



2020년 7대 사이버 공격 전망

Dec. 2019

Data-Driven Cyber Attack Forecast 2020
by Cyber Threat Intelligence Network



We Will be a Global Leader in the Internet & Security Field

01 2019년 사이버 공격 동향

02 2020년 사이버 공격 전망

2020년 7대사이버 공격전망

1 KISA 일상 속으로 파고든 보안 취약점,
보이지 않는 위협



2 AhnLab 랜섬웨어, 개인에서
공공기관·기업으로 피해 확대



3 INCA 취약한 가상통화 거래소,
반복되는 해킹 사고



4 HAURI 문자 메시지, 이메일 안으로
숨어드는 악성코드



5 ESTsecurity 은밀하게 정교하게,
진화하는 지능형 표적 공격



6 NSHC 모바일까지 확대되는
소프트웨어 공급망 공격



7 Bitscan 융합 서비스를 노리는
새로운 보안 위협의 등장





We Will be a Global Leader in the Internet & Security Field

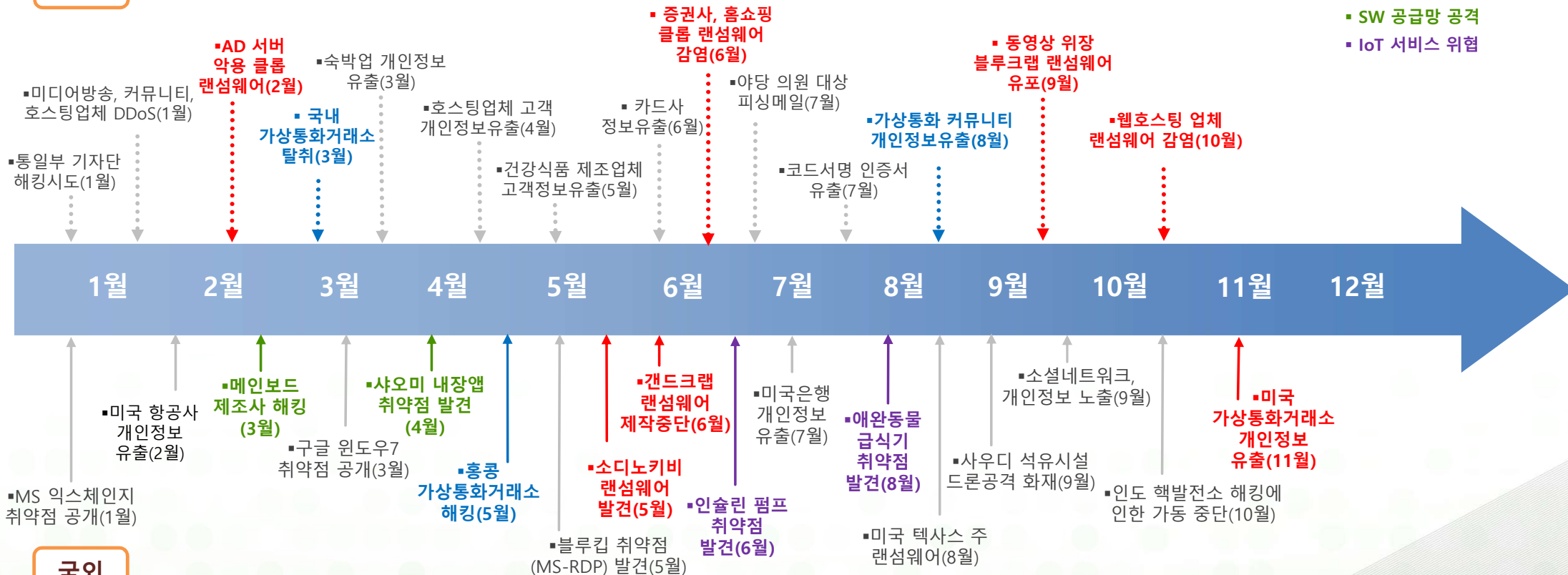
01 2019년 사이버 공격 동향

02 2020년 사이버 공격 전망

1

2019년 국내·외 사이버 공격 동향

국내



1.1 2019년 주요 랜섬웨어 공격

■ 클롭(Clop) 랜섬웨어 등장(3월~)

