APT 보안

피싱을 통한 정보 유출 시나리오 구현 및 대응 방안 제시

월척

이여민(PM), 이승환, 이재우, 이재환, 이정호, 김경진, 서희영

>> CONTENTS

1 팀원 소개

2 프로젝트 배경

3 프로젝트 목표

4 프로젝트 계획

5 프로젝트 범위

1

팀원 소개

Part 1 >>

팀원 소개

이재윤 멘토님

손승호 (PL)

이정호

이여민 (PM)

이승환

이재우

이재환

김경진

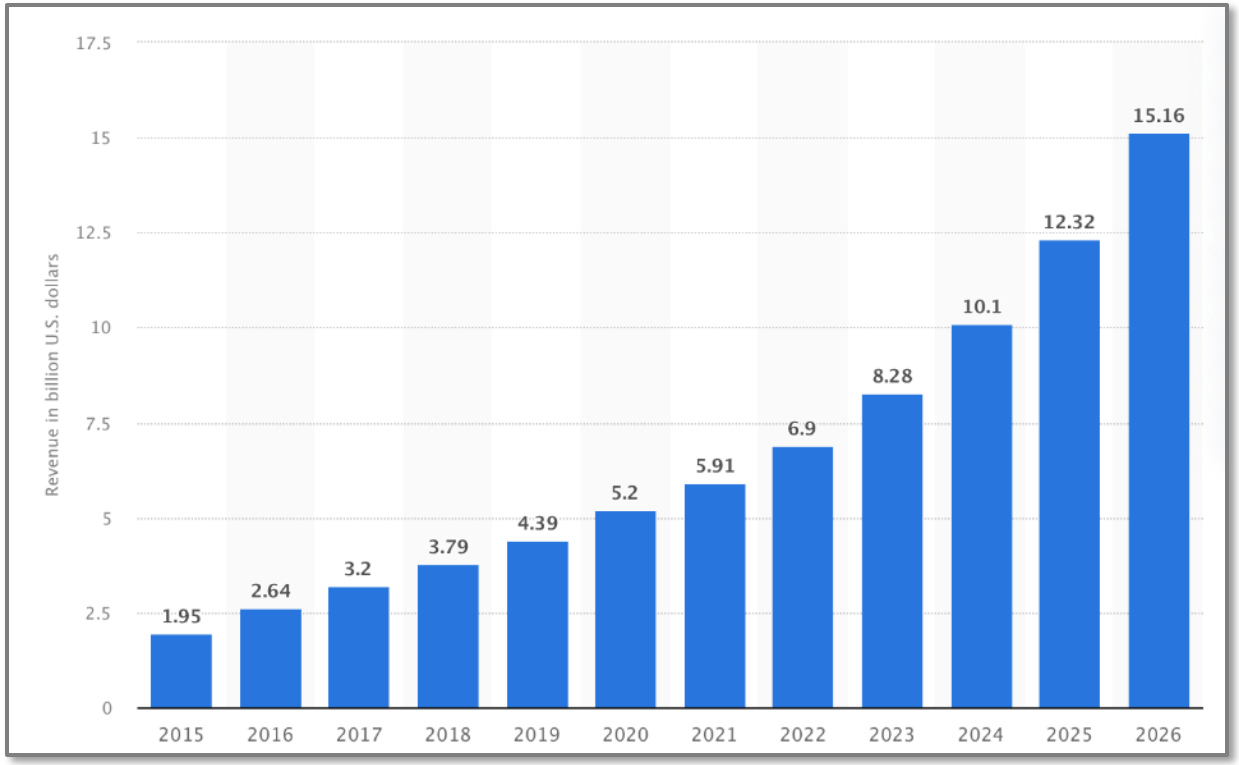
서희영

2

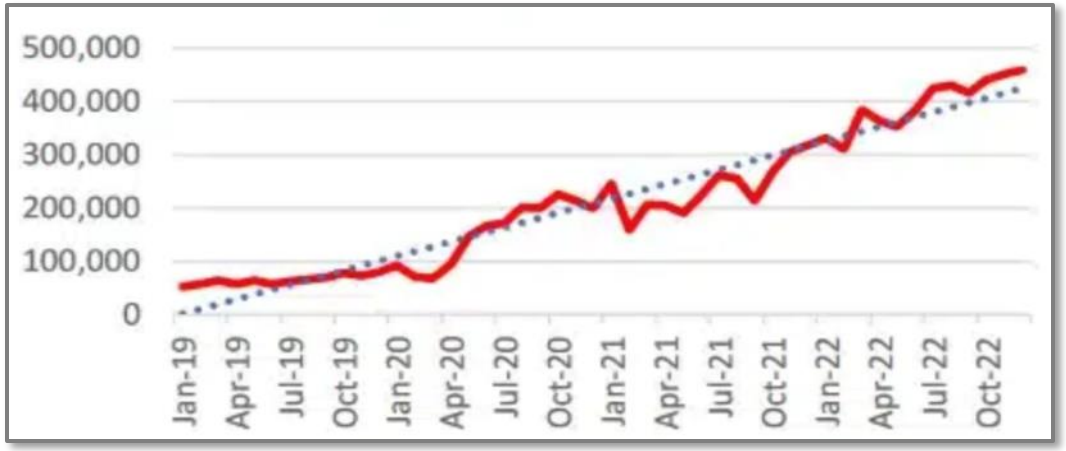
프로젝트 배경

- 주제 선정 배경
- APT 스피어피싱 공격

Part 2 >> 주제 선정 배경



2015 - 2026, 현재 및 예상되는 미래 APT 보안 시장, 출처: Statista (단위 : 미국 달러)

