Crime Script Analysis Table: TU/e Cyberattack (January 2025)

Based on Cornish (1994) Seven-Stage Crime Script Framework

Main Crime Script Table

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools
1. PREPARATION	Pre-Jan 6, 2025	**Adversary obtained leaked credentials and prepared attack infrastructure**	• Obtained leaked credentials for account_lp2 and account_lp3 [p.11-12] • Fox-IT found credentials in publicly available leak document [p.12] • Researched TU/e infrastructure • Identified VPN without MFA [p.11] • Prepared exploitation tools	**TA0043: Reconnaissance** • T1589.001: Gather Victim Identity Information: Credentials • T1590: Gather Victim Network Information • T1592: Gather Victim Host Information **TA0042: Resource Development** • T1583.003: Acquire Infrastructure: Virtual Private Server • T1588.002: Obtain Capabilities: Tool • T1586.001: Compromise Accounts: Social Media Accounts	• Credential leak databases [p.11-12] • VPS hosting infrastructure [p.11] • Advanced IP Port Scanner [p.16, p.23] • SoftPerfect Network Scanner [p.16, p.23] • ShareFinder [p.16, p.23] • AnyDesk [p.16-17, p.23] • TeamViewer [p.16-17, p.23] • CrackMapExec [p.5, p.12]

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools
2. ENTRY	Jan 6, 2025 13:57-14:13	**Adversary gained initial access via VPN using leaked credentials**	• 13:57 - Failed login: account_lp1 from ip_adversary_1 [p.11] • 14:08 - **SUCCESSFUL LOGIN:** account_lp2 from ip_adversary_1 [p.11] • 14:13 - **SUCCESSFUL LOGIN:** account_lp3 from same IP [p.11] • Established VPN access to internal network [p.11] • Fox-IT considers this incident start [p.11, p.22]	**TA0001: Initial Access** • T1078: Valid Accounts • T1078.002: Valid Accounts: Domain Accounts • T1133: External Remote Services • T1110.004: Brute Force: Credential Stuffing	• Leaked valid credentials [p.11-12] • VPS from hosting provider [p.11] • VPN client software
3. PRE-CONDITION (Initial Reconnaissance)	Jan 6-10, 2025	**Adversary performed network reconnaissance and mapped Active Directory infrastructure**	• 15:14 (Jan 6) - account_lp2 connected to multiple systems [p.11] • Connections atypical for account_lp2 [p.11] • Rapid succession = automated authentications [p.11] • Automated network reconnaissance [p.11] • Mapped network infrastructure • Identified domain controllers and AD structure [p.13] • Located: SYSTEM_DC1_PROD, SYSTEM_DC2_PROD, SYSTEM_DC3_PROD, SYSTEM_DC4_PROD [p.13, p.24]	**TA0007: Discovery** • T1087: Account Discovery • T1087.002: Account Discovery: Domain Account • T1018: Remote System Discovery • T1046: Network Service Discovery • T1069: Permission Groups Discovery • T1069.002: Permission	• Network scanning tools • VPN access [p.11] • Compromised user credentials [p.11]

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools
				Groups Discovery: Domain Groups • T1482: Domain Trust Discovery **TA0008: Lateral Movement** • T1021: Remote Services (reconnaissance attempts)	
4. INSTRUMENTAL PRE-CONDITION (Privilege Escalation Prep)	Jan 6-11, 2025	**Adversary identified authentication protocol weaknesses to enable privilege escalation**	• Identified DCs accepting NTLMv1 authentication [p.13-14, p.24] • Discovered lmcompatibilitylevel=1 on prod DCs [p.14, p.24] • Table 12: 4 prod DCs with level 1 [p.24] • Prepared coercion attack infrastructure [p.13-14] • Targeted ACCOUNT_DC4_PROD for credential theft [p.13-15] • Set up hash cracking capability [p.13-14]	**TA0007: Discovery** • T1201: Password Policy Discovery • T1033: System Owner/User Discovery **TA0004: Privilege Escalation** (preparation) • T1558: Steal or Forge Kerberos Tickets (preparation) **TA0006: Credential Access** (preparation) • T1003: OS	• NTLM relay tools • Hash cracking infrastructure [p.13-14] • Coercion attack tools [p.13-14]

