AI 및 빅데이터를 이용한 침해대응체계 고도화

한국인터넷진흥원 사이버침해대응본부

임진수 팀장

KISA

Contents

1 사이버 위협 동향

2 주요 침해사고 현황

3 사이버보안빅데이터센터

4 사이버보안빅데이터 활용

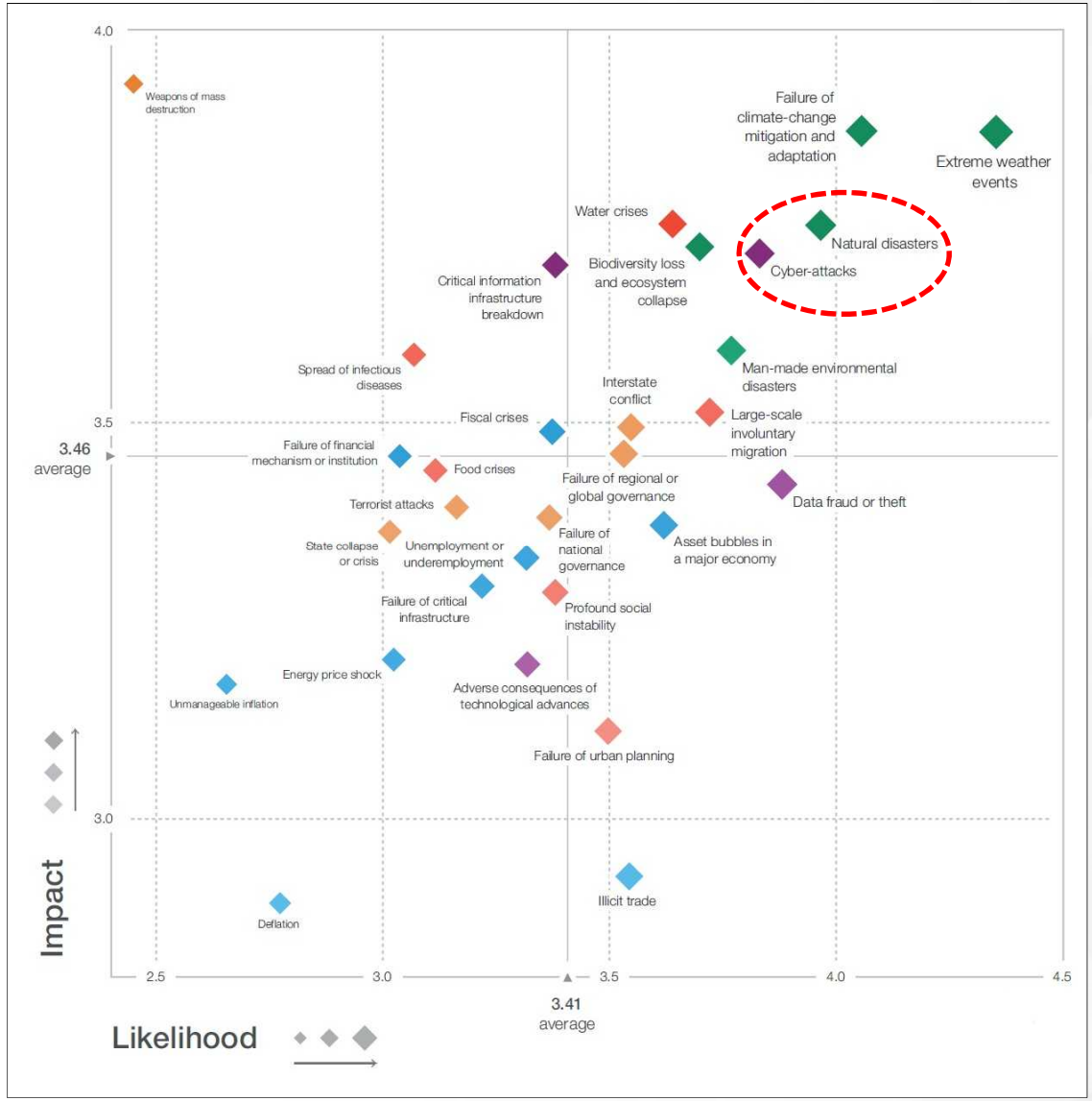
1 사이버 위협 동향

The Global Risks 2019

Top 5 Global Risks in Terms of Likelihood

Extreme weather events	Weapons of mass destruction
Failure of climate-change mitigation and adaptation	Failure of climate-change mitigation and adaptation
Natural disasters	Extreme weather events
Data fraud or theft	Water crises
Cyber-attacks	Natural disasters

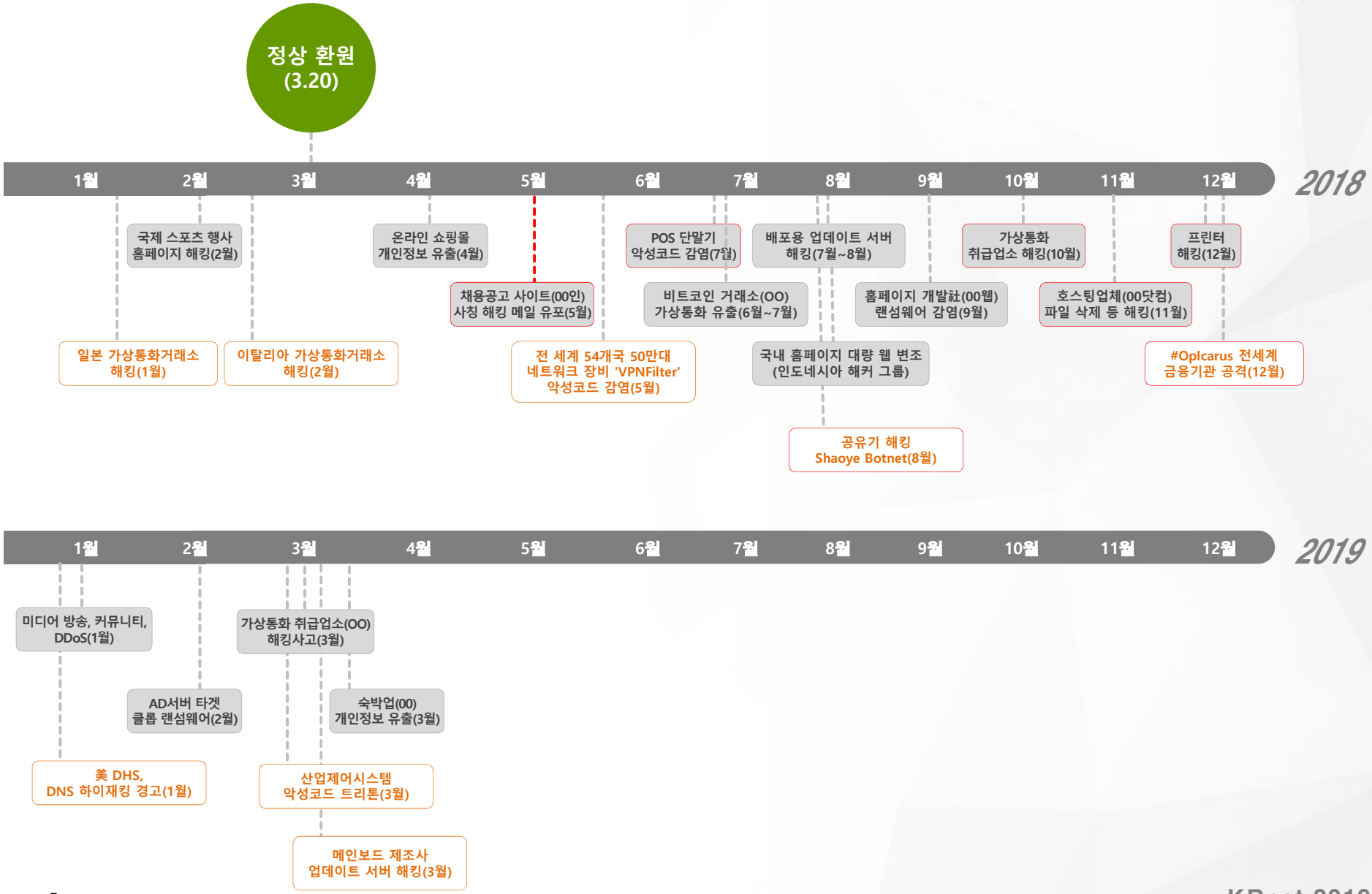
Top 5 Global Risks in Terms of Impact



Economic Environmental Geopolitical Societal Technological

참조 : The Global Risks Report 2019 (WEF)

사이버 위협 현황 (2018~2019년)



19년도 사이버위협 전망

1. 다양한 경로를 통한 크립토재킹 확산 : 안랩

- ▶ 모바일 기기의 보편화로 인한 채굴 악성 앱 유포
- ▶ 취약한 IoT 기기를 대상으로 대량 감염 및 채굴 시도
- ▶ 웹 브라우저에서 동작하는 채굴 스크립트 유포 지속

2. 소셜 네트워크를 이용한 악성코드 유포 : 이스트시큐리티

- ▶ 유명한 소셜 네트워크 해킹을 통한 대규모 악성코드 유포
- ▶ 허위 프로필을 이용한 미인계 SNP(Social Network Phishing)
- ▶ SNS 메신저를 이용한 맞춤형 APT

3. 엔드포인트 보안취약점을 겨냥한 공격 : NSHC

- ▶ 스크립트 악성코드와 윈도우 OS의 시스템 관리 기능을 이용한 공격 심화
- ▶ 공개용 코드와 모의해킹 S/W를 활용한 공격 심화
- ▶ 보안 S/W의 정상기능을 악성코드 감염 및 제어 수단으로 활용한 공격 심화

4. 지능화된 스피어피싱과 APT 공격 : 하우리

- ▶ 인공지능 기술로 강화된 개인 맞춤형 스피어 피싱 메시지 및 공격 등장
- ▶ 가짜뉴스 등 자극적 이슈 소재를 이용한 악성코드 유포 가능성 증대
- ▶ 보안이 취약한 중소기업을 대상으로 한 APT 공격 증대

5. 사물인터넷을 겨냥한 신종 사이버 위협 : 잉카인터넷

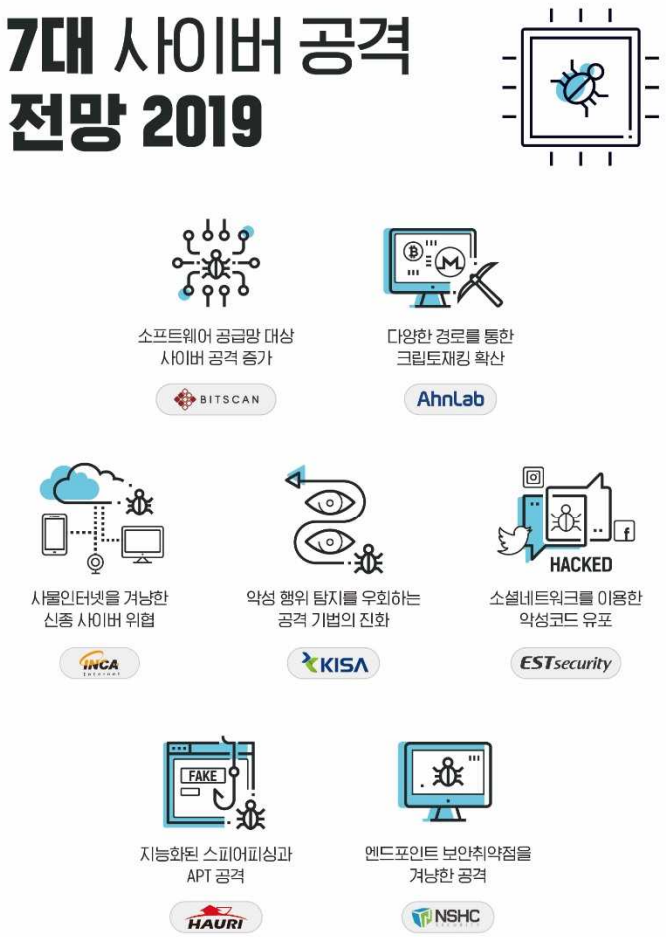
- ▶ IoT 봇넷의 변종 및 다양한 봇넷 출현으로 IoT기기의 좀비기기화 증가
- ▶ IoT 봇넷을 이용한 DDoS 공격으로 블록체인 및 암호화폐 네트워크 공격
- ▶ 좀비화된 IoT기기를 통한 개인정보 탈취 및 악성코드 유포의 숙주로의 악용

6. 소프트웨어 공급망 관련 사이버 공격 증가 : 빛스켄

- ▶ 소프트웨어, 웹사이트 개발업체 대상 공격 증가
- ▶ 소프트웨어 취약점을 악용한 해킹 및 정보유출 증가
- ▶ 소프트웨어 코드서명 인증서를 해킹하는 공격 증가

7. 악성 행위 탐지를 우회하는 공격 기법의 진화 : 한국인터넷진흥원

- ▶ DGA를 이용하여 C&C 차단을 회피하는 악성코드 증가
- ▶ 머신러닝기반 백신 및 탐지 시스템을 우회하는 사이버 위협의 진화
- ▶ 패치관리, 보안관리 등 중앙관리 S/W의 취약점을 악용한 공격 지속



과학기술정보통신부 KISA 한국인터넷진흥원

ICT 환경변화 " 현실-사이버 경계 붕괴 "

KISA

스마트 자동차

자율주행(구글 웨이모)

커넥티드카(현대자동차)

스마트 의료

비접촉 체온계(파트론)

호흡 재활(라이프 시멘틱스)

스마트 홈·가전

아마존, 에코

애플 팟

네이버, 웨이브 / 프랜즈

카카오 미니

산업간 경계의 붕괴 = 사이버영역 확장

스마트 제조

스마트 공장(아디다스)

스마트 물류(아마존)

» 인공지능(AI), 클라우드, 사물인터넷(IoT), 블록체인 등 4차 산업혁명 기술과, 자동차, 의료, 홈· 가전, 제조 등 전통 산업간 융합 가속화