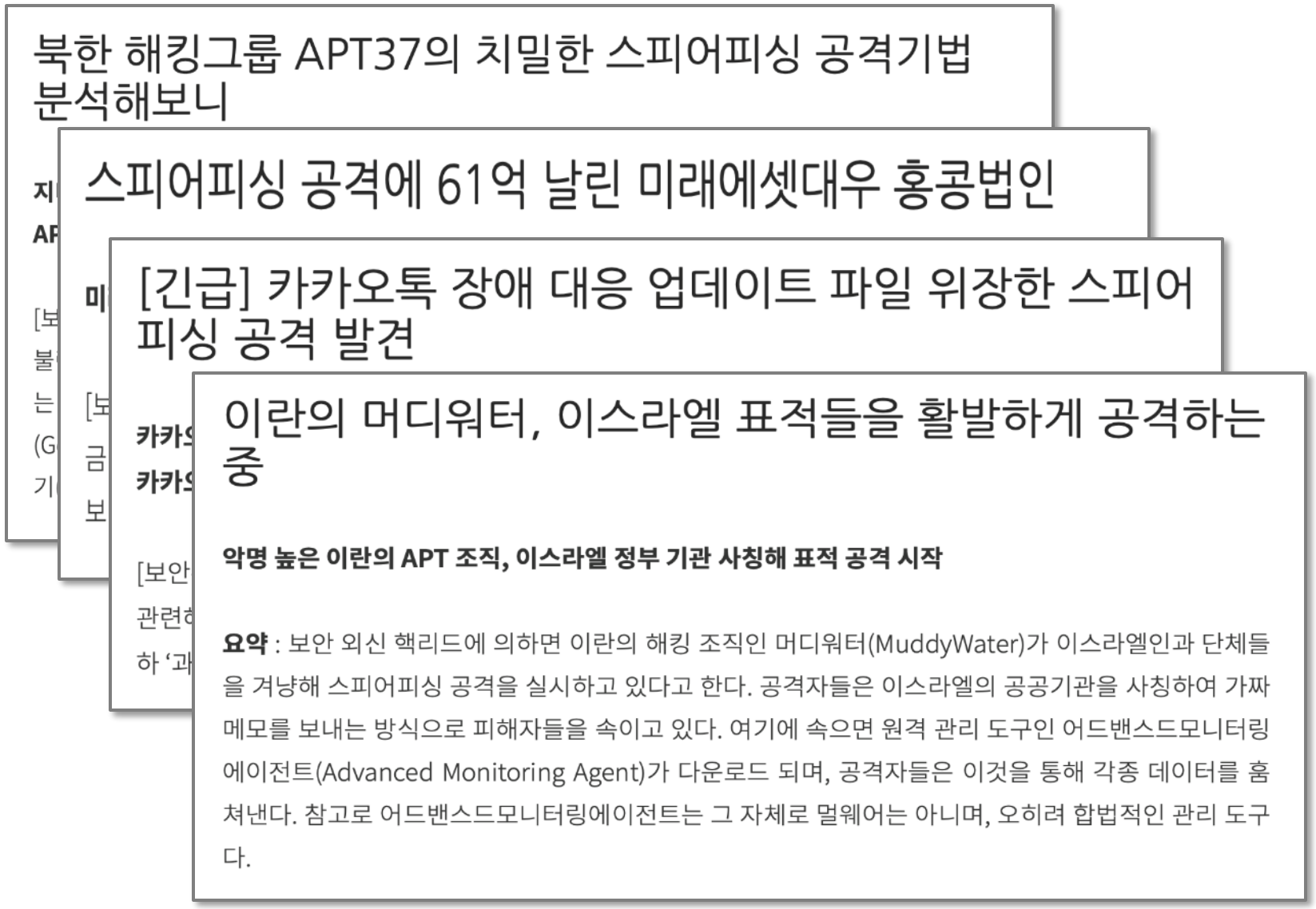


19.01 – 22.10, 증가하는 피싱 건수, 출처: APWG

늘어나는 **APT 공격**을 대비하기 위한
보안 시장의 예상 성장 규모

달마다 늘어나는 **피싱 피해 사례** 건수

Part 2 >> 주제 선정 배경