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	S
				Credential Dumping (preparation) • T1212: Exploitation for Credential Access		
5. INSTRUMENTAL INITIATION (Privilege Escalation)	Jan 11, 2025 19:59-21:07	**Adversary executed coercion attack, performed DCSync, and obtained enterprise admin privileges**	**First DCSync Attempt (19:59):** [p.13] • Auth to SYSTEM_DC4_PROD using ACCOUNT_DC4_PROD • DCSync attempt - **UNSUCCESSFUL** (Defender detected) **Coercion Attack (~19:59-20:59):** [p.13-14] • Table 4: NTLMv1 auths from DC accounts to DCs from VPN IPs [p.13] • Likely coerced SYSTEM_DC4_PROD into NTLMv1 auth [p.14] • Captured & cracked ACCOUNT_DC4_PROD NTLMv1 hash [p.14] **Successful DCSync (20:59):** [p.13] • Auth to SYSTEM_DC1_PROD as ACCOUNT_DC4_PROD • DCSync attack - **SUCCESSFUL** [p.13] • Retrieved all NTLM	**TA0006: Credential Access** • T1557: Adversary-in-the-Middle • T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay • T1003.006: OS Credential Dumping: DCSync • T1212: Exploitation for Credential Access • T1556: Modify Authentication Process **TA0004: Privilege Escalation** • T1078.002: Valid Accounts: Domain Accounts • T1068: Exploitation for Privilege	• Cracked DC computer account credentials [p.14-15] • DCSync tools [p.13] • Pass-the-hash capabilities [p.15]	

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools
			hashes from SYSTEM_DC1_PROD [p.15] • Obtained hash for account_hp1 [p.15] **Domain Compromise (21:07):** [p.15] • Auth using account_hp1 hash (pass-the-hash) • **ENTERPRISE ADMIN ACHIEVED** [p.12, p.15]	Escalation **TA0008: Lateral Movement** • T1550.002: Use Alternate Authentication Material: Pass the Hash	
6. INSTRUMENTAL ACTUALIZATION (Post-Exploitation)	Jan 11, 21:07 - Jan 12, 01:17	**Adversary performed discovery, established persistence via accounts and remote tools, and targeted backup systems**	**Discovery Activities:** [p.16] • 22:43 - Advanced IP Scanner on system_srv2 [p.16] • 22:53 - SoftPerfect Scanner on tfe290 [p.16] • 23:56 - ShareFinder on SYSTEM_SRV4 [p.16] • 00:58 - Domain admin enumeration [p.20] **Account Persistence:** [p.17] • Compromised: account_hp2 (22:00), account_hp3 (22:01) • Created: account_hp4 (22:46), account_hp5 (23:11) **Tool Persistence:** [p.16-17] • AnyDesk: system_srv1 (23:27), system_srv3 (23:29),	**TA0007: Discovery** • T1046: Network Service Discovery • T1135: Network Share Discovery • T1087.002: Account Discovery: Domain Account • T1069.002: Permission Groups Discovery: Domain Groups • T1018: Remote System Discovery **TA0003: Persistence** • T1136.002:	• Enterprise admin privileges [p.12, p.18] • AnyDesk [p.16-17] • TeamViewer [p.16-17] • Advanced IP Scanner [p.16] • SoftPerfect Network Scanner [p.16] • ShareFinder [p.16] • PowerShell [p.17, p.20] • CrackMapExec [p.5, p.12]

