침해사고 유형과 대응 방안

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

1. 침해사고 유형
2. 저장장치 파괴 악성코드
3. 침해사고 대응
4. 침해사고 절차

침해사고 유형

침해사고 유형

▪ 악성코드

- 대부분의 침해사고는 악성코드에서 시작하여 악성코드로 끝남
- 특정 목적을 이룰 때까지 지속적으로 사용됨

- **최근 악성코드 유형**
  - ✓ **다운로더/드롭퍼** : 추가적인 악성코드 설치
  - ✓ **백도어** : 원격 접속 기능 필요
  - ✓ **스틸러/스파이웨어** : 정보를 빼내감
  - ✓ **보안 소프트웨어 위장** : 감염된 것처럼 위장해 결제 유도
  - ✓ **시스템 자원 사용** : 감염 시스템 자원을 다른 공격에 사용 (DDoS, email relay, VPN 등)
  - ✓ **접근 차단** : 특정 자원을 접근하지 못하도록 막은 후 결제 유도 (랜섬웨어, 암호화 등)
  - ✓ **데이터 파괴** : 시스템 중요 데이터를 파괴 (MBR 파괴, 특정 문서 삭제 등)

침해사고 유형

- **침해사고 감염 유형**
  - **웹**을 통한 감염
  - **웹하드**를 통한 감염
  - **이메일**을 통한 감염
  - **외장저장장치**를 통한 감염
  - **업데이트/관리 서버**를 통한 감염
  - … …

- **모든 감염 유형은 APT 또는 TT의 시작이 될 수 있음!!**
  - **APT –** Advanced Persistent Threat
  - **TT –** Targeted Threat

침해사고 유형

1. 웹을 통한 감염 (계속)

- **OWASP** - 10대 웹 애플리케이션 취약점

OWASP Top 10 – 2010	OWASP Top 10 – 2013
A1 – 인젝션	**A1** – 인젝션
A3 – 인증과 세션 관리의 결함	**A2** – 인증과 세션 관리의 결함
A2 – 크로스 사이트 스크립팅 (XSS)	**A3** – 크로스 사이트 스크립팅 (XSS)
A4 – 안전하지 않은 직접 객체 참조	**A4** – 안전하지 않은 직접 객체 참조
A6 – 잘못된 보안 설정	**A5** – 잘못된 보안 설정
A7 – 안전하지 않은 암호화 저장 –A6에 통합 ➔	**A6** – 중요 정보 노출
A8 – URL 접근 제한 실패 – A7으로 확장 ➔	**A7** – 단계적 접근 제어 기능의 누락
A5 – 크로스 사이트 요청 변조 (CSRF)	**A8** – 크로스 사이트 요청 변조 (CSRF)
<A6: 잘못된 보안 설정 묻혀 있던>	**A9** – 알려진 취약한 컴포넌트 사용
A10 – 리다이렉트와 포워드의 검증 미흡	**A10** – 리다이렉트와 포워드의 검증 미흡
A9 – 불충분한 전송 계층 보호	2010-A7과 함께 2013-A6에 통합

침해사고 유형

1. 웹을 통한 감염 (계속)

- **악성코드 은닉 사이트 방문 시 감염**
  - ✓ 드라이브-바이 다운로드(Drive-by Downlod) vs. 워터링 홀(Wartering-hole)
  - ✓ 언론사 페이지와 같이 사용자는 많지만 보안에 취약한 웹 서비스 공략
  - ✓ 페이스북, 트위터 등의 SNS 활용
  - ✓ goo.gl, bitly. tynyURL, mcaf.ee 등 짧은 URL 사용
  - ✓ (모바일/PC) 웹 브라우저의 취약점을 이용

침해사고 유형

1. 웹을 통한 감염 (계속)

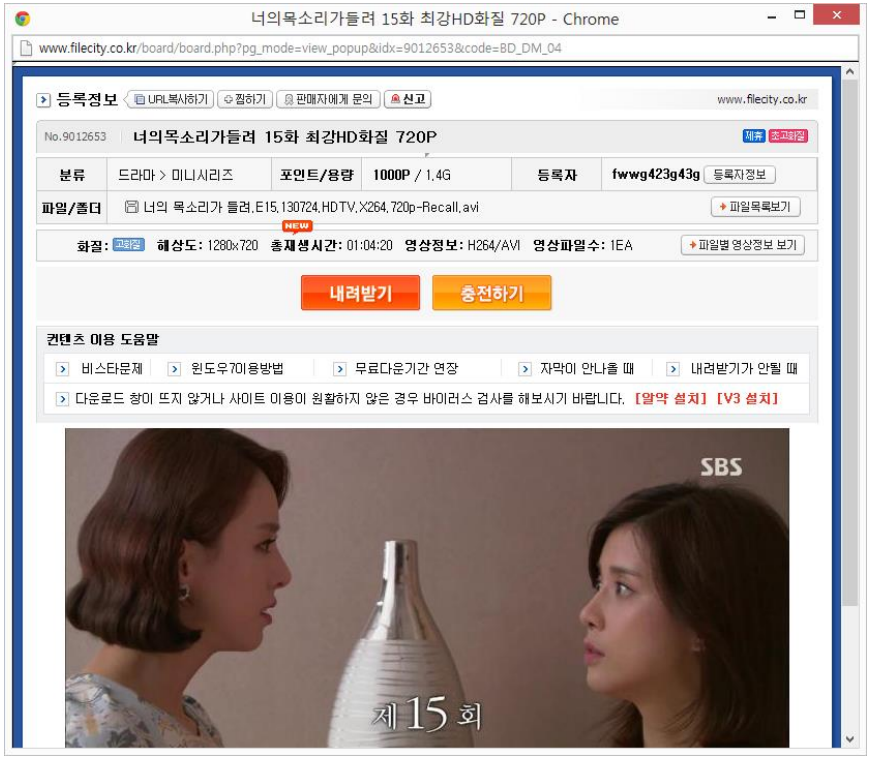
- **악성 ActiveX 설치 유도**
  - ✓ 동영상 플레이어, 보안 프로그램 등으로 위장하여 설치 유도