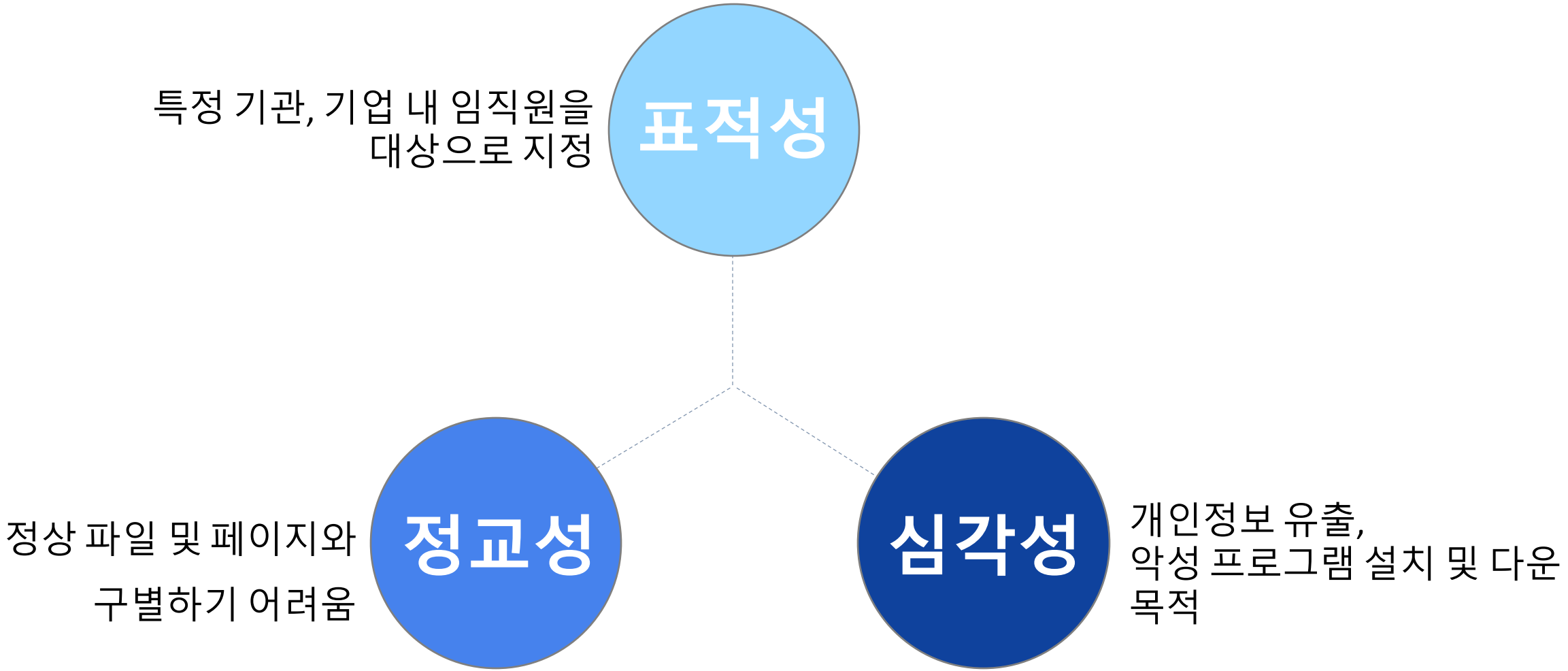
- 2023, 북한 해킹그룹, 스피어피싱
- 2020, 61억 손해본 미래에셋대우
- 2022, 카카오톡 위장 스피어 피싱
- 2023, 이란-이스라엘 스피어 피싱

계속해서 **증가**하는 APT, 스피어피싱
끊이지 않는 **피해**

WHY?