» ICT 기기 보급의 확대로 全 산업· 생활 분야까지 사이버 영역 확장

현실로 파고드는 사이버 위협

전세계 사물인터넷(IoT) 기기 전망

※ 출처 : 가트너, '17

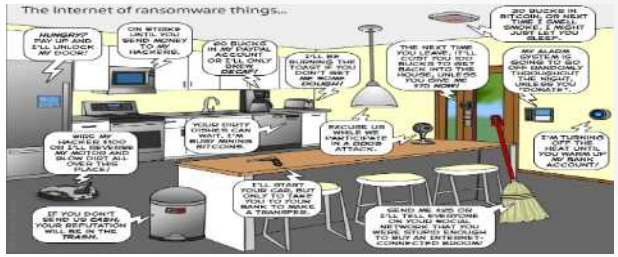
IoT 취약점 대응 건 수 3년간 455% 증가

※ 출처 : KISA

스마트 자동차 보안위협

※ 출처 : "커넥티드 카 해킹 막아라" 글로벌 업체 비상, 동아일보

스마트 홈·가전 보안위협



※ 출처 : The internet of ransomware things, The Joy of Tech comic

» 인공지능 스피커, 지능형 로봇 등 첨단 ICT 기술의 일상생활과 산업에 적용됨에 따라 보호 대상이 정보에서 사물로 빠르게 전환 · 확산

» 정보를 탈취하고 서버를 마비시키는 기존 사이버 침해사고와 달리 국민의 생명과 안전에 직접적인 피해를 야기

기하급수적으로 팽창하는 사이버 위협

현재

안전 위협 사례

- 폭스바겐 차량 수백만대 마스터키 해킹 취약('18.5월)

사생활 위협 사례

- 허술한 IP 카메라 해킹한 일당 적발, 4,648대 IP 카메라 무단접속('18.11월)

미래

» **커넥티드카, 2022년까지 약 1억 7,500만대 이상 보급 전망 (카운터포인트, '18.7월)**

» **국내 공공 CCTV 보급 대수는 '17년 기준 약 96만대이며, 매년 10%씩 성장한다고 가정하면 '22년에는 약154만대로 증가**

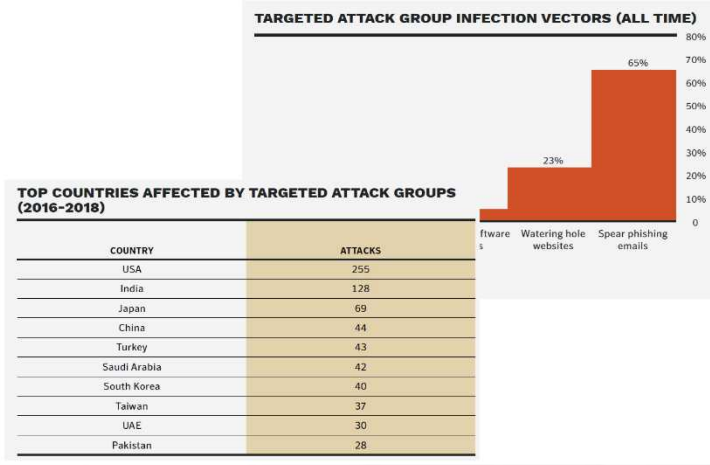
» 5년 내에 보안에 취약한 융합제품(커넥티드카, IP카메라 등)이 기하급수적으로 증가할 것으로 예측되고 있어 **융합보안에 대한 선제적 대응 필요**

2 주요 침해사고 현황

해킹메일

이메일을 악용한 사이버 공격 사례 증가

날짜	스피어피싱 사고사례 언론보도
→ 1.4	'2019 북한 신년사 평가' 한글 문서를 이용하여 통일부 사칭
→ 1.7	통일부 기자단을 타깃으로 한 APT 공격
→ 1.20	알약 보안 모듈로 위장한 공격
→ 1.23	설 선물 내용으로 위장한 엑셀 파일을 사용한 공격
→ 2.6	직장인 연말정산 주제로 개인 맞춤형 스피어피싱 메일 기승
→ 2.8	설 연휴 탈북민 대상 네이버 계정 탈취 시도
→ 2.9	'비건 방한 분석' 문서 위장 사이버 공격
→ 2.12	구글 번역 홈페이지로 위장한 피싱 공격(2차 스피어피싱 공격 시도)
→ 2.21	2차 북미정상회담 좌담회 개최 가짜 한글문서를 사용한 APT 공격
→ 2.27	포스텍(포항공대) 교수 계정정보 탈취 후 이를 사칭한 스피어피싱 메일 배포
→ 2.28	2차 북미정상회담 이슈를 활용한 APT 공격
→ 3.21	"기업 60%가 APT 공격에 당했다" (아이뉴스)

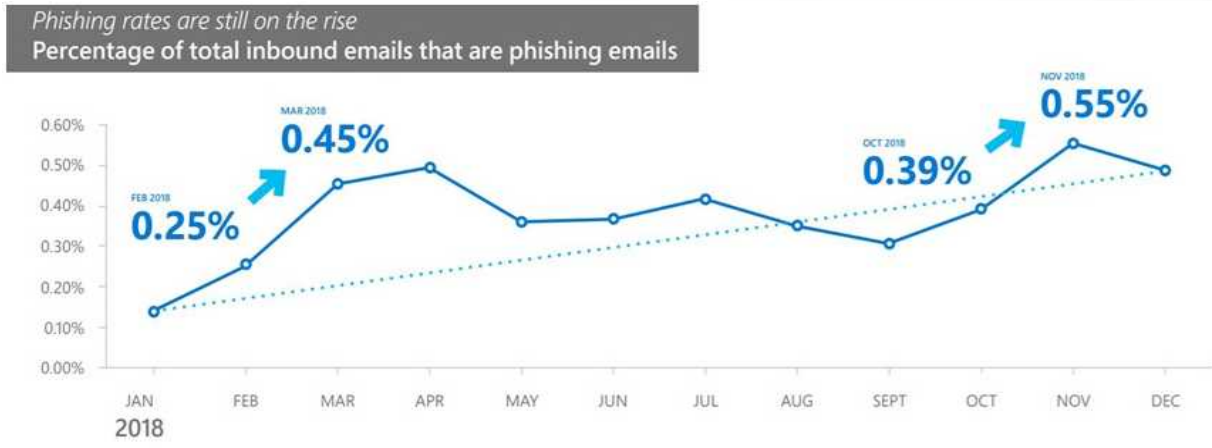


TOP COUNTRIES AFFECTED BY TARGETED ATTACK GROUPS (2016-2018)

COUNTRY	ATTACKS
USA	255
India	128
Japan	69
China	44
Turkey	43
Saudi Arabia	42
South Korea	40
Taiwan	37
UAE	30
Pakistan	28

(출처 : 시만텍 2019년 2월 발표)

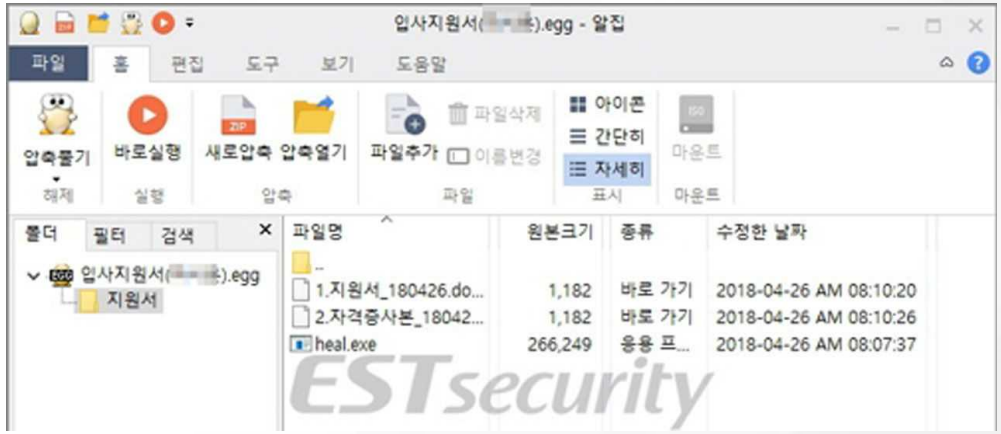
- 지난 3년 국내 APT 공격 40회(7위) 발생, APT 공격중 해킹메일이 65% 차지



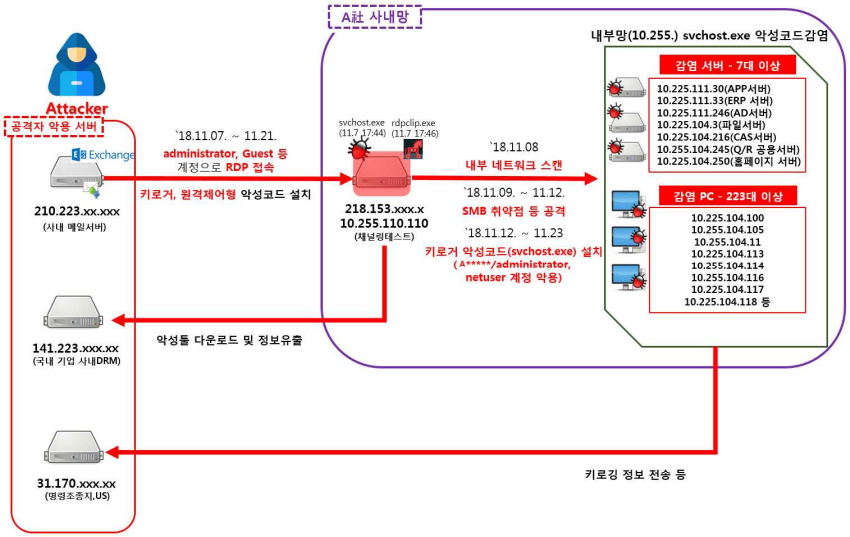
(출처 : MS Security Intelligence Report Vo.24)

사회공학적 기법을 이용한 랜섬웨어 기승

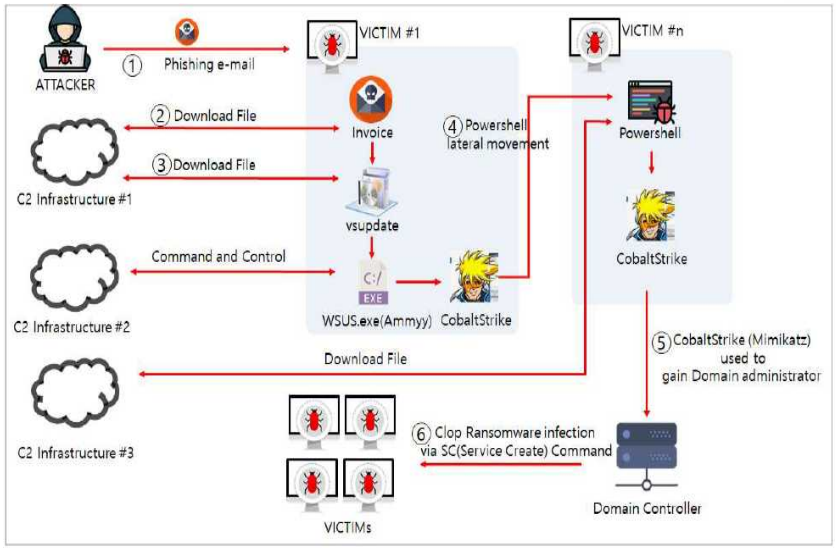
국내 맞춤형 갠드크랩 랜섬웨어 기승



AD 악용 랜섬웨어 유포



A사(제조업) Attack Life Cycle ('18.11월)



전술	Clop & CobaltStrike
초기침투	악성파일이 첨부된 피싱 이메일
실행	파워셸 실행
	서비스 실행
	취약점을 이용한 임의의 코드 실행
권한 상승	취약점을 이용한 권한 상승
	UAC(User Account Control) 우회
	Access Token 조작
탐지회피	코드 서명
	파일 또는 정보 난독화
자격증명 액세스	자격증명 덤프
탐색	계정 탐색
	공유 네트워크 검색
내부 확산	Windows 관리자 공유
	원격 파일 복사
명령 및 제어	일반적으로 사용되는 포트 이용
	데이터 인코딩
	원격 파일 복사
	다중 대역 통신
지속	서비스 생성
	작업스케줄러 예약

