SK 쉴더스

EQST Annual Report

# 2023 보안 위협 전망 보고서

# Contents

# EQST insight

## 2022년 보안 Trend 및 이슈 리뷰

### 2022 년 5 대 보안 위협 리뷰

2022 년에도 국/내외를 가리지 않고 랜섬웨어 공격이 크게 성행했다. 국내 기업을 타깃으로 한 귀신(GWISIN) 랜섬웨어가 출현했으며, 복호화 키, 중요 정보 유출, 취약점 리포트 제공 등을 빌미로 3 중 협박을 통한 금전 요구도 발생했다. 고도화된 전략과 탐지 회피 기법으로 파급력 높은 랜섬웨어 공격이 계속해서 발생하고 있으며, 협박 형태 또한 진화하고 있다.

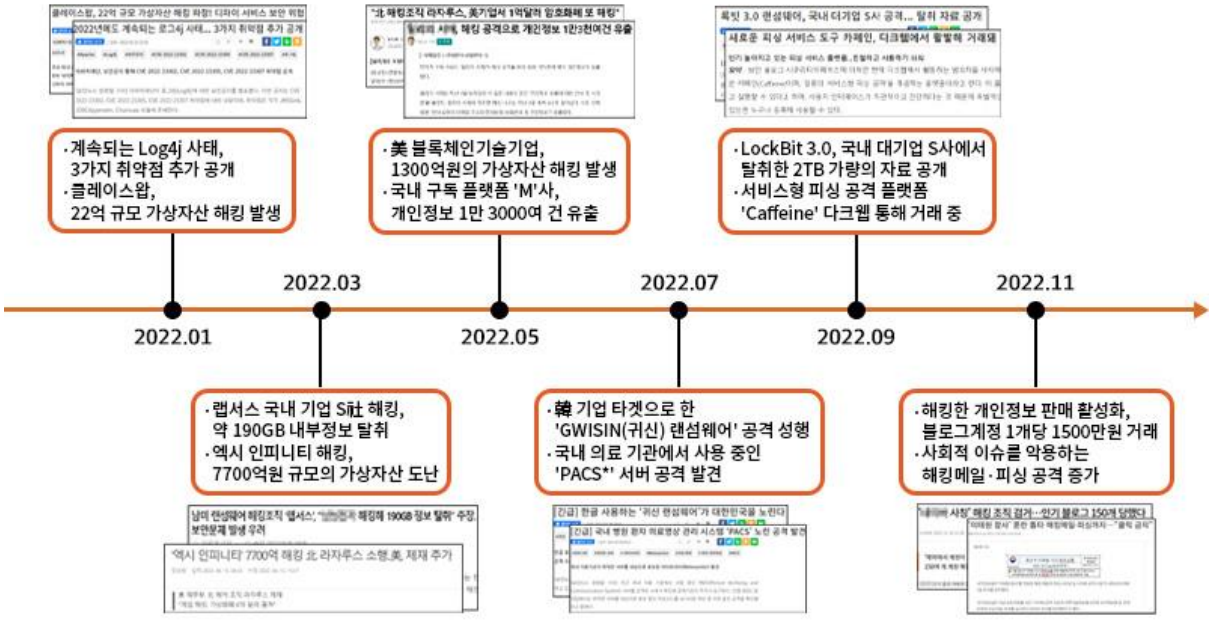
또한, 디지털 트랜스포메이션에 대한 개인 및 기업의 관심이 높아짐에 따라 다양한 분야에서 스마트 환경을 구축해 이용하고 있다. 개인 일상과 사회생활 속에 IoT 환경이 스며들면서 2022 년에도 꾸준히 해커들의 관심과 공격이 이어졌다. IoT 기기들을 봇넷화하여 수사기관의 추적을 피하거나, 공공·정부 기관을 대상으로 해킹을 시도하는 등 취약한 IoT 기기를 공격에 활용하는 사례도 다수 발생했다.

의료산업도 공격자들의 타깃에서 벗어나지 못했다. 피싱을 통해 획득한 계정으로 의료 시스템에 접근해 민감정보를 탈취했으며, 의료 시스템에 악성코드를 배포하여 의료 인프라를 마비시켜 의료 서비스 제공을 방해하는 식의 피해도 발생했다.

이 외에도 올해 3 월에 발발한 러·우 전쟁의 여파로 각종 산업 제어 시스템과 공공·정부 기관을 대상으로 한 공격이 이어졌으며, 국가 시스템이 마비되는 피해가 발생했다. 또한, OT/ICS 시스템을 대상으로 공격이 발생해 공장 생산 라인이 멈추는 피해도 보고되었다.

SK 쉴더스의 화이트해커 그룹 EQST(이큐스트)는 2022 년 주요 보안 이슈를 분석하고, 2023 년 5 대 보안 위협을 전망해 보았다.

## 2022 년 주요 사이버보안 사고 리뷰




[2022 년 주요 사이버보안 사고]

올해 1 월에는, 2021 년 12 월 말 취약점이 발견되어 큰 이슈가 된 Log4j 의 추가 취약점들이 공개되었다. Java 로깅 라이브러리인 Log4j 에서 발생하는 취약점으로 사용 범위가 넓어 파급력 또한 높기 때문에 사용자들의 각별한 주의가 필요하다. Log4j 취약점 최초 발견 이후, 관련 취약점이 꾸준히 제보되고, 위험도 높은 제로데이 취약점이 연달아 발견되면서 국내외로 큰 이슈가 되었다.