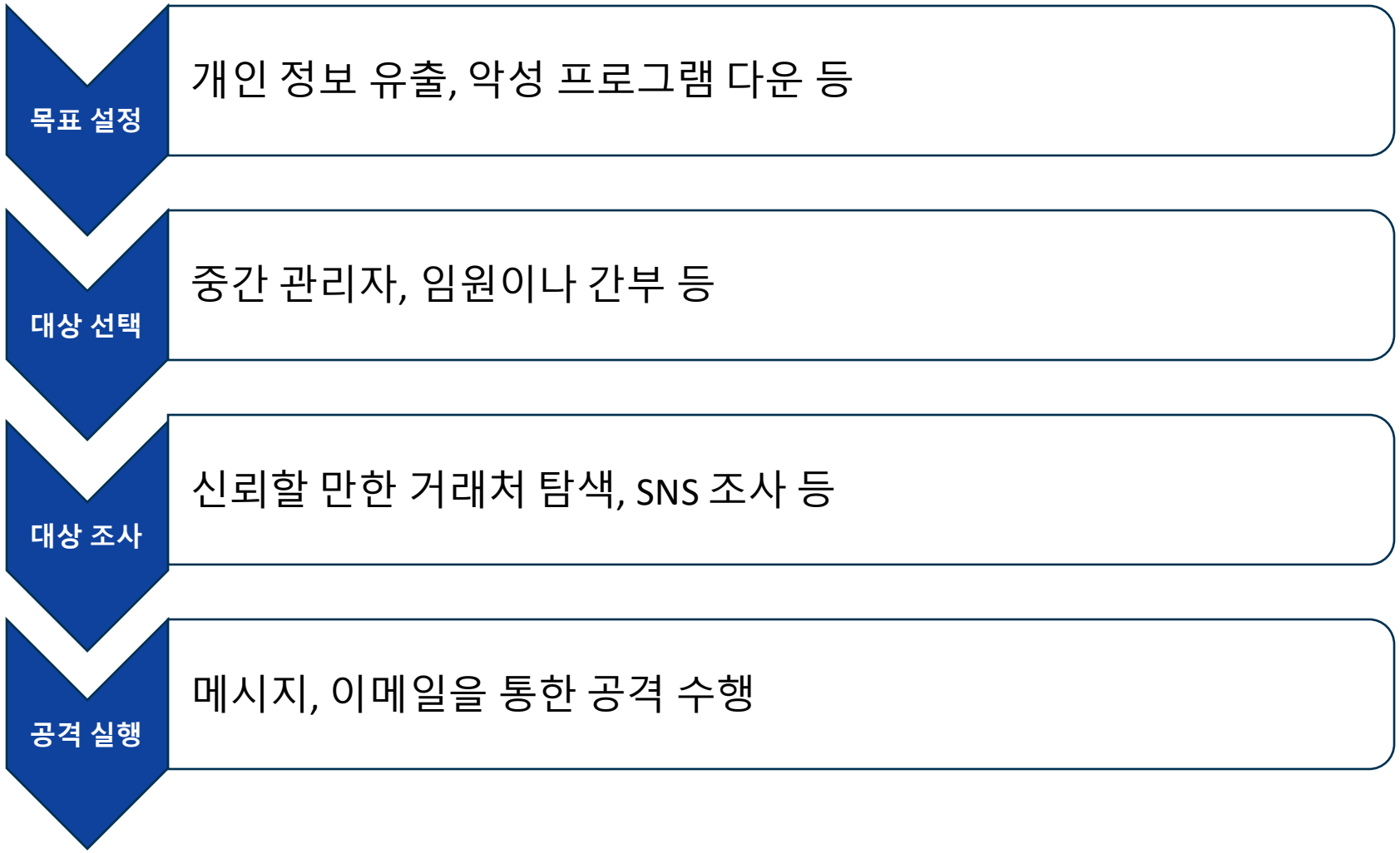
구현을 통해 **학습**해보자!

스피어피싱이란?