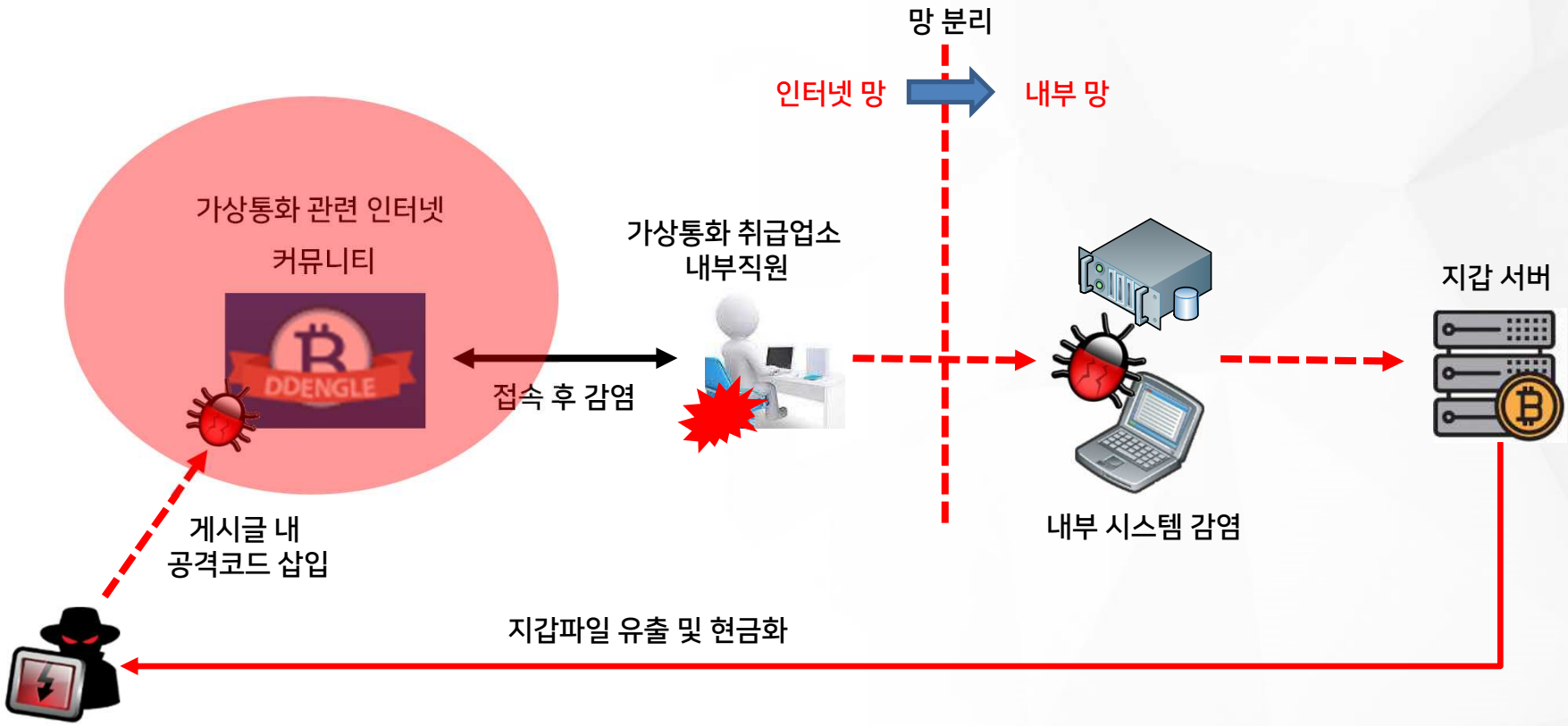
MITRE ATT&CK

가상통화 취급업소 해킹

사고가 끊이지 않는 가상통화 취급업소

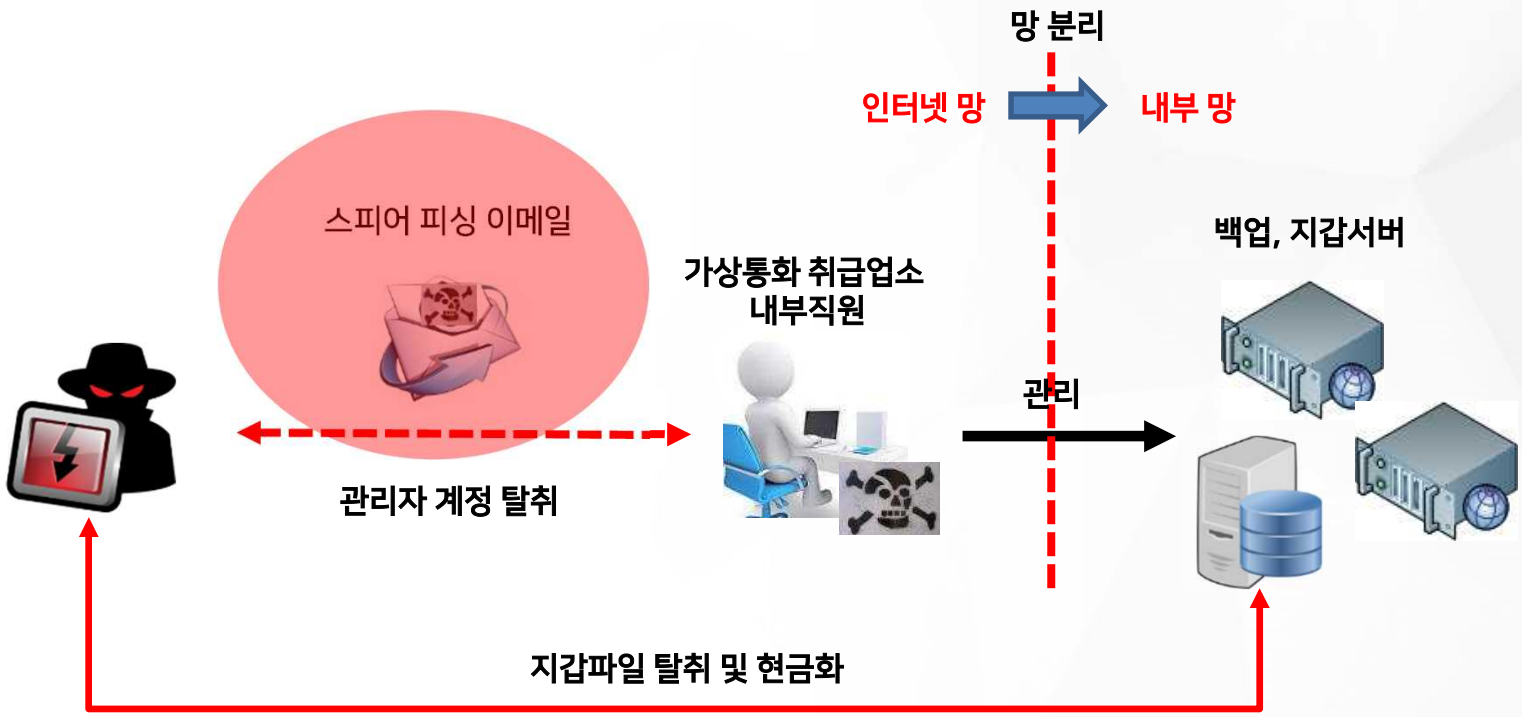
가상통화 취급업소 사고 원인(1/2)

워터링홀을 이용한 가상통화 취급업소 침투



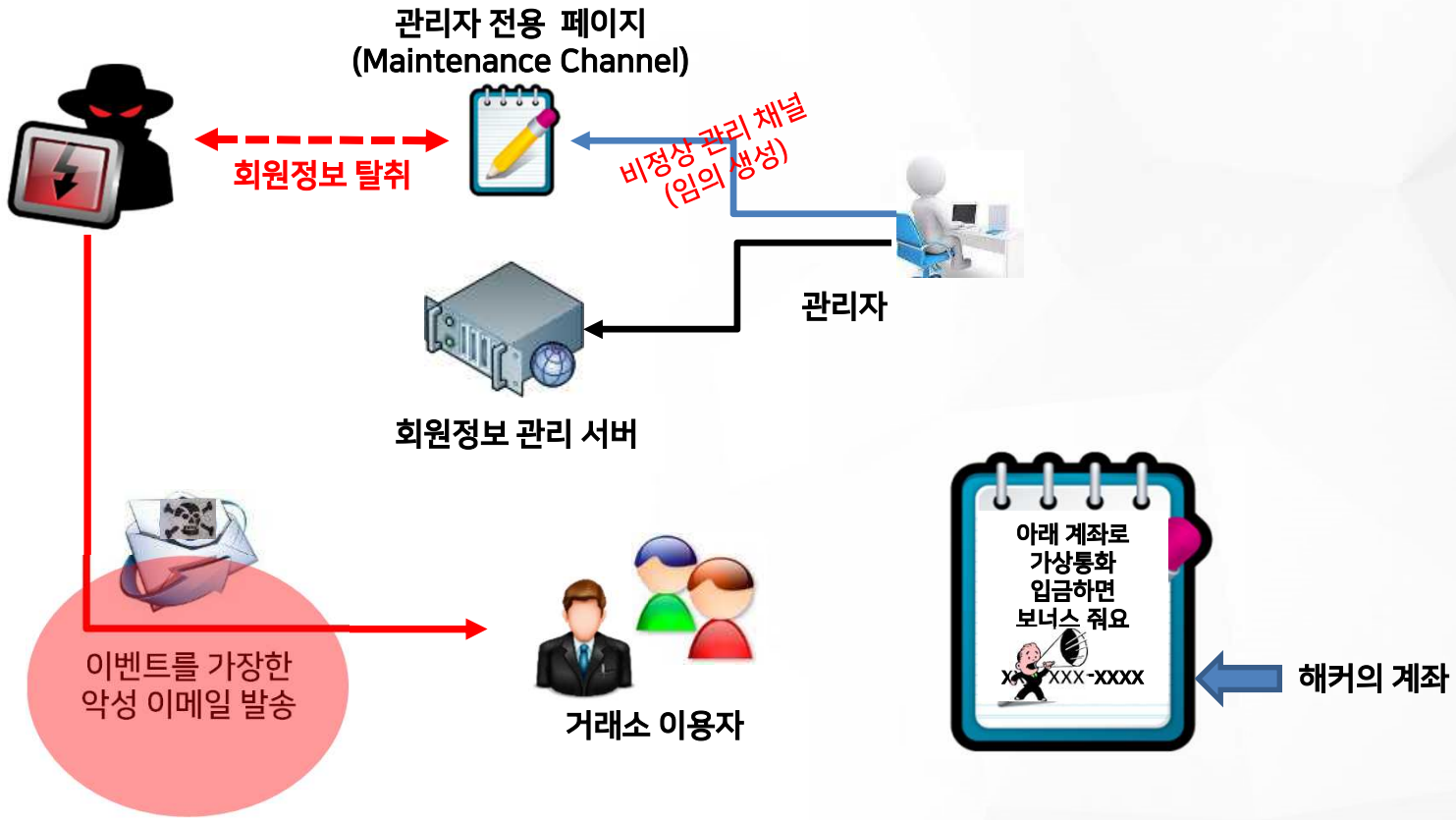
가상통화 취급업소 사고 원인(2/2)

스피어피싱을 이용한 가상통화 취급업소 침투



개인정보 유출에 의한 2차 피해 발생

가상통화 취급업소 개인정보 탈취 및 악용



공급망 공격 (Supply Chain Attack)

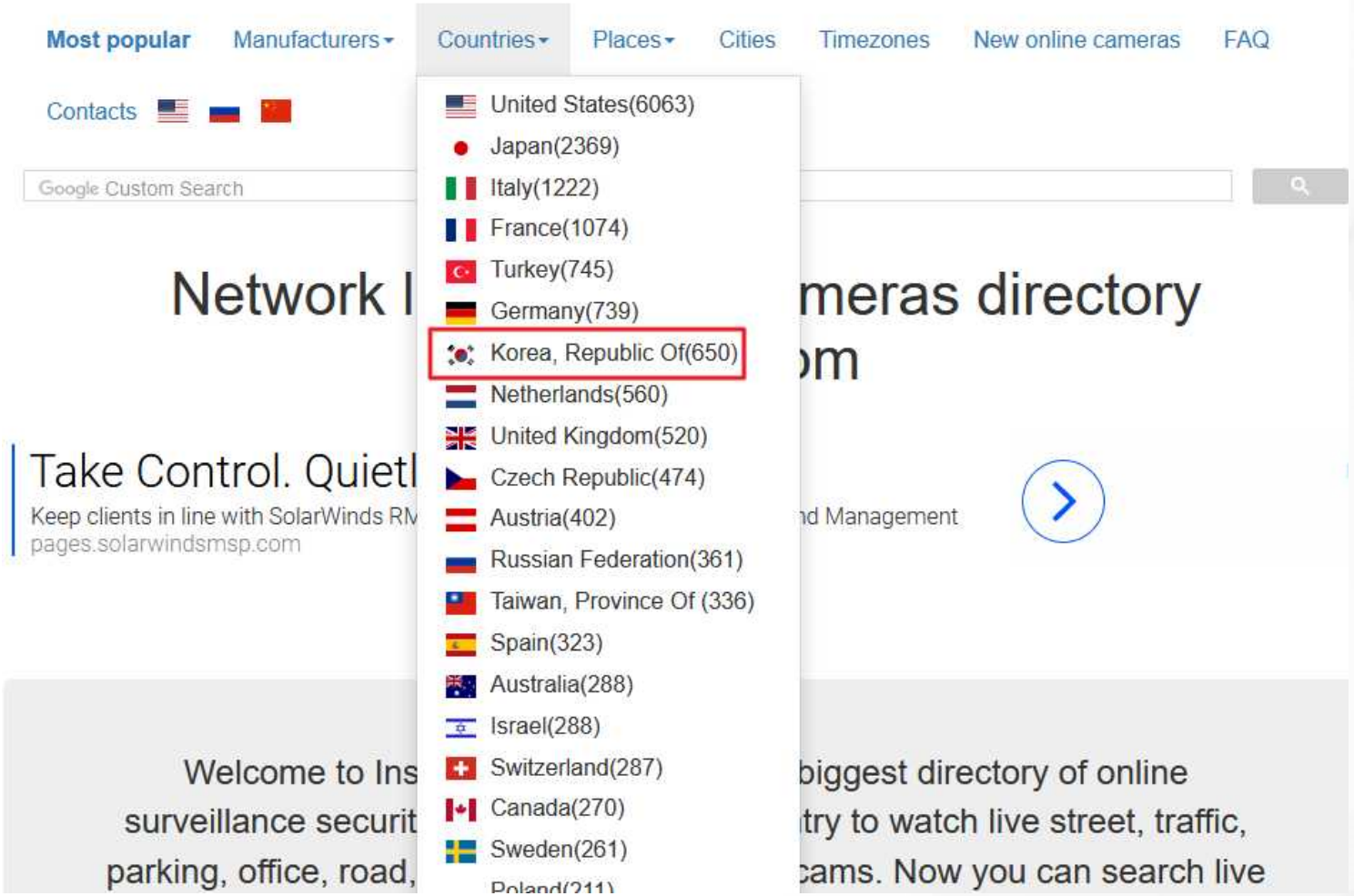
1) 제품 업데이트 서버 설정 파일 변조

2) 제품 배포 서버 관리 페이지 취약점을 통한 배포 서버 장악

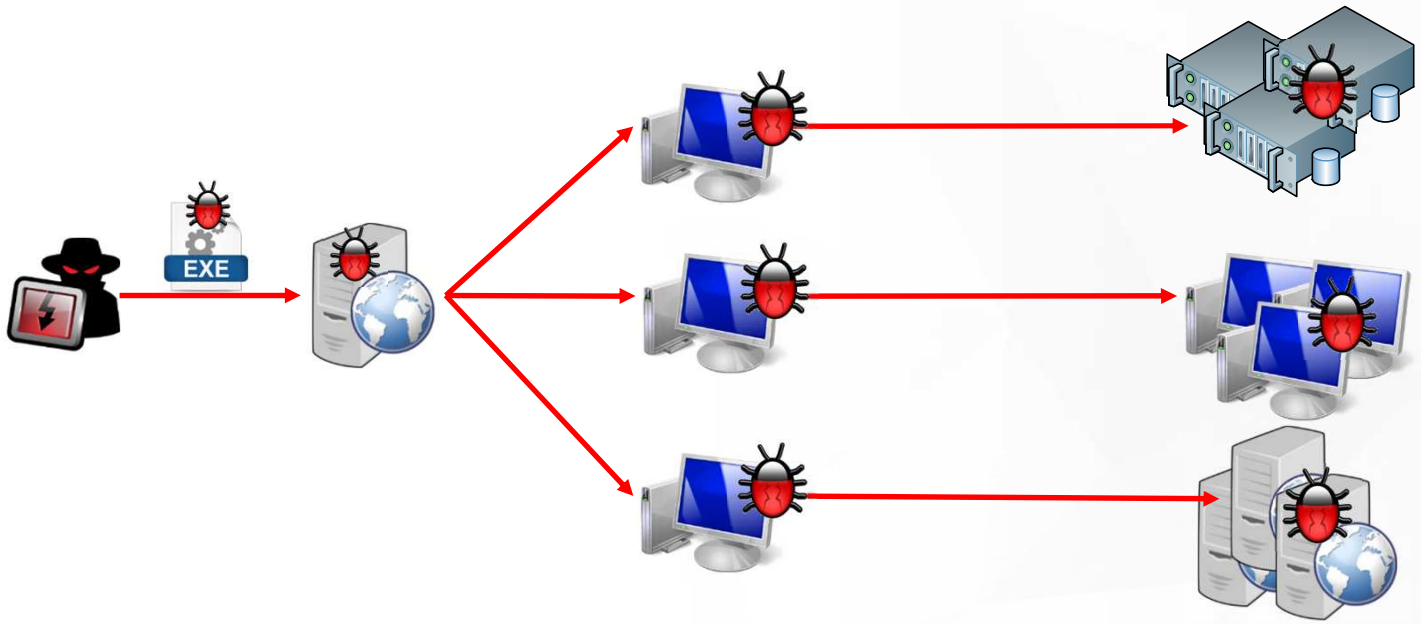
3) 영업 지원 웹 취약점을 통한 내부망 침투

IoT 위협 (취약한 IoT 기기 공격 노출)

