국가수사본부
안보수사국

수사 현장에서 경험한 중소기업 보안

23.12.04.

경찰청 안보수사국
임정현

목 차

여러분의 회사 보안은 안녕한가요?

□ 업무 소개

– 경찰청 안보수사국

□ 중소기업 침해사고 대응 유형(처음 현장방문)

– (침묵…) // 우리 경영진은 바뻐요…무슨 일 있나요?

– 우리 회사는 너무 어려워요…돈이 없어요…!

– 이! 우리 회사에 아무것도 없어요…가지고 갈 것도 없는데…!

– 아! 기업이 경찰을 심문 하네…! 누가 경찰인지?

□ 침해사고 수사 현장 이야기를 여러분께 전달하며

– 우리 회사의 현 위치는 어디인가?

– [생각합시다]보안을 할 것인가? 보완을 할 것인가?

– 역시 현장은 애드리브지??

업무자료 관리 취약(망분리)

□ 망분리 **없는** 업체(OO기술 독점)

– 상황

1) 주요 자료는 별도의 시스템과 분리된 HDD에 보관하고 있어 유출 가능성이 없다는 업체 사장의 언동!

2) 업무는 역시 유무선 모두 편하게 사용하자!

3) 우리회사에 고정IP는 없다!

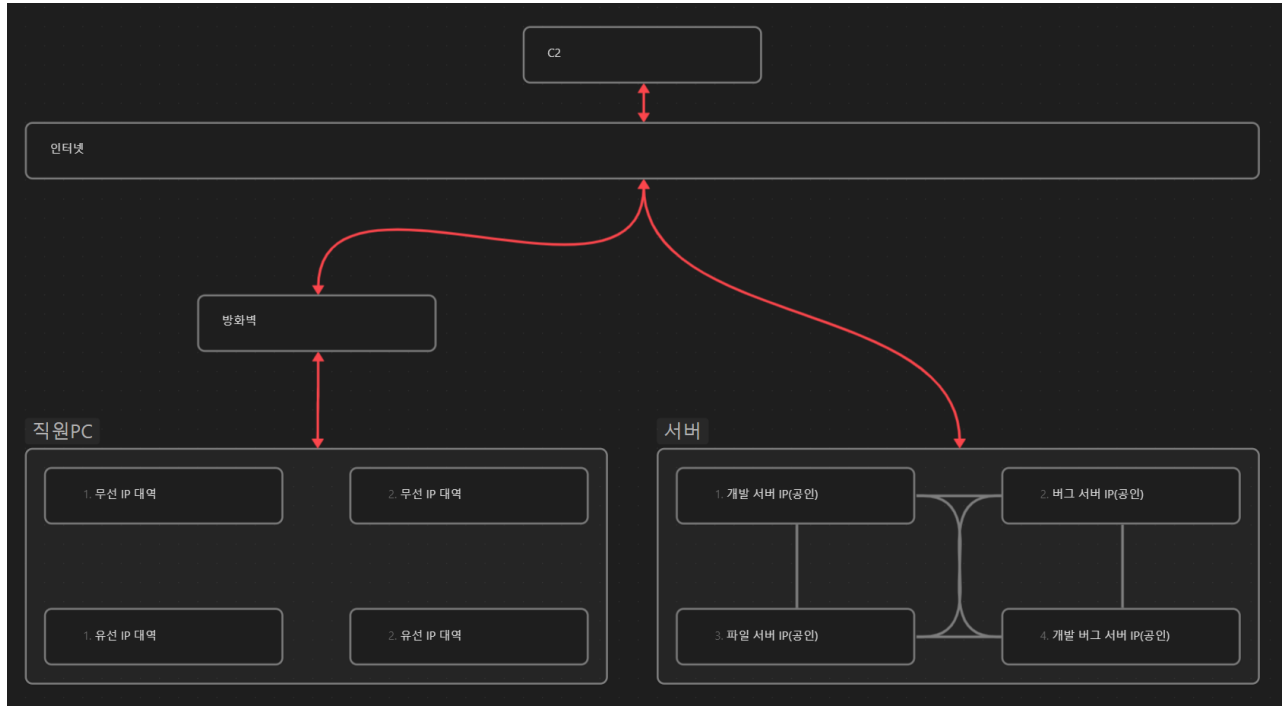
4) 서버는 무조건 공인IP지!