또한, 국내 최대 규모 DeFi(Decentralized Finance, 탈중앙화 금융) 서비스인 KLAYswap[1]에서 22 억 규모의 가상자산이 탈취되는 해킹이 발생했다. 가상자산 탈취에 사용된 해킹 기법은 BGP Hijacking[2]으로, BGP 프로토콜을 악용하여 공격자가 설정한 라우팅 테이블로 네트워크 흐름을 조작한 후 정상 SDK 파일로 위장한 악성코드를 다운로드하는 방식이다. 악성코드가 설치된 피해자가 가상자산 거래를 이용할 경우, 공격자의 지갑으로 가상자산이 전송되는 형태로 공격이 이루어졌다.

3 월에는 국제적인 해킹그룹인 랩서스(Lapsus$)의 글로벌 IT 기업 및 제조업을 대상으로 한 공격이 발생했다. 국내 S 社에서는 190GB 의 소스코드가 유출되었으며, L 社에서는 임직원 이메일 계정 및 비밀번호 약 9 만 건이 탈취되었다. 또한 국외에서는 반도체 기업인 N 社의 시스템이 해킹 당해 회로도, 펌웨어 등 기밀 데이터 1TB 가 탈취되었다. 랩서스는 다크웹 및 피싱 메일을 통해 임직원의 계정 정보를 획득하여 내부 시스템에 침투, 내부 정보를 탈취하는 방식으로 공격을 진행했다.

또한, 블록체인 비디오 게임 '엑시 인피니티'에서 7,700 억 원 규모의 가상자산이 도난당하는 사건이 발생했다. 탈취한 7,700 억 원 중 1,100 억 원가량이 북한 소속의 해킹 그룹 '라자루스'의 가상자산 지갑으로 이동한 것이 확인되었다.

5~6 월에도 북한의 가상자산 탈취는 계속 이어졌다. 미국의 블록체인 기술 개발 기업인 'Harmony'에서 1 억 달러(약 1,300 억 원)의 암호화폐가 도난당하는 사고가 발생했으며, 1 억 달러의 암호화폐 중 41%를 거래 추적을 숨기는 서비스인 '토네이도 캐시 믹서'로 보낸 것이 확인되었다. 사이버 보안 업체 'Trellix'의 발표에 의하면 북한은 외화 탈취를 위해 신종 랜섬웨어 4 종을 유포하는 등 많은 나라의 다양한 기업에 대한 가상자산 탈취를 꾸준히 이어오고 있다고 한다.

또한, 국내 구독형 플랫폼 M 社에서 13,182 명에 달하는 회원들의 개인정보가 해킹으로 유출되는 사고가 발생했다. 유출된 정보는 이메일 주소와 암호화된 전화번호 및 비밀번호이며, 회원마다 유출된 정보는 다른 것으로 밝혀졌다.

[1] KLAYswap: 국내 K 社의 블록체인 플랫폼 클레이튼(Klaytn)을 기반으로 한 DeFi 서비스

[2] BGP hijacking: BGP 라우터에 침투하여 지속적인 브로드 캐스트를 통해 라우팅 테이블 정보를 조작

7 월에는 서비스 및 의료업 등 국내 기업을 타깃으로 한 귀신(GWISIN) 랜섬웨어의 공격이 성행했다. 국내 기업 맞춤형 공격을 하는 귀신(GWISIN) 랜섬웨어는 국내 기업 내부에서 사용하는 통합 관리 솔루션을 악용하거나 국내의 보안 정책, 보안 솔루션 취약점을 악용하는 등 국내 보안 현황에 대한 인식이 뛰어난 것으로 파악된다. 또한 랜섬웨어 복호화, 중요 정보 유출 및 추가 공격 협박을 하는 등 3 중 협박을 통해 피해를 증가시키고 있으며, 고도화된 탐지 회피 등 지능적으로 변화하고 있다.

이 외에도, 국내 의료 기관에서 사용 중인 영상 정보 관리 시스템, PACS(Picture Archiving and Communication System)의 취약한 서버를 대상으로 한 공격이 발견되었다. PACS 는 다양한 의료 장비로부터 받은 환자의 진료 영상 정보를 디지털로 관리 및 전송하는 시스템으로 현재 많은 병원에서 사용 중이다. 공격자는 취약한 PACS 서버를 대상으로 악성코드를 유포하는 공격을 감행했다. 많은 병원에서 널리 사용되고 있는 만큼, 취약한 버전을 사용하고 있다면 최신 버전으로 패치해야 하며 보안 솔루션을 설치해 안전하게 관리해야 한다.