- 러시아 해킹그룹(TA505)에 의해 제작, 침투한 기업 내 취약한 AD(Active Directory) 서버를 악용하여 유포
- (국내) 증권사 직원 PC 감염 및 전산 장애 발생(6월)

■ 소디노키비(소딘, 블루크랩) 랜섬웨어 등장(5월~)

- 갠드크랩 랜섬웨어와 유사하게 입사지원서, 금융회사 등을 사칭한 이메일을 통해 유포
- 갠드크랩과 달리, 윈도우 권한상승 취약점 등으로도 전파됨

■ 갠드크랩(GandCrab) 배포 중단(6월~)

- '18년 1월 처음 등장한 갠드크랩의 제작자가 판매 중단 선언
- 전문지식 없이도 공격 가능한 서비스형 랜섬웨어의 대표적인 케이스로서 랜섬웨어 공격 증가의 주요 원인이 되었음



출처: 빅카인즈(BIG KINDS)

1.2 2019년 주요 가상통화 거래소·커뮤니티 공격

■ 국내 가상통화 커뮤니티, 회원정보 유출(8월)

- 국내 최대 가상통화 커뮤니티, 사이트 내 악성 스크립트로 인해 회원 아이디와 비밀번호 유출
- 탈취된 회원 계정으로 커뮤니티 측에 협박성 쪽지 발송, 커뮤니티 이미지 실추를 위한 가짜뉴스 유포도 시도

■ 홍콩 바이낸스, 가상통화(5월) 및 회원정보(8월) 유출

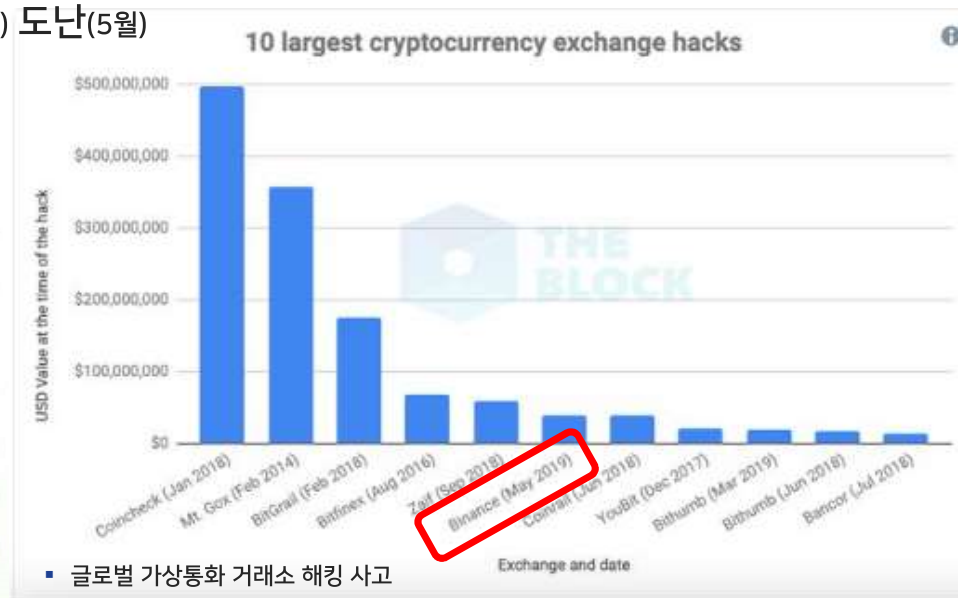
- 가상통화 거래소 바이낸스, 해킹 사고로 인해 비트코인(약 470억 원) 도난(5월)
- 바이낸스 회원정보 수백 여건이 텔레그램을 통해 유출 (8월)