5) 우리회사에 방화벽이 있다니?

– 문제

1) 그 기술을 통해 직원들이 개발을 하고 있는 모순

2) 모두 유출



업무자료 관리 취약(망분리)

□ 망분리 업체(망분리이해 부족)

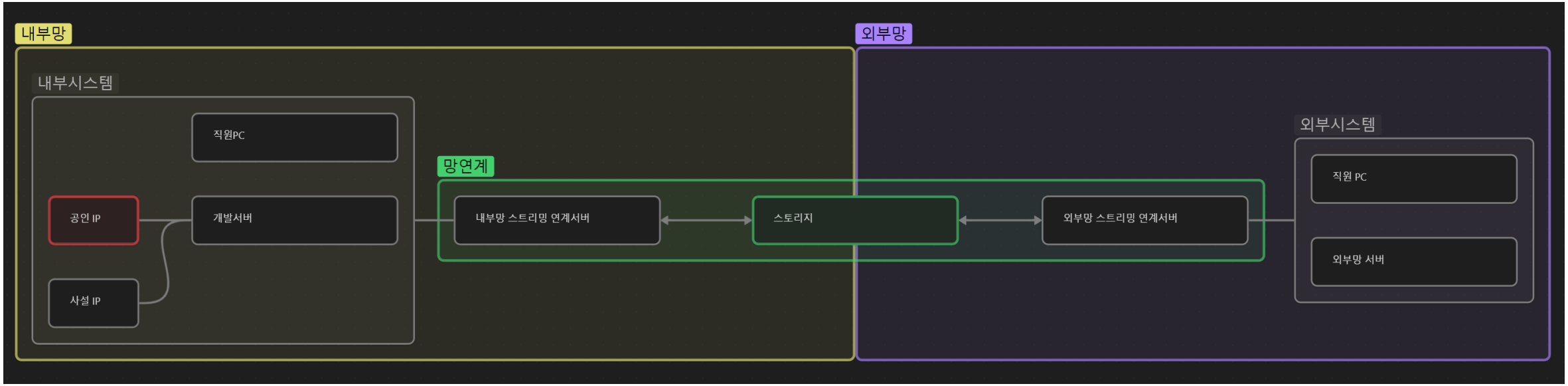
※ 망분리
"**망분리**"란 **외부 인터넷망을** 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 '업무망'과 '**외부 인터넷망**'을 분리하는 망 차단조치를 말합니다.
(개인정보보호위원회고시 제2020-5호 **개인정보의 기술적·관리적 보호조치 기준 제2조(정의)제5호)**

– 상황

1) 외부망에서 내부망에 있는 개발서버 **테스트 목적으로 망연계 솔루션 포트 오픈** 후 원복 안함

2) 문서 암호화/중앙화 솔루션을 일부 사용하지 않은

– 문제: 자료 탈취 (cf. **내부망**에 **공인IP를 왜** 사용하는지…)