전 세계에 실시간 중계되는 IP 카메라



RDP 원격코드 실행 취약점(CVE-2019-0708)



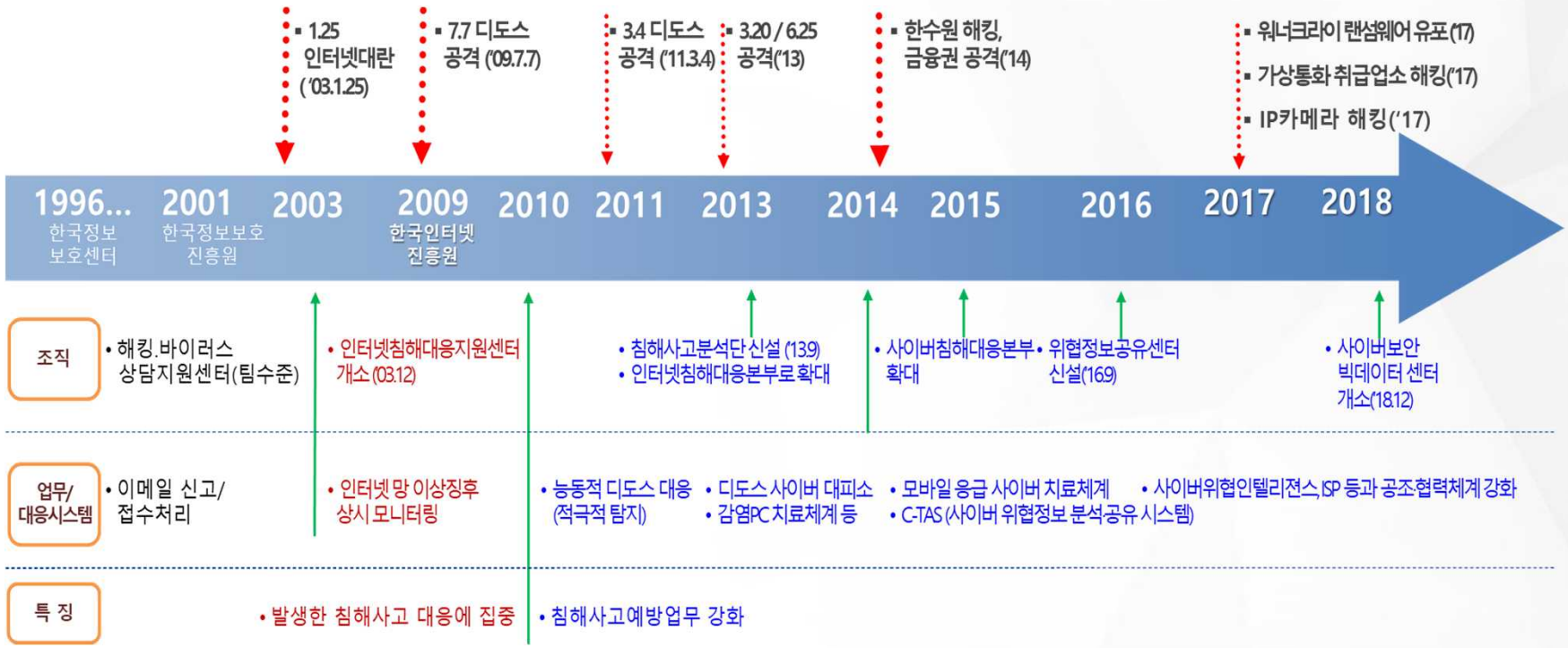
원격에서 공격자가 공격대상 윈도우 시스템(RDP를 사용)에 조작된 RDP 패킷을 전송하여 악성코드 설치 및 실행 가능

서비스거부공격 및 랜섬웨어 감염에 악용될 수 있음

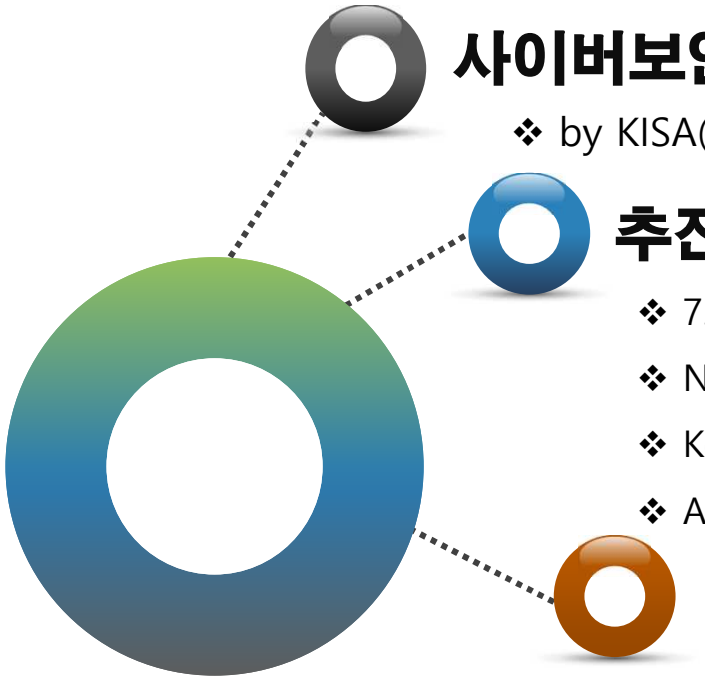
Windows XP, 7, Windows Server 2003, 2008에 취약점에 영향을 받음

3 사이버보안빅데이터센터

KISA 사이버침해대응체계 연혁



KISA 사이버보안 빅데이터센터



사이버보안 빅데이터 센터

❖ by KISA(Korea Internet & Security Agency), December 2018

추진배경

❖ 7.7 DDoS Attack (2009) & 3.4 DDoS Attack (2011)

❖ NH APT Attack (2011) & 3.20 APT Attack (2013, DarkSeoul)

❖ Korea Hydro & Nuclear Power Hacking (2014)

❖ AlaphaGo seals 4-1 victory over Go grandmaster Lee Sedol (2016)

추진경과

❖ 12.05 ~ 12.11 : MMS 1.0 & MML 1.0

❖ 13.08 ~ 13.12 : MMS 1.1 & MML 1.1

❖ 13.09 ~ 14.07 : C-TAS 1.0 & C-TAS 1.0 (14.08 ~)

❖ 15.05 ~ 15.12 : C-TAS 1.1 & C-TEX 1.1 (MMS -> TIMS)

❖ 16.05 ~ 16.12 : C-TAS 1.2 & C-TEX 1.2 (with STIX 1.2)

❖ 17.05 ~ 17.12 : C-TAS 2.0 & C-TEX 2.0 (with STIX 2.0)

❖ 18.06 ~ 18.12 : BACS 1.0 & Multiple File Formats (C-TEX, STIX, Custom JSON)

❖ MMS : Malware Management System

❖ MML : Malware Markup Language

❖ C-TAS : Cyber Threat Analysis & Sharing system

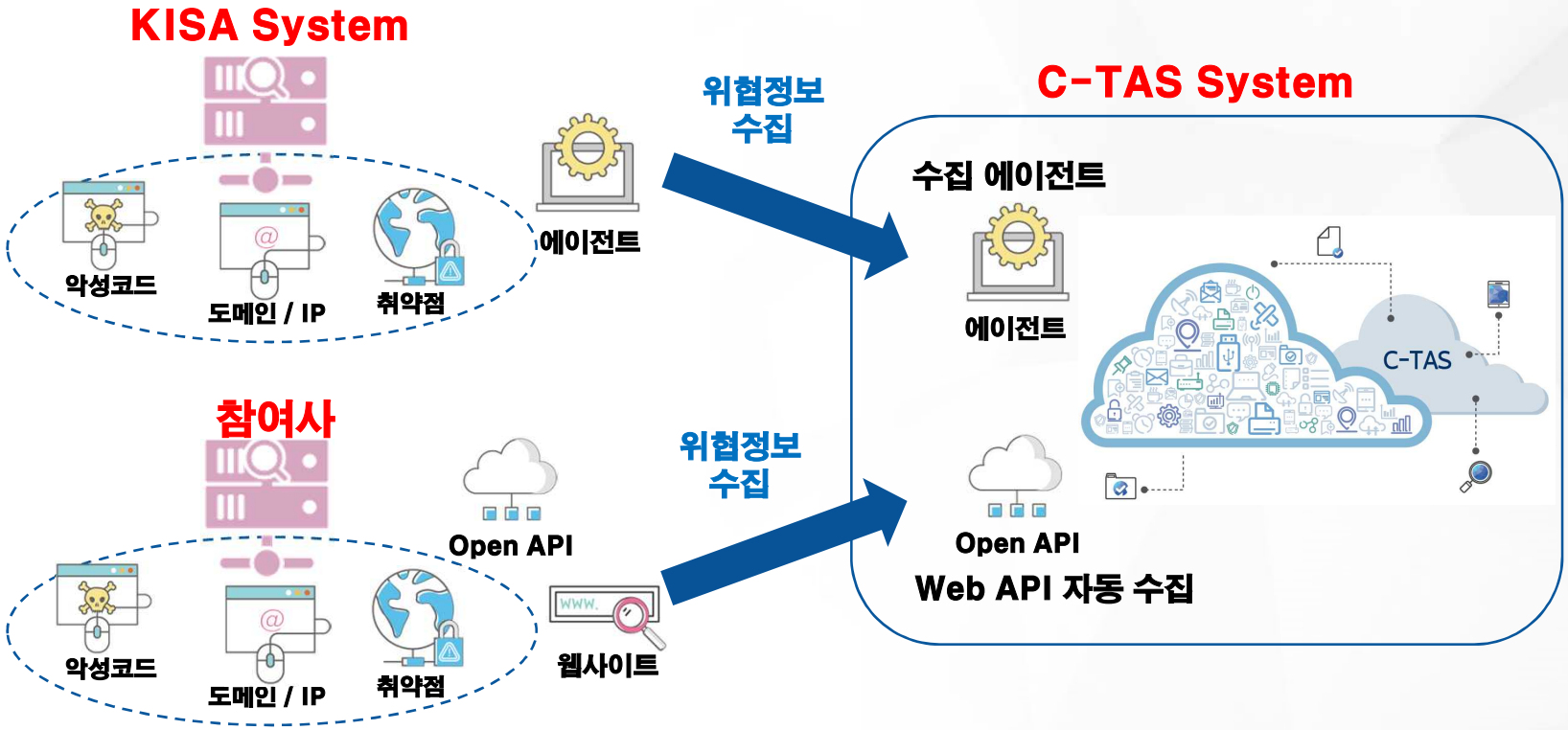
❖ C-TEX : Cyber Threat Expression

❖ TIMS : Threat Intelligence Management System

❖ BACS : Bigdata Analytics system for Cyber Security

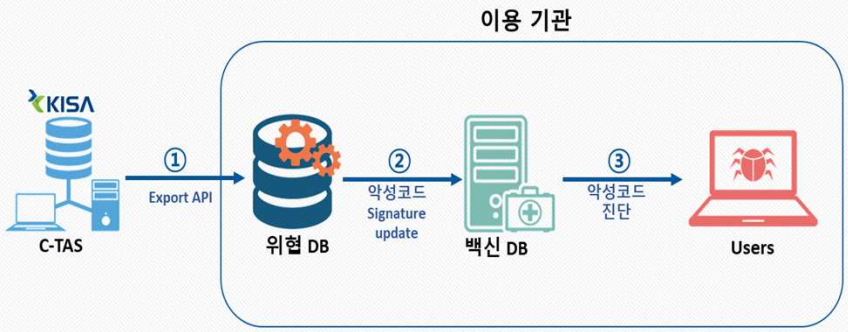
C-TAS 개요

- 수집정보 : 악성코드, C&C, 유포지, 침해사고 정보 등
- 수집방법 : 수집 에이전트, 웹사이트, 웹API 등을 통해 수집



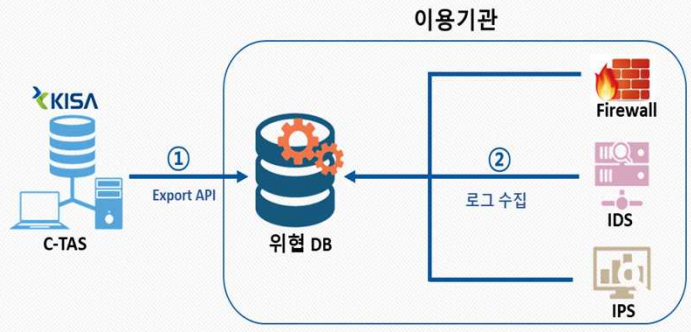
C-TAS 활용 사례

보안서비스 | C-TAS to Anti-Virus



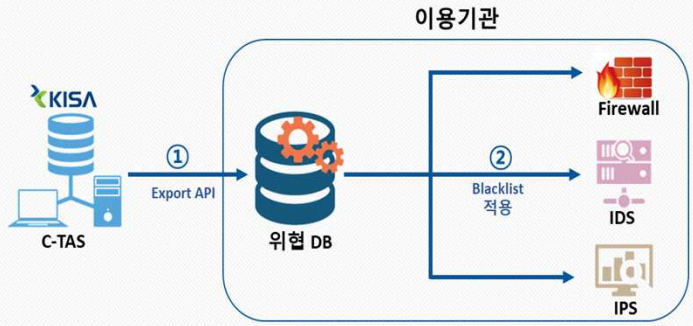
- C-TAS에서 전송되는 위협정보를 사내 위협DB로 저장(악성코드 정보)
- 악성코드 Signature를 백신 DB에 업데이트
- 업데이트된 악성코드 정보를 활용하여 악성코드 탐지 룰 강화