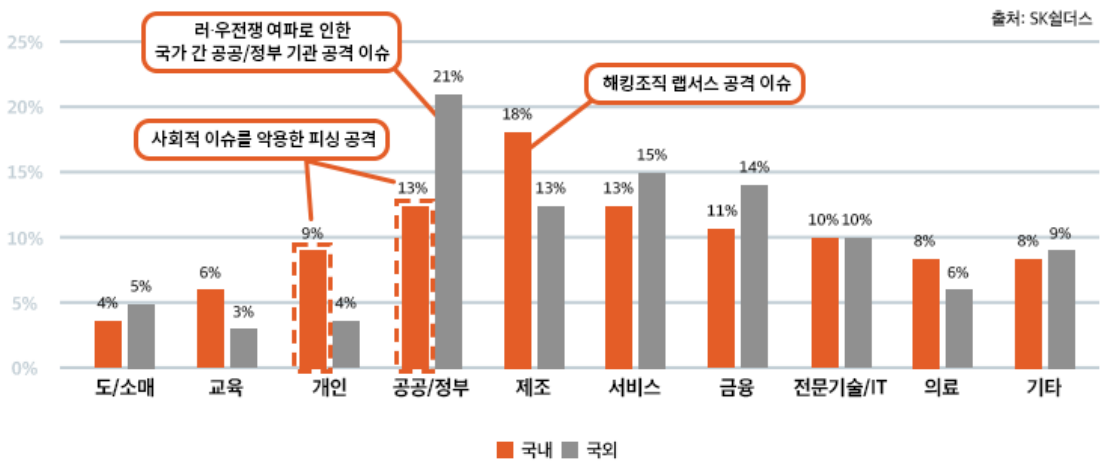
9 월에는 서비스형 랜섬웨어(RaaS)인 LockBit 3.0 이 국내 대기업 S社에서 탈취한 2TB 가량의 자료를 자신들의 홈페이지에 업로드하는 사건이 발생했다. 탈취한 데이터인 S社 임직원 PC 의 폴더 캡처, 품의문 등 내부 문서를 자신들의 홈페이지에 공개했으며, 이 파일들은 다운로드도 가능했다. LockBit 3.0 은 2022 년 가장 많은 활동을 하며 피해를 입힌 랜섬웨어로, 북한과 관련 있는 것으로 알려진 비너스락커(VenusLocker) 랜섬웨어 그룹이 사용하는 것으로 알려져 있다. 최근에는 입사지원서를 위장한 한글(HWP) 파일의 형태로 유포되고 있어 개인 및 기업의 각별한 주의가 요구된다.

또한, 서비스형 피싱 공격 플랫폼인 ‘Caffeine’이 발견되었다. Caffeine 은 다크웹을 통해 활발히 거래되었으며, 서비스형 피싱 공격을 제공하는 플랫폼으로 PhaaS(Phishing-as-a-Service)라고 불린다. 직관적인 인터페이스를 가지고 있으며 정교한 수법을 사용하여 맞춤형 피싱 키트를 제작할 수 있다. 누구나 검색 엔진을 통해 쉽게 접근 가능하며, 서비스 이용에 이메일만 요구되고 있어 피싱에 대한 진입 장벽이 낮아지고 있음을 알 수 있다.

11 월에는 국내 최대 포털사이트의 인기 블로그 계정 500 여 개를 해킹하여 판매한 일당이 검거되었다. 이들은 메일의 도메인 주소를 일부 변경한 후 사용자에게 해당 포털 사이트를 사칭하는 피싱 메일을 전송해 인기 블로그 사용자의 비밀번호를 탈취했다. 탈취한 계정을 1 개당 1,000 ~ 1,500 만 원에 마케팅 업자에게 판매해 2 억 원의 범죄 수익금을 획득한 것으로 알려졌다. 이외에도 나라사랑 포털에서 로그인 정보를 비롯한 사용자의 웹 브라우저 정보, 웹캠을 통해 촬영한 사용자의 사진 등 개인정보 1,000 여 건이 유출되어 다크웹을 통해 거래되는 사건도 있었다. 해커가 탈취한 중요정보가 일정 금액으로 판매되거나, 다크웹을 통해 활발히 거래되고 있는 것을 알 수 있다.

또한, 최근 불특정 다수를 대상으로 울진 산불, 코로나 19, 국내 K 社 서비스 장애 등 사회적 이슈를 악용한 해킹 메일 및 피싱 공격이 활발히 일어났다. 특히 지난 10 월 국내 기업 K 社의 서비스 장애 사태를 악용하는 공격이 발생했다. 북한 업계 종사자 및 탈북민을 대상으로 발생했으며, K 社에서 배포하는 업데이트 설치 파일로 위장해 악성 프로그램 설치를 유도하는 형태로 이루어졌다. 기존의 피싱 공격보다 더 많은 대상을 타깃으로 하여 성공률을 높이기 위해 사회적 이슈를 악용하는 사례가 점차 증가하고 있기 때문에 개인 및 기업의 주의가 요구된다.