특정 기관, 기업 내 임직원을
대상으로 지정
표적성
정상 파일 및 페이지와
구별하기 어려움
정교성
심각성
개인정보 유출,
악성 프로그램 설치 및 다운
목적

Part 2 >> APT 스피어피싱(Spear Phishing) 공격

스피어피싱 단계

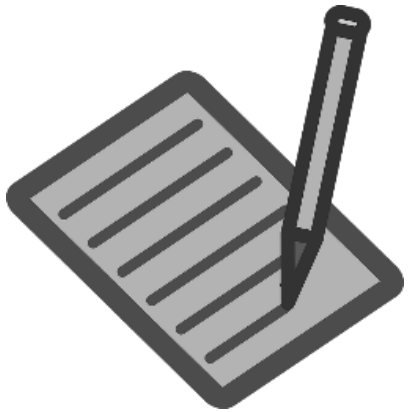


3

프로젝트 목표

- 프로젝트 목표
- 프로젝트 아키텍처
- 대응 프레임워크

Part 3 >> 프로젝트 목표



- **스피어피싱 방식으로 침투하는 APT 시나리오 제작 및 구현**
  - 웹사이트 피싱을 통해 사용자의 개인정보 탈취 및 악성코드 유포
  - 침투, 영역 확장, 데이터 추출 등 전반적인 시나리오 전체 구성

