CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

최근 침해사고 동향 및 대응방안

임채태 단장

KISA
Korea Internet & Security Agency

CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

Contents

KISA
Korea Internet & Security Agency

1. 최근 국내 침해사고 현황 – 타임라인

[1월] 개인정보유출 [2월] 웹변조, 디도스 [3월] 공급망 공격, 랜섬웨어 [4월] 가상자산거래소 해킹 [5월] 전자책 유출 [6월] 공급망 공격 [7월] 메신저 피싱

1. 최근 국내 침해사고 현황 – 통계

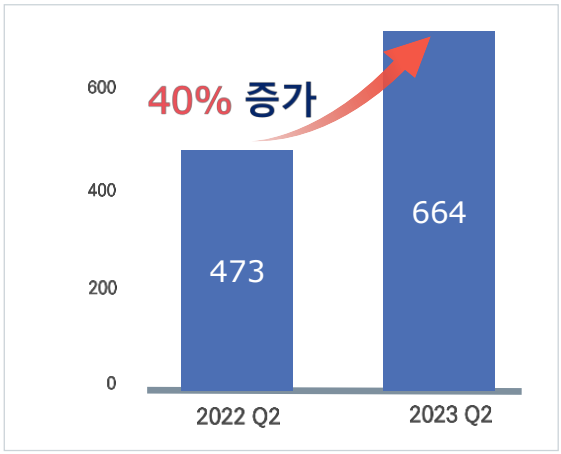
- (신고건수) 전년 동기 대비 **40% 증가**(473건 → 664건)
- (침해유형) 디도스 공격은 전년 동기 대비 **2.6배 증가**
- (업종유형) **제조기업**의 경우 전년 동기 대비 **63% 증가**

`21년 침해사고 신고건수(640건)를 초과

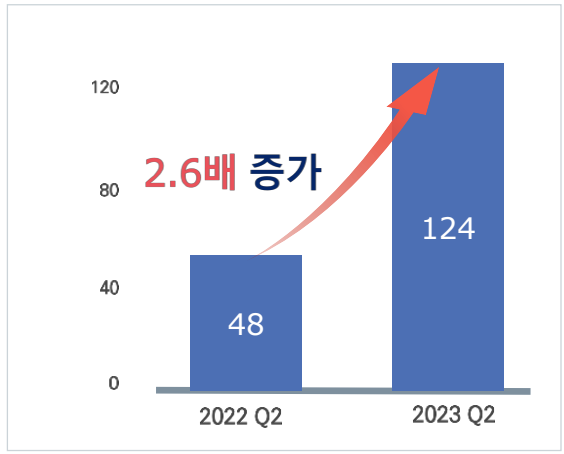
호스팅社 DDoS 공격 증가(1건 → 17건)

대부분 랜섬웨어 피해가 발생

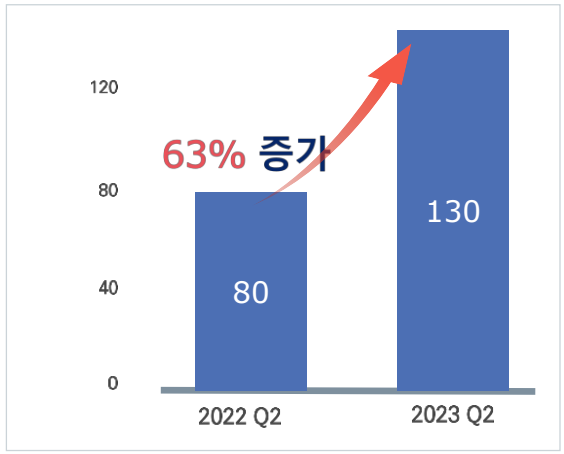
[침해사고 신고 건수]



[DDoS 공격 건수]



[제조업 침해사고 신고 건수]



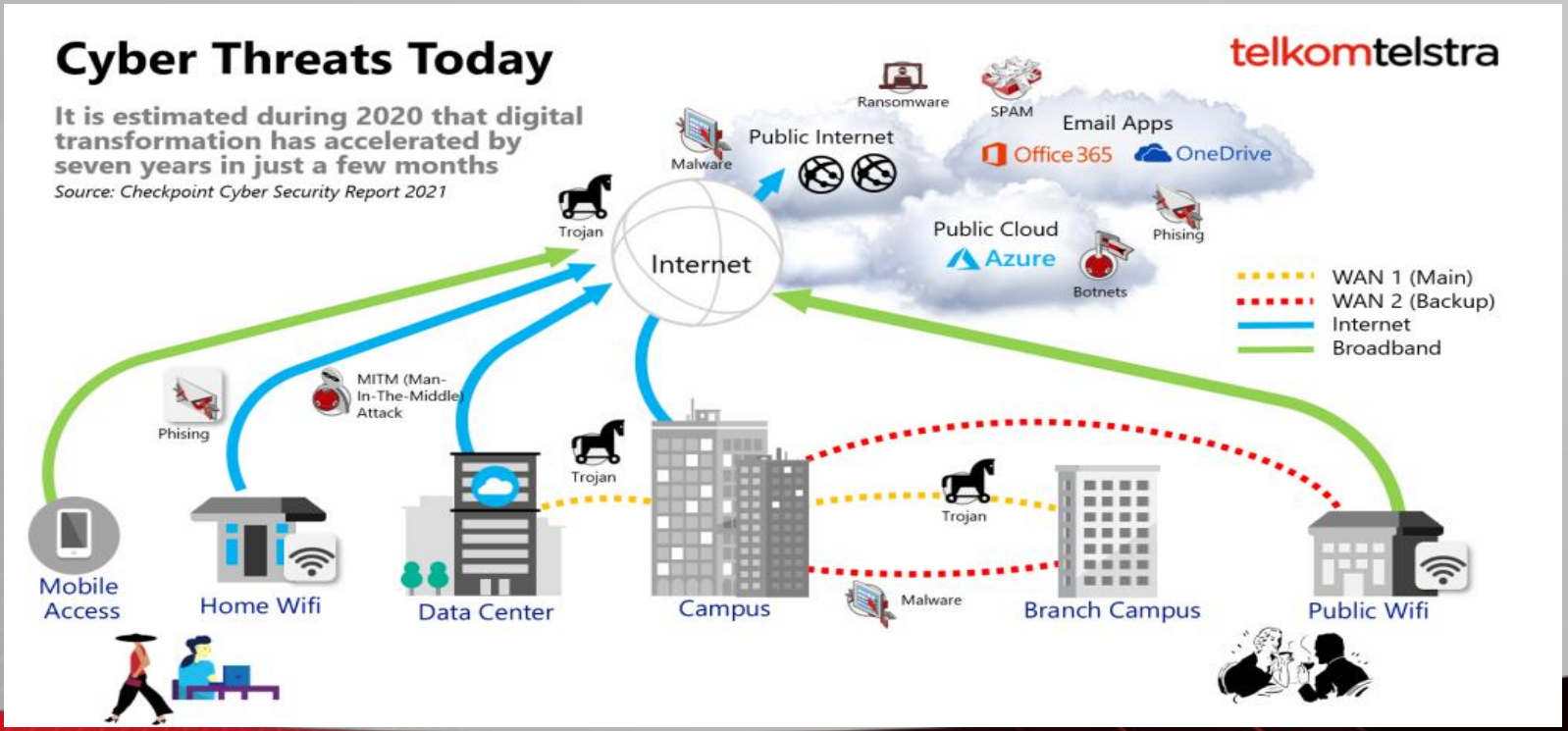
2. 원인 : ① 코로나로 인한 사회 환경의 급격한 디지털 전환(1/2)

- 기업의 재택근무확산과 협력사와의 온라인 협업확대
  - 재택 근무 및 업무 협업 서버 관련 IT 자산 증가
    - 그룹웨어와 자원관리서버, 메일서버 등 주요 IT 자산의 외부 노출
- 의류, 식품, 외식 등 사업의 급격한 디지털 전환 → 관련 매출 급증
  - 고객 니즈에 대한 기업의 실시간 서비스 반영이 매출과 직결
  - 이로 인해 클라우드 기반의 개발 운영 환경(DevOps) 도입 증가

2. 원인 : ① 코로나로 인한 사회 환경의 급격한 디지털 전환(2/2)