## 업종별 침해사고 발생 통계




[2022 년 업종별 침해사고 발생 통계]

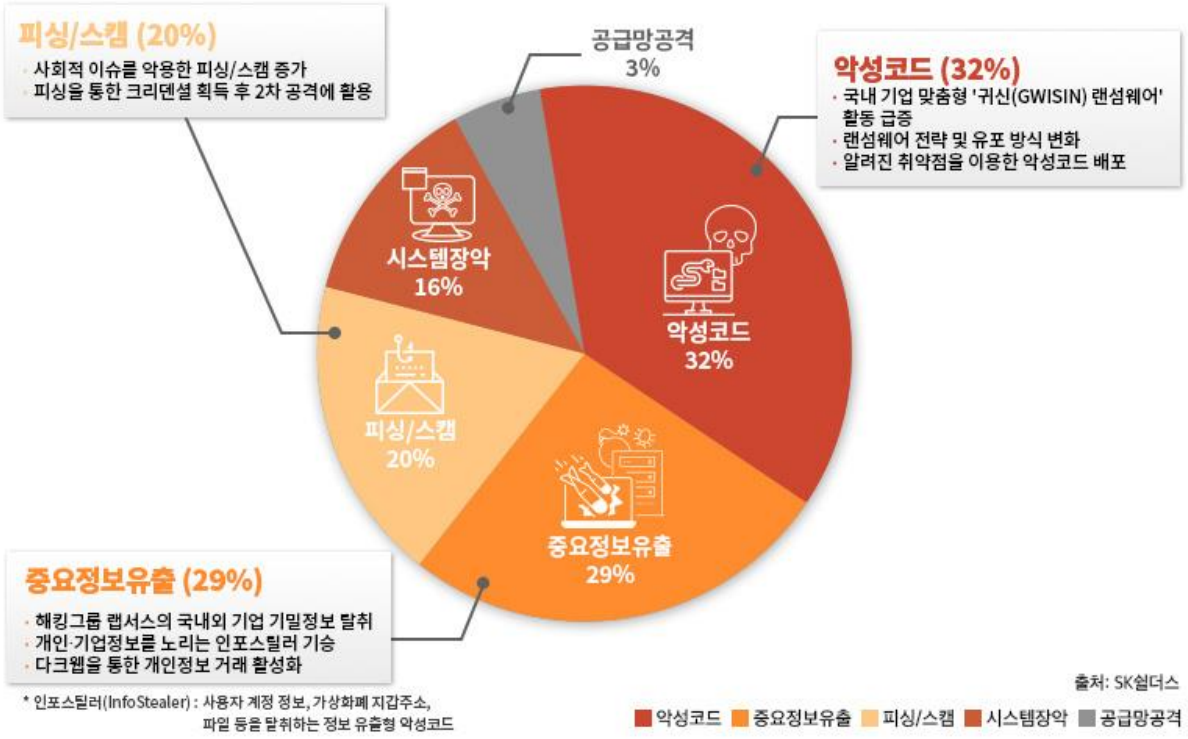
2022 년 업종별 침해 사고 발생 통계를 살펴보면, 국내 기준 제조가 18%, 서비스 및 공공/정부가 13%로 가장 많은 사고가 발생했다. 또한 금융이 11%, 전문기술/IT 가 10%, 의료가 8%를 차지했다. 국외 기준으로는 공공/정부 분야가 21%로 가장 높은 수치를 보였으며, 서비스와 금융, 제조가 뒤를 이었다.

올해 상반기 국내외 제조업 및 전문기술/IT 기업을 대상으로 한 해킹그룹 랩서스(Lapsus$)의 공격이 있었다. 특히 국내 대기업 S 社, L 社 공격에 성공하여 큰 이슈가 되었다. 하반기에는 국내 기업을 타깃으로 한 귀신(GWISIN) 랜섬웨어가 성행하여 의료/서비스업에서의 침해사고가 집중적으로 발생했다.

또한, 하반기에는 울진 산불, 코로나 19, 국내 K 社 서비스 장애 등 사회적 이슈를 악용한 해킹 메일과 피싱 공격이 활발히 일어나 국내 공공/정부 및 개인의 침해사고 비율이 높게 나타났다.

국외의 경우 러·우전쟁의 여파로 인해 공공/정부를 대상으로 한 국가 간 사이버 공격이 지속되면서 가장 높을 비율을 차지했다.

## 유형별 침해사고 발생 통계




[2022 년 유형별 침해사고 발생 통계]

2022 년 유형별 침해사고 발생 통계를 살펴보면 악성코드 감염이 32%, 중요정보 유출이 29%, 피싱/스캠이 20%를 차지했다. 그 외 시스템 장악이 16%, 공급망 공격이 2%로 뒤를 이었다.

악성코드 감염으로 인한 침해사고 발생이 가장 높은 비율을 차지한 것은 특히 국내 기업을 타깃으로 한 귀신(GWISIN) 랜섬웨어의 영향이 크다. 귀신(GWISIN) 랜섬웨어는 국내 기업 내부에서 사용하는 통합 관리 솔루션 및 보안 정책을 악용했으며, 3 중 협박을 통해 피해를 가중시켰다. 또한, 2021 년 12 월 말에 등장한 Log4j 취약점을 비롯해, 알려진 취약점을 이용한 악성코드 배포 역시 활발히 일어났다.