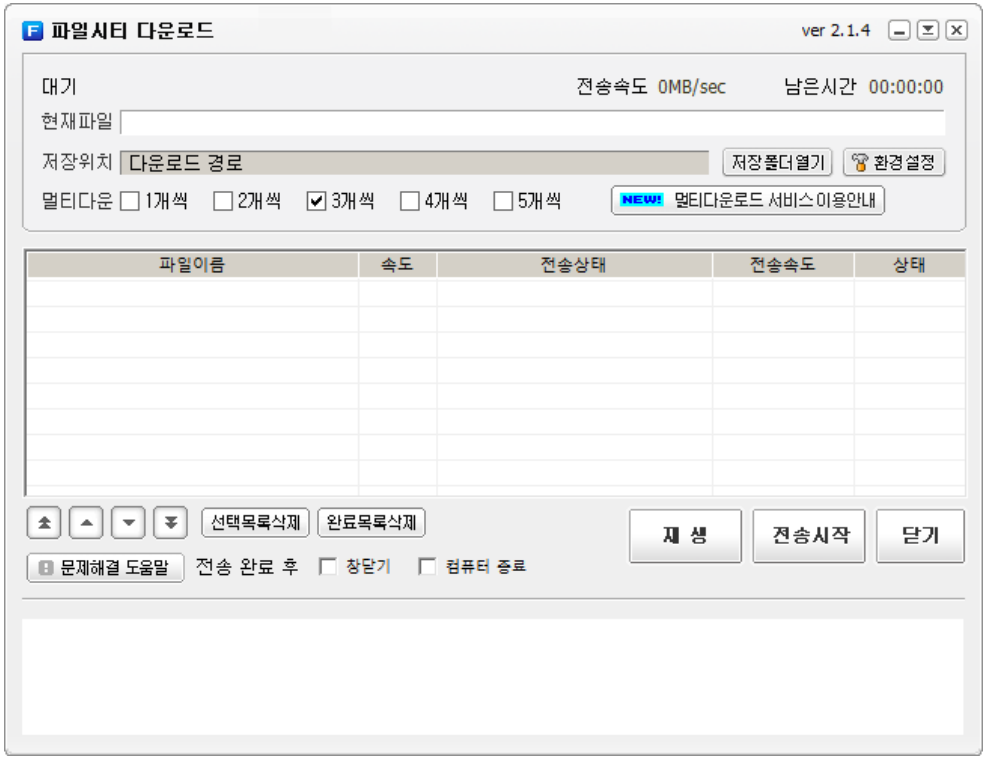
- **웹 애플리케이션 취약점**
  - ✓ 웹 키보드 보안 모듈, 공인인증서 모듈 등의 취약점 이용

- **악성 파일 다운로드 실행**
  - ✓ 동영상, 토렌트 파일의 확장자 변조 (.avi.exe, .torrent.exe)
  - ✓ 애플리케이션(동영상 플레이어, 한글, 오피스 등) 취약점 활용

2. 웹하드를 통한 감염 (계속)

- **웹하드 다운로드 관리자 감염**
  - ✓ 7.7 DDoS, 3.4 DDoS, 6.25 사이버테러의 원인
  - ✓ 웹하드 서버를 공격하여 "다운로드 관리자" 프로그램 감염





2. 웹하드를 통한 감염

- **웹하드 불법저작물/음란물에 포함된 악성코드에 감염**
  - ✓ **관심도가 높은 파일에 악성코드를 포함시켜 업로드**
    - 무료 추가 다운로드.exe
    - 무료 다운로드 방법.html
  - ✓ **자체 압축 풀림(self-extracting archive, SFX)으로 배포**
    - SFX로 배포하는 정상 파일인지, 악성코드인지 인지하기 어려움
  - ✓ **애플리케이션 취약점 활용**
    - 동영상 플레이어의 취약점을 악용하는 파일 배포

침해사고 유형

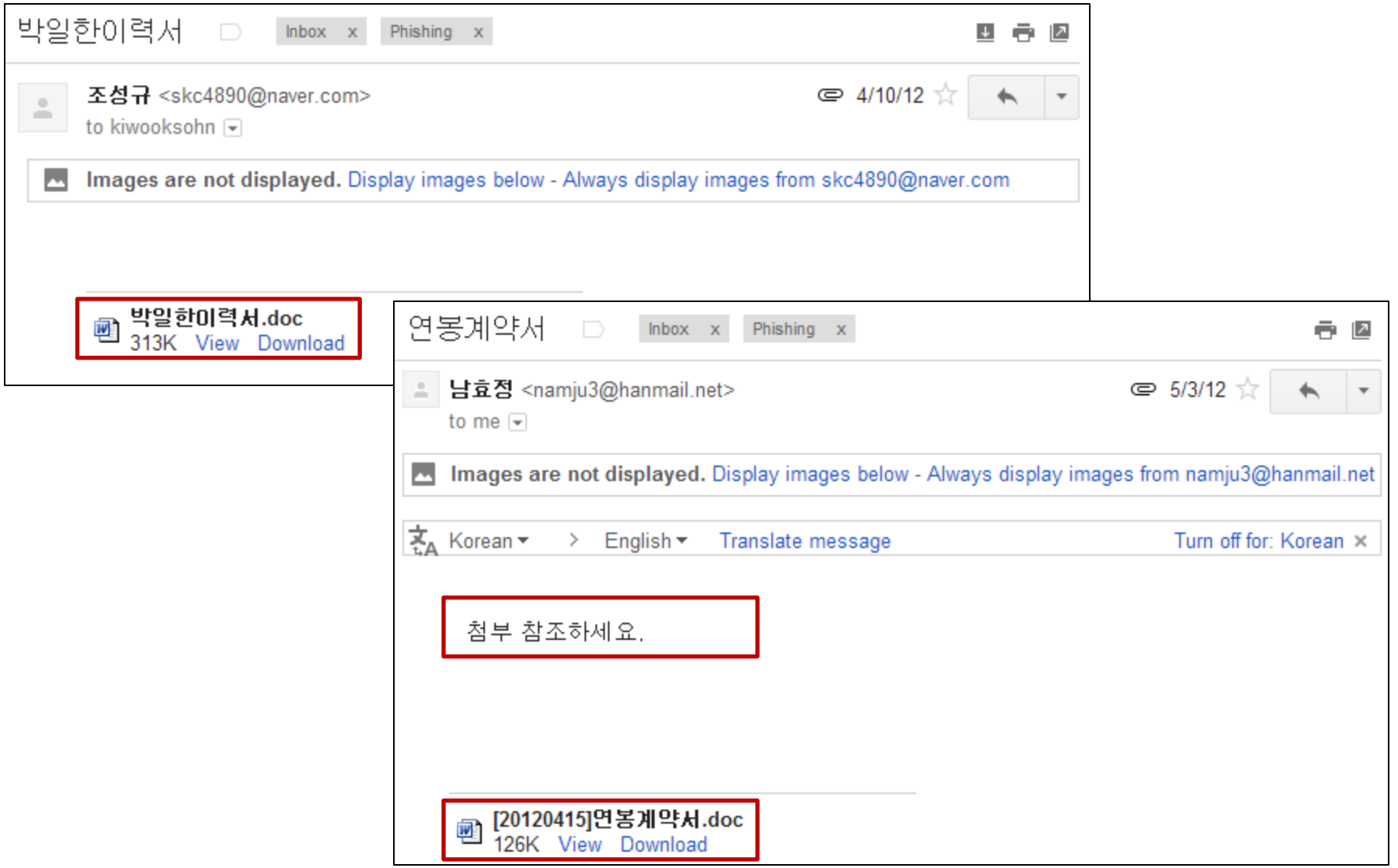
3. 이메일을 통한 감염 (계속)

- **무작위 스팸 vs. 사회적 관심사(올림픽,사고 등) 이용 vs. 특정 조직 대상(스피어피싱)**

- **악성사이트 접속 유도**
  - ✓ 정상 이메일처럼 사용자를 다른 사이트로 접속 유도
  - ✓ 금융 정보, 휴대폰 요금, 동창회/교우회 등 조직 사칭 등