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools
			system_rootdc2_prod (00:23), system_dc1_prod (00:44) • TeamViewer: system_ws2 (22:36), system_ws1 (23:32), system_srv3 (23:58) • Confirmed connections to system_srv3 and system_srv1 [p.16] **Ransomware Prep:** [p.17] • 00:52 - Accessed Veeam backup on system_srv5 • 00:57 - Attempted to stop Veeam services **Scope:** [p.18] • 14 hands-on-keyboard systems • 77 authentication-only systems • **Total: 91/350 systems accessed** [p.18, Table 9]	Create Account: Domain Account • T1098: Account Manipulation • T1219: Remote Access Software • T1543: Create or Modify System Process **TA0005: Defense Evasion** • T1562.001: Impair Defenses: Disable or Modify Tools **TA0040: Impact** (preparation) • T1490: Inhibit System Recovery • T1485: Data Destruction (preparation)	
7. DOING (Criminal Objective - INTERRUPTED)	Jan 11-12, 2025	**Adversary prepared for ransomware deployment but was detected and contained**	**Intended (Not Achieved):** [p.20-21] • Ransomware deployment across domain (likely based on TTPs) • Mass system encryption • Double-extortion	**TA0009: Collection** • T1005: Data from Local System • T1039: Data from Network Shared Drive	• Full domain control [p.15, p.18] • Remote admin tools [p.16-17] • Multiple high-privileged accounts [p.17]

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools
		before execution	scenario **Accomplished:** • ~2.1 GB data exfiltrated (Jan 5-12) [p.19] • Contents: VPN data, AD info (system names, usernames, password hashes) [p.19-20] • No large-scale data exfiltration [p.20, p.22] • ShareFinder results file deleted [p.16] • Full enterprise admin access [p.18] • Multiple persistence mechanisms [p.16-17] • Backup disruption attempted [p.17] **DETECTION & INTERRUPTION:** [p.5, p.12] • 21:55 (Jan 11) - SURFsoc alerted [p.5] • 63 security alerts generated [p.12] • 22:48 - Escalated to TU/e [p.5] • 23:20 - FoxCERT informed [p.5] • 00:15 (Jan 12) - Intake call [p.5] • **01:17 - Network isolated** [p.5, p.22] • Attack contained before ransomware [p.22]	• T1119: Automated Collection **TA0010: Exfiltration** • T1041: Exfiltration Over C2 Channel • T1020: Automated Exfiltration **TA0011: Command and Control** • T1071: Application Layer Protocol • T1132: Data Encoding • T1573: Encrypted Channel **TA0040: Impact** (intended, not achieved) • T1486: Data Encrypted for Impact • T1490: Inhibit System Recovery • T1491: Defacement	• Backup access [p.17] • C2 infrastructure [p.19]

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools
8. EXIT (Post-Crime)	Jan 12, 2025 onwards	**Network isolation forced adversary exit; extensive forensic evidence remained for investigation**	**Forced Exit:** [p.5, p.22] • 01:17 - Network disconnection terminated all connections [p.5] • VPN sessions terminated • C2 channels severed • Ransomware deployment prevented [p.22] **Evidence Left:** • Forensic artifacts on 91 systems [p.18] • 63 SOC alerts in SIEM [p.12] • VPN authentication logs [p.11, p.23, Table 11] • Windows Event logs [p.13-15] • Installed remote tools: AnyDesk, TeamViewer [p.16-17, p.23] • Created accounts: account_hp4, account_hp5 [p.17, p.23] • PowerShell history with Cyrillic comments [p.16-17, p.20] • Firewall logs showing 2.1 GB transfer [p.19] • IOCs [p.23, Table 10] **Adversary Attribution:** [p.20-21] • Cyrillic characters (Russian language) [p.20] • Off-the-shelf tools = commodity ransomware	**N/A - Post-Incident Activities:** **Defender Response:** • Incident Response • Forensic Analysis • Threat Hunting • Malware Analysis • Indicators of Compromise (IOC) Collection • Timeline Reconstruction • Attribution Analysis	• N/A (Exit forced by defender) [p.5]