〈 최근 3년간 가상통화 취급업소 해킹관련 기술지원 사례 〉

사건 발생월	피해 업소	피해 내용	경제적 피해추정 규모 (언론보도 추정)
2017. 4월	가상통화 거래소	- 가상통화 유출	약 55억
2017. 6월	가상통화 거래소	- 개인정보 약 3.6만건 유출 ※ 해킹메일 열람(직원 개인pc) 후 악성코드에 감염-외부(개인pc)에서 개인정보 열람-개인정보 유출	약 70억
2017. 9월	가상통화 거래소	- 가상통화 유출	약 21억
2017. 12월	가상통화 거래소	- 가상통화 유출	약 170억
2018. 6월	가상통화 거래소	- 가상통화 유출	약 500억
2018. 6월	가상통화 거래소	- 가상통화 유출	약 350억
2018. 10월	가상통화 거래소	- 가상통화 유출	확인 불가
2019. 3월	가상통화 거래소	- 가상통화 유출	약 100억~200억
합계			약 1,266억

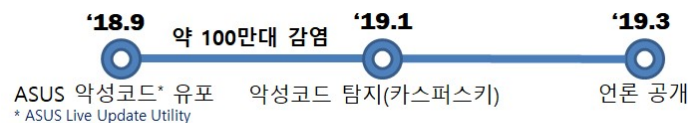
※ 출처 : 신용현 의원실(과학기술정보통신부, 한국인터넷진흥원 제출자료 재구성)

※ 경제적 피해규모는 언론보도 등을 통해 추정된 것으로 실제 피해액과 다를 수 있음



- 글로벌 가상통화 거래소 해킹 사고

1.3 2019년 주요 소프트웨어 공급망 공격

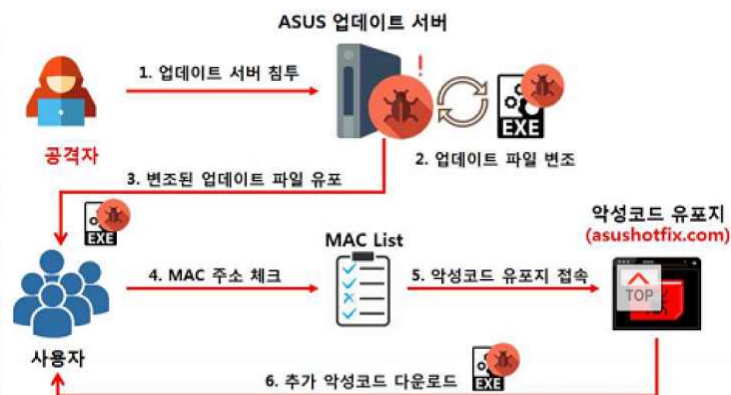


■ PC 제조사 대상 SW 공급망 공격(3월)

- 대만 PC 제조사인 에이수스(ASUS)의 소프트웨어 업데이트 서버를 통해, 100만여 대의 고객 PC가 악성코드에 감염
- 공격자는 업데이트 서버에 침투하여 정상적인 코드 인증서로 서명된 악성코드를 유포, 600여대의 PC에만 악성코드 추가 설치

■ 샤오미 스마트폰 내장 앱 취약점 발견(4월)

- 스마트폰 내장 보안 앱(가드 프로바이더)에서 트래픽을 암호화하지 않고 전송하는 취약점 발견
- 스마트폰 내장 Mi 브라우저와 구글 플레이의 Mint 브라우저에서 URL 스푸핑 취약점 발견



- ASUS 업데이트 서버를 통한 SW 공급망 공격



1.4 2019년 IoT 서비스 대상 주요 사이버 위협

■ Medtronic 인슐린 펌프 취약점 발견 (6월)

- 美 Medtronic社의 인슐린 펌프(MiniMed 508, Paradigm 시리즈)에서 무선 RF(Radio Frequency) 통신 취약점 발견
- 취약점을 악용할 경우, 펌프에 데이터를 주입하거나 설정을 변경함으로써 인슐린 투여의 제어가 가능

■ 샤오미 애완동물 급식기 취약점 발견 (10월)

- 샤오미 애완동물 급식기(Furrytail Pet Smart Feeder)에서 WiFi 칩셋(ESP8266) 펌웨어 취약점 발견
- 취약점을 악용할 경우, 펌웨어 업데이트를 통해 급식기를 원격에서 제어하거나 DDoS 공격에 이용 가능