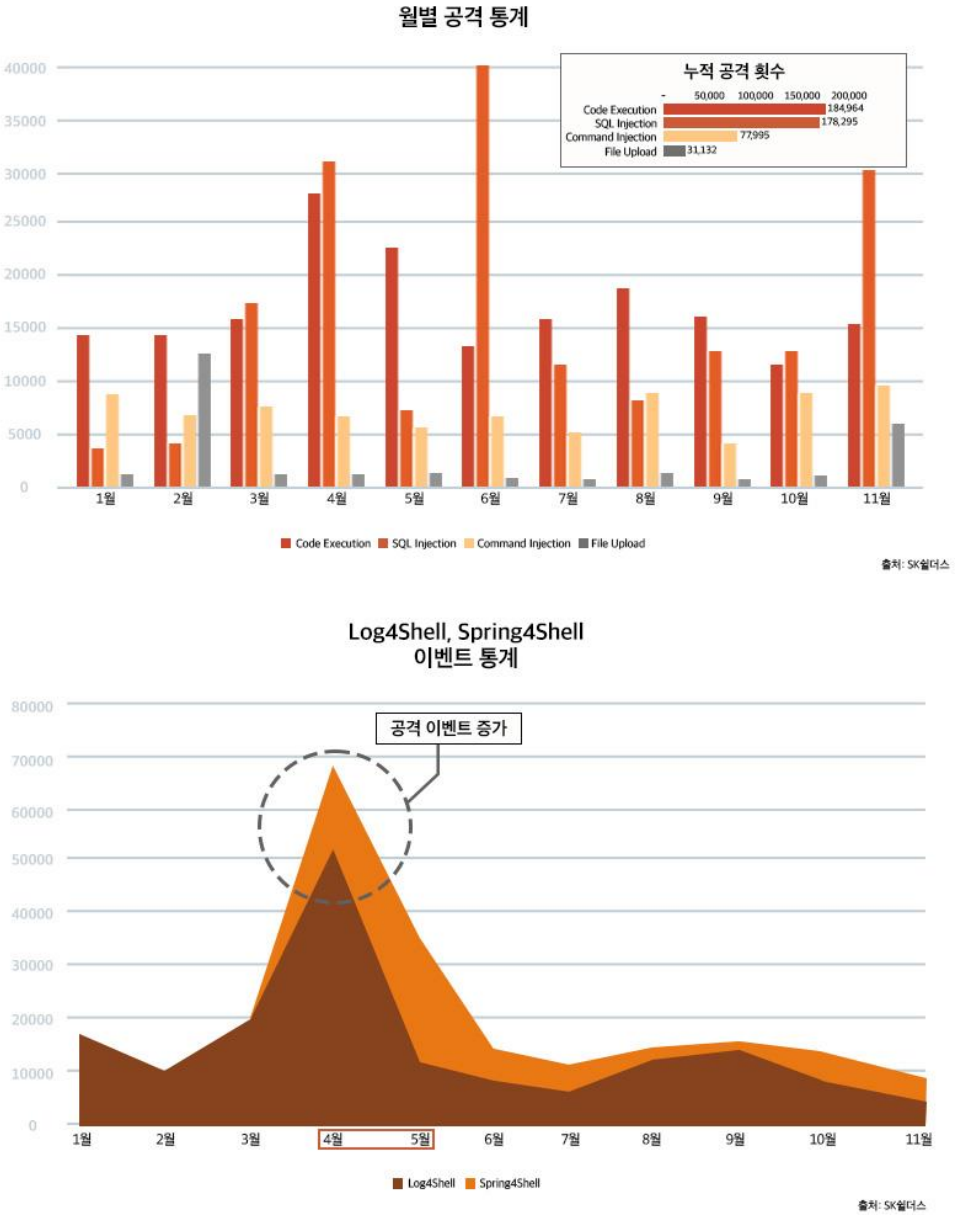
악성코드 감염 다음으로 중요 정보 유출이 29%의 비율을 차지했다. 해킹그룹 랩서스(Lapsus$)가 국내외 기업에 대한 공격에 성공하여 기밀정보를 탈취하는 사례가 있었으며, 개인 및 기업 정보를 노리는 정보 유출형 악성코드 인포스틸러[3]가 기승을 부렸다. 탈취한 정보를 2 차 공격에 활용하거나 다크웹과 같은 블랙마켓을 통한 개인정보 거래가 활성화되고 있어 주의가 필요하다.

피싱/스캠[4]의 비중이 상반기 대비 4%가량 증가한 것을 볼 수 있다. 올 한 해, 사회적 이슈를 악용한 피싱/스캠이 증가했으며 이를 통해 획득한 크리덴셜은 2 차 공격에 악용이 가능하다. 출처가 불분명한 URL 을 의심하고 접근하지 않도록 개인 및 기업은 피싱 공격에 대한 각별한 주의가 필요하다.