03 비밀번호

비밀번호 관리 취약

□ 외부 업체 용역에 의한 보안 취약점

– 상황: 정기적으로 시스템 점검을 위해 방문하는 외부 업체 용역이 장비 및 원격 서버 접속 비밀번호를 담은 엑셀 파일을 자신의 PC에 저장함

– 결과: 침투한 공격자가 이 파일을 발견하여 내부 네트워크를 장악함

□ 숨김 처리된 비밀번호 리스트의 부적절한 관리

– 상황: 외부 업체 용역이 사내 보안 담당자로부터 받은 비밀번호 리스트를 숨김 처리하여 PC에 저장함

– 결과: 공격자가 이 숨김 처리된 시트를 발견하여 내부망을 장악함

□ 직원 PC에 저장된 관리자 계정 정보

– 상황: 관리자 계정 정보가 무차별적으로 직원 PC에 저장됨

– 결과: 해커가 이 정보를 악용하여 서버에 침입함

비밀번호 관리 취약

□ 중소 홈페이지 개발 업체의 비밀번호 관리 실패

– 상황: 중소 홈페이지 개발 업체에서 **동일한 형식**의 비밀번호를 자주 사용함

– 결과: 해커가 패턴을 유추하여 다수의 홈페이지를 쉽게 악용함

□ 중소 호스팅 업체의 비밀번호 보관 실패

– 상황: 중소 호스팅 업체에서 주요 시스템 접속 비밀번호를 **포털 메일에 저장**함

– 결과: 포털 메일 탈취, 보안 위협에 노출됨(관리자는 자신의 포털 메일함에 비밀번호 보관한 이력조차 기억이…)

□ 서버 임대 업체의 초기 비밀번호 유출

– 상황: 서버 임대 업체에서 제공한 **초기 비밀번호가 유출**되고, 사용자들이 이를 변경하지 않음

– 결과: 해커가 이 초기 비밀번호를 이용하여 서버를 장악함(서버 임대 업체의 잘못? 서버를 임대한 고객의 잘못?)

04 취약프로그램

취약한 프로그램 사용

□ 보안인증 솔루션 취약한 버전 사용

– 이OO, 드OO, OOO 등

– 목적: 목표 시스템 완전 장악

□ 오픈소스 설치형 블로그/플러그인 등 취약한 버전 사용

– 워드프레스, 그누보드 등

– 목적: 악성코드 유포지, 웹 쉘 등 주로 경유지로 악용

□ 사례

– 대대적 언론보도 후에도 취약한 버전을 계속 사용중인 업체(본인들이 홍보하고 본인들이 패치 안하고)

– 망분리 되어 있는 시스템, 취약점 패치를 안하고 있는 업체(업로드 취약점 이용해서 웹 쉘 설치 및 C2거점 사용)

보안솔루션 / 내부보안 관리 미흡

□ 보안솔루션 부재

– 문제: 네트워크 접근 제어(NAC), 망분리, 침입 탐지 시스템(IDS), 침입 방지 시스템(IPS), 방화벽(F/W), 안티바이러스, 엔드포인트 탐지 및 대응(EDR), 네트워크 탐지 및 대응(NDR), 보안 정보 및 이벤트 관리(SIEM) 보안 이벤트 관리(ESM) 등 필수 보안 솔루션이 존재하지 않음

□ 외부 업체에 의한 보안 노출

– 문제:

1) 원격 유지보수 및 장애 처리를 위한 방화벽 정책 설정이 미흡하여 전산 장비 접속 IP, 포트 외부 노출

2) 관리자 접속 페이지가 외부에 노출, 심지어 웹 쉘을 업로드하여 고객사 관리

3) 보안관제 업체 고객사 서버에 점검 스크립트 결과 값 저장(공격자의 일을 보안관제 업체가 대신…)

□ 방화벽 관리의 미흡

– 문제: 방화벽이 설치되어 있으나 적절한 관리 및 정기적인 업데이트가 이루어지지 않음

보안솔루션 / 내부보안 관리 미흡

□ 원격 접속 보안 취약점

– 문제

1) 서버 별 **원격 접속**에 대한 접근 제어 목록(ACL) 또는 허용 IP **설정이 미흡**하여 외부 공격자의 원격 접속 가능

2) **인바운드 및 아웃바운드** 트래픽 관리 부족

□ 로그 관리 부재

– 문제: 보안 로그의 축적 및 분석이 이루어지지 않아 보안 **사고 발생 시 추적 및 대응이 어려움**

□ NAC 장비 등 활용 부족

– 문제

1) NAC 장비를 통한 내부망 PC 접근 제어 정책 미흡

2) 비인가 프로그램 사용 차단 및 퇴근 후 **PC 전원** 자동 **종료** 정책 등이 설정되어 있지 않아 보안 취약점 발생

취약점 점검 미시행

□ 보안 컨설팅 미이행 문제

– 상황: 한국인터넷진흥원(KISA)에서 제공하는 관리적, 물리적, 기술적 보안 조치를 위한 보안 컨설팅 서비스가 이용 가능함에도 불구하고, 업무 과중을 이유로 해당 서비스를 활용하지 않음