■ Medtronic 인슐린 펌프 취약점 발견



■ 샤오미 애완동물 급식기 취약점 발견



We Will be a Global Leader in the Internet & Security Field

01 2019년 사이버 공격 동향

02 2020년 사이버 공격 전망

2

2020년 사이버 공격 전망

7대 전망



- I 일상 속으로 파고든 보안 취약점, 보이지 않는 위협 (KISA)
- II 랜섬웨어, 개인에서 공공기관·기업으로 피해 확대 (안랩)
- III 취약한 가상통화 거래소, 반복되는 해킹 사고 (잉카인터넷)
- IV 문자 메시지, 이메일 안으로 숨어드는 악성코드 (하우리)
- V 은밀하게 정교하게, 진화하는 지능형 표적 공격 (이스트시큐리티)
- VI 모바일까지 확대되는 소프트웨어 공급망 공격 (NSHC)
- VII 융합 서비스를 노리는 새로운 보안 위협의 등장 (빛스캔)

2.1 일상 속으로 파고든 보안 취약점, 보이지 않는 위협

- 지능형 CCTV, AI 스피커 등 IoT 결합 서비스 대상 사이버 위협 증가
- 윈도우 RDP 취약점(블루킵) 미패치 시스템을 노린 제2의 워너크라이 등장 우려
- 지원 중단 혹은 예정 운영체제(윈도우7/XP, 서버 2008/2003 등) 취약점 공격 시도

■ IoT 결합 서비스 위협 증가



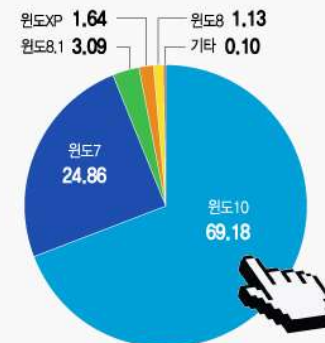
■ RDP 취약점 미패치 시스템 공격



■ 지원중단 예정 OS 국내 점유율

국내 PC 윈도우 운영체제 점유율

*단위: %, 올해 9월 기준



*자료: 스탯카운터(statcounter)
그래픽: 이승현 디자인기자

2.2 랜섬웨어, 개인에서 공공기관·기업으로 피해 확대

- 공공기관·기업으로 사칭하여 APT와 결합된 랜섬웨어 유포
- APT와 결합된 랜섬웨어 공격, PC 공격보다 높은 금액 요구
- 랜섬웨어 감염 시 백업 파일까지 암호화 및 피해 발생

■ 공공기관·기업 표적 랜섬웨어 (19년도)

시기	랜섬웨어	대상 기관	요구금액
1월	록커고가	프랑스 엔지니어링 컨설팅 업체	-
3월	류크	美 조지아 잭슨카운티 행정망	\$400,000
3월	록커고가	美 합성수지, 실리콘 업체	-
3월	록커고가	노르웨이 알루미늄 업체	-
3월	-	국내 주식 거래 서비스	-
3월	-	영국웨일즈경찰연합	-
4월	-	美 날씨 방송사	-
4월	-	美 클리블랜드 홉킨스 국제공항	-
5월	로빈후드	美 매릴랜드 볼티모어 공공망	\$76,000
6월	-	벨기에 비행기 부품 업체	-
6월	-	美 플로리다 리비에라 비치 시	\$600,000
7월	클롭	국내 증권사	-
7월	-	남아프리카공화국 전력 기업	-
8월	-	美 텍사스 23개 도시	-

■ 개인에서 공공기관·기업으로 피해 확대



■ 블루크랩 (소디노키비) 랜섬노트

Your computer has been infected

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - 7ywf50q723-Decryptor

You can do it right now. Follow the instructions below. But remember that you do not have much time

7ywf50q723-Decryptor price

Time is over Current price **0.21992923 BTC**
* You didn't pay on time, the price was doubled. = 2,700 USD

Bitcoin address: 3Nk1D1b1S2FwP2CjL4mUu8G2F50d * BTC will be recalculated in 4 hours with an actual rate