- 기업 IT **자산의 무분별한 도입 증가**와 **업무 효율성 우선** 주의

  ☞ **자산의 관리 소홀**과 **일관된 보안 정책을 적용하기 어려움**

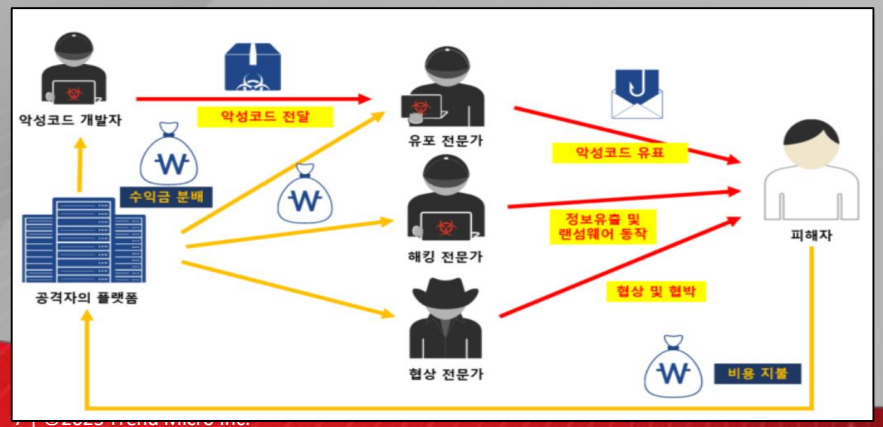


2. 원인 : ② 익명성이 보장된 다크웹, 가상자산시장 활성화(1/2)

다크웹 및 가상자산 시장의 활성화 → 서비스形 랜섬웨어 범죄 사업화

- 익명성이 보장되고 자금세탁에 유용한 다크웹 및 가상자산 시장 활성화
- 전문지식이 없어도 비용만 지급하면 랜섬웨어 공격을 할 수 있게 서비스 형태 제공
  - RaaS (Ransomware as a Service), 제작자, 공격자의 수익금 분배 구조
  - RaaS로 인해 사이버 범죄는 분업화, 전문화로 진화되어 범죄를 저지르게 되는 문턱도 낮아짐

▪ RaaS 플랫폼(SecureNomad 블로그 참고)



▪ 다크웹의 활성화

CIO / CSO / 검색|인터넷 / 랜섬웨어 / 보안 / 분쟁|갈등 / 비즈니스|경제 / 악성코드 2021.04.01

'이 사이트 해킹해주세요'… 다크웹 내 긱 이코노미 부상 중

Andrada Fiscutean | CSO

'2,000달러에 사이트 해커 구함', '이 사이트 해킹 대가 1만 달러', '경쟁사 웹 사이트에서 정보 수집 가능?', '리뷰 삭제 가능? 예산 300달러.'

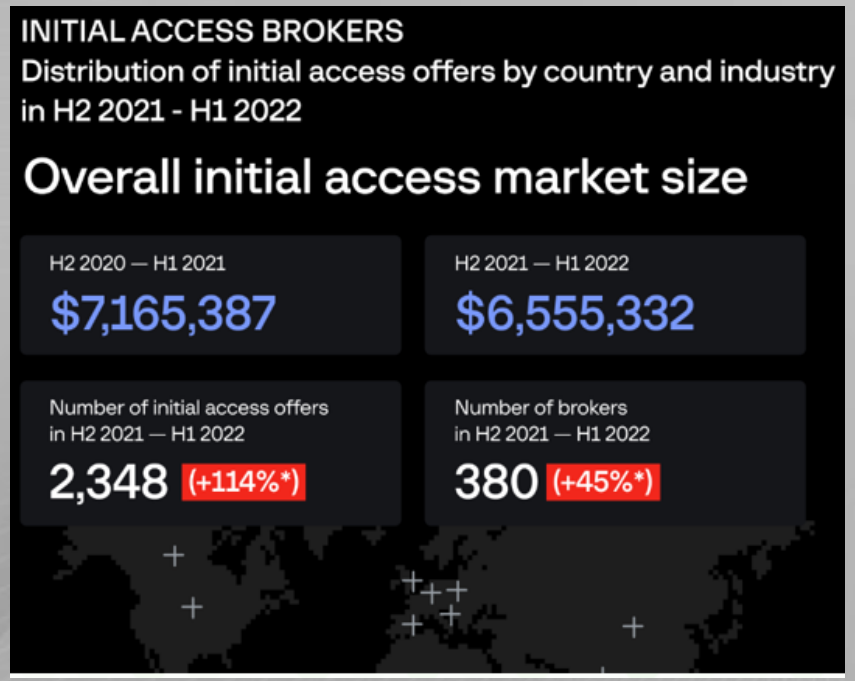
블랙햇(Black Hat)을 고용하려는 이런 게시물이 다크웹(Dark Web) 내 해킹 포럼에 넘쳐나고 있다. 메시지의 대부분은 웹 사이트 공격, 고객 데이터베이스 구매 및 판매, 기업 웹 리소스 액세스 확보 등에 관한 것이다. 구매 글이 많지만, 판매를 하는 사람들도 있다. 초보 및 숙련된 사이버 범죄자들은 자신이 제공할 수 있는 것을 광고하면서 자신의 법률 위반 전문 지식과 의향을 드러낸다.

▪ 가상자산 시장의 활성화

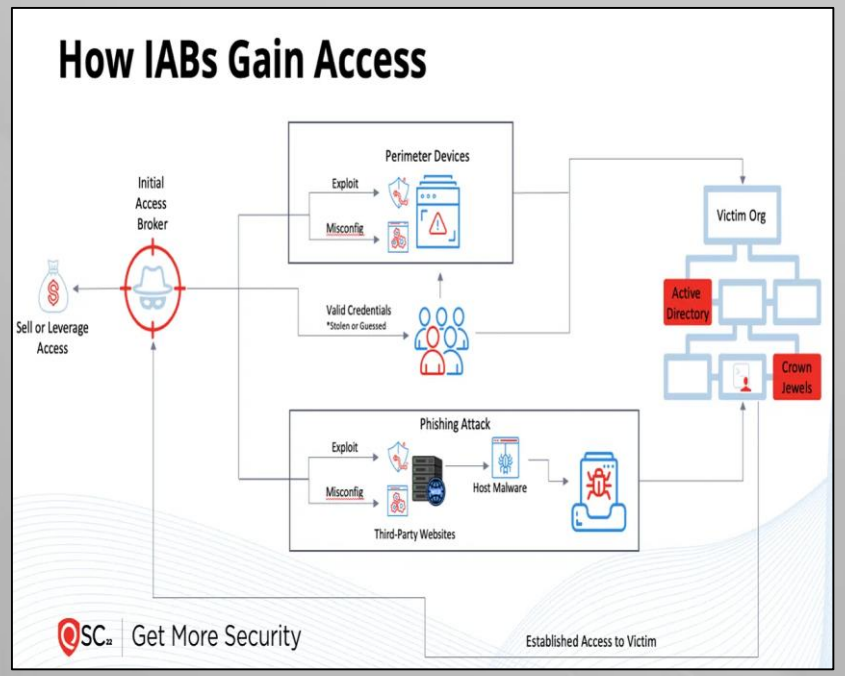
2. 원인 : ② 익명성이 보장된 다크웹, 가상자산시장 활성화(2/2)

특히 다크웹을 통해 시스템 관리자 계정(RDP, VPN)을 전문적으로 판매 브로커 증가

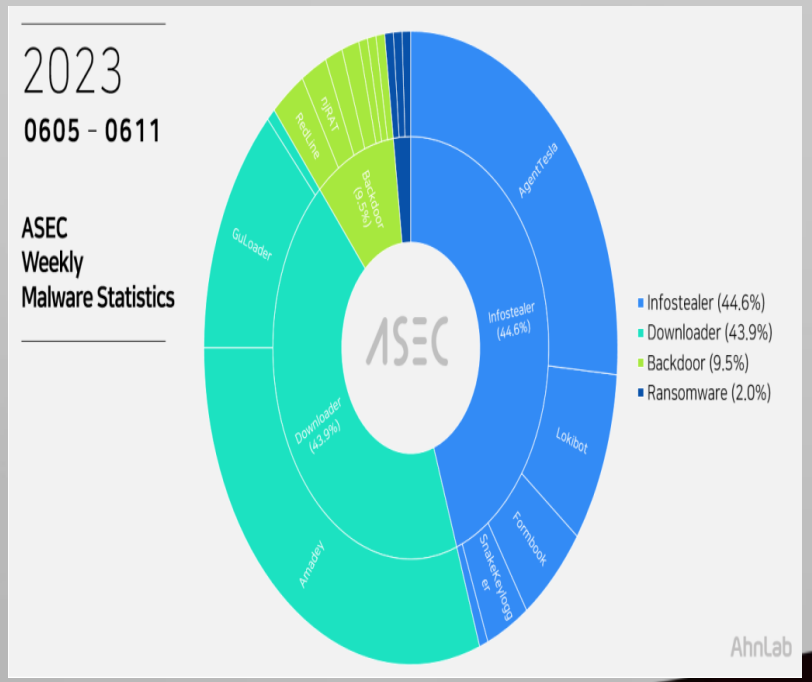
- IAB 판매시장 증가 (Group-IB '23.1월 보고서)



- 계정획득방법(피싱, 내부침투, 외부노출장비 등)