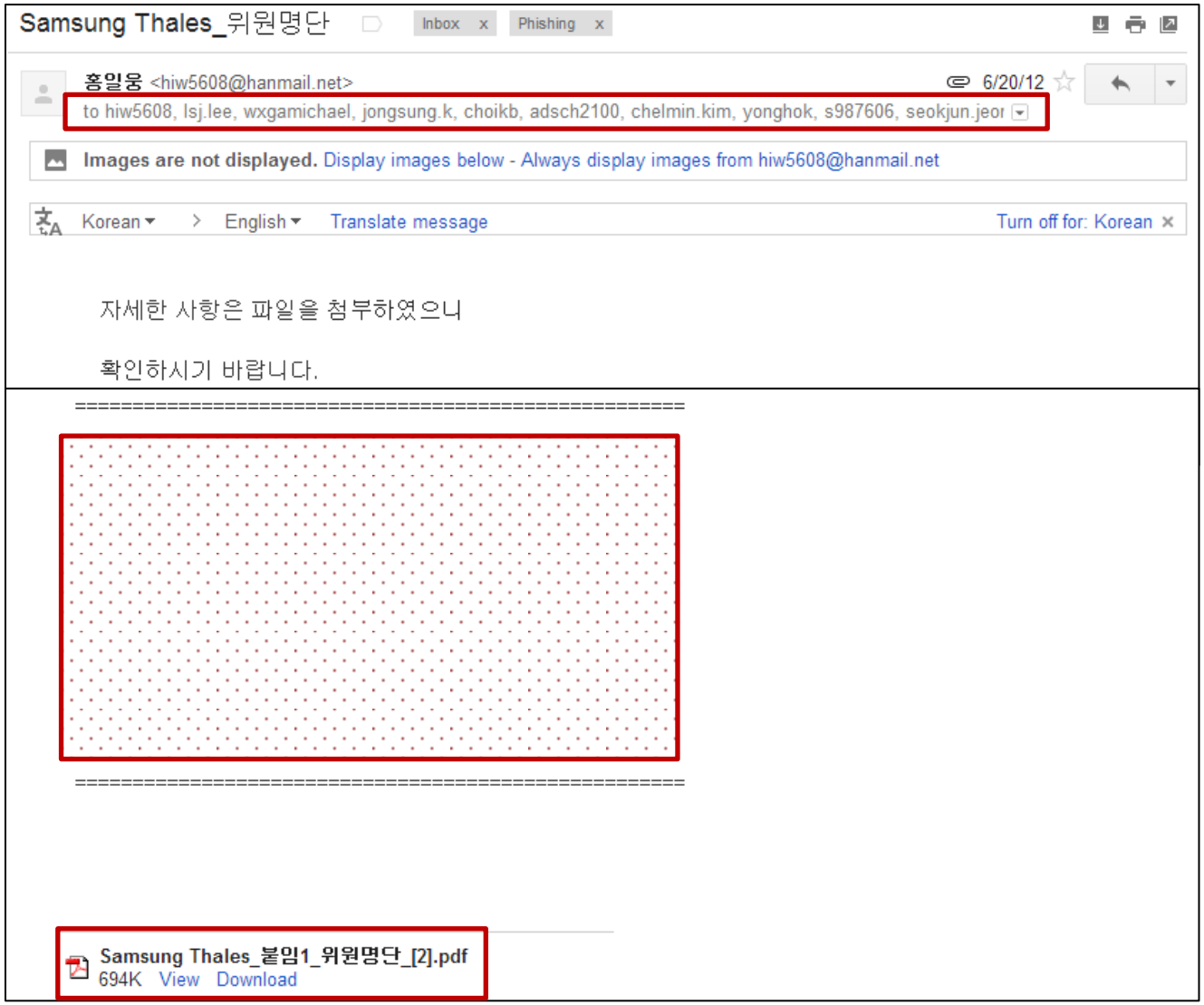
- **악성 첨부파일 실행 유도**
  - ✓ 무작위 스팸, 사회적 관심사(올림픽, 테러 등) 이용, 특정 조직을 대상
  - ✓ 한글, 워드, 엑셀 등의 문서 애플리케이션 취약점을 이용
  - ✓ 어도비 플래시/리더 취약점 이용

3. 이메일을 통한 감염 (계속)



침해사고 유형

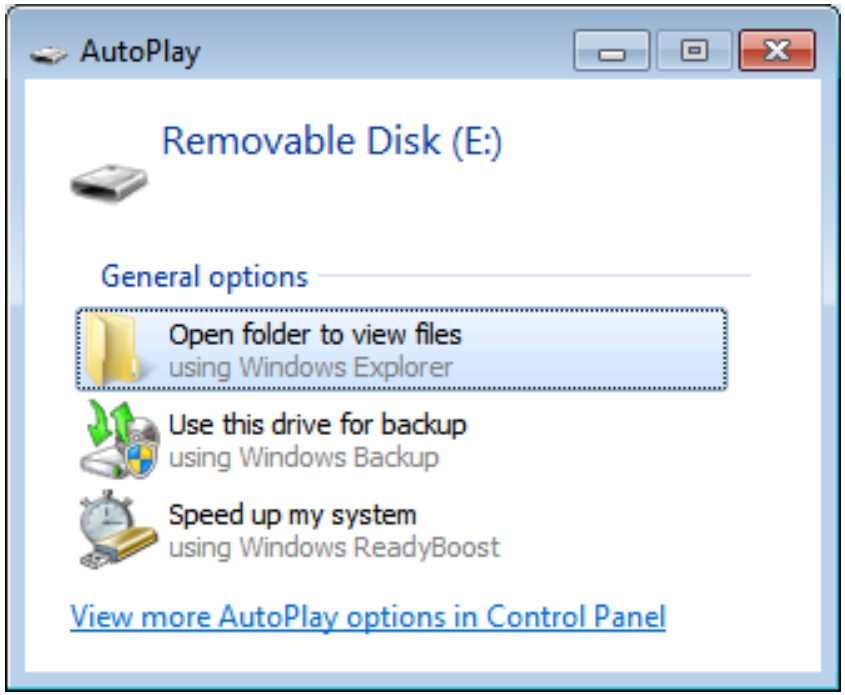
3. 이메일을 통한 감염 (계속)



4. 외장저장장치를 통한 감염

- **감염된 외장저장장치(USB) ➔ 연결 시 자동 실행**
  - ✓ 국가 기간망(스턱스넷, 듀크, 플레임)과 같이 폐쇄망을 타겟
  - ✓ 농협 전산망 마비와 같이 내부 시스템 감염을 위해 사용

- **MS 보안 업데이트**
  - ✓ 자동 실행 기능을 비활성화 방법
  - ✓ http://support.microsoft.com/kb/967715/ko



5. 업데이트/관리 서버를 통한 감염

- **업데이트 서버**
  - ✓ 대형 개인정보 유출사고와 기밀 유출 사고의 원인
  - ✓ 주로 애플리케이션 개발사에서 운용　　최근 자체적으로 내부 업데이트 서버를 유지
  - ✓ 기업 내부로 침투할 수 있는 가장 효과적인 방법
  - ✓ 업데이트 서버의 설정을 조작하여 특정 기업만 침투하기도 함
  - ✓ 대상 기업의 보안성 >> 업데이트 서버의 보안성