Stage	Date/Time	High-Level Abstraction	Activities	MITRE ATT&CK Tactics & Techniques	Resources/Tools	S
			actor [p.20-21] • Non-stealthy techniques = not APT [p.20]			

Key Findings Summary

Category	Details
Attack Duration	January 6, 14:08 - January 12, 01:17, 2025 = **5 days, 11 hours, 9 minutes** [p.11, p.5, p.22]
Initial Access Method	Leaked credentials + VPN without MFA [p.11-12, p.22]
Privilege Escalation	NTLMv1 coercion attack → DCSync → Pass-the-hash [p.13-15, p.22]
Highest Privilege Obtained	Enterprise Administrator (full domain control over DOMAIN_1 and DOMAIN_2) [p.12, p.15, p.22]
Systems Compromised	91 systems (14 hands-on-keyboard, 77 authentication only) out of 350 total [p.18, p.22]
Data Exfiltrated	~2.1 GB (primarily AD info: system names, usernames, password hashes); no large-scale exfiltration found [p.19-20, p.22]
Threat Actor Profile	Ransomware operator (commodity, non-APT) with Russian language indicators [p.20-21, p.22]
Criminal Objective	Ransomware deployment (presumed based on TTPs, not achieved) [p.20, p.22]
Detection Point	SURFsoc alerts, January 11 at 21:55 (63 alerts generated) [p.5, p.12]
Containment Action	Network isolation, January 12 at 01:17 [p.5, p.22]
Outcome	Attack interrupted before ransomware deployment; swift containment prevented catastrophic damage [p.22]

Critical Vulnerabilities Exploited

Vulnerability	Stage	Impact	Mitigation
No MFA on VPN [p.11]	Stage 2	Enabled initial access with leaked credentials [p.11-12]	Implement MFA on all remote access solutions [p.11]
NTLMv1 acceptance on domain controllers [p.14, p.24]	Stage 4-5	Enabled privilege escalation via coercion attack and hash cracking [p.13-15]	Disable NTLMv1, set lmcompatibilitylevel=5 on all DCs [p.14, p.24, Table 12]
Insufficient DC replication logging [p.15, p.24]	Stage 5	Delayed DCSync detection; only failure events logged [p.15, p.24, Table 13]	Enable success logging for Directory Service Replication events [p.15, p.24]
Leaked credentials in public breaches [p.11-12]	Stage 1-2	Provided valid access to VPN [p.11-12]	Credential monitoring, proactive password resets, breach notification monitoring [p.12]
Weak audit policies [p.15, p.24]	Stages 3-6	Limited visibility into adversary activities [p.13-18]	Comprehensive logging and SIEM integration [p.9, Table 2]
No EDR on domain controllers [p.9]	Stage 6	Delayed detection of remote administration tool installation [p.16-17]	Deploy EDR on all critical infrastructure [p.9, Table 2]

MITRE ATT&CK Tactics Summary by Stage

Stage	Primary MITRE ATT&CK Tactics
1. Preparation	TA0043: Reconnaissance, TA0042: Resource Development
2. Entry	TA0001: Initial Access
3. Pre-condition	TA0007: Discovery, TA0008: Lateral Movement
4. Instrumental Pre-condition	TA0007: Discovery, TA0004: Privilege Escalation (prep), TA0006: Credential Access (prep)
5. Instrumental Initiation	TA0006: Credential Access, TA0004: Privilege Escalation, TA0008: Lateral Movement
6. Instrumental Actualization	TA0007: Discovery, TA0003: Persistence, TA0005: Defense Evasion, TA0040: Impact (prep)

Stage	Primary MITRE ATT&CK Tactics
7. Doing	TA0009: Collection, TA0010: Exfiltration, TA0011: Command and Control, TA0040: Impact (intended)
8. Exit	N/A - Post-Incident (Defender Response)

Reference: Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies, 3*, 151-196.