- 인포스틸러악성코드 증가(안랩 6월통계)



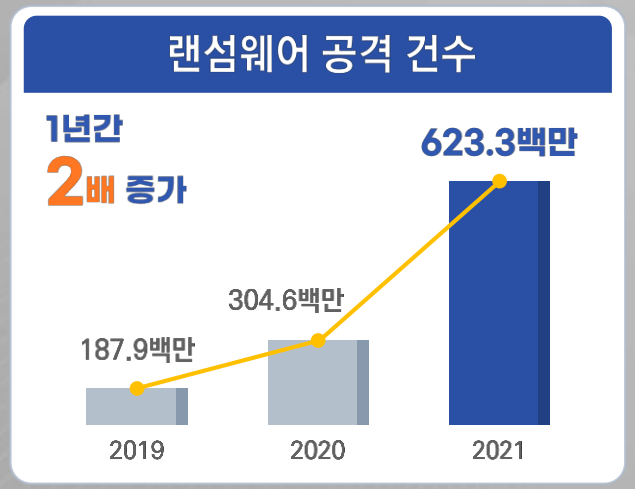
3. 렌섬웨어 증가 및 진화 (1/2)

전세계 랜섬웨어 공격 2배 증가

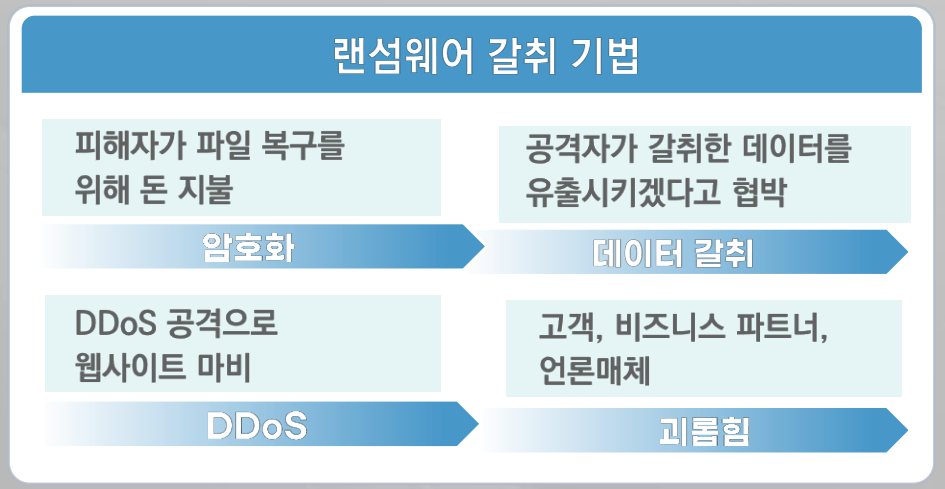
- 다크웹 사이트 등에 평균 4시간 마다 1개 조직의 피해 개시('22년 피해 조직 : 2,679개, 전년대비 4% 증가, 피해자 41%가 협상)
- 원인 : ① 서비스형 랜섬웨어 부상, ② 높은 랜섬웨어 수익율 ③ 개인정보 유출 등에 따른 과태료

랜섬웨어 다중 갈취(Multi-extortion) 수법 꾸준히 증가

- 정보유출 사이트 등을 통한 데이터 갈취는 전년대비 30%, 언론매체 등을 통한 괴롭힘 수법은 20% 증가
- 1차 갈취 : 복호화 비용 , 2차 갈취 : 데이터 유출 협박, 3차 갈취 : 피해자 대상 유출 협박(예: 성형외과)



* Source: Statista, 2022.8

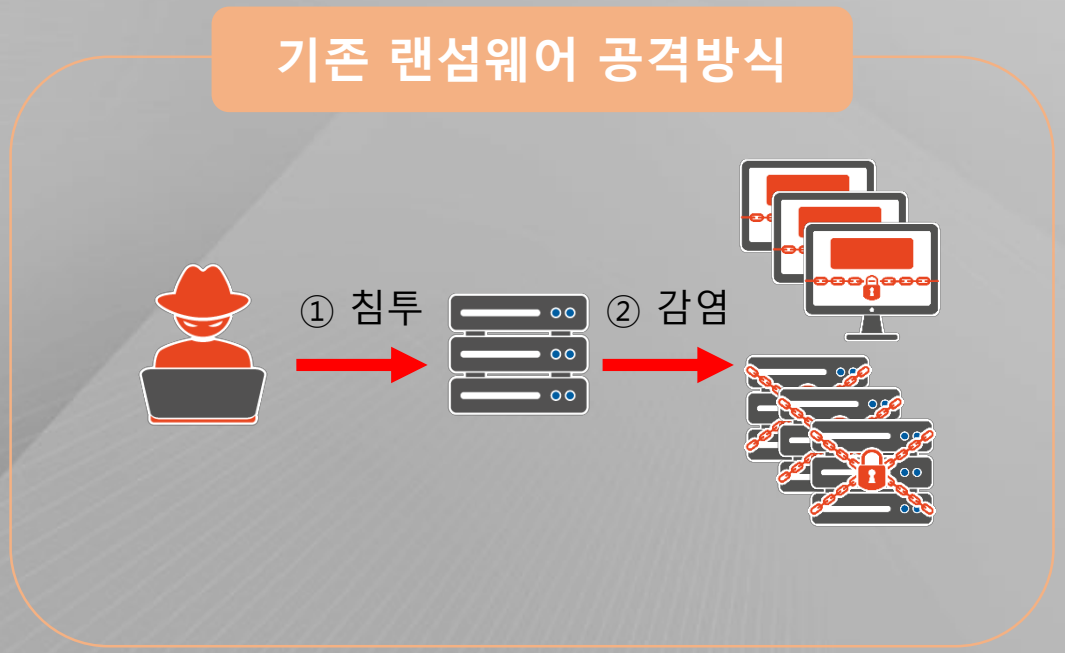


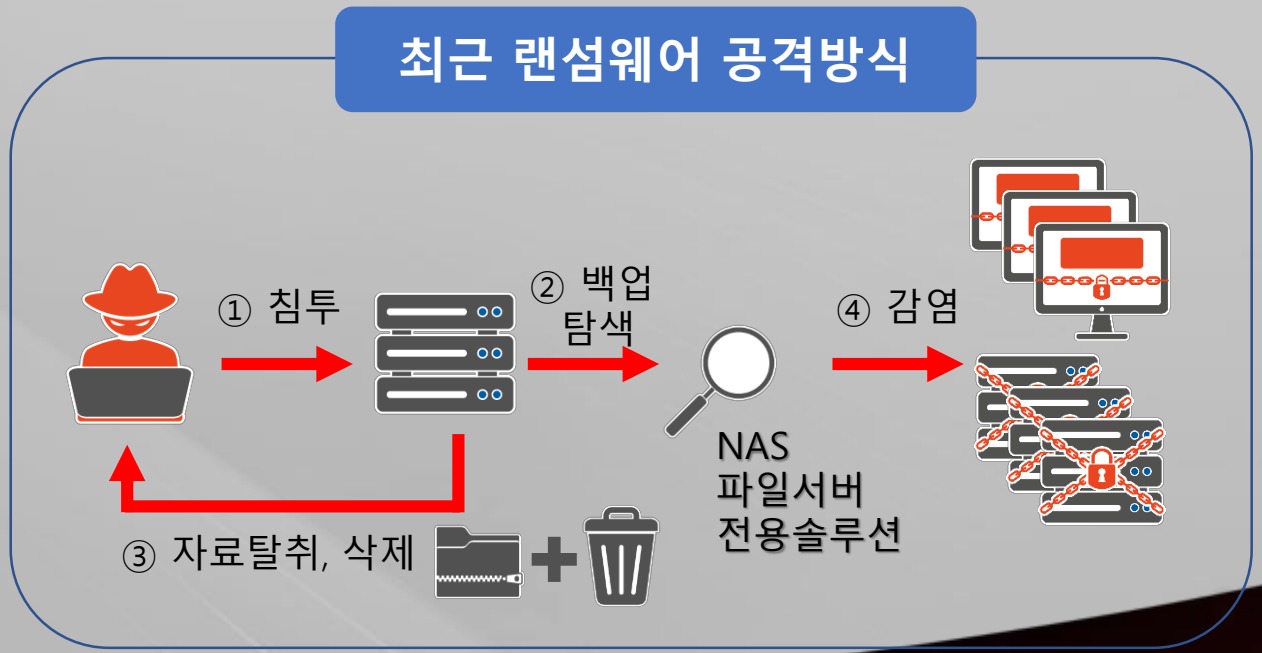
* Source: Paloalto/UNIT42, 2023.5

3. 렌섬웨어 증가 및 진화(2/2)