All | C-TAS to Security Solution



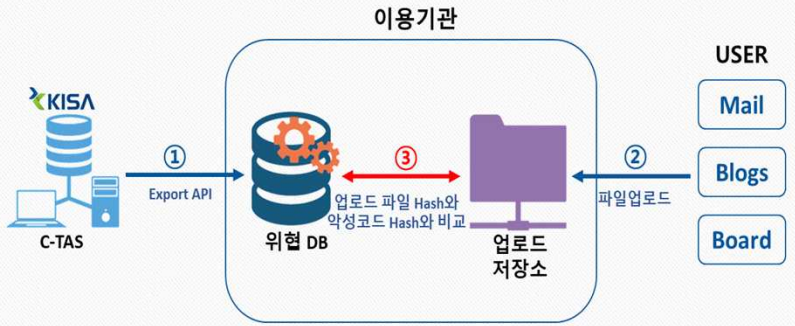
- C-TAS에서 전송되는 위협정보를 사내 위협DB로 저장(악성URL)
- 보안장비의 로그 수집
- 위협DB와 로그를 비교하여 위협정보 탐지

All | C-TAS to Security Solution



- C-TAS에서 전송되는 위협정보를 사내 위협DB로 저장(악성URL)
- 보안장비의 Blacklist로 적용

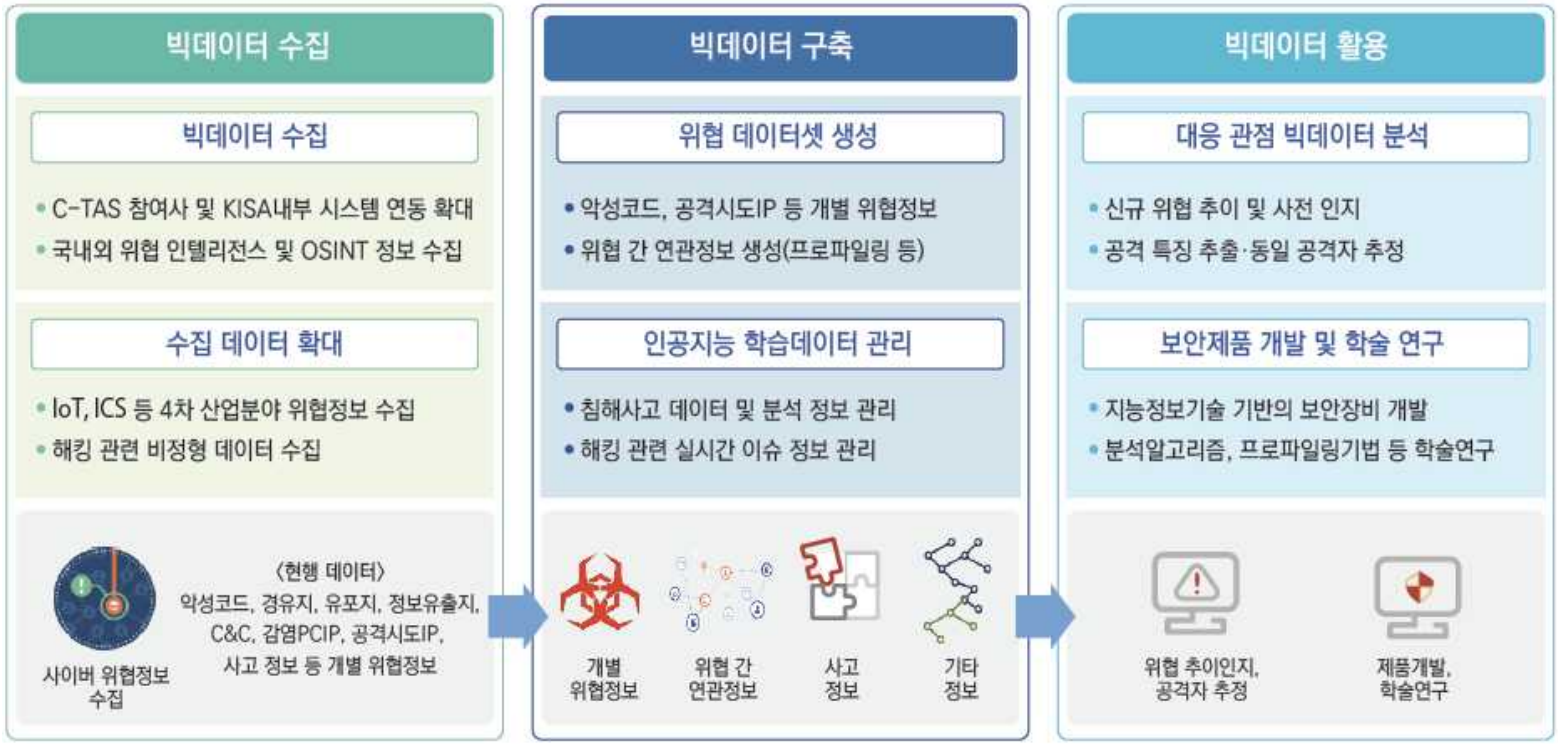
웹서비스 | C-TAS to Online Board



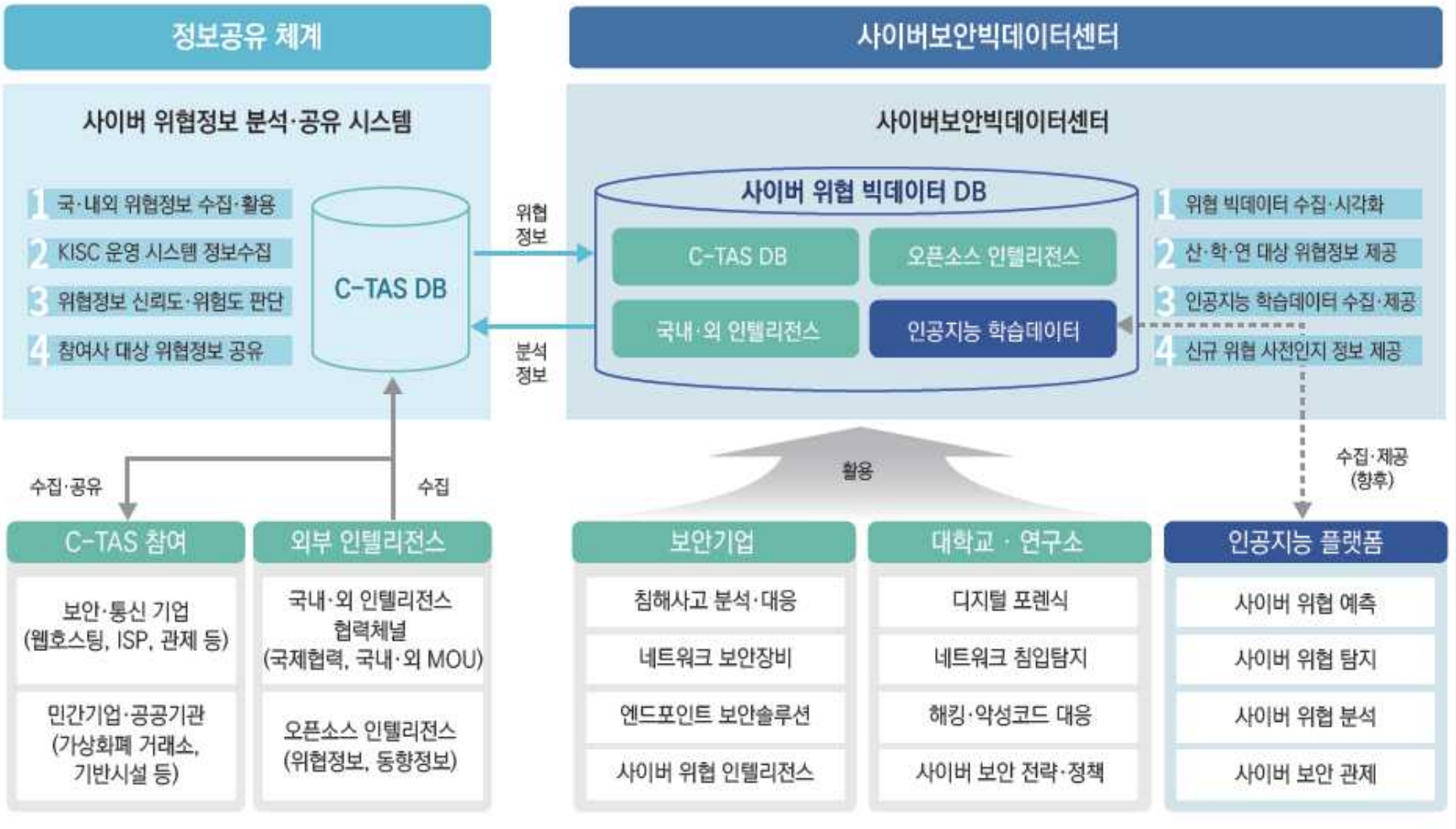
- C-TAS에서 전송되는 위협정보를 사내 위협DB로 저장(악성코드)
- 웹서비스 사용자가 게시판, 메일 등에 파일 업로드
- 악성코드 Hash값과 업로드된 파일 Hash값 비교하여 악성코드 차단

빅데이터센터 소개

- (KISA) 빅데이터분석을 통해 침해사고 대응역량 강화
- (산·학·연) 위협 빅데이터와 분석 플랫폼을 제공하여 제품개발 및 연구 지원



빅데이터센터 소개


정보공유 체계
사이버보안빅데이터센터
사이버 위협정보 분석·공유 시스템
1 국·내외 위협정보 수집·활용
2 KISC 운영 시스템 정보수집
3 위협정보 신뢰도·위험도 판단
4 참여사 대상 위협정보 공유
C-TAS DB
위협 정보
분석 정보
사이버보안빅데이터센터
사이버 위협 빅데이터 DB
C-TAS DB
오픈소스 인텔리전스
국내·외 인텔리전스
인공지능 학습데이터
1 위협 빅데이터 수집·시각화
2 산·학·연 대상 위협정보 제공
3 인공지능 학습데이터 수집·제공
4 신규 위협 사전인지 정보 제공
수집·공유
수집
활용
수집·제공 (향후)
C-TAS 참여
외부 인텔리전스
보안기업
대학교 · 연구소
인공지능 플랫폼
보안·통신 기업 (웹호스팅, ISP, 관제 등)
민간기업·공공기관 (가상화폐 거래소, 기반시설 등)
국내·외 인텔리전스 협력체널 (국제협력, 국내·외 MOU)
오픈소스 인텔리전스 (위협정보, 동향정보)
침해사고 분석·대응
네트워크 보안장비
엔드포인트 보안솔루션
사이버 위협 인텔리전스
디지털 포렌식
네트워크 침입탐지
해킹·악성코드 대응
사이버 보안 전략·정책
사이버 위협 예측
사이버 위협 탐지
사이버 위협 분석
사이버 보안 관제

빅데이터센터 운영

사용자

- 빅데이터를 이용/활용/개발 하고자 하는 모든 개인/법인/단체

이용자격

- 연구 및 분석 목적을 명확하게 작성하고 승인을 득함
- 센터 운영규정 준수 및 분석결과의 공익 목적 활용 동의

활용 절차

- 방문 신청(이메일)
- 승인 확인(이메일)
- 방문 및 이용
- 퇴소

데이터 이용

- 제공되는 모든 데이터 이용 가능
- 원본 데이터가 아닌 분석 결과 및 보고서 반출 가능

분석 환경

- 폐쇄망 PC 및 분석 서버(VM) 제공

이용수칙

- 일정 기간 동안 분석 환경 유지

빅데이터 분석 • 활용

(대응) 민간의 침해사고 대응능력 강화에 활용

- 홈페이지를 연관분석하여 가장 많이 악용되고 있는 홈페이지 및 이용되고 있는 취약점 파악 가능
  - 해당 홈페이지와 취약점을 우선적으로 대응(집중 모니터링, 대응방법 안내 등)