5. 업데이트/관리 서버를 통한 감염

- **관리 서버**
  - ✓ 3.20 사이버테러의 확산 원인
  - ✓ 기업 내부에 침투한 후 감염을 확장시키기 위한 용도로 사용
  - ✓ 초기 설치 이후 제대로 관리되지 않음

저장장치 파괴 악성코드

저장장치 구조

- **MBR Slack**
  - MBR과 볼륨의 첫 시작인 VBR 사이의 사용되지 않는 영역
  - **윈도우 XP/2K3**
    - ✓ 63 섹터 (FDISK의 트랙 할당 방식)
  - **윈도우 Vista 이후**
    - ✓ 2,048 섹터 (1MiB 할당 방식)

저장장치 파괴 악성코드

악성코드의 변화

- **7.7 DDoS (2009)**
  - MBR 파괴
  - DOC, PPT, XML 등 주요 확장자 파일 암호화

- **3.4 DDoS (2011)**
  - MBR 파괴 (4MB/512바이트)
  - DOC(X), PPT(X), XLS(X), GUL, HWP, PDF 등 주요 파일 파괴

- **3.20 사이버테러 (2013)**
  - MBR 파괴
  - VBR 파괴
  - VBR~200섹터 파괴

악성코드의 변화

- **6.25 사이버테러 (2013)**
  - MBR부터 256번 루프를 돌면서 64섹터씩 임의의 데이터를 덮어씀
  - MBR 다시 복원

  - 재부팅 시 파일 삭제
    - ✓ EXE, DLL, OCX, SYS 파일 즉시 삭제
    - ✓ JPEG, PNG, GIF, BMP, MP4, HTML, ASP, JSP, PHP 등 이름 변경 후 삭제
    - ✓ 그 밖의 파일은 랜덤한 문자열로 덮어쓰기

악성코드의 동향

- **부팅 방해**
  - MBR, VBR 영역 손상
- **데이터 영역 삭제**
  - 데이터 영역의 일정 영역을 특정 문자열 혹은 랜덤 데이터로 덮어쓰기
- **파일 삭제**
  - 확장자 기반의 주요 사용자 데이터 파일을 특정 문자열 혹은 랜덤 데이터로 덮어쓰기
- **왜 전체를 덮어쓰지 않고 일부 데이터만 삭제??**

저장장치 복원

- **MBR, VBR 손상**
  - 100% 복원 가능

- **특정 영역 혹은 파일 덮어쓰기**
  - 덮어쓴 파일을 복원 불가

대응 방안

- **주요 포렌식 데이터 복원**
  - 파일시스템 메타데이터, 레지스트리, 프리패치, 바로가기 파일, 로그 파일 등

- **주요 데이터 로깅 강화**
  - 분석에 필요한 포렌식 데이터를 수시로 중앙 로깅

- **신속한 대응 절차 마련**
  - 대응 절차 마련과 모의 훈련을 통한 숙달 필요

침해사고 대응

침입이 예상될 때

- **관제**
  - 보안 장비/솔루션 모니터링 ➔ 의심 이벤트 발견
  - 트래픽 모니터링 ➔ 의심 트래픽 발견
- **관리자 점검**
  - 비정상 로그
  - 권한, 설정 변경
  - 사용자 계정이나 시스템 자원의 불법 사용
- **장비/솔루션 오작동**
- **사용자 인지**

침입이 예상될 때 – 대응

- **악성으로 확인**
  - 해당 트래픽 격리 혹은 탐지 패턴 추가
  - 소스 IP 확인 ➔ 해당 부서에 통보
  - 포맷?!
- **발생 이벤트의 원인 파악은 누가?!**
- **포맷으로 인해 취약한 부분은 그대로 유지…**

침입이 확실시 될 때

- **관제**
  - 보안 장비/솔루션 모니터링 ➔ 악성 이벤트 발견
  - 트래픽 모니터링 ➔ 악성 트래픽 발견
- **비정상 서비스**
  - 웹 페이지 변조, 게임머니 상승, 저장매체 파괴, 랜섬 웨어 등
- **관리자 정기 점검**
  - 웹쉘 탐지, 악성 로그 확인 등
- **공격자의 의도적 노출**
  - 유출 정보 노출, 협박, 조롱 등

침입이 확실시 될 때 – 대응

- **법률 미저촉**
  - 서비스 원상 복구, IP 차단, 패턴 추가
  - 해당 시스템 포맷?!
  - 발생 이벤트의 원인 파악은 누가?!

- **법률 저촉**
  - 수사기관 혹은 소관부서에 신고 ➔ 보안팀 수사기관에 대응
  - 사내 분석은 누가?!

침해사고의 일반적 문제 (1/5)

- **리스크 중심의 방어**
  - 리스트 높음
    - ✓ 외부 노출 서비스
    - ✓ 불특정 다수 서비스
    - ✓ DMZ
  - 리스크 낮음
    - ✓ 내부망, 내부 서버
    - ✓ 클라이언트
- **APT 공격의 대부분은 '리스크가 낮은 단계'에서 이루어짐**

침해사고의 일반적 문제 (2/5)

- **자산 관리의 낮은 인식**
  - 관리자의 잦은 인사이동
  - 빈번한 자산 조사
  - 비합리적인 자산 배정
  - 파악되지 않는 자산
  - 귀찮음, 하찮은 일 ➔ 자기 희생이 필요

- **관리되지 않는 자산은 보안에 매우 취약**

침해사고의 일반적 문제 (3/5)

- **로그 관리의 문제**
  - **로그는 많이 남길수록 좋다?**
    - ✓ 저장소 문제
    - ✓ 빅데이터 활용 필요?!
    - ✓ 로그 분석이 가능한가?!
  - **기본 로그가 남으니깐?**
    - ✓ 사고 발생 시 분석이 어려움
- **로그는 분석에 가장 중요한 데이터 (로그 vs. 포렌식 아티팩트)**
- **목적에 맞게 선별적 로그 관리 필요 혹은 로그 이중화**
- **법적 대응을 위해서라고 로그는 필수적**

침해사고의 일반적 문제 (4/5)

- **규정 미준수**
  - **내 PC는 내가 지킨다!!**
  - **다양한 우회 기법을 이용해 사내 보안 시스템 우회**
    - ✓ NIC 이중화로 망분리 우회
    - ✓ 포트 변경으로 애플리케이션 차단 우회
    - ✓ SSH 터널링, 포트 포워딩을 통한 우회
    - ✓ 외부 프록시, IP 주소를 이용해 차단 사이트 우회

- **아무리 강력한 지침을 마련하더라고 익숙해지면 결국....**

- **인식의 전환 필요, 제재 조치 마련**

침해사고의 일반적 문제 (5/5)

- **장치 관리의 어려움**
  - BYOD (Bring Your Own Device)
  - CYOD (Choose Your Own Device)
  - COPE (Corporate Owned, Personally Enabled)

- **BYOD 솔루션**
  - NAC (Network Access Control)
  - MDM (Mobile Device Management)

- **CYOD < BYOD < COPE**

1. 문제 인식의 전환

- **침해사고를 막아보자?**
  - 보안 장비/솔루션을 겹겹이 쌓으면 막을 수 있나?
  - 보안팀 규모를 10배로 늘리면 1/10로 위험이 줄어드는가?
  - 회사 영업이익을 모두 정보보호에 투자한다고 하여 막을 수 있나?