(랜섬웨어) 바이오 기업 및 제조업체를 대상으로,
인터넷에 노출된 자산과 백업서버를 최우선하여 집중 공격

- **백업 서버도 랜섬웨어에 감염된 비율 : ('22 上) 23.1% → ('23 上) 42.9%**





CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

Contents

KISA
Korea Internet & Security Agency

1. 자동차 부품 제조업체 랜섬웨어 감염 사고

협력사와의 협업을 위한 물품관리 서버에 계정 임의 대입 공격을 통해 침입
→ 내부망 장악 후 **생산관리(MES) 및 전사자원관리(ERP) 등 수십대 서버 암호화**(일주일 간 생산 중단)

①외부에 열려있는 품질관리 서버에 계정 대입공격을 하여 기업 내부 네트워크에 침입, ②연결된 시스템들을 확인하고 원격 접속, ③서버들의 백신을 비활성화 후 랜섬웨어 실행

별도 망에 백업 체계가 갖추어져 있었으나 생산 공정 정상화까지 많은 시간 소요, 외부에 노출된 자산의 보안 정책 및 관리는 미흡

문제점

- **서버 접근제어 및 원격제어 보안 설정 부재**
  - 모든 IP에서 원격접속 가능, 2차 인증 없음
- **관리자 계정 관리 미흡**
  - 유추하기 쉬운 비밀번호 사용, 장기간 동일한 비밀번호 사용
- **주요 서버 모니터링 부재**
  - 약12시간 동안 무작위 대입공격이 진행되었으나 미인지
  - 백신이 악성코드를 탐지하였으나 관리자 미확인

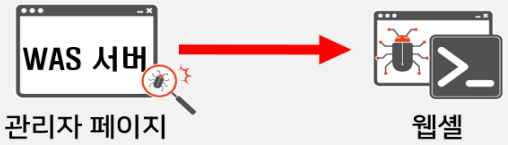
2. 통신사 고객정보 유출 사고

보안에 취약했던 고객인증시스템(WAS)을 통해 침투 → 29만명 고객정보유출

1. 정찰

공격자는 외부에서 접근 가능한
고객인증시스템 및 취약한 관리 페이지 확인

2. 최초침투(웹셸업로드)



취약점(초기암호 미변경) 이용, 관리자 페이지 접속
웹 취약점(파일업로드)를 악용한 웹셸 업로드

3. 정보수집

웹셸을 이용한 서버 내 테스트 목적의
고객정보, DB 설정 파일 등 중요정보를 수집

4. 정보유출

① 웹셸을 이용, DB에 접근하여 고객 정보 유출
② 서버 내 존재하는 고객 파일 유출

< 개인정보유출 시나리오 >

문제점

- **비정상 행위 탐지 · 차단 대응체계 부재**
  - 대용량의 데이터 외부 유출에 대한 실시간 탐지·통제 불가
- **네트워크 및 시스템 자산 보호관리 미흡**
  - 불필요한 주요 네트워크 정보의 외부노출
  - IT자산에 대한 관리 및 점검 부실
- **전문 보안인력 및 정보보호 투자 부족**
  - 부족한 전문인력 및 정보보호 조직의 권한 부족
  - 他통신사 대비 저조한 정보보호 예산
- **보안 인식제고 방안 및 실천 체계 부재**
  - 반복적인 동일 모의 훈련 진행, 형식적인 교육 및 매뉴얼

2. 쇼핑몰 고객정보 유출 사고 (클라우드)

✔ 소스코드저장소에 저장 되어있던 클라우드 접속 권한을 탈취, 고객정보 620만건 유출

①개발자에게 피싱메일을 보내 계정과 OTP 입력 유도, 입력 즉시 이를 이용해
②소스코드저장소에 접속하여 저장 되어있던 클라우드 접속정보 탈취,
③클라우드에 접속하여 ④클라우드 내의 개인정보 유출

클라우드의 다양한 보안 기능을 이용하여
개인 정보를 보호하였으나, 개발 환경에 대한 보안 미흡

문제점

✔ 개발 환경에 대한 보안 정책 부재

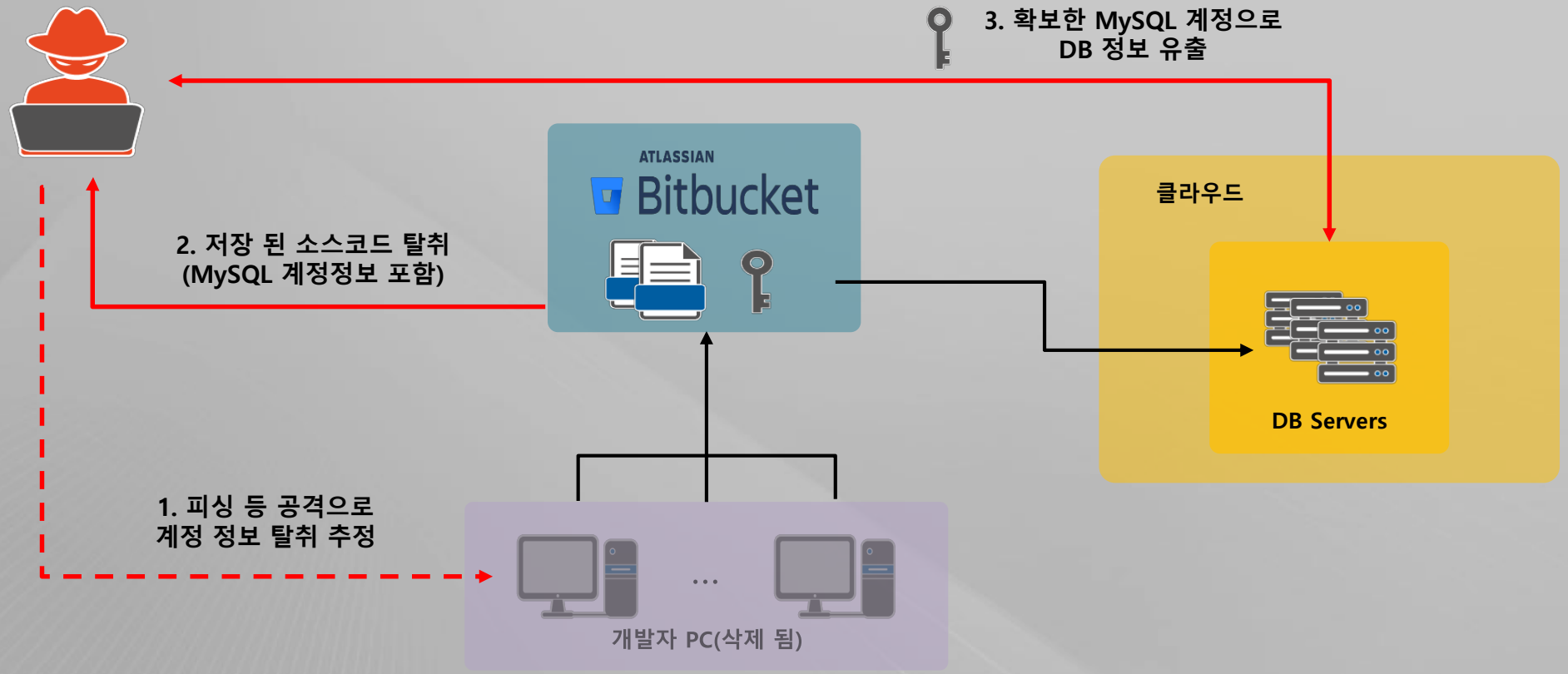
- 개발 편의를 위해 클라우드 관리자 키를 소스코드에 포함
- 중요 소스코드저장소를 외부에서 운영