[3] 인포스틸러(InfoStealer): 사용자 계정 정보, 가상화폐 지갑 주소, 파일 등을 탈취하는 정보 유출형 악성코드

[4] 스캠(SCAM): 기업 이메일 정보를 해킹해 거래처 등으로 둔갑시켜서 거래 대금을 가로채는 해킹 수법

## 주요 공격 이벤트 통계(1)

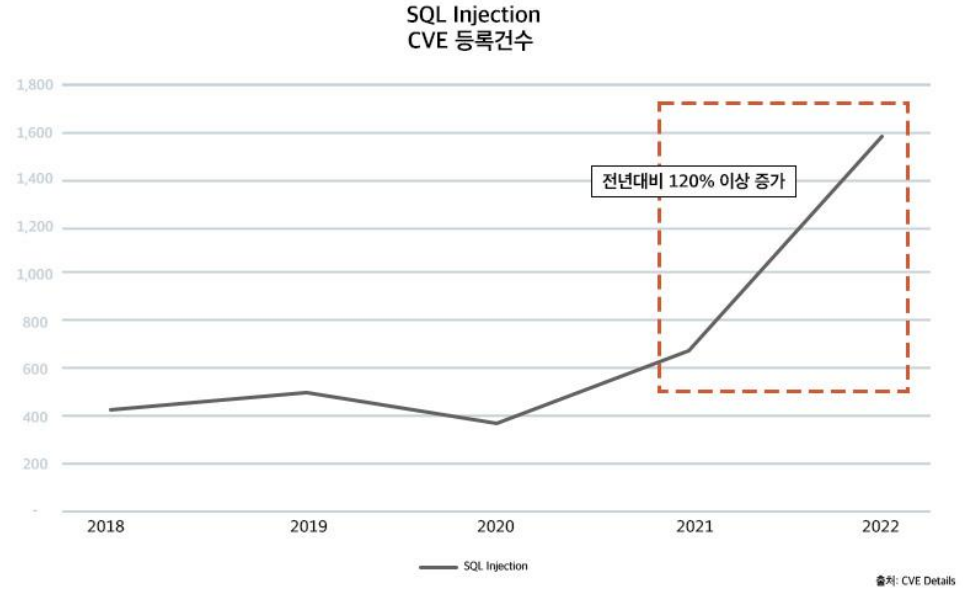


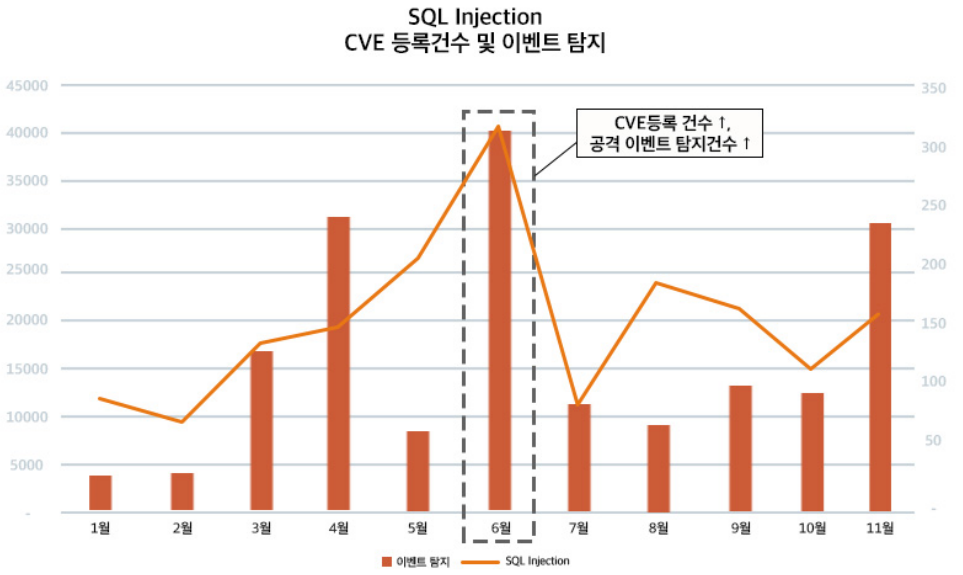

[2022 년 주요 공격 이벤트 통계(1)]

올해는 공격자가 입력한 코드 실행이 가능한 취약점인 Code Execution이 18만 건으로 가장 많이 집계되었으며, 웹 취약점인 SQL Injection이 17만 건으로 뒤를 이었다. 또한 운영체제에 임의의 명령을 실행하는 Command Injection이 7만 건, File Upload가 3만 건으로 집계되었다.

Code Execution 이벤트는 라우터 취약점 또는 PHP, Apache 의 프레임워크 등의 알려진 취약점을 이용한 공격이 주를 이뤘다. 특히 올해 이슈가 되었던 Log4Shell 과 Spring4Shell 의 연간 공격이 꾸준히 발생한 것을 볼 수 있다. 지난해 12 월 말부터 이어진 Log4Shell 공격은 올해 들어 점차 감소하는 추세를 보였으나, Spring4Shell 이 등장한 3 월 이후 공격이 증가한 것을 볼 수 있다. 이로 인해 4 월, 5 월에 공격 이벤트가 증가했으며, 이후에는 두 공격 모두 감소하는 추세를 보였다. 파급력이 크고 이슈가 되었던 취약점이 현재까지도 활발히 공격에 이용되고 있는 만큼 지속적인 관심이 필요하다.