- **그렇다면 어떻게?**

침해사고 대응

1. 문제 인식의 전환

- **'공격은 막을 수 없다'에서부터 출발**
  - 막을 수 없다면, 가능성을 최대한 낮추고 신속하고 체계적인 대응으로 피해를 최소로...

- **가능성 낮추기!!!**
  - 표준적인 정보보호 예산을 지속적으로 투자
  - 적재적소에 보안 장비/솔루션 도입, 능동적인 관제 서비스
  - 보안팀의 규모 확장, 보안 교육을 통해 직원의 인식 전환

- **위험을 낮출 수는 있어도 없앨 수는 없다...**

2. 현장 대응 방안, 클라이언트

1. 라이브 데이터 수집

- 활성데이터 – 프로세스 정보, 네트워크 정보, 로그온 정보 등
- 비활성중요데이터 – 파일시스템 메타데이터, 레지스트리, 이벤트로그 등
- 물리메모리, 패킷

2. 시스템 종료

- 본체 뒤 케이블 분리 혹은 전원 공급기 차단

3. 원인 분석

- (해당부서) 분석팀에게 저장매체만 전달
- (인프라팀) 표준 환경 재설치 (고스트 등 이용)
- (분석팀) 저장매체 압축 이미징 ➔ 정밀 분석

2. 현장 대응 방안, 서버

1. 라이브 데이터 수집

- 활성데이터 – 프로세스 정보, 네트워크 정보, 로그온 정보 등
- 비활성중요데이터 – 파일시스템 메타데이터, 레지스트리, 이벤트로그 등
- 물리메모리, 패킷,

2. 시스템 종료 vs. 라이브 대응

- 시스템 종료에 따른 영향 평가 후 종료가 가능하다면 정상 종료 절차

3. 원인 분석

- (분석팀) 라이브 혹은 로컬/원격 이미징
- (인프라팀) 백업 시스템을 이용해 재설치
- (분석팀) 이미지 정밀 분석

3. 침해사고 분석팀을 만들자!!

- 기존 관제, CERT 팀의 역할이 아닌 **새로운 역할**
- 대응보다 **원인 파악에 초점**을 맞춘 분석 ➔ **APT 대응**

- **평시**
  - 신규 취약점과 침해사고 연구
  - 침해지표 관리
  - 모의해킹 로그 분석

- **전시**
  - 정밀 분석을 통해 원인 규명 ➔ 장비/솔루션에 반영

4. 침해사고 랩(LAB)을 구축하자!!

- 포렌식 랩이 아닌 침해사고(IR)에 초점을 맞춘 랩 구축
- 침해사고 데이터 수집 및 분석이 가능한 랩
- 가상 침해사고 케이스 분석 ➔ 침해 지표 생성
- 패치, 업데이트에 따른 영향력 테스트
- 새로운 장비/솔루션 도입 시 영향력 테스트

5. 형상관리를 하자!!

- **포맷이 답은 아니다**
  - 인지된 클라이언트는 APT 공격의 과정일 수도 있음

- **저장장치는 교체 후 이미징하여 보관**
  - 중요도에 따라 최소 3개월 보관
  - 추후 원인 파악, 법률적 대응에 활용

- **저장장치 비용 문제**
  - 압축하여 용량 최소화

5. 침해지표를 관리하자!!

- **IOC (Indicators Of Compromise)**
  - 침해 혹은 감염을 확인할 수 있는 포렌식 아티팩트

- **전통적인 침해 지표**
  - IP 주소, 악성코드의 해시 및 CRC 체크섬, C2 URL

- **향상된 침해 지표**
  - 악성코드 실행으로 생성되는 시스템 상의 모든 흔적

- **침해 지표의 활용**
  - 특정 조직 내의추가적인 침해시스템 탐지
  - 유사한 유형의 침해 흔적을 다른 조직에 적용할 때
  - 침해사고 이외에 안티포렌식 탐지 등으로 확장 적용 가능

6. 침해사고 준비도를 갖추자!!

보안 사고에 따른 비용을 최소화하기 위해 사고가 발생하면 신속히 잠재적인 흔적을 법적 능력을 유지한 상태에서 수집하고 분석할 수 있도록 사전에 준비를 갖추는 일

- **대부분의 보안 투자는 사고 가능성을 낮추기 위한 사전적 투자**
- **침해사고 준비도도 사전적 투자이긴 하지만,,,**

  사고 발생시 어떻게 하면 신속하고 효과적으로 대응할지에 목적을 둠
- **침해사고 준비도 평가**
  - 적합한 규제와 법적 요구사항을 만족할만한 대응 전략을 갖추고 있는가?
  - 침해사고에 따른 역할과 책임을 각 개인이 인지하고 있는가?
  - 사고를 빠르게 탐지할 수 있는 매커니즘을 보유하고 있는가?
  - 잠재적인 데이터 유출에 대응할 수 있는 절차를 갖추고 있는가?
  - 대응할 수 있는 필요한 하드웨어와 소프트웨어를 갖추고 있는가?

7. 침해사고 대응 절차를 마련하자!!

- **조직의 상황에 맞는 적절한 침해사고 대응 절차를 마련**

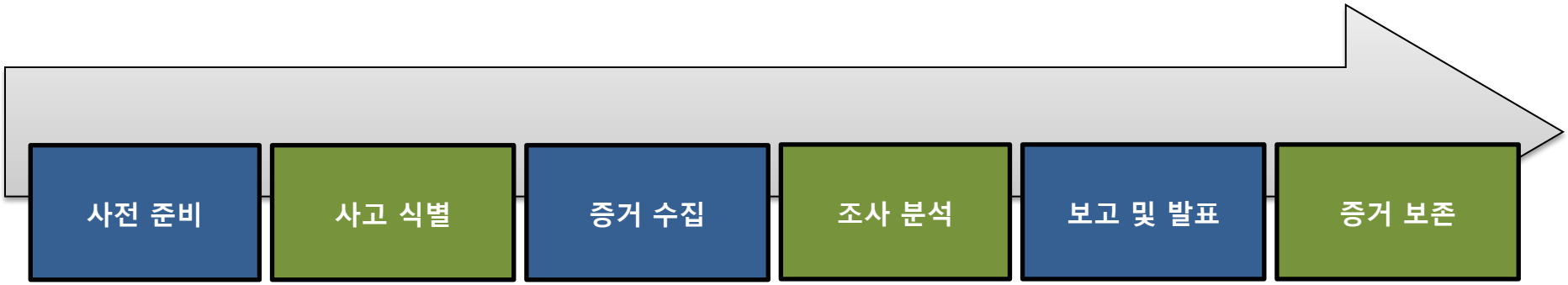
- **대응 절차 참고**
  - 2012.10 – 침해사고 조치 가이드 , 한국인터넷진흥원
    - ✓ http://www.krcert.or.kr/kor/data/technicalView.jsp?p_bulletin_writing_sequence=1404
  - 2012.03 – 디지털 포렌식 방법을 활용한 침해사고 대응 절차, 삼성SDS저널
    - ✓ http://www.sds.samsung.co.kr/knowledge/sjis/treatise23.jsp
  - 2010.01 – 침해사고 분석 절차 안내서, 한국인터넷진흥원
    - ✓ http://www.kisa.or.kr/public/laws/laws3.jsp