– 결과: 필요한 보안 조치들이 미흡하게 남겨져, 보안 취약점이 발생할 위험성 증가

은폐

□ 은폐 및 거짓 정보 제공

– 상황: 유선상으로는 보안 취약점이나 문제가 없다고 주장, 실제로 현장을 방문하여 검증했을 때 상황이 다르게 드러남
예를 들어, 유선상으로는 특정 IP에 포트가 열려있지 않다고 주장했지만, 현장 임장 및 분석을 통해 ERP 서버가 실제로 침해당한 사실을 확인함

– 결과: 협조하지 않은 시스템에 대해 필요한 보안 조치들이 미흡하게 남겨져, 보안 취약점이 발생할 위험성 증가

유휴서버(관리미흡서버)/Legacy System 사용

□ 관리 미흡으로 유휴서버와 레거시 시스템의 사용

– 상황

1) 기업의 자산 파악 불가, 수사관이 서버 랙에서 랜선 체크

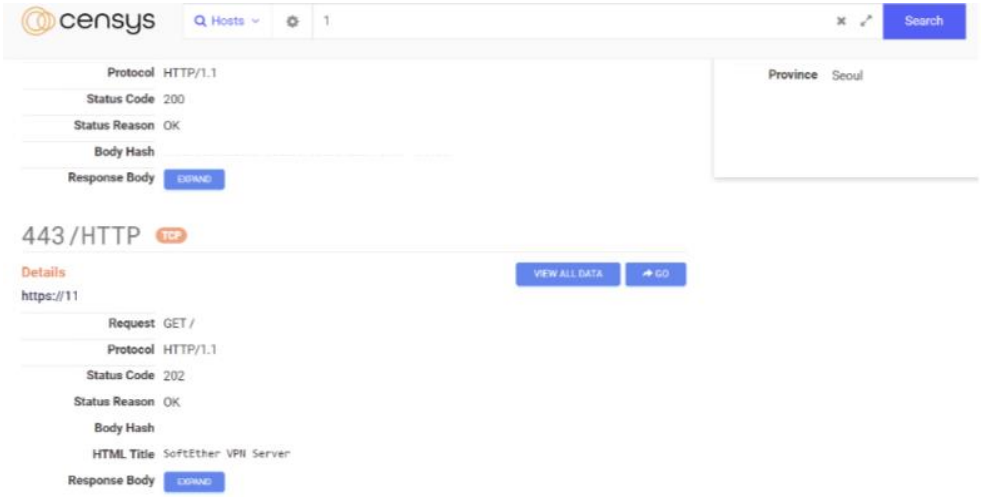
2) 서버 접속 비밀번호를 잃어버림

3) 대다수 기업에서 오래된 레거시 시스템을 계속 사용

– 문제

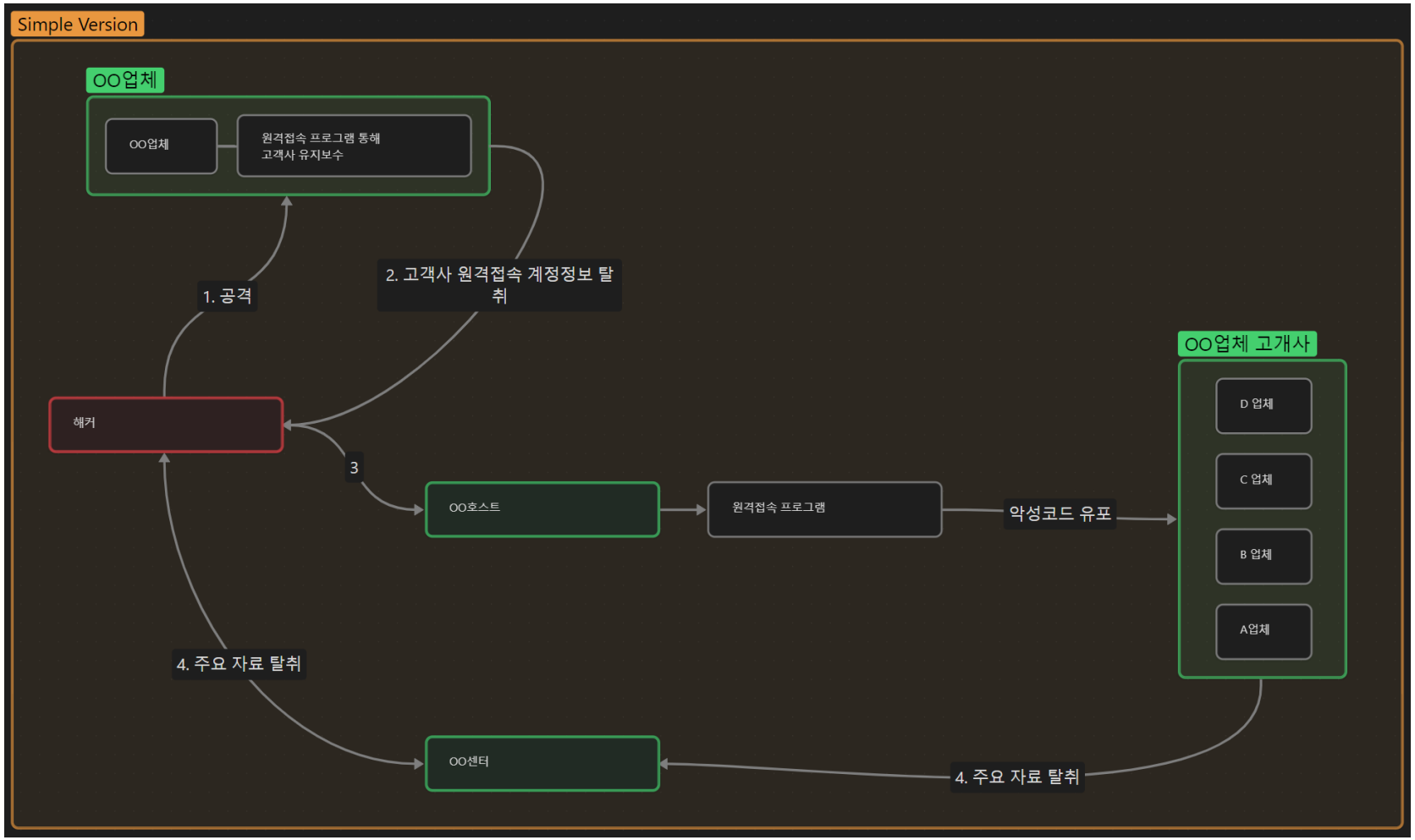
1) 이러한 레거시 시스템의 지속적인 사용과 버전 패치의 부족으로 인해 다수의 보안 취약점이 존재함