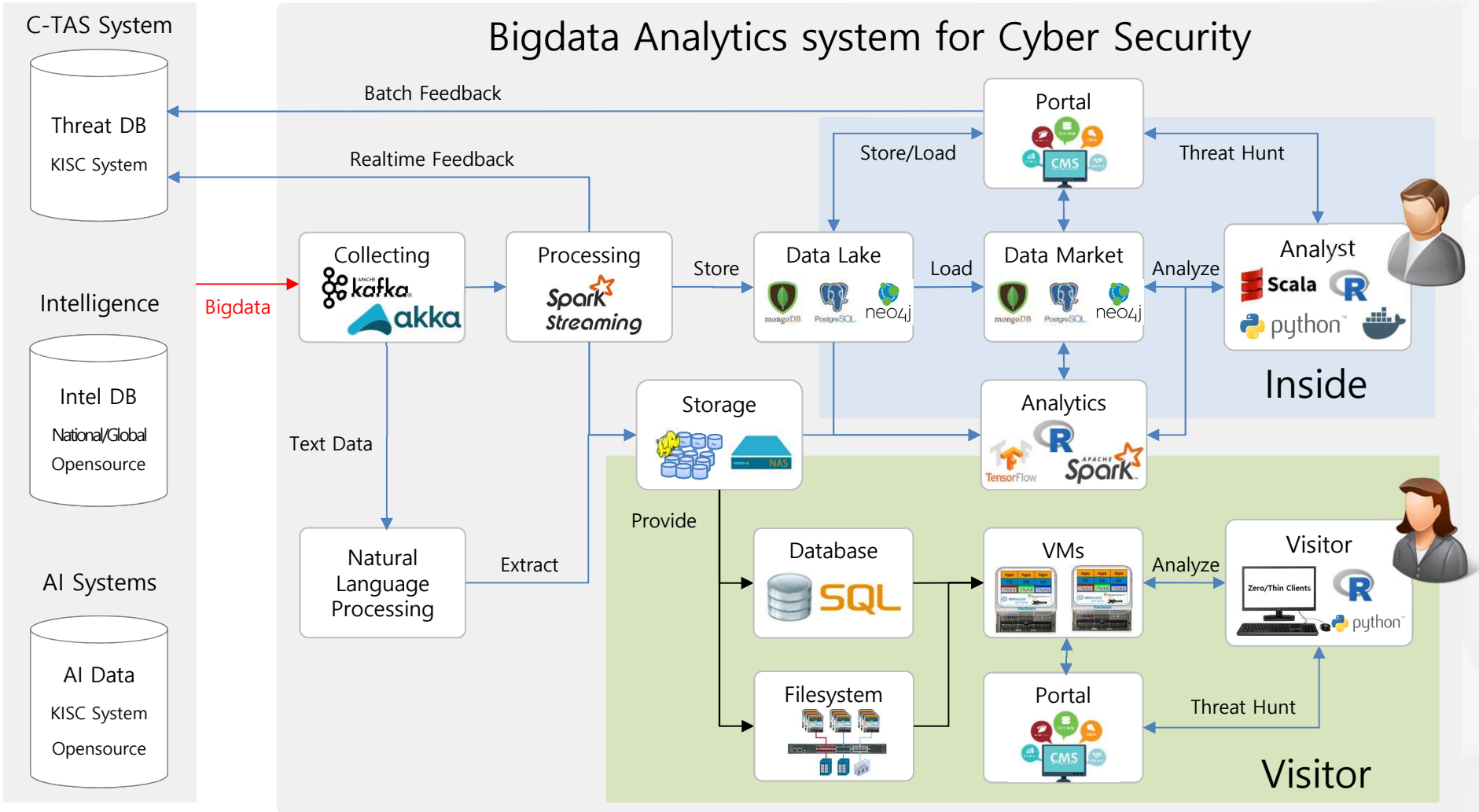
(연구) 대학 등 학계 연관분석 연구 데이터로 활용

- 새로운 공격 발생 시 과거 사고와의 연관성을 분석
  - 해당 공격 그룹이 목표로 하는 주요 대상 및 취약점, 공격 방법에 대한 추정이 가능

(산업) 악성 행위 탐지율을 높일 수 있는 알고리즘 개발에 활용

- 악성코드가 자동으로 생성하는 서버 이름을 판별해주는 인공지능 알고리즘 개발

빅데이터 아키텍쳐

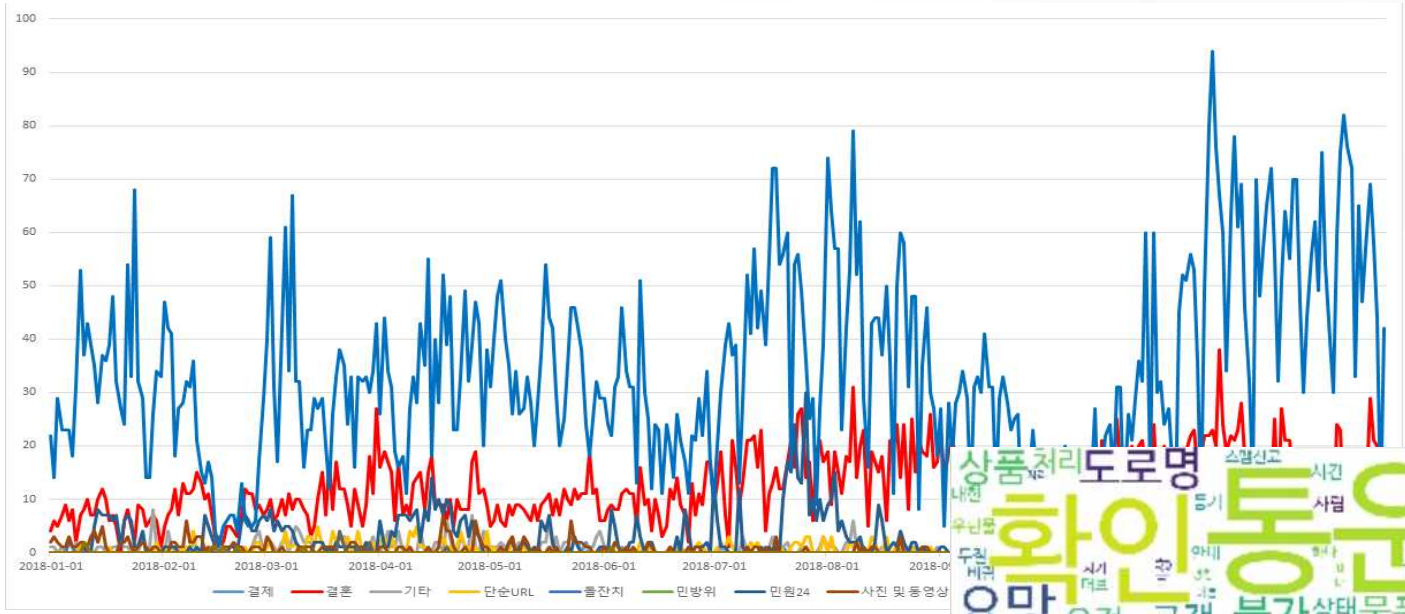

C-TAS System
Threat DB
KISC System
Intelligence
Intel DB
National/Global
Opensource
AI Systems
AI Data
KISC System
Opensource
Bigdata Analytics system for Cyber Security
Batch Feedback
Realtime Feedback
Bigdata
Collecting
kafka
akka
Processing
Spark Streaming
Store
Data Lake
mongoDB
PostgreSQL
neo4j
Load
Data Market
Portal
CMS
Store/Load
Threat Hunt
Analyze
Analyst
Scala
python
Inside
Storage
NAS
Analytics
TensorFlow
Spark
Text Data
Natural Language Processing
Extract
Provide
Database
SQL
Filesystem
VMs
Analyze
Visitor
Zero/Thin Clients
python
Portal
CMS
Threat Hunt
Visitor

4 사이버보안빅데이터 활용

빅데이터 분석 사례(시각화 분석 #1)

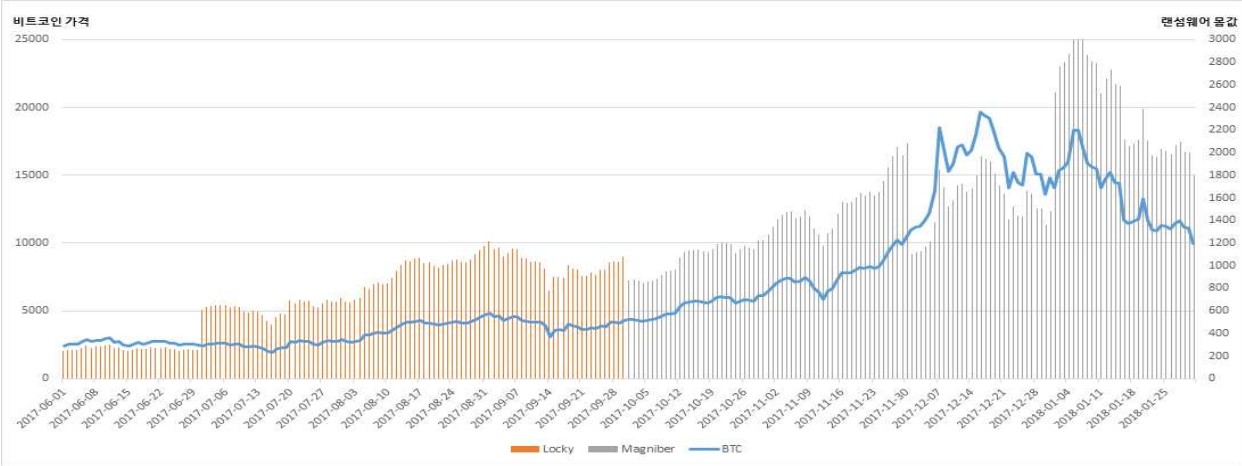
스미싱 키워드 별 추이 비교 결과

- 대체적으로 결혼 및 택배 키워드가 많이 사용
- 택배 키워드는 명절, 연말에 가장 많이 사용

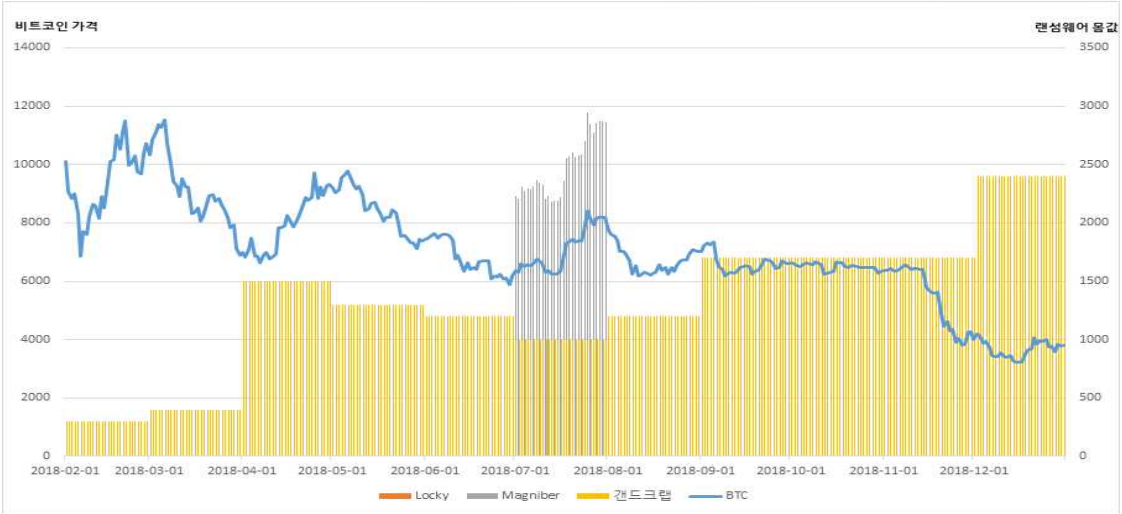


빅데이터 분석 사례(시각화 분석 #2)

비트코인 시세와 랜섬웨어 요구금액과의 상관관계 시각화 분석



<비트코인 시세와 랜섬웨어 요구 금액(2017.6월~2018.1월)>

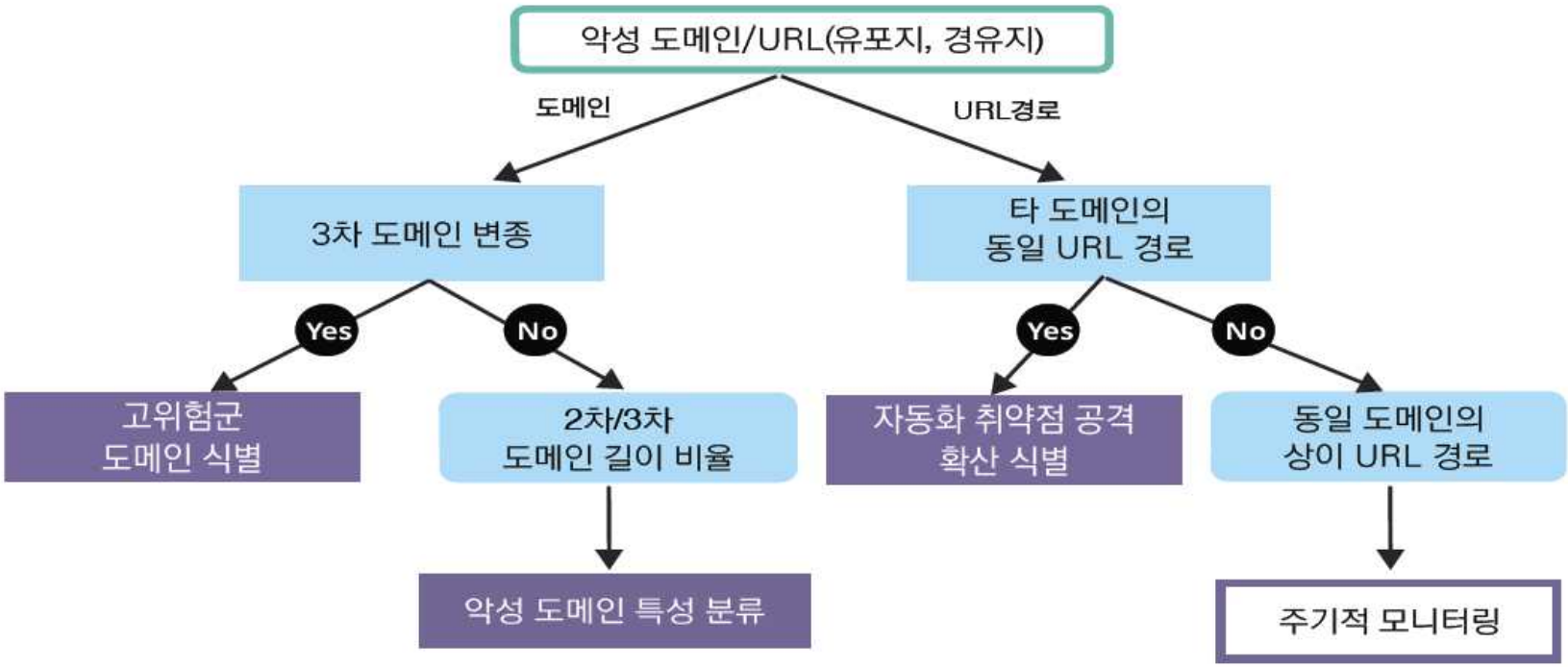


<비트코인 시세와 랜섬웨어 요구 금액(2018.2월~2018.12월)>

랜섬웨어 종류	요구 비트코인(단위 BTC)
Locky	0.25~0.5(110~220만원)
Magniber	0.2 (200만원)
GANDCRAB	$600~$1500