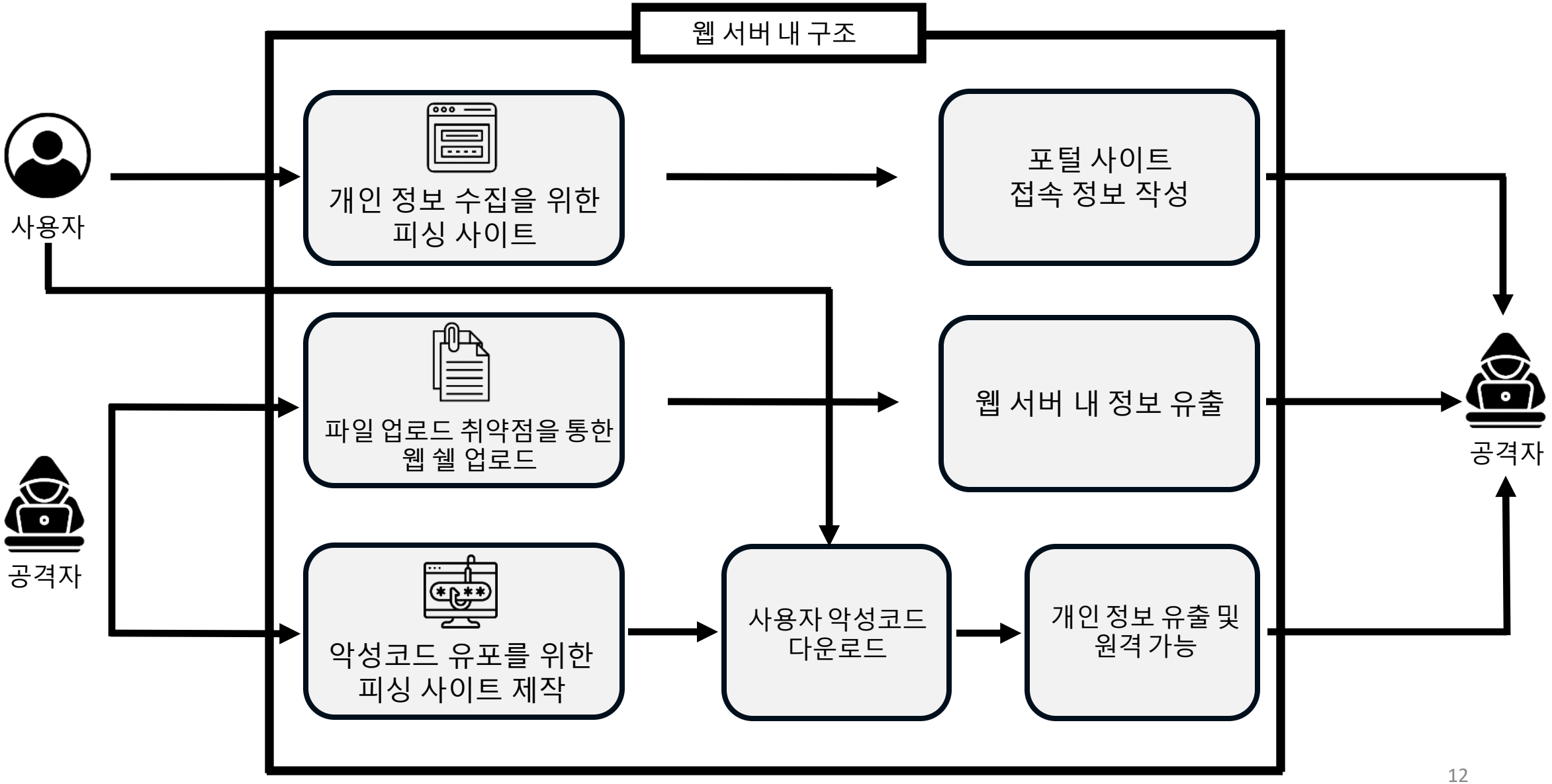
    ① 악성 URL 접속 후, 개인정보 입력 유도

    ② 웹 쉘 업로드 공격

    ③ 악성코드 설치 유도

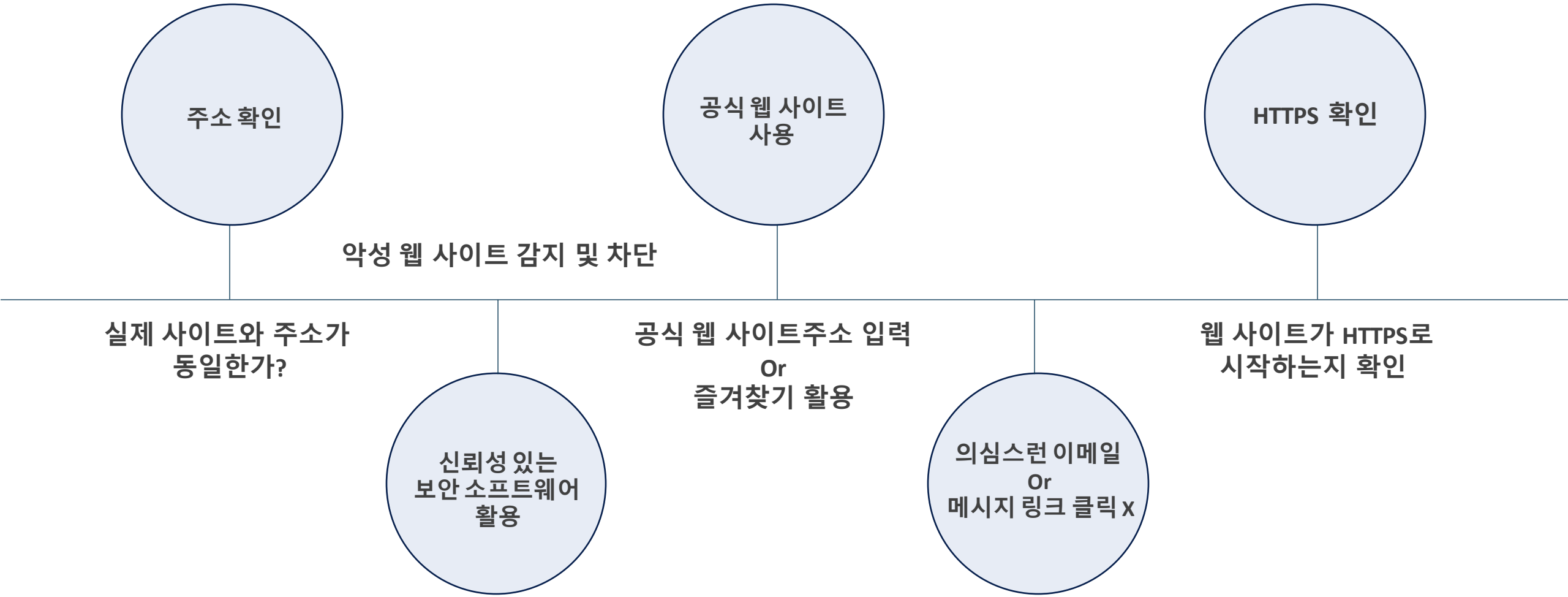
- **제작된 APT 공격에 효과적인 대응 방안 구축 및 구현**
  - 대응 구현 후 가이드라인 제작
  - 대응 구축 및 구현 결과에 따른 논문 제작