✔ 내부 직원의 보안인식 부족

- 개발자가 피싱사이트에 OTP 계정까지 입력하고 공격자가 즉시 이를 이용, 소스코드저장소에 부정 접속

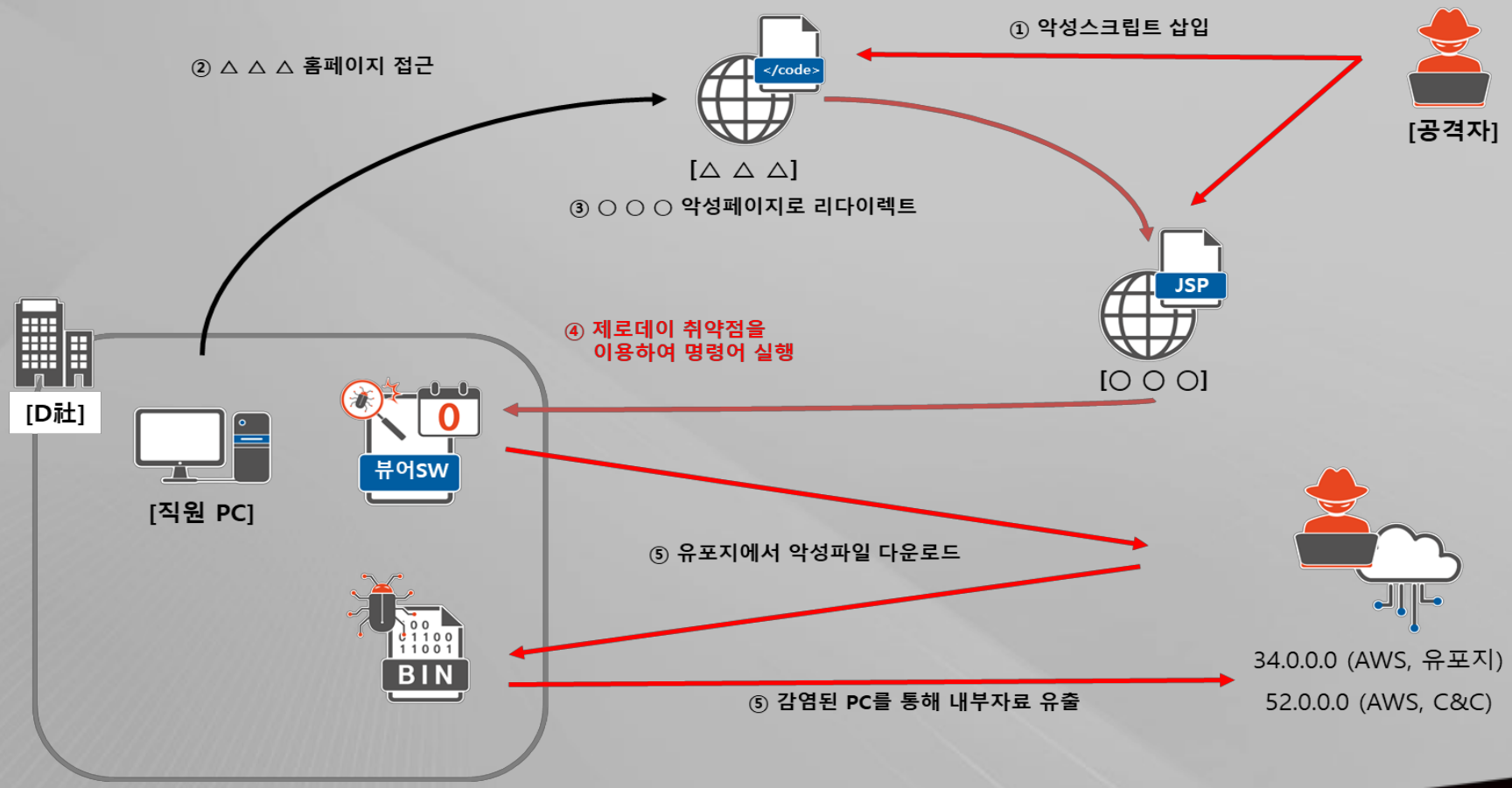
2. B社 DB계정 탈취를 통한 정보유출 (클라우드)

- (유출경로) ① 피싱 메일(추정) → ② 소스코드저장소 접속 → ③ 클라우드 접속 → ④ 정보유출



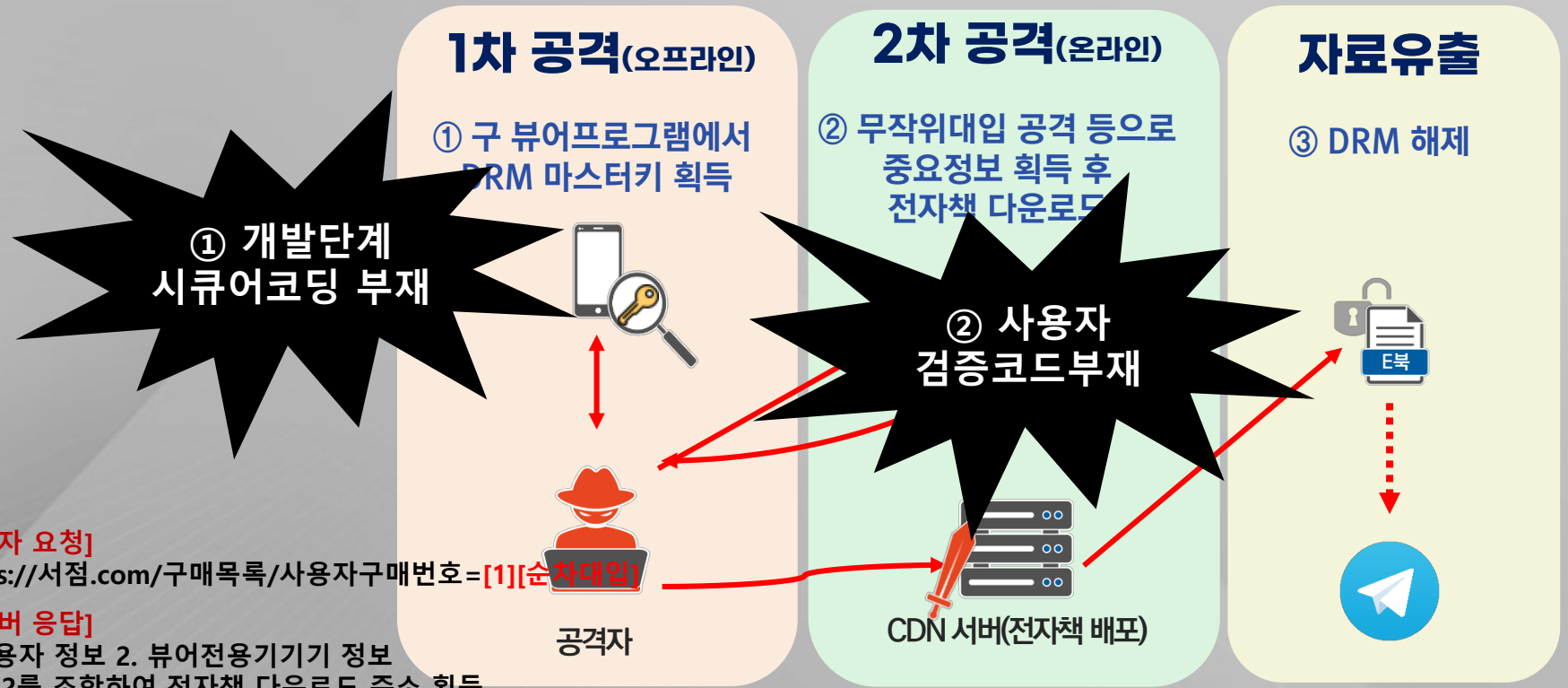
2. D社 시스템 담당자 PC 해킹을 통한 정보유출 (클라우드 관리업체)

(유출경로) ① 운영자 PC 해킹(원격제어 악성코드 감염) → ② 정보유출



2. 온라인 서점 전자책 유출 사고

- 웹서버 및 뷰어SW 취약점으로 암호화된 전자책을 복호화, 5,000권을 텔레그램 공개



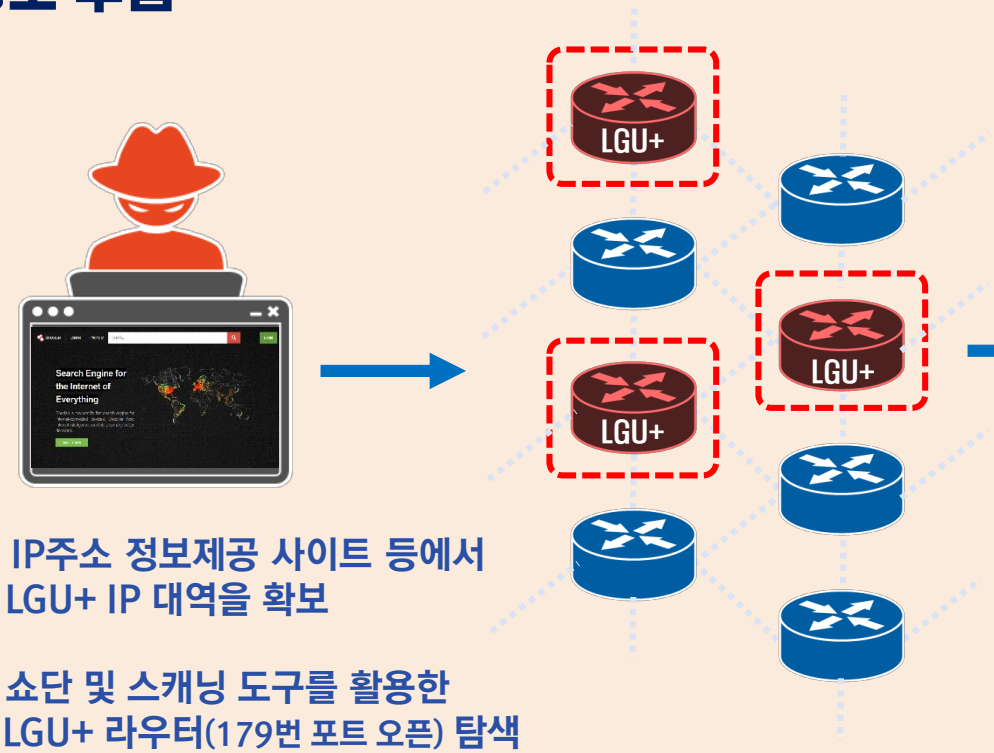
[공격자 요청]
hxxps://서점.com/구매목록/사용자구매번호=[1][순차대입]