INSTRUCTIONS CHAT SUPPORT

How to decrypt files?
 You will not be able to decrypt the files yourself. If you try, you will lose your files forever.
 To decrypt your files you need to buy our special software - 7ywf50q723-Decryptor

Buy Bitcoins with Bank Account or Bank Transfer

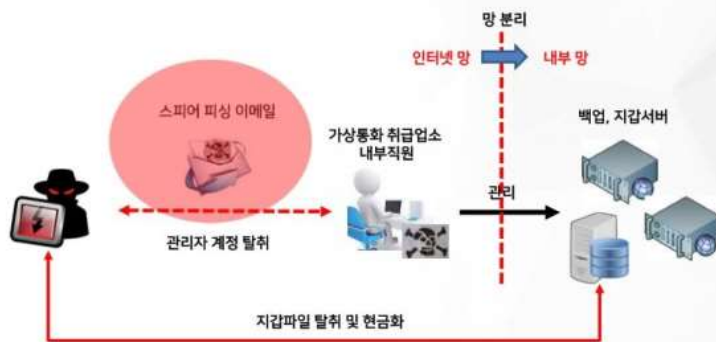
- ◉ Coimama
- ◉ Kiorbi
- ◉ Coinfloor

2.3 취약한 가상통화 거래소, 반복되는 해킹 사고

- 가상통화 탈취 및 가치 조작을 목적으로 가상통화 거래소를 꾸준히 공격
- 가상통화 거래소 사칭 및 지갑 프로그램으로 위장한 악성코드 유포 증가
- 피해를 눈치채기 힘든 채굴형 악성코드의 지속적인 유포 및 감염 시도

■ 가상통화 거래소 해킹

스피어피싱을 이용한 가상통화 취급업소 침투



■ 가상통화 거래소 사칭

☆ 두나무 김대현 팀장입니다. ☎

보낸사람 Upbit info <info@upbit.com> 19.10.04 22:15 주소주가 수신자단

이여사님, 두나무(업비트) 김대현 팀장입니다.명절때 보내주신 선물 잘받았습니다.

레이브코인(RVN) 하드포크에 따른 입출금이 일시 중단되었습니다.
이여사님은 현재 우리거래소의 레이브코인(RVN) 60%이상 보유하고 있습니다.하여 입출금 지원 중단
업비트 계정에 입금이 반영되지 않을 수 있으며 발생 시 복구 불가능할 수 있습니다.
이 점 유의하시어 입출금 지원 중단 시점 이후 절대로 입금하지 않아주시기 바랍니다.

그리고 사전에 이여사님께서 불편해 하셨던 입출금 관련 지연문제에 대해선, 내부 회의결과, 직원전용
승인절차없이 검토과정 없이 출금이 가능합니다.보안상 관계로 다운로드 방식은 FTP연결방식으로 보
코인잔액도 확인해주시기 바랍니다.
이용중 문제점이 있으시면 언제든지 메일주시면 바로 답변해 드리겠습니다.

FTP://FILE.BITIS.IO

아래 그림과 같이 브라우저 창구가 아닌 바탕화면 내PC 주소창에서 FTP://FILE.BITIS.IO 주소를 붙여넣기하세요.

지갑파일을 바탕화면으로 옮겨 옮기시면 됩니다.