침해사고 절차

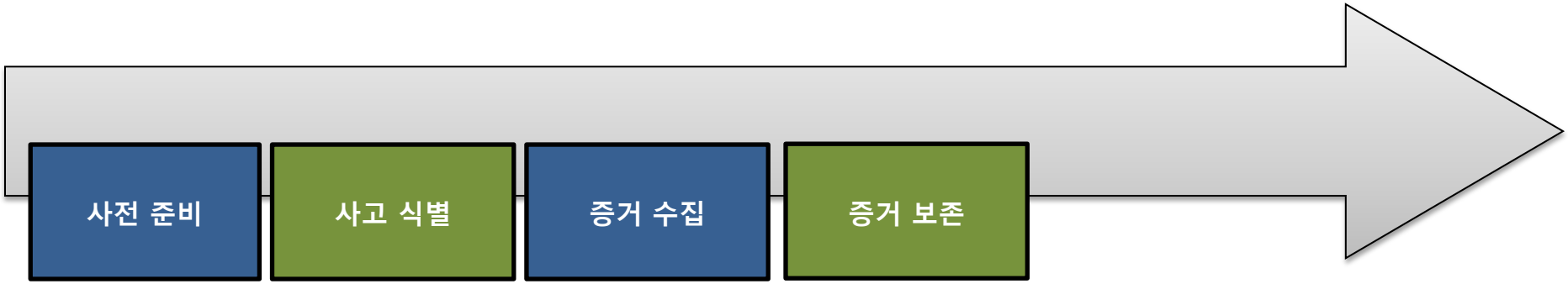
디지털 포렌식 절차 – 6단계

디지털 포렌식 절차

침해사고 대응 절차 – 6/4단계



침해사고 대응 절차 6단계



침해사고 대응 절차 4단계

침해사고 절차

1단계 – 사전 준비

- 신규 취약점 흔적 연구
- 침해사고 가상 케이스 분석
- 침해지표 관리
- 모의해킹 로그 분석
- 수집 및 분석 도구 테스트
- 조사 및 분석 방법론 정비
- 사본 및 아카이빙 저장용 저장장치 준비

2단계 – 사고 식별

- **침해사고 인가??**
  - IT/보안 장비/솔루션 모니터링 ➔ 의심 이벤트/트래픽
  - 관리자 점검 ➔ 비정상 로그, 권한 설정 변경, 시스템 자원 불법 사용
  - 장비/솔루션 오작동
  - 사용자 인지

- **침해사고군!!**
  - IT/보안 장비/솔루션 모니터링 ➔ 악성 이벤트/트래픽
  - 비정상 서비스 ➔ 웹 페이지 변조, 게임머니 상승, 저장장치 파괴, 랜섬웨어 등
  - 관리자 점검 ➔ 웹셸 탐지, 악성 로그 확인 등
  - 공격자 노출 ➔ 유출 정보 노출, 협박, 조롱 등

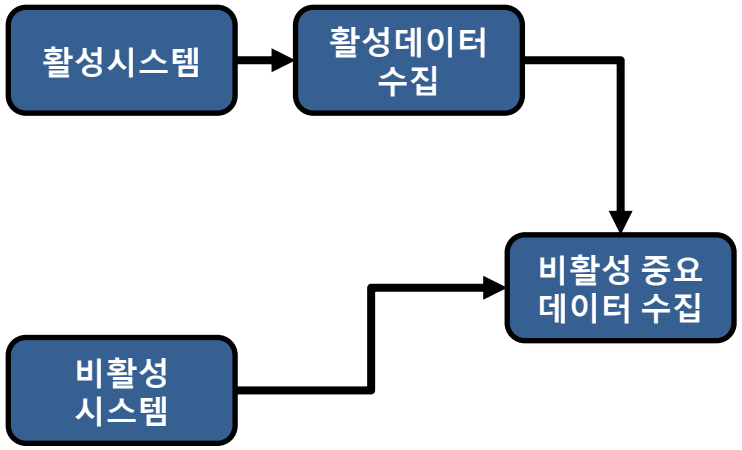
2단계 – 사고 식별

- **인터뷰**
  - 효율적인 분석을 위해 대상 시스템 사용자와 반드시 면담
  - 이벤트 발생 시점 전, 후 혹은 최근 행위에 대한 조사

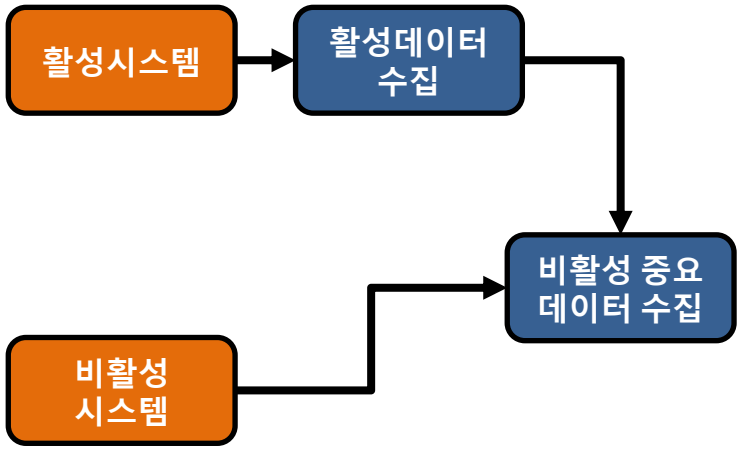
- **조사 및 분석 범위 결정**
  - 시스템 전체 구성도 확인
  - 증거 가치가 있는 대상 시스템 및 장치 식별

침해사고 절차

3단계 – 증거 수집



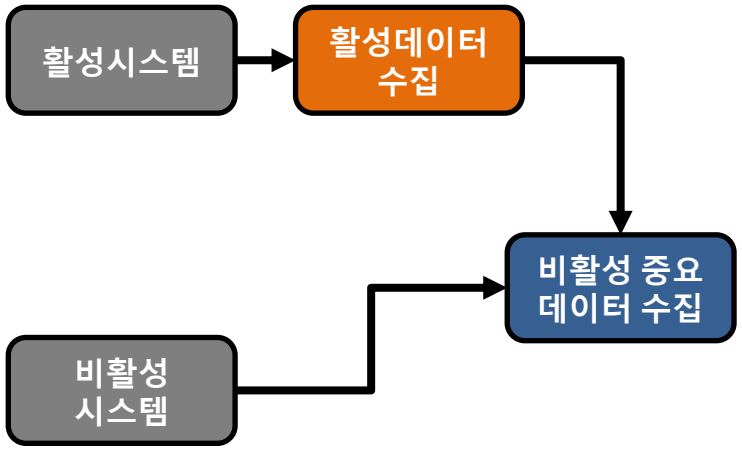
3단계 – 증거 수집



- **활성(라이브) 시스템**
  - 조사 대상 시스템의 전원이 켜져 있는 경우

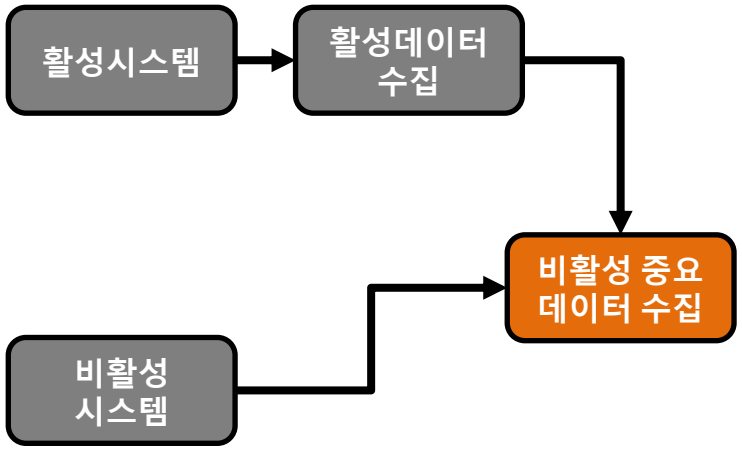
- **비활성시스템**
  - 조사 대상 시스템의 전원이 꺼져 있는 경우