[웹서버 응답]
1. 사용자 정보 2. 뷰어전용기기기 정보
→ 1, 2를 조합하여 전자책 다운로드 주소 획득

3. 통신사 유선인터넷망 디도스 사고

- 광대역데이터망 라우터에 대한 5차례(120분) 디도스 공격으로 전국적인 네트워크 장애 발생

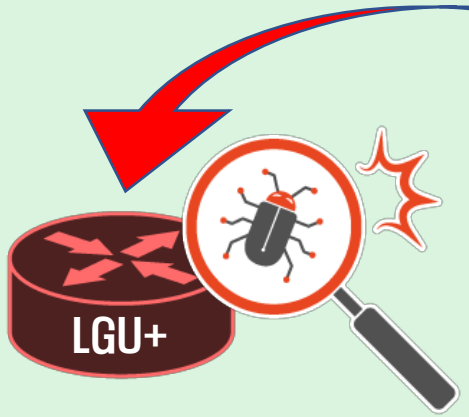
정보 수집



① IP주소 정보제공 사이트 등에서 LGU+ IP 대역을 확보

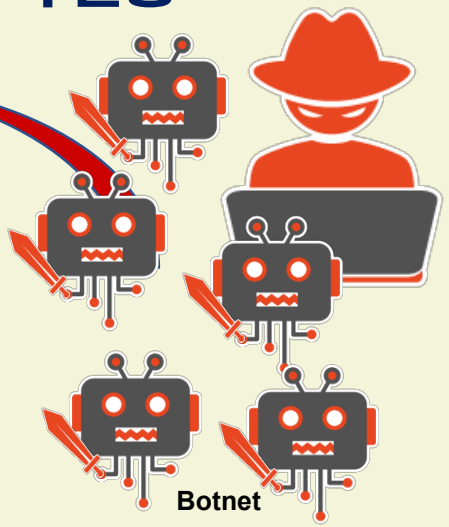
② 쇼단 및 스캐닝 도구를 활용한 LGU+ 라우터(179번 포트 오픈) 탐색

공격 준비



③ LGU+ 라우터 장비의 취약점 확인
『*BGP포트* 오픈(179번)*』

공격 실행



④ BGP포트 오픈 라우터 대상 디도스 공격(1,2차)

⑤ 추가 디도스 공격(3,4,5차)

** BGP포트 : Boarder Gateway Protocol은 라우터가 경로 정보를 주고받는 표준통신규약으로 최신 경로 정보를 갱신하기 위해 주기적으로 통신

4. 국내 침해사고 사례 – 웹변조

(웹변조) 취약한 학회나 협회 누리집 공격, SNS에 공개하여 자신의 능력을 과시

韓정부 해킹 예고했던 '샤오치잉'...알고보니 고전적 수법에 당했다

머니투데이 | 이정현 기자

2023.04.11 18:00

KISA(한국인터넷진흥원) 사고분석팀은 10일 샤오치잉의 공격 기법과 대응방안을 담은 보고서를 발표했다. KISA는 지난 1월부터 샤오치잉이 해킹한 자료를 텔레그램 등 소셜미디어에 공개하고 홈페이지를 변조(디페이스)하는 식의 공격을 감행하자 이에 대응해왔다.

▪ 홈페이지 변조화면

우리는 계속해서 한국의 공공 네트워크와 정부 네트워크를 해킹할 것이고, 우리의 다음 트워크를 해킹할 것이다. 네, 우리는 다시 돌아왔습니다.

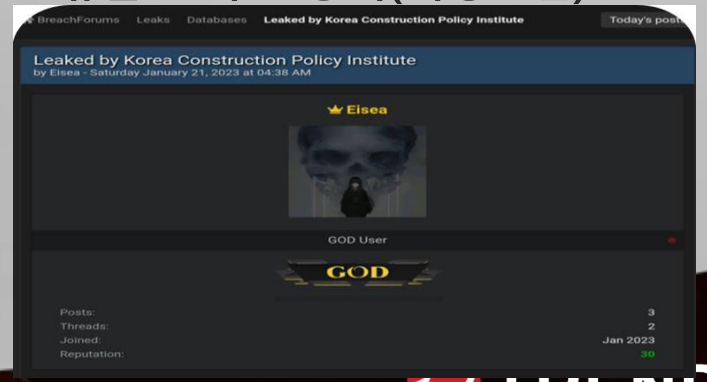
晓骑营

CYBER SECURITY TEAM

샤오치잉이 해킹한 웹 사이트에 업로드한 웹 페이지 유형/사진제공=한국인터넷진흥원

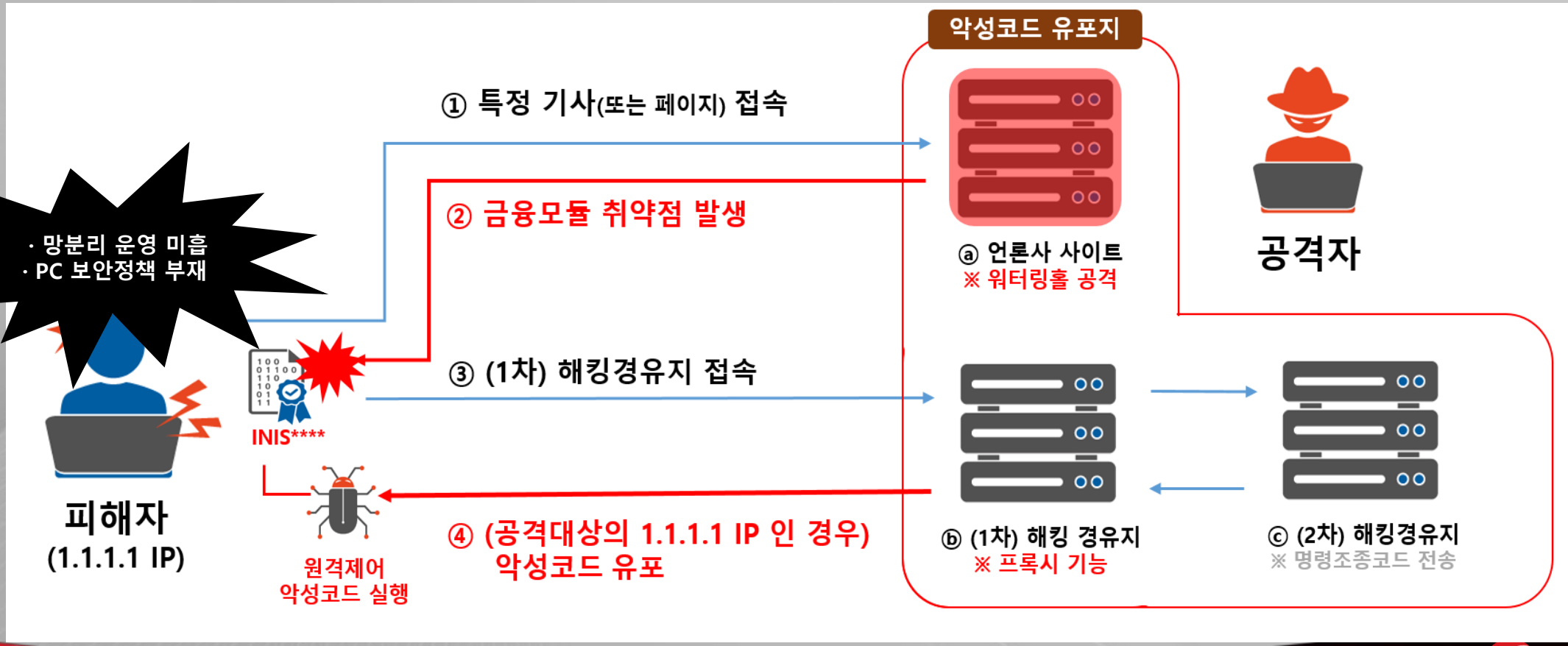
▪ 유출된 자료 공개(텔레그램)

▪ 유출된 자료 공개(해킹포럼)