■ 채굴형 악성코드 탐지 현황

탐지건수
13만 여건



2018년

탐지건수
68만 여건



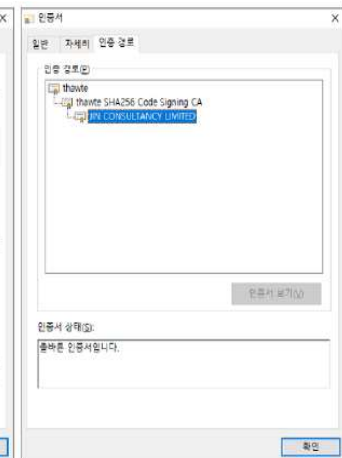
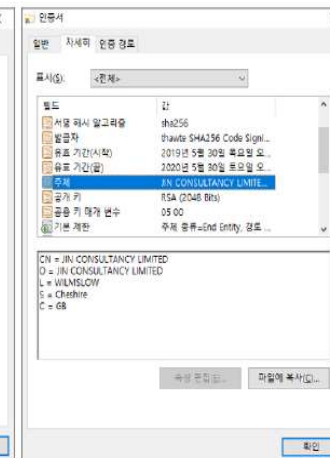
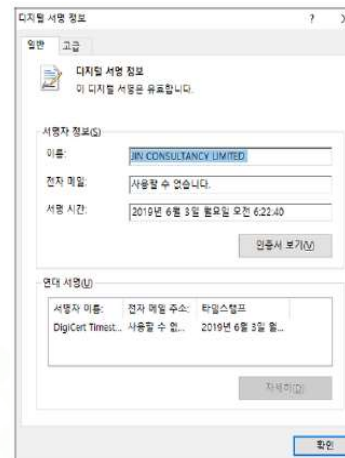
2019년

2.4 문자 메시지, 이메일 안으로 숨어드는 악성코드

- 문자 메시지, 이메일 속 링크를 이용하여 악성 앱을 감염시키는 모바일 표적 공격
- IoT 기기 보급 확산에 따른 대규모 IoT 봇넷 등장 및 DDoS 공격의 재개
- 유효한 코드서명 인증서 탈취 시도 및 이로 서명된 악성코드 유포·감염 증가

■ 링크로 유도된 악성 앱

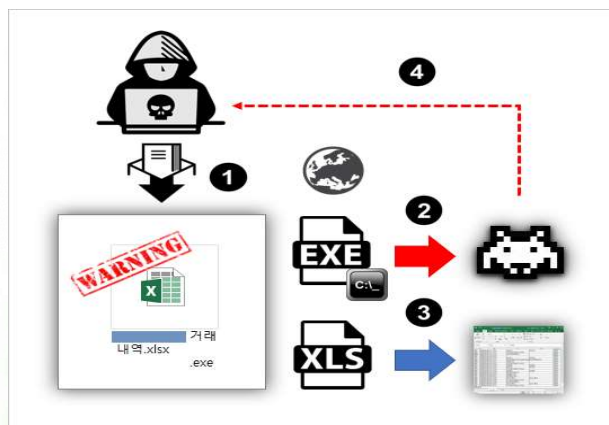
■ 코드서명 인증서 탈취 및 악용



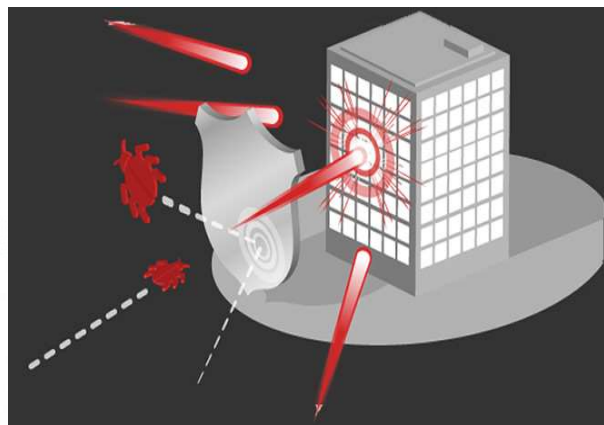
2.5 은밀하게 정교하게, 진화하는 지능형 표적 공격

- 견적 의뢰서, 보도자료 등 정상 문서 파일을 위·변조한 스피어 피싱의 정교화
- 문서 소프트웨어의 자체 보안 기능을 통한 보안위협 탐지 시스템 회피 증가
- 구글 드라이브나 드롭박스, 슬랙 등의 정상 서비스를 활용해 악성코드 통신 기법 활용