3단계 – 증거 수집



- **활성(라이브) 데이터 수집**
  - **시스템 스크립트** (윈도우: 배치 스크립트, 리눅스/유닉스: 셸 스크립트)
  - 수집 순서는 휘발성 정도에 따라 혹은 중요도에 따라
  - 물리메모리 덤프, 네트워크 패킷
  - 네트워크 연결, 프로세스 정보, 로그인 사용자, 서비스 목록, 클립보드
  - 시스템 정보, 네트워크 인터페이스 정보, 작업 목록, 자동실행 정보, 감사 정책 정보 등

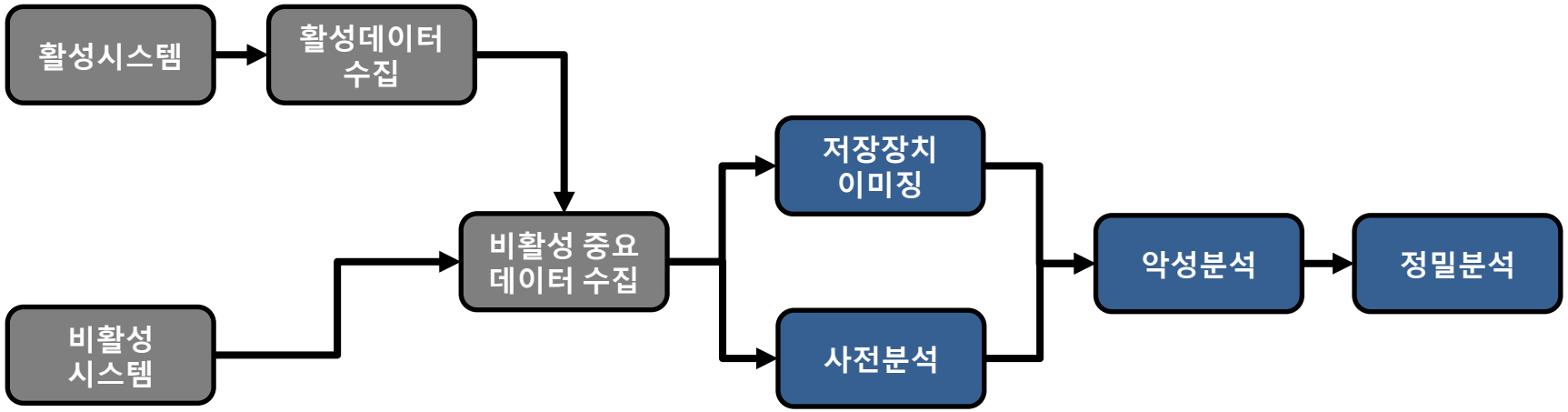
3단계 – 증거 수집



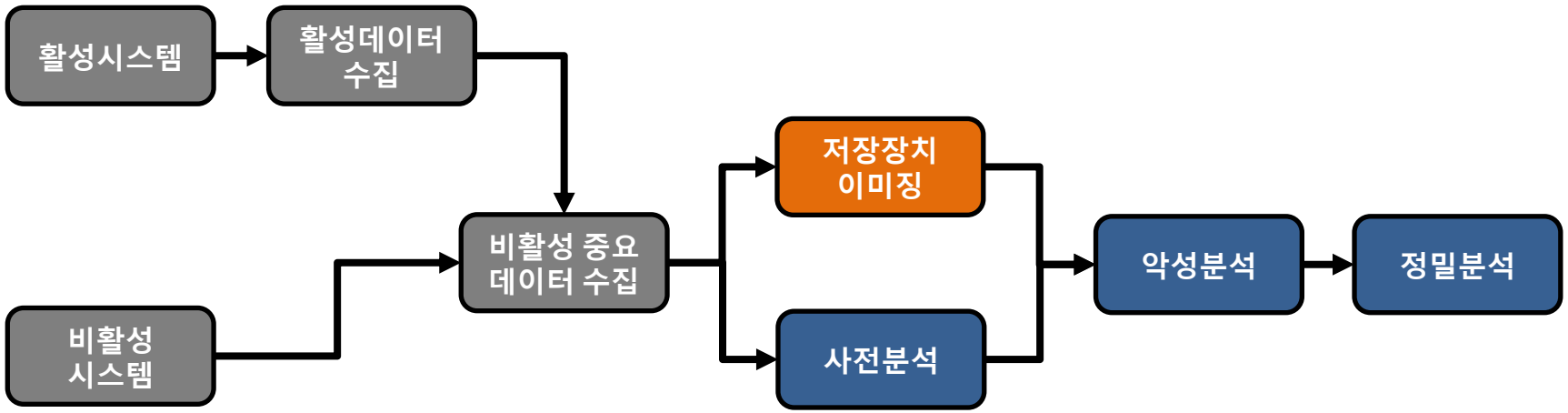
- **비활성 중요 데이터 수집**
  - 사전 분석에 활용할 수 있는 비활성 중요 데이터 수집
  - MBR, 파일시스템 메타데이터($MFT), 레지스트리 파일, 프리패치, 웹 브라우저 흔적, 로그 등
  - **활성시스템 :** 활성데이터 수집 스크립트에 포함 ➔ 저수준 수집 도구 필요
  - **비활성시스템 :** 쓰기방지장치 하에서 저장장치 마운트 후 주요 데이터 추출