2) 전세계 해커들의 올림픽 개최



07 고찰

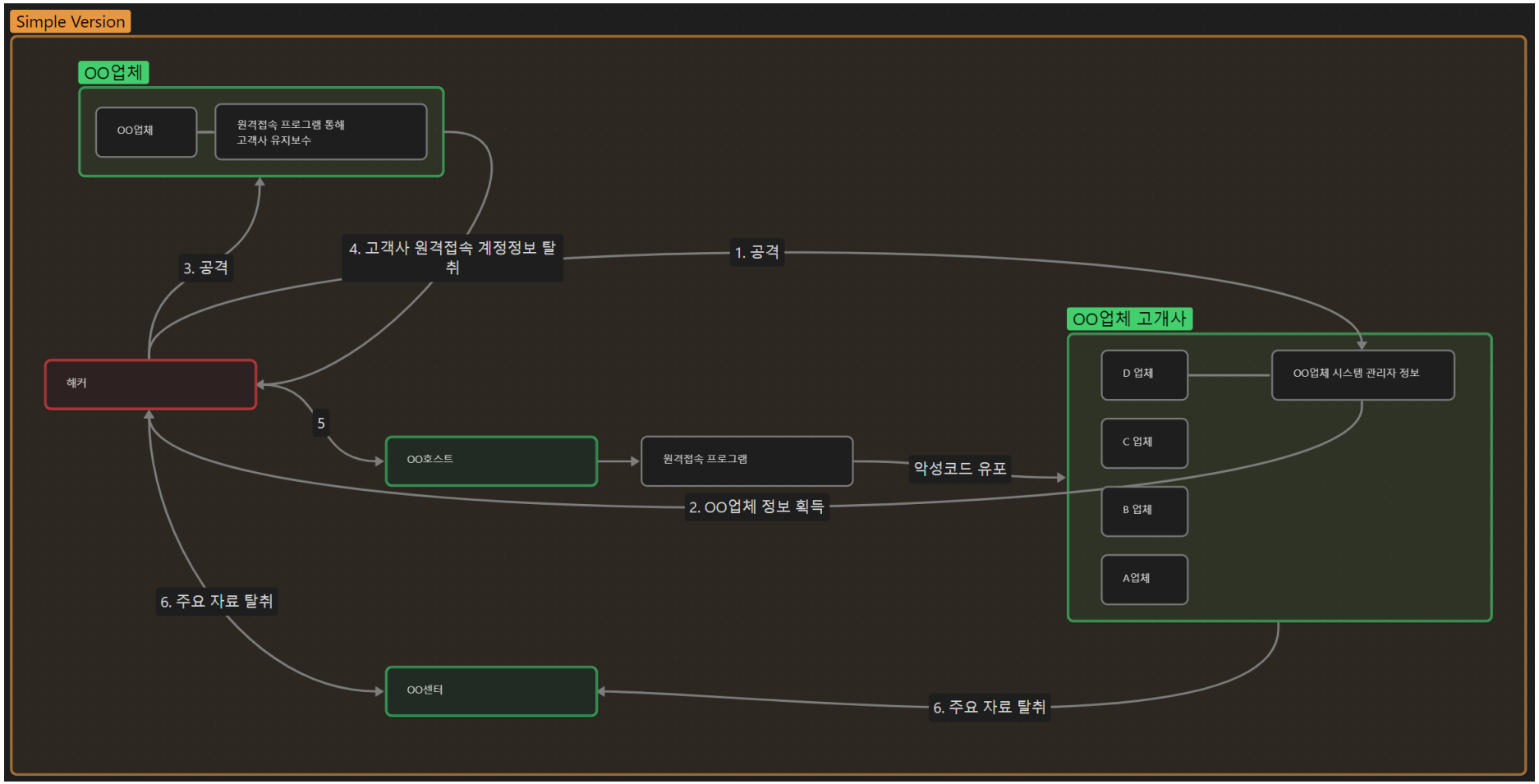
우리의 위치는???


Simple Version
OO업체
OO업체
원격접속 프로그램 통해
고객사 유지보수
1. 공격
2. 고객사 원격접속 계정정보 탈취
해커
3
OO호스트
원격접속 프로그램
악성코드 유포
OO업체 고개사
D 업체
C 업체
B 업체
A업체
4. 주요 자료 탈취
OO센터
4. 주요 자료 탈취

07 고찰

국가수사본부
안보수사국

우리의 위치는???



07 고찰

Q & A

경찰청 안보수사국