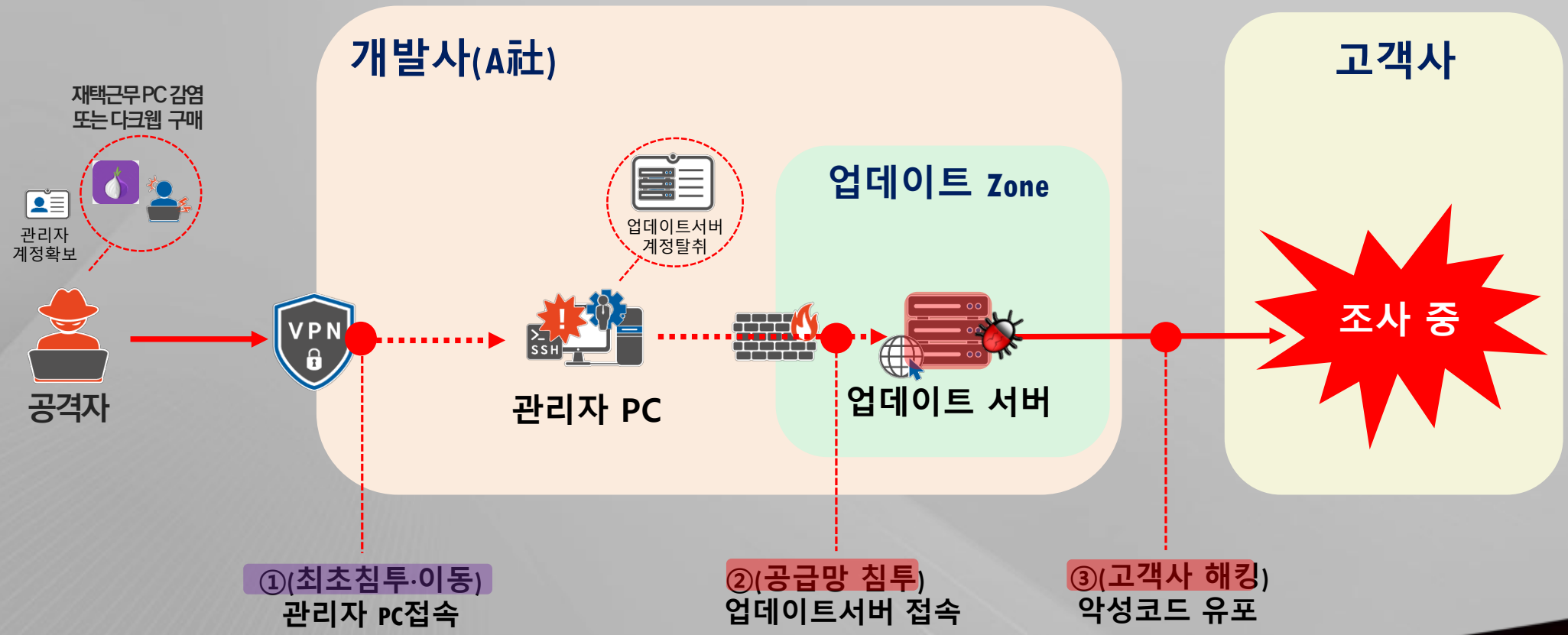
5. 금융보안모듈 SW 개발사 취약점 악용 사고

✔ 언론사 특정 기사를 해킹하고, 사전 확보한 피해기관 IP(금융보안모듈SW 설치PC)가 접속 시에만 악성코드 감염 → **내부자료 유출**



5. 중앙관리솔루션 개발사 업데이트 서버 해킹 사고

✔ 특정 기업 해킹사고 조사 중 중앙관리솔루션 개발사 업데이트서버를 통해 고객사 악성코드 유포 정황



CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

Contents

KISA Korea Internet & Security Agency

1.먼저 '나'를 알자

☑ 내부의 보안 상황을 객관적인 시각으로 재 진단

① 내부 자산에 대한 재점검 (특히 외부에 노출되거나 내부에 방치된 쉐도우 자산 점검)

② 자산의 중요도에 따라 등급 재분류 (특히 배포기능과 공급망 위협 자산은 중요관리)

③ 중요 자산의 위치는 필요에 따라 재배치

④ 중요 자산의 접근 주체에 명확하고 최소한의 업무 권한만 부여

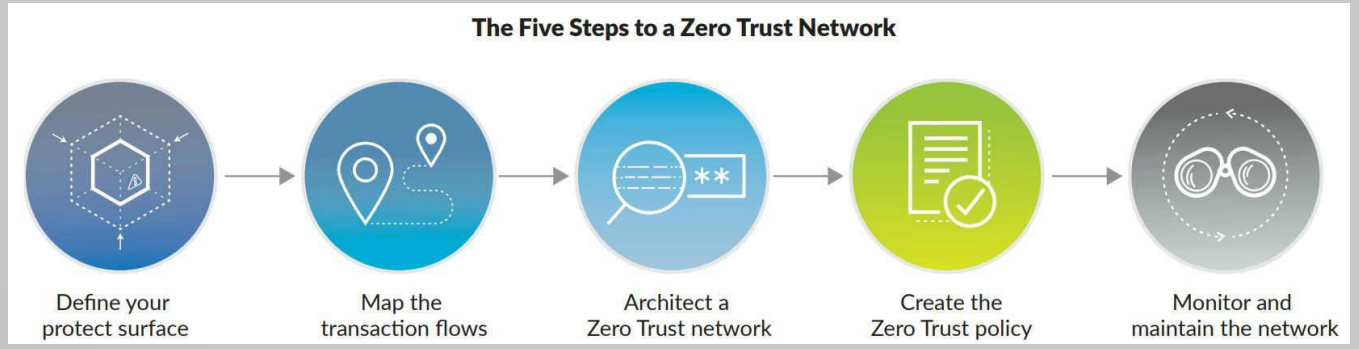
⑤ 중요 자산의 가시성과 무결성 확보되도록 지속 모니터링

⑥ 기업의 존폐와 연관된 자산의 경우 업무 지속성이 보장된 백업체계 운영

※ 서비스망과 물리적 다른 장소 또는 별도의 폐쇄망에서 운영, 전용 백업 보안 솔루션 도입 검토

2. 모든 것을 검증하는 보안체계 구축(제로트러스트 보안모델링)

- 항상 검증하고
- 최소한의 권한
- 침해사고가 발생한것으로 가정



(포레스터 리서치)

- 다단계 인증, 종단 탐지·대응, 데이터 탈취 대비 암호화, 숙련되고 권한 부여된 보안팀 구성
- 즉각적 보안패치 적용, 데이터 백업 주기적 테스트 및 오프라인 유지
- 제3자 평가에 의한 보안 취약점 확인, 피해를 가정한 사고 대응계획 수립 및 테스트
- 핵심 기업 네트워크를 일반적인 인터넷 사용환경과 분리 검토

충분한 시간을 갖고 장기적 도입 적용검토

3. '적'을 알자

☑ 자체 대응과 외부 인텔리네트워크를 활용한 대응역량 강화

① (내부) 사소한 위협도 원인을 확인하고 대응하여 공격자 정보를 수집

② (외부) 인텔리네트워크를 활용한 지속적인 공격자 정보를 수집

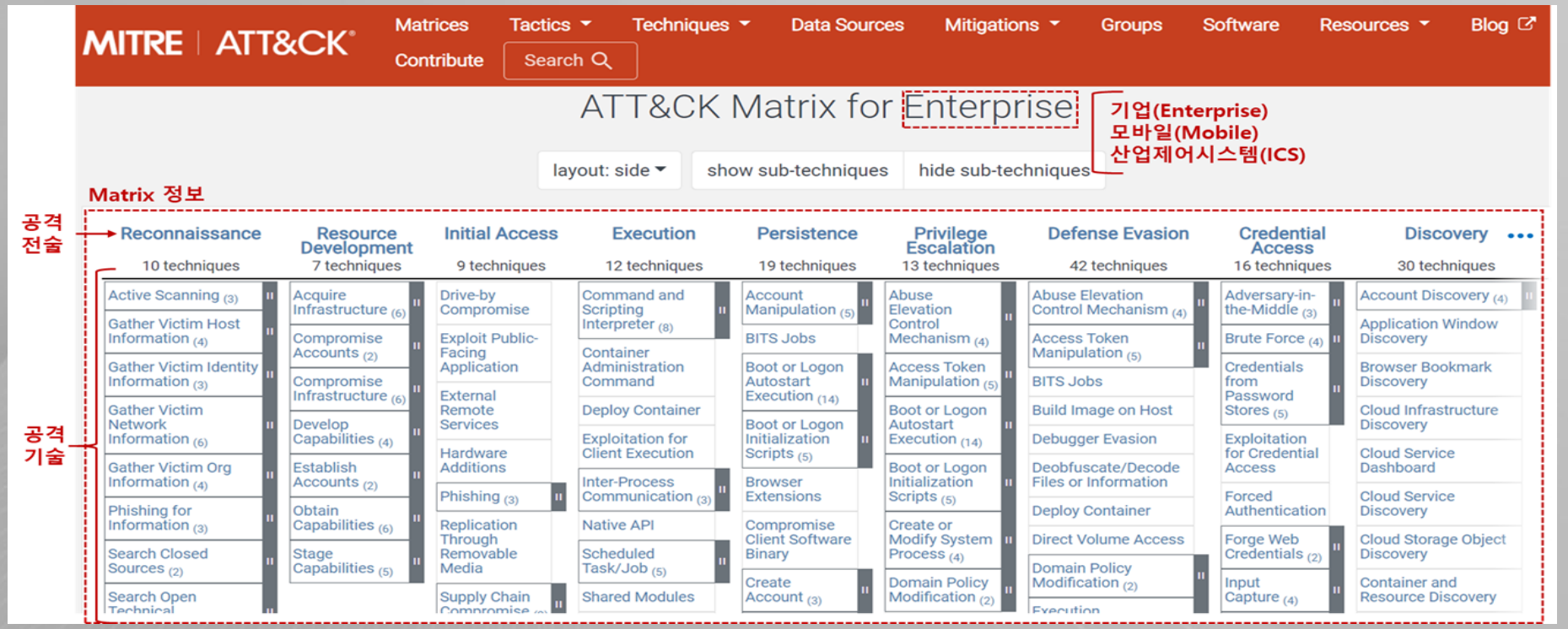
③ '①②' 를 활용한 연관성 분석이 가능하도록 대응 체계 구축, 역량 강화