침해사고 절차

4단계 – 조사 분석

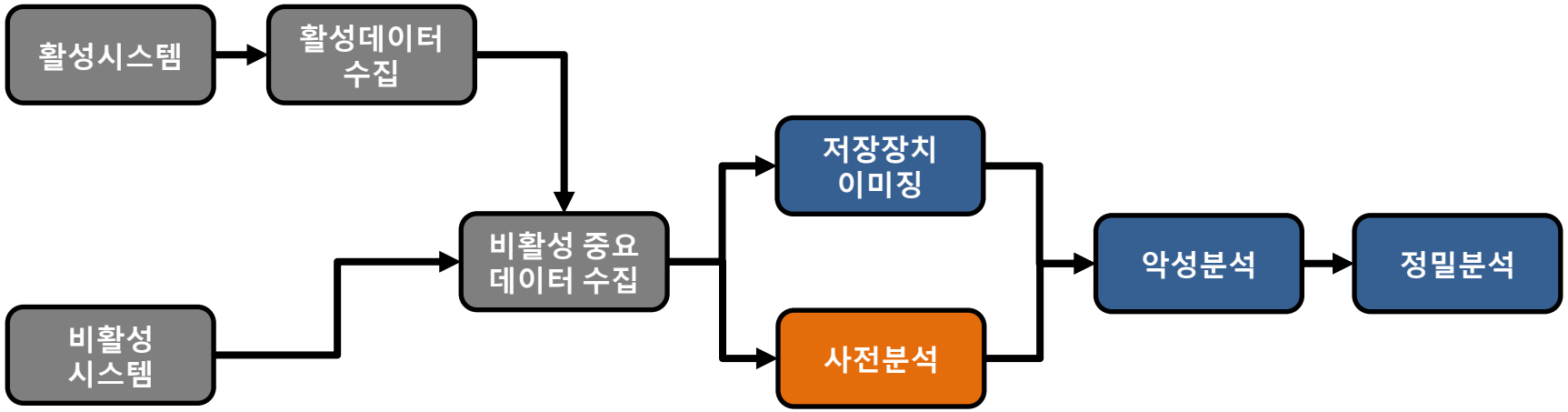


4단계 – 조사 분석



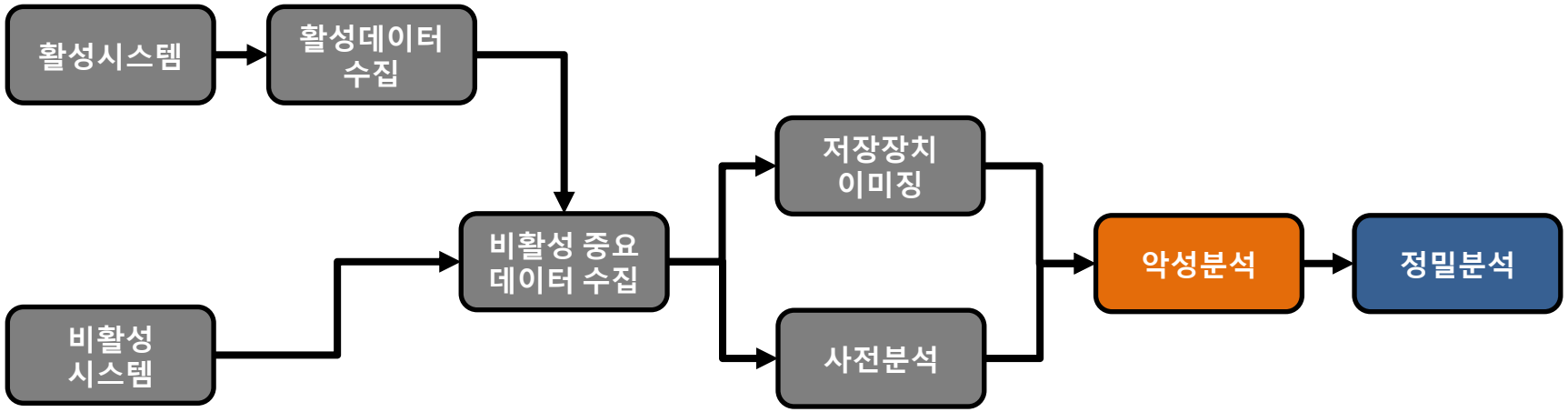
- **저장장치 이미징**
  - 전문 포렌식 이미징 장비 사용
    - ✓ Logicube Falcon / Tableau TD3 / Image MASSter Solo-4
  - 라이브 CD, 쓰기 방지 장치, 네트워크 케이블

4단계 – 조사 분석



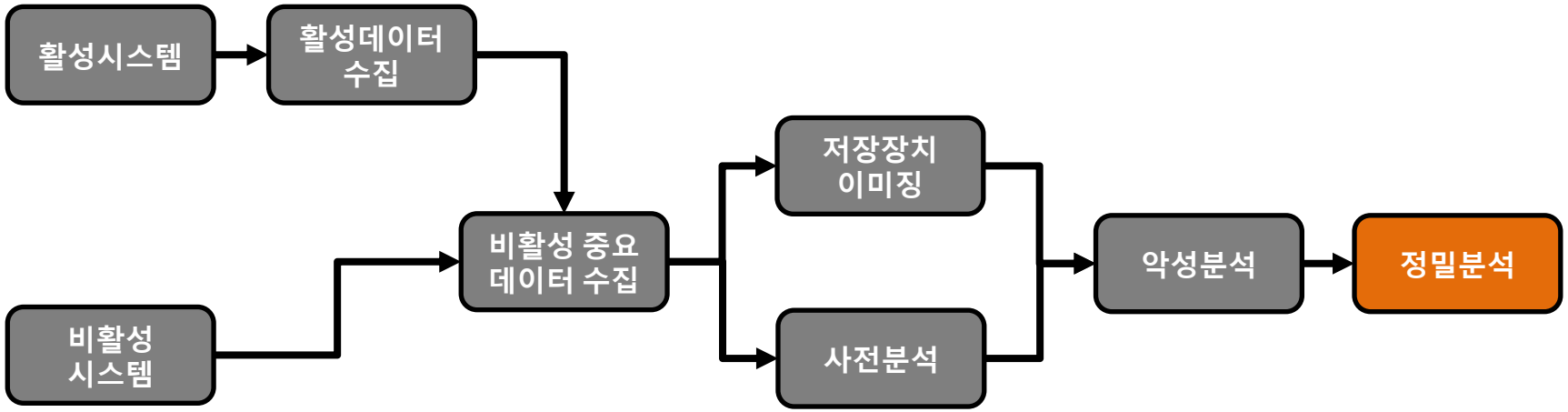
- **사전 분석**
  - 저장장치 이미징 과정과 병행하여 분석 진행
  - 수집한 활성/비활성 데이터로 침해 흔적/타임라인 분석
  - 사전 분석을 통해 침해 경로, 시점, 정밀 분석 대상 선별

4단계 – 조사 분석



- **악성 분석**
  - 이미징 완료 후 사전 분석 결과를 토대로 수행하는 초기 분석
  - 침해지표(IOC) 확인, 해시 분석, 다양한 AV 탐지, 악성 URL 분석 등

4단계 – 조사 분석



- **정밀 분석**
  - 통합 타임라인 분석, 악성코드 분석, 파일시스템 분석, 로그 분석
  - 가상환경 분석, 파일 포맷 분석

5단계 – 보고 및 발표

- **보고 대상에 맞춘 수준별 보고서 및 발표 준비**
- **보고서**
  - 일일 보고서
  - 최종 보고서

6단계 – 증거 보존

- **4단계**
  - 추후 분석을 위해 수집한 증거 보관 절차
  - 상황에 따라 수집 증거를 압축 보관
  - 사고 식별, 증거 수집 단계의 문서 포함

- **6단계**
  - 케이스의 장기 보관이 필요한 경우 증거 보관 절차
  - 상황에 따라 수집 증거를 압축 보관
  - 케이스의 식별부터 보고에 이르는 전 과정의 문서 포함

질문 및 답변