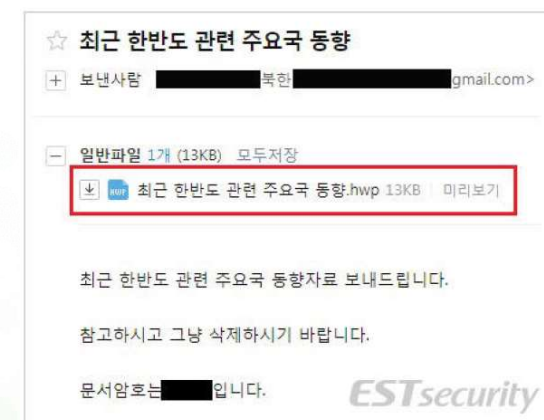
■ 정상 문서 파일 위·변조



■ S/W 보안 기능을 이용한 탐지 회피



■ 암호화된 문서 파일 이용



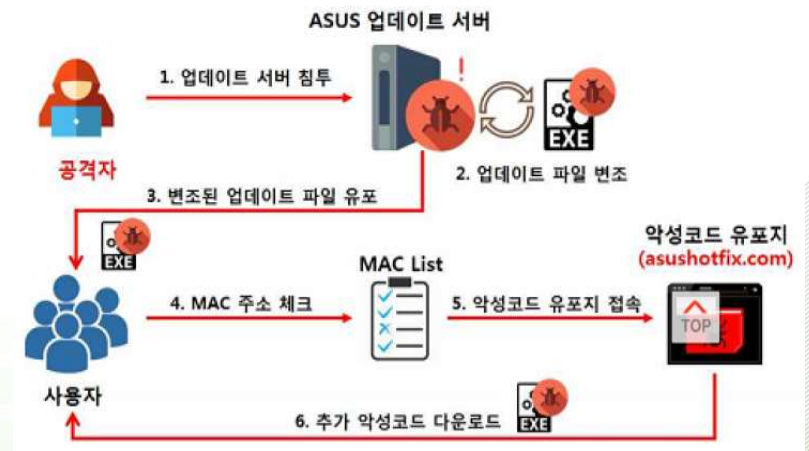
2.6 모바일까지 확대되는 소프트웨어 공급망 공격

- 모바일 앱, 스마트폰 제조사를 대상으로 S/W 공급망 공격 확대
- 스마트카, 의료기기에 설치되는 S/W에 악성코드 삽입을 노리는 공격 시도
- S/W의 특정 사용자만을 선별하여 감염된 악성코드를 실행하는 표적 공격

■ 모바일 소프트웨어 공급망 공격



■ 특정 사용자 대상 S/W 공급망 공격



2.7 융합 서비스를 노리는 새로운 보안 위협의 등장

- 교통 시스템 해킹을 통한 교통 마비와 CCTV 무력화와 같은 스마트 시티 보안위협 등장
- 스마트 공장의 유지보수 과정에서 전파되어 정보를 수집하고 시스템을 파괴하는 악성코드
- 의료 시스템 해킹을 통한 환자 개인정보·처방전 데이터 유출 및 의료기기 오작동 유발

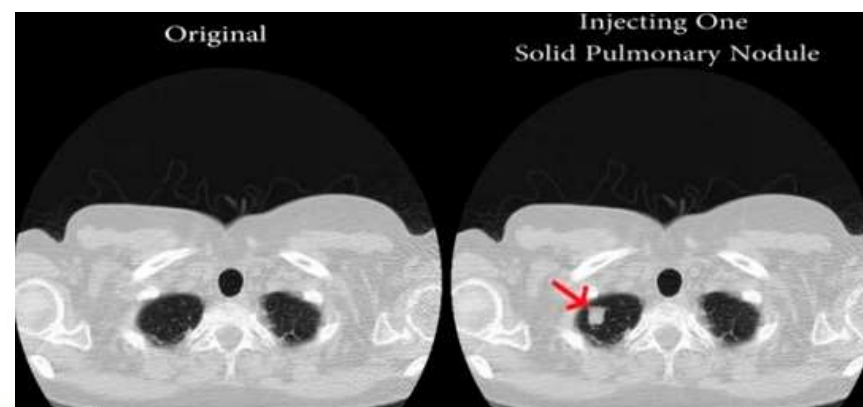
■ 스마트 시티 위협



■ 스마트 공장 위협



■ 의료 영상기록 변조



Internet On, Security In!

감사합니다