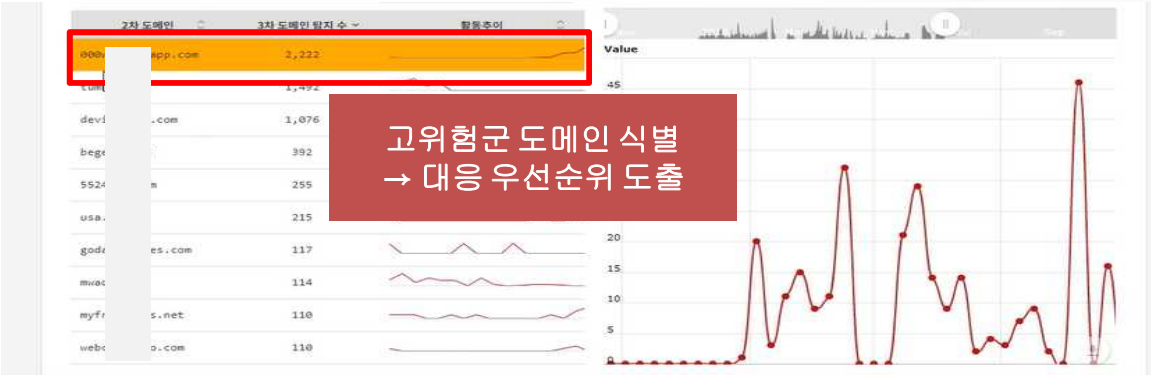
빅데이터 분석 사례(대응체계 고도화 #1)

- 악성 도메인·URL 연관분석을 통해 **집중 모니터링 대상(고위험군) 판별 및 우선순위 대응**



빅데이터 분석 사례(대응체계 고도화 #1)

- 악성 도메인 변종 분석
- 2차 도메인 별 3차 도메인 탐지 수로 **악성도메인(경유지, 유포지 등)의 공격 규모 판단**



- 악성도메인의 2차, 3차 도메인 문자 길이 비율을 통해 **악성도메인 판단**

빅데이터 분석 사례(대응체계 고도화 #1)

- URL 경로와 악성도메인 분석
- 동일한 URL경로를 기준으로 상이한 도메인 수를 집계하여 취약점의 유사성 분석

#	URL Path	도메인 수
1	/recovery-answer.html	255
5	/update.php/	92
6	/recovery-chekpoint-login.html/	73
7	/payment-update-01.html	61
8	/~mustashfa/ids/	54
9	/recovery-answer.html/	52
10	/Payment-update-0.html/	41

자동화 취약점 공격 확산 식별
→ 대규모 취약점 공격 보안공지

#	/recovery-answer.html's Host Name	등록일자
1	aryi tapp.com	2018-05-27
2	bonar tapp.com	2018-05-26
3	recovery-a ebhostapp.com	2018-04-11
4	security-no webhostapp.com	2018-04-10
5	abe pp.com	2018-04-10
6	security-accou 00@webhostapp.com	2018-04-09
7	notificat: bhostapp.com	2018-04-08
8	recov stapp.com	2018-04-08
9	signr tapp.com	2018-04-08
10	secu tapp.com	2018-04-08

- 도메인을 기준으로 상이한 URL경로를 분석하여 고위험에 노출되어 있는 도메인 도출

#	URL Host	Count
1	[redacted]	128
2	[redacted]	126
3	[redacted]	116
4	[redacted]	101
5	[redacted]	77
6	[redacted]	75
7	chach [redacted] app.com	73

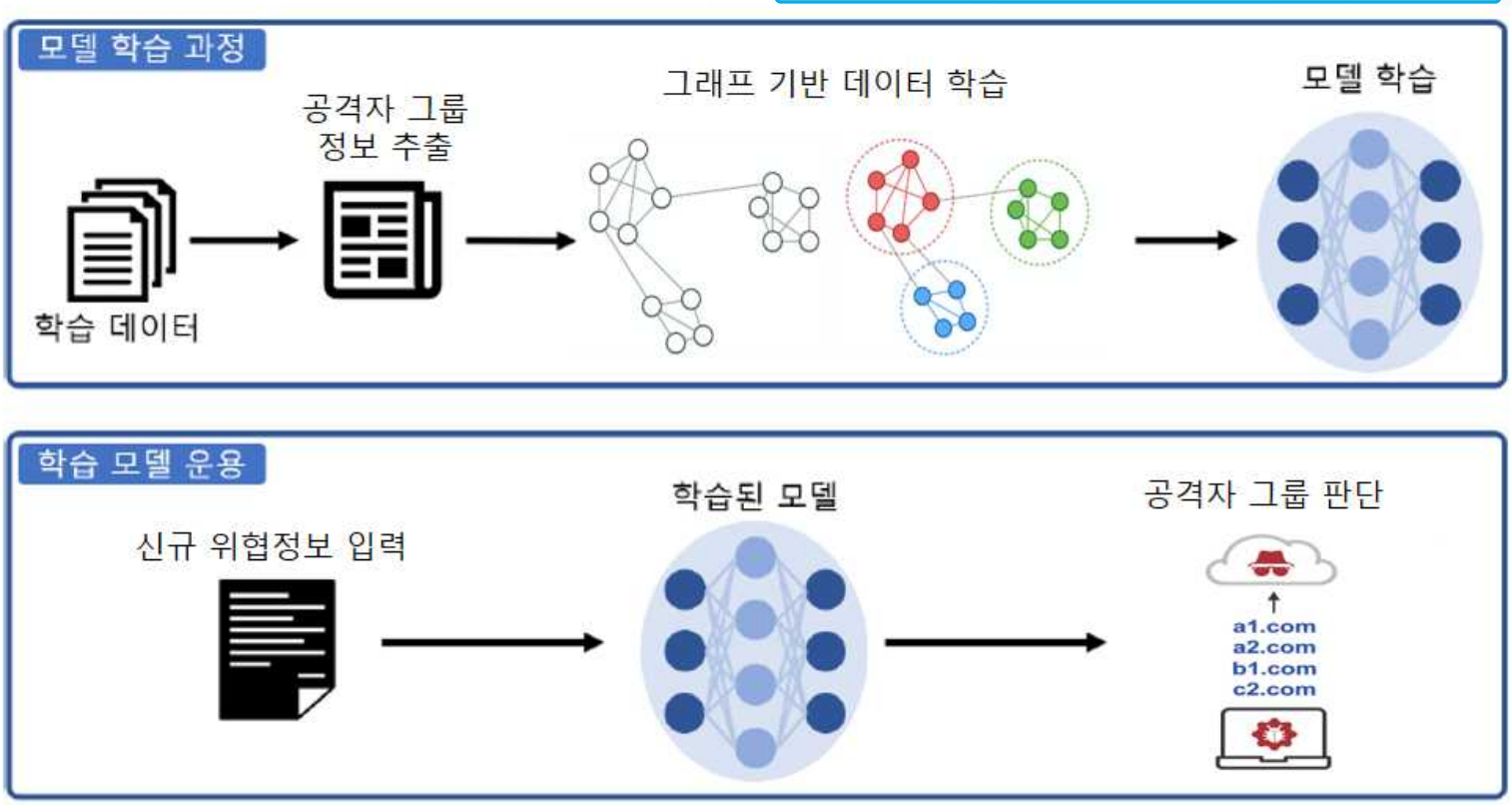
주기적 모니터링

#	eco.sym-global.com URL Path	등록일자
1	blu/747ea/?	2018-05-15
2	/tinymce/source/-/blu/238c2/?	2018-05-15
3	/tinymce/source/-/blu/81754/?	2018-05-15
4	/tinymce/source/-/blu/058ac/?	2018-05-15
5	/tinymce/source/-/blu/65145/?	2018-05-15
6	/tinymce/source/-/blu/664ef/?	2018-05-15
7	/tinymce/source/-/blu/8fabc/?	2018-05-15

빅데이터 분석 사례(대응체계 고도화 #2)

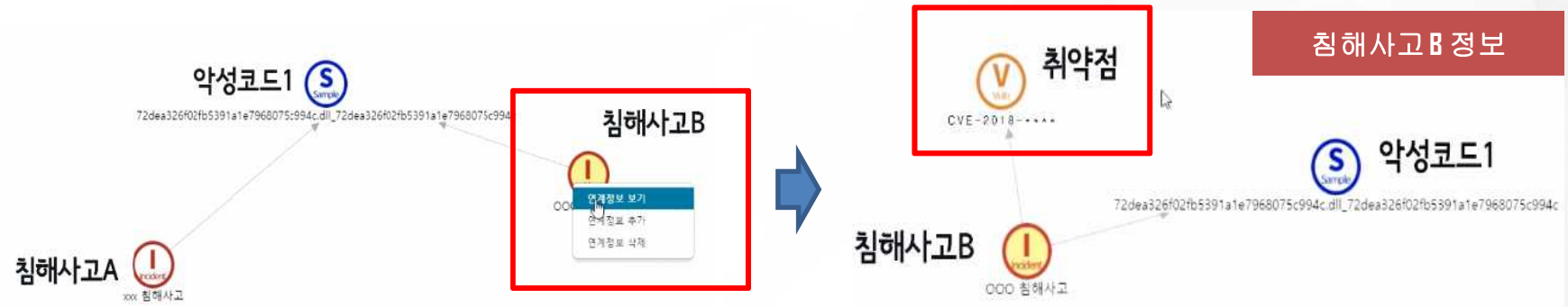
- 공격그룹 프로파일링 및 활동 모니터링

- 신규위협정보에 대한 공격자 그룹 예측
- 추가 악성 행위를 조기 인지 및 사전 예측



빅데이터 분석 사례(대응체계 고도화 #2)

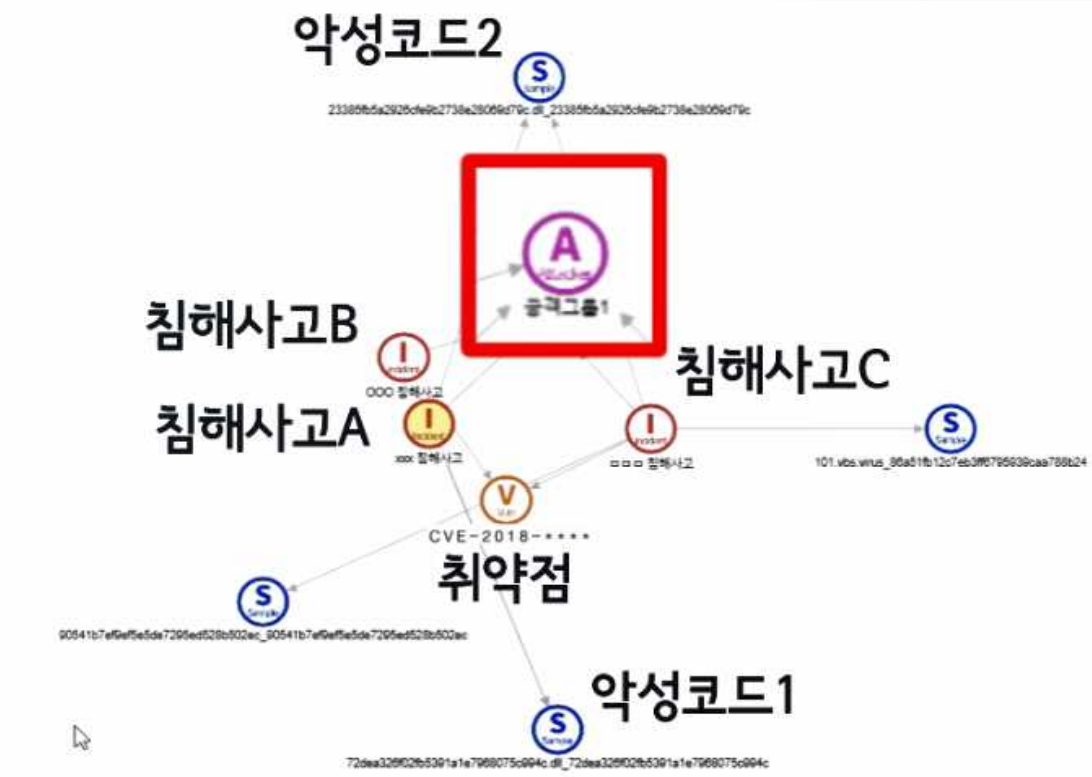
- 공격그룹 프로파일링 및 활용 모니터링
- 악성코드1에 연관된 침해사고B 정보 확인



- 악성코드2에 연관된 침해사고C 정보 확인

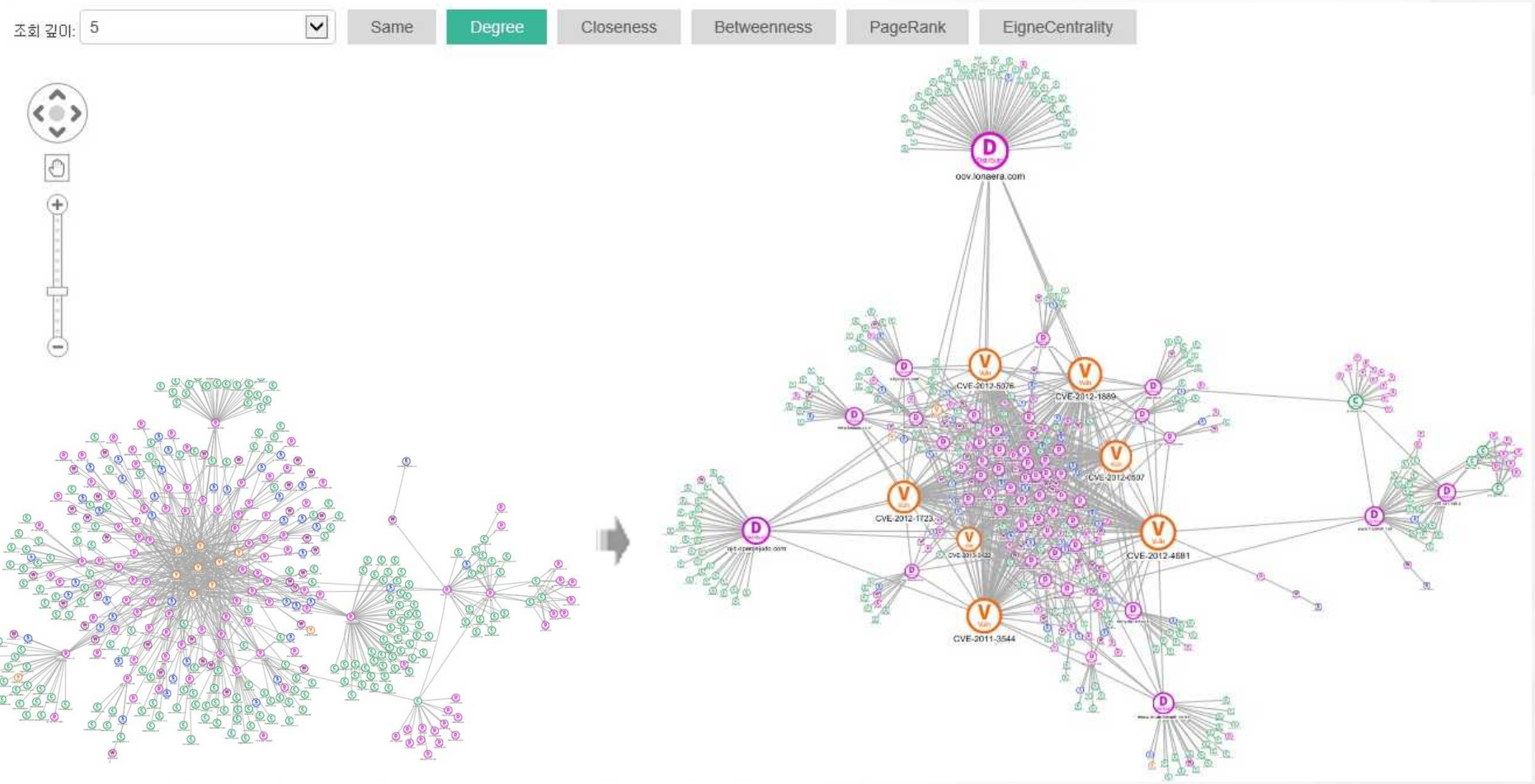
빅데이터 분석 사례(대응체계 고도화 #2)

