-value systems in the environment.
Instrumental pre-condition Acquiring the tools, skills, or knowledge for the crime.	Obtains ransomware loader, privilege escalation tools, sets up exfiltration server, and prepares command and control servers as needed.
Instrumental initialization Finalizing preparations just before the crime.	Deploys necessary tools into the environment, creates ransomware payload but does not execute, and collects credentials for lateral movement into the network. Conducting discovery activities to look for reachable networks and systems.
Instrumental actualization Executing the actions necessary to commit the crime.	Using remote administration tools to access more systems. Creating more domain accounts. Adversary elevates themselves to the highest privilege, domain administrator enterprise privilege. Coercing multiple domain controllers into downgrading and authenticating to the adversary. In addition, cracking the challenge/response hashes can be added here.
Doing Committing the crime.	Attacker deploys ransomware to encrypt data and exfiltrate it outside of TU/e. Includes sensitive data but can also include usernames and passwords for long-term access.
Post-Condition Taking responsive action after the crime.	Deletes files and backup from TU/e servers to prevent data being retrieved. May also leave notes that direct TU/e towards a method to retrieve their data after paying a ransom. May also corrupt backup servers.
Exit Leaving the crime location.	Disconnects from the VPN, close any shells, and lock out legitimate administrator accounts, clear their logs to hide activity in the event of forensic reconstruction.

This is the original robbery script that was created by Cornish. However, there are further additions that can be made if we want to make it more specific.

- For example, we can add 'script actions', these essentially, indicate with tools as to what the adversary is going to do.
- We can add ways of failing and add explanations for them as well. These can be useful for SOCs to detect activity or logs that indicate failure.
- Cornish also mentions intervention points for situational measures. These are specific controls that can be placed to prevent the situation from getting out of hand.
    - For the TU/e example, that would be to have MFA activated for the VPN (which they have now obviously).
    - I personally think this might be a good touch, since it does add what a SOC or company can to do mitigate the actions of the adversary at specific points in time.

Advantages over the flat TTP lists

- Ordered attack flow with motivation and intent.
- Can show prerequisites and conditions required.
- There are branching pathways in terms of what the attacker can generally do.
- Can show SOCs where the intervention points are, what systems they can set up or what requirements they must fulfil.
- This is more easier to read for analysts, and it's technicality or abstract level can be reduced depending on who the report is for.

Claude Crime Script of TU/e report

High Level Abstraction Written Out and Info Check

Preparation (correct, a VPS is not explicitly mentioned in the resources but it can be inferred)	The attacker gathers intelligence and acquires credentials that will allow access to the target system. Furthermore, the attacker identifies potential weaknesses in the target infrastructure, in this case in the authentication infrastructure.	TA0042 – Resource Development - T1583 – Acquire Infrastructure - T1588 – Obtain Capabilities - T1589 – Gather Victim Identity Information TA0043 – Reconaissance

	The malicious actor was able to obtain leaked credentials which were available on the dark web. There were also two data breaches for the second account that was used to gain access. The attacker conducted thorough research about the TU/e infrastructure since they were able to identify that the VPN did not require MFA.	- T1590 – Gather Victim Network Information - T1591 – Gather Victim Org Information
Entry (correct, also limited the login to entry, did not add the login for initial reconnaissance)	The attacker leverages the previously obtained credentials and their knowledge of the target infrastructure's weaknesses to gain unauthorized access to the internal network. However, this is done through a legitimate access pathway. The malicious actor used the leaked credentials to successfully login to multiple accounts and was able to establish VPN access to the TU/e network.	TA0001- Initial Access - T1078 – Valid Accounts - T1133 – External Remote Services.
Pre-condition (mostly correct, the automatic network reconnaissance can be inferred and so can the domain controllers, although they're not explicitly mentioned)	The attacker uses the compromised and authenticated accounts to perform automated reconnaissance to map the network and identify valuable accounts. The malicious actor leverages the authenticated accounts to attempt to connect to multiple systems to map the network and look for more valuable accounts like domain controllers.	TA0007 – Discovery - T1018 – Remote System Discovery - T1046 – Network Service Scanning - T1069 – Permission Groups/Domain Groups Discovery - T1482 – Domain Trust Discovery
Instrumental Pre-condition (correct, a lot of inference is done from the report in terms of the tools needed, but they	The attacker identifies and prepares the tools needed for privilege escalation to exploit	TA0042- Resource Development - T1588- Obtain Capabilities

are correct, except the coercion attack does not have irrefutable evidence).	the authentication issues present in the infrastructure. The malicious actor gathers the required coercion and hash-cracking tools, and modifies the infrastructure to exploit the NTLMv1 vulnerability on the TU/e domain controllers.	
Instrumental Initiation (incorrect, there are some issues here because they do not belong to this stage, the actual coercion attack, the successful DSync and elevated privileges belong to the following stage. This phase would only have the testing.)	The attacker conducts tests to check whether the environment is exploitable and creates these test. This is the last step before conducting activity to compromise the domain. The malicious actor performs the preliminary replication and coercion attempts, while also capturing the domain controller authentication material. These steps will confirm that the environment can be properly exploited according to the information that was previously gathered.	TA0004 – Privilege Escalation TA0006 – Credential Access - T1003.006 – DCSync - T1110.002 – Password Cracking - T1552.004 – Private Keys - T1557 – Adversary-in-the-Middle TA0007 – Reconnaissance - T1590 – Gather Victim Network Information - T1592 – Gather Victim Host Information TA0042 – Resource Development - T1588 – Obtain Capabilities
Instrumental Actualization (mostly correct but should start with privilege escalation and the previously mentioned steps from stage 5,)	The attacker performs a successful privilege escalation and has robust control of the environment. They proceed to exact further control through lateral movement and weaken recovery. These actions are conducted to prepare the	TA0003 – Persistence - T1136 – Create Account - T1543.003 – Create or Modify System Process.

	environment for ransomware deployment. The malicious attacker successfully escalates their privilege in the environment and conduct extensive internal discover while establishing persistence through multiple systems. Remote access tools were also used to prepare the environment for deploying ransomware.	- T1547 – Boot or Logon Autostart Execution. - TA0007 – Discovery - T1018 – Remote System Discovery - T1046 – Network Service Discovery - T1069.002 - Permission Groups Discovery - T1083 – File and Directory Discovery TA0008 – Lateral Movement - T1021.001 - T1021.006 - T1550 .002 – Use Alternate Authentication Material.
Doing (mostly correct, contains the relevant information for this stage, even if the intended objective was not achieved, some things need to be moved around though)	The attacker is conducting the crime by initiating actions that are associated with ransomware deployment and mass data exfiltration. This was prevented but some data was exfiltrated before the incident response. Without the incident response the attacker looked to be conducting a double extortion ransomware attempt.	TA0005 – Defence Evasion - T1027 – Obfuscated Files or Information - T1070 – Indicator Removal - T1562 – Impair Defences TA0009 – Collection - T1005 – Data from Local System

		- T1039 – Data from Network Shared Drive TA0010 – Exfiltration - T1020 – Automated Exfiltration - T1041 – Exfiltration over C2 Channel - T1567 – Exfiltration over Web Service TA0040 - Impact - T1486 – Data Encrypted for Impact - T1489 – Service Stop - T1490 – Inhibit System Recovery -
Exit	The attacker’s operations were abruptly terminated when the network was switched off. As a result, there is numerous forensic evidence and tool traces that were left behind, since there was no time to do a cleanup operation.	TA0005- Defence Evasion - T1036 - Masquerading - T1070 – Indicator Removal on Host