공격자의 전략(T)과 기술(T), 절차(P)를 이해하고 대응

4. 美 마이터 ATT&CK Matrix 프레임워크 활용

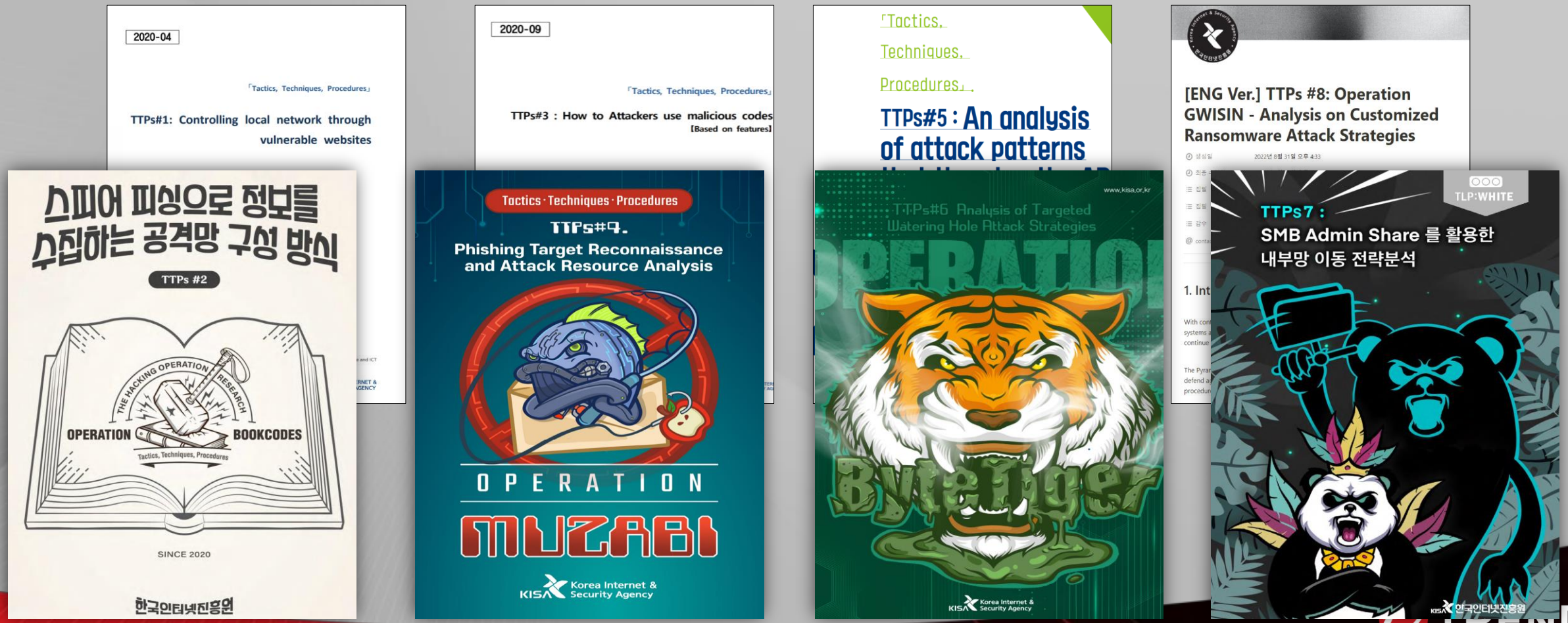
공격 그룹별의 공격 전략, 전술, 절차를 구체화하여 정리 제공

- 14개 이상의 공격 전술과 200개 이상의 실제 공격에 쓰인 공격 기술로 구성



[참고] KISA 최신 APT形 공격그룹 기술 보고서 활용

- 공격의 진행 과정을 전략· 전술 중심으로 분석한 TTP 보고서 배포(8종)

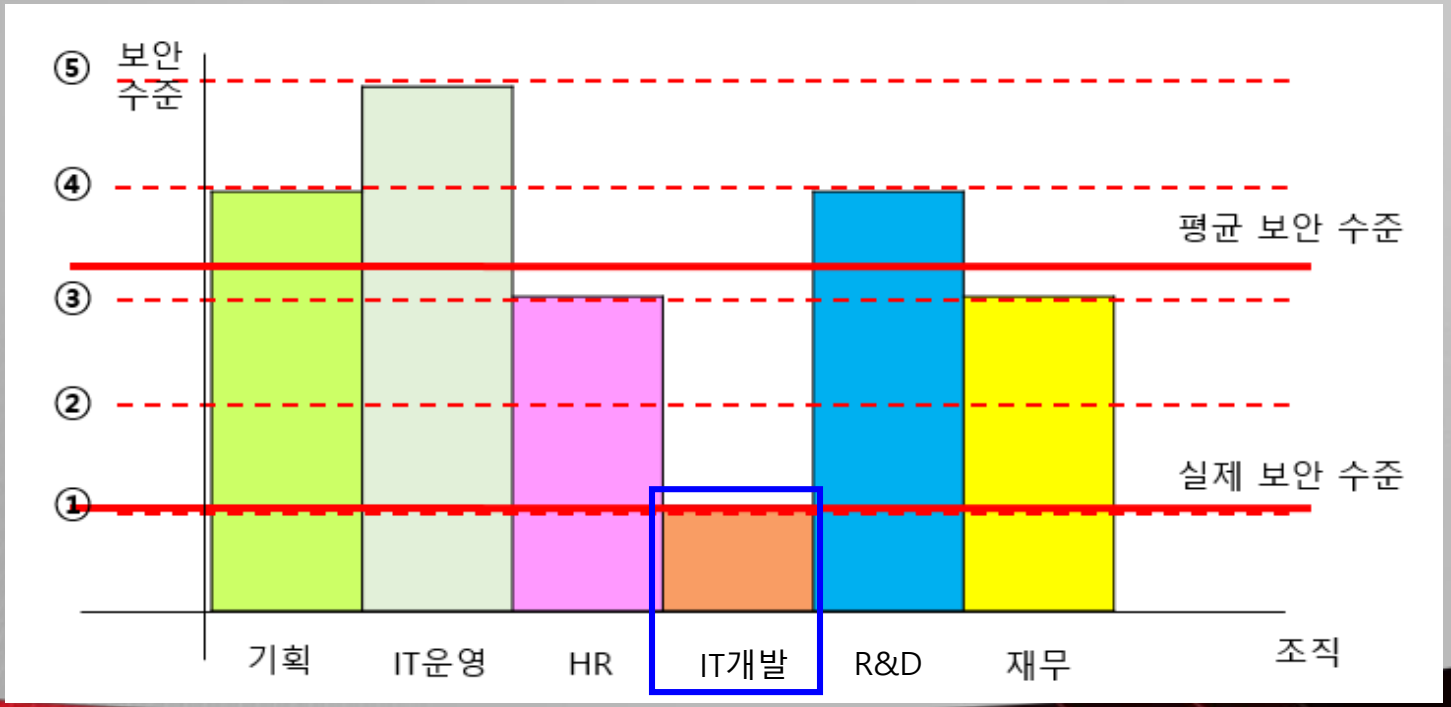


5. 일관된 보안정책

☑ 기업 내 보안강화(불편함)와 이윤을 위한 업무효율(편의성)은 항상 상충

☑ 고위 임직원들이 업무효율을 중시한 보안정책이 선택될 경우,

☞ 이에 대한 최소한의 보완 대책이 반드시 마련되고 지속 관리!!!!



감사합니다.

QnA

침해대응단장 임채태

(cht.im@kisa.or.kr)