## 주요 공격 이벤트 통계(2)



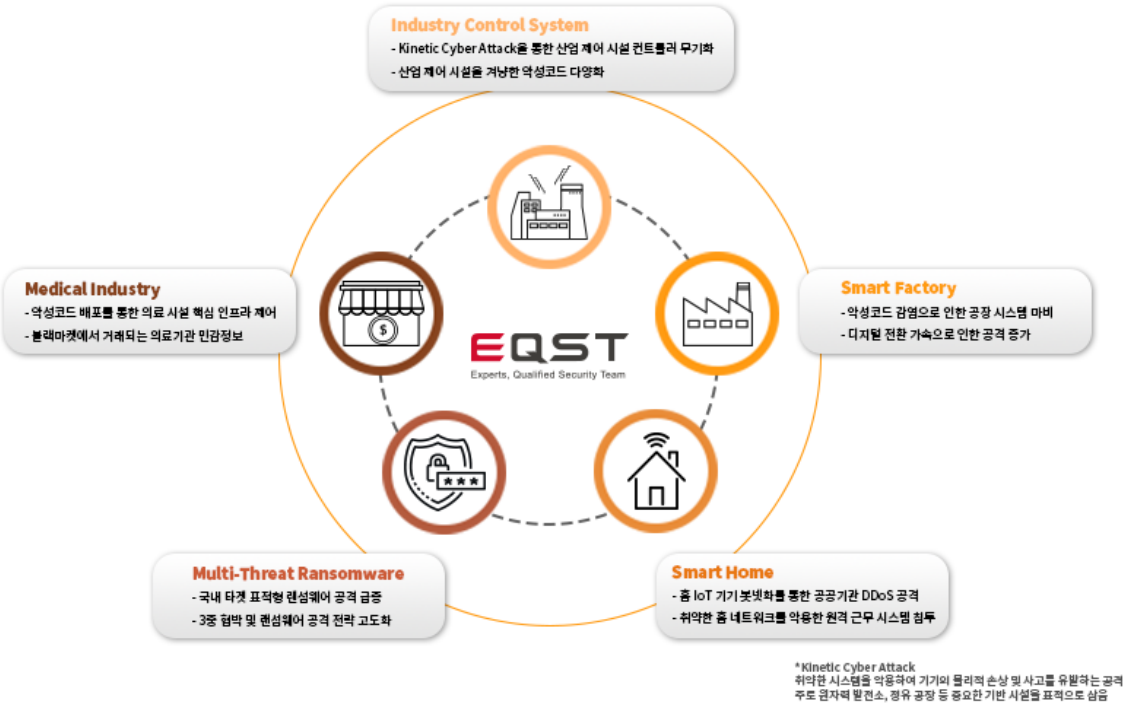

[2022 년 주요 공격 이벤트 통계(2)]

2022 년 누적 공격 이벤트 탐지 횟수가 두 번째로 높았던 SQL Injection 의 경우, CVE 에 등록된 취약점 건수는 2021 년 741 건에서 2022 년 1,678 건으로 집계되어 전년 대비 120% 이상 증가했다. 또한, 등록건수는 6 월 313 건으로 가장 높았으며, 공격 이벤트 역시 39,970 건으로 가장 많이 탐지되었다.

CVE Detail 사이트를 통해 SQL Injection 의 2022 년 CVE 등록 정보를 조회한 결과, CMS(Content Management System, 콘텐츠 관리 시스템)와 같은 시스템에서 발견된 SQL Injection 이 가장 많았다. 또한 WordPress, Django, ZenDesk, SonicWall 등 다수의 프레임워크 및 소프트웨어에서 SQL Injection 취약점이 발견되었다.

특히 올해 6 월에는 환자 기록 관리 시스템, 자동차 예약 관리 시스템 등 각 시스템에 있는 하위 페이지에서 SQL Injection 이 연달아 발견되면서 CVE 등록건수가 가장 높게 나타났다. 따라서 구성한 시스템의 취약점 정보에 주의하여 시스템을 운영해야 한다. 또한, PHP 오픈소스 소프트웨어나 WordPress 의 다양한 플러그인에서도 SQL Injection 취약점이 자주 발견되고 있으므로 사용 시 주의가 요구된다.

## 2022년 보안 이슈 리뷰




[2022 년 보안 이슈 Review]

Industry Control System 부분에서는 Kinetic Cyber Attack 의 위험성이 수면 위로 드러난 해였다. Kinetic Cyber Attack 이란, ICS 를 통해 물리 장치를 직접 조작하여 물리적 손상 및 사고 등의 재난을 야기하는 공격이다. 한 해킹 그룹은 이란의 대형 철강회사인 '모바라케'와 '후제스탄' 공장에서 Kinetic Cyber Attack 을 이용해 화재를 일으켰다고 주장하며 발화 장면이 촬영된 CCTV 영상을 공개하기도 했다.

또한, 산업 제어 시스템을 겨냥한 악성코드가 계속해서 등장하고 있다. 해당 악성코드들은 산업 제어 시스템에 기기 가동 중지, 안전 제어 시스템 비활성화 등을 명령해 기기 파괴, 인명 손실 등을 야기할 수 있는 기능을 포함하고 있어 주의가 필요하다.

Smart Factory 부분에서는 3 월 초 도요타자동차의 협력사가 랜섬웨어에 감염되어 도요타자동차의 생산 공장 전체가 가동 중단된 사실이 알려졌다. 도요타자동차에 부품을 납품하는 코지마프레스공업사가 '로빈 후드'로 추정되는 해커 집단에게 공격당해 랜섬웨어에 감염되었고, 사내 시스템이 마비되어 부품 생산이 중단되었다.