- 공격그룹 프로파일링 및 활용 모니터링
- 동일 공격자 그룹 추정



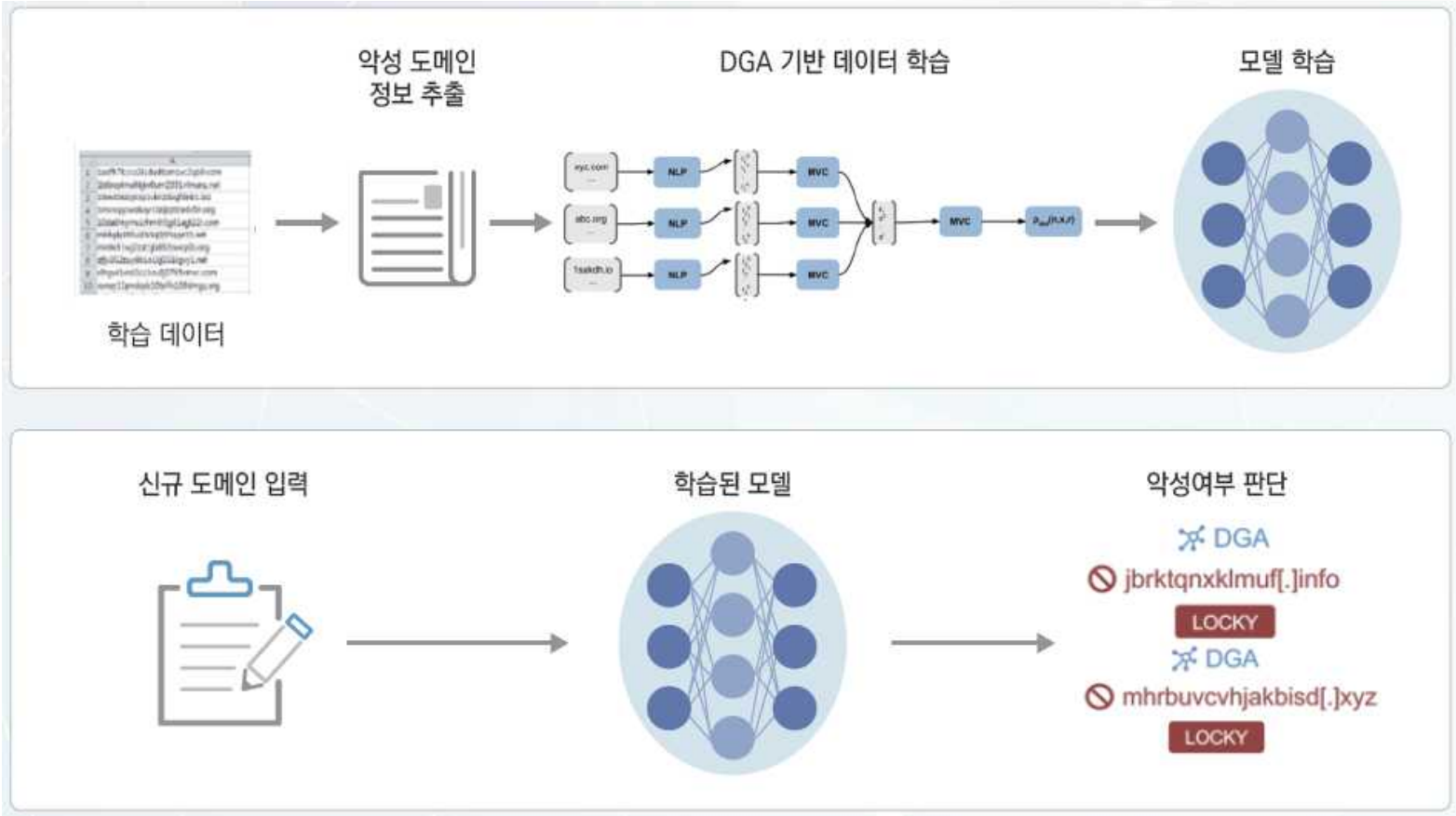
빅데이터 분석 사례(대응체계 고도화 #2)

- 악성 도메인·IP주소, 악성코드, 취약점 등 사이버위협에 대한 위험도 판단



빅데이터 분석 사례(대응체계 고도화 #3)

- 딥러닝을 이용한 악성 도메인 탐지 및 사전 차단

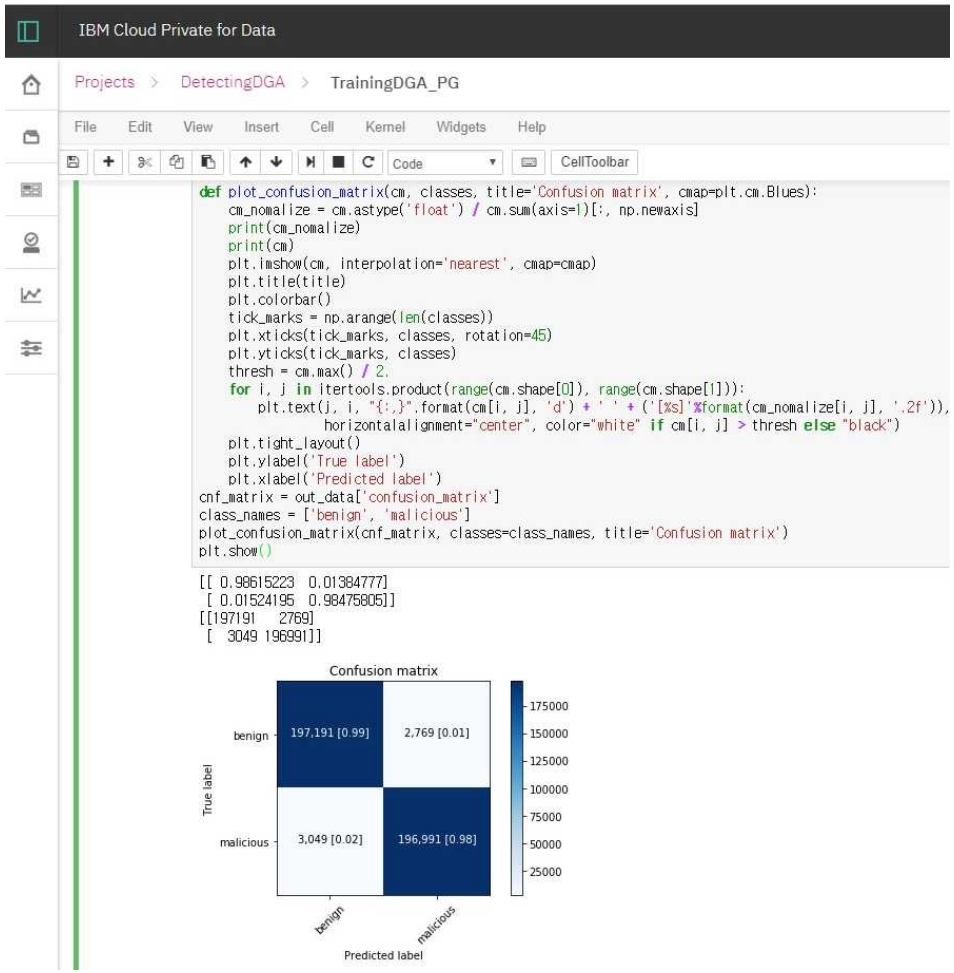


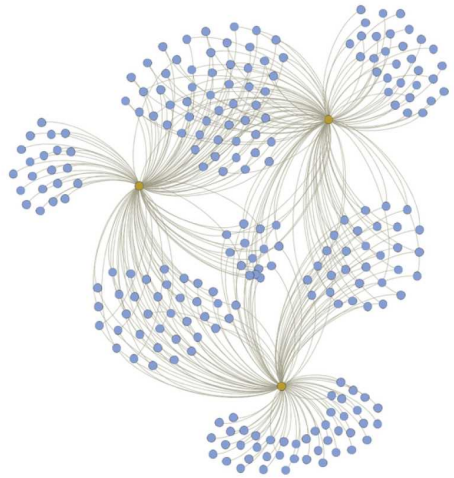
빅데이터 분석 사례(대응체계 고도화 #3)

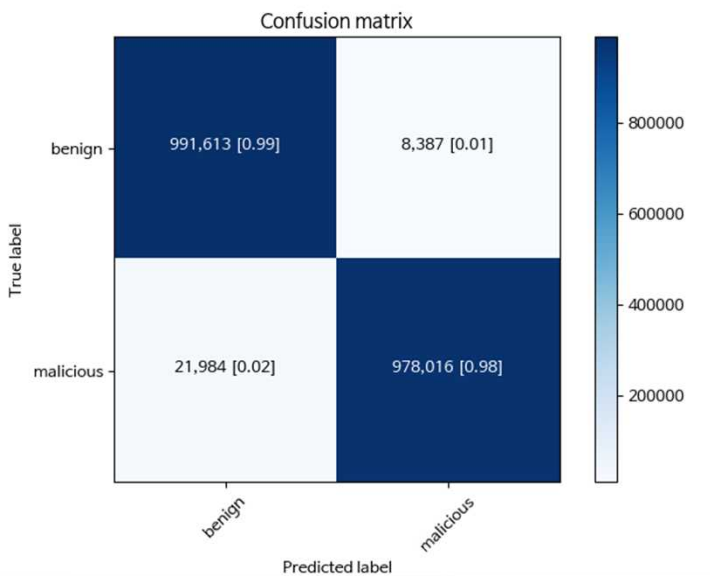
- 딥러닝을 이용한 악성 도메인 탐지 및 사전 차단

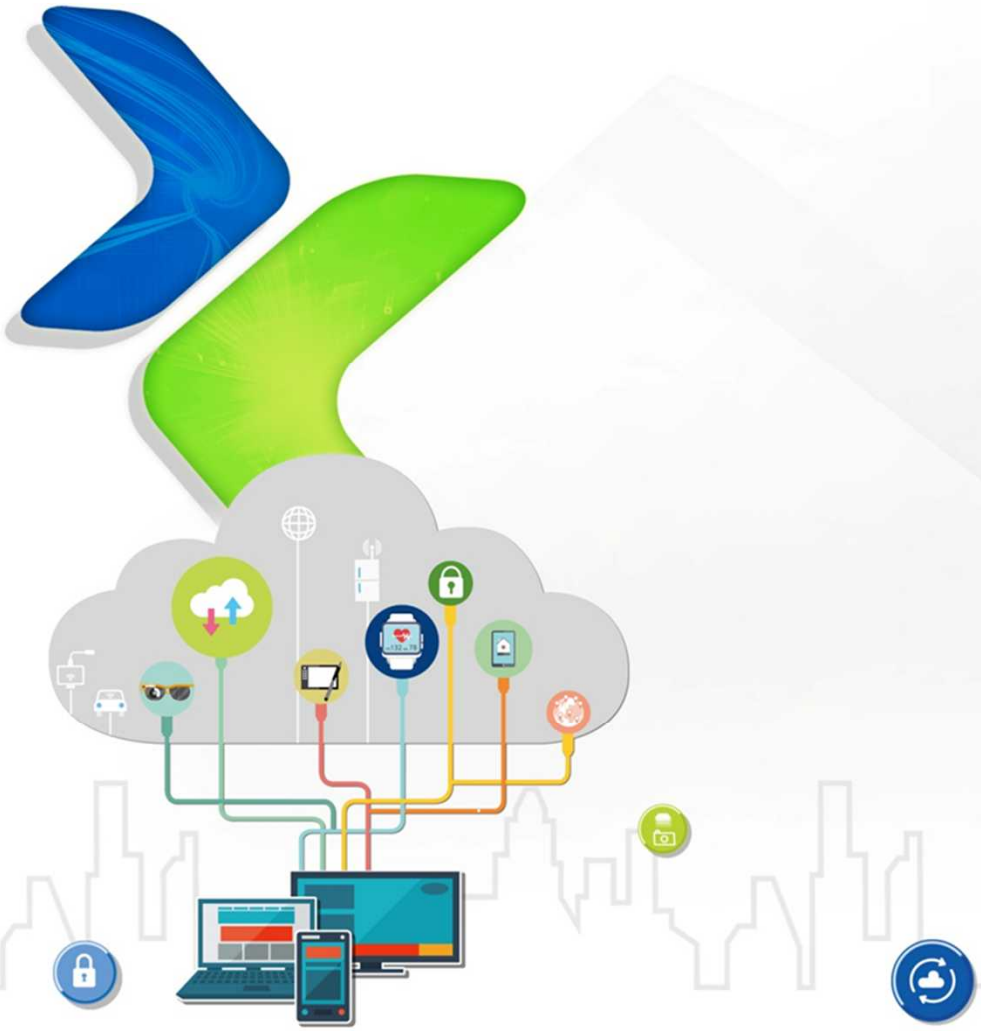
빅데이터 분석 사례(대응체계 고도화 #3)

- 딥러닝을 이용한 악성 도메인 탐지 및 사전 차단









감사합니다