Part 3 >> 프로젝트 아키텍처



>> 대응 프레임워크 ① 악성 URL 접속 후, 개인정보 입력 유도

- 기본 대응 체계



>> 대응 프레임워크 ② 웹 쉘 업로드 공격

정상 상황

- 평상시의 업무 상황
- 방화벽 설정 및 웹 서버 로그 기록, 모니터링

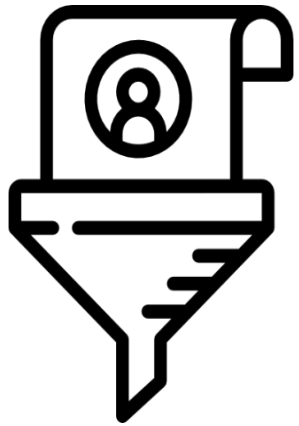
이상 행동 감지

- 시스템 로그의 신규 서비스 등록 모니터링
- 업로드 파일 경로 실행권한 제거

침투 흔적 발견

- 웹 쉘 제거
- 이동 파일 모니터링
- 로그인 성공 이벤트 모니터링
- 삭제 행위 관련 명령 실행여부 모니터링

<u>가이드라인</u> 작성 과정



- 웹 쉘 업로드 방지를 위한 필터링 구현
- 필터링을 통한 대응 및 조치 가이드라인

Part 3 >> # 대응 프레임워크 ③ 악성코드 설치 유도

정상 상황

- 평상시의 업무 상황
- 방화벽 설정 및 웹 서버 로그 기록, 모니터링

이상 행동 감지

- 시스템 로그의 신규 서비스 등록 모니터링
- 업로드 파일 경로 실행권한 제거

침투 흔적 발견

- 악성 프로세스 즉시 중단
- 이동 파일 모니터링
- 로그인 성공 이벤트 모니터링
- 삭제 행위 관련 명령 실행여부 모니터링

가이드라인 작성 과정

- 일반 포털 사이트와 피싱 사이트 차이점 파악
→ 가이드라인 제시

➢ **개인정보 유출**

➢ **악성코드 다운**

2가지 방법에 대한 대응 가이드라인 제작

4

프로젝트 계획

- 일정

Part 4 >> 일정

계획		11월					12월			
		1주	2주	3주	4주	5주	1주	2주	3주	4주
시작 단계	WBS작성									
	수행계획서 작성									
	프로젝트 아키텍처 작성									
	킥오프 서면 보고 자료 작성									
	시나리오 조사									
구축 단계	APM 기반 웹 서버 구축									
	피싱 사이트 구축									
	웹 쉘 기능 구현									
	악성 코드 환경 구축									
공격 단계	악성 코드 제작									
	악성 코드 유포									
	정보 유출 시나리오 구현									
대응 및 조치	공격 유형별 대응 방안 연구									
	대응 방안 적용 및 테스트									
마무리	논문 작성									
	가이드라인 작성									
	최종 발표									

5

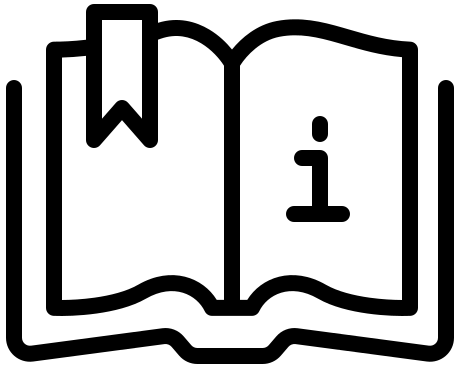
프로젝트 범위

- 예상 산출물
- 기대 효과

Part 5 >>

예상 산출물

1 가이드라인



스피어피싱 대응 및 조치
가이드라인, 시연 영상

2 논문

적절한 스피어피싱 공격 플로우, 대응
방안을 주제로 논문을 작성할 예정

Part 5 >> 기대 효과

1

구체화된 솔루션 제시

여러 APT 시나리오 중
스피어피싱에 대한
구체화된 **시나리오 및 솔루션 제시**

2

웹 사이트 피싱에 대한
이해 향상

피싱 웹 사이트 구축 및 공격을 통한
개인정보 수집 및 보관의 취약점 분석

3

스피어피싱 공격 피해 최소화

산출물로 논문을 제시하여 취약점을
분석 및 공격한 과정을 공개함으로써
피해 최소화 및 사회 안정에 기여

>> END

감사합니다.