APT 시나리오 분석 문제

Target : <https://blog.naver.com/sk_shieldus/222704110870>

1. 각 스텝별로 MITRE ATT&CK Matrix 의 어느 분류에 속하는지 정의하시오

( 분류 : Reconnaissance / Resource Development / Initial Access / Execution / Persistence / Privilege Escalation / Defense Evasion / Credential Access / Discovery / Lateral Movement Collection / Command and Control / Exfiltration / Impact )

Step 1: 이메일 주소 수집

Reconnaissance

Phishing for Information (T1598.002)

Step 2: 계정 정보 탈취

Credential Access

Spearphishing Link (T1566.002)

Spearphishing Attachment (T1566.001)

Input Capture: Keylogging (T1056.001)

Step 3: 악성 메일 유포

Initial Access

Spearphishing via Service (T1566.003)

Execution

Malicious File (T1204.002)

Step 4: 2차 공격(확장 또는 추가 피해)

Privilege Escalation

Valid Accounts (T1078)

Collection

Data from Local System (T1005)

Exfiltration

Exfiltration Over Command and Control Channel (T1041)

Impact

Data Encrypted for Impact (T1486)

(Reconnaissance 와 같은 대분류만 작성해도 정답처리)

1. 2022년 북한 해킹조직 김수키는 FTP관련 1-day 취약점을 사용하였다. 해당 취약점의 CVE 번호와 대상 소프트웨어의 이름을 서술하시오

Follina (CVE-2022-30190)

(2-1) 이미 패치 버전이 배포된 소프트웨어의 취약점을 이용한 공격임에도 파급력이 존재하는 이유와 해결 방안을 서술하시오

구버전 소프트웨어를 여전히 사용하고 있는 이용자가 있었기 때문이다

(관련 내용 정답처리)