Smart Home 부분에서는 Smart Home 내부의 IP 카메라를 해킹하여 사생활을 촬영하고, 이를 판매한 정황이 포착되었다. 해킹 프로그램을 다운받아 7,000 대가 넘는 카메라 해킹에 성공해 불특정 다수의 영상을 촬영한 것이 확인되었다.

또한, Smart Home 내부의 IoT 기기들을 악성코드에 감염시켜 봇넷으로 활용하는 사례들이 보고되었다. 공격자는 감염된 봇넷들을 경유지로 사용하여 수사망에 혼란을 주거나, 봇넷들을 이용해 국가기관/공공기관 등에 DDoS 공격을 진행했다.

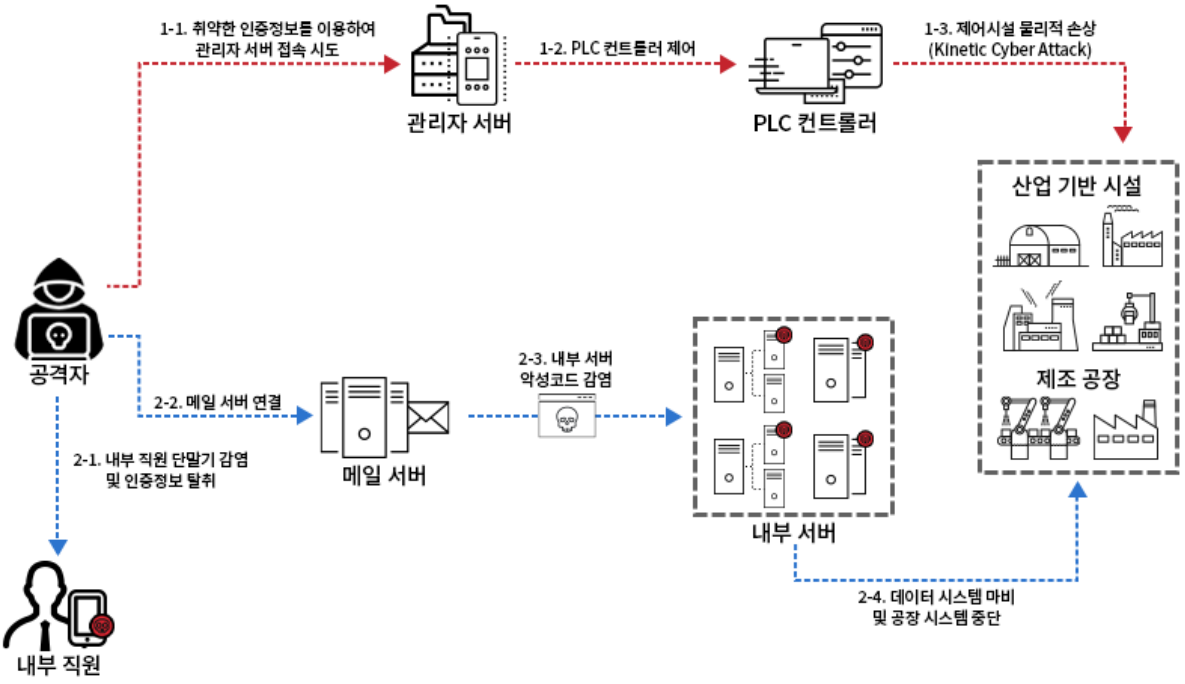
재택근무자들을 대상으로 한 피싱 공격도 꾸준히 발생했다. 공격자는 공유기를 공격해 관리자 권한을 획득하고, 공유기를 거점 삼아 홈 내부의 업무용 기기들에 대한 2 차 공격을 진행하여 회사 VPN 계정을 획득하거나, 중요 문서들을 탈취했다.

2021 년에는 약 2 억 5 천만 가구에서 스마트 홈을 사용했으며, 2023 년에는 스마트 홈이 약 3 억 5 천만 가구까지 늘어날 것으로 예측되어 스마트 홈을 대상으로 한 해킹 시도는 앞으로도 계속 발생할 전망이다.

Multi-Threat Ransomware 부분에서는 다양한 전략과 탐지 회피 기법을 적용한 랜섬웨어가 등장했다. 올해 가장 큰 이슈가 되었던 'GWISIN(귀신)' 랜섬웨어는 이벤트 로그 삭제, 안전모드 부팅 등 다양한 회피 기법을 적용했으며, 복호화 키 제공 여부, 중요 정보 유출 협박, 취약점 리포트 제공에 대한 3 중 협박 전략을 통해 피해자를 위협했다. 또한, 실행 시 필요한 키 값과 랜섬노트에 피해 기업명을 사용하고, 수사 기관, 정보보호 관리체계 기입 등 철저한 사전 조사를 통해 공격을 시도한 것으로 확인되어 국내 기업들을 두려움에 떨게 했다. 이 뿐만 아니라 LockBit 3.0 을 포함하해 Phobos, Magniber, Masscan 등 다양한 랜섬웨어 그룹들이 불특정 다수 또는 기업을 타깃으로 표적 공격을 시도하고 있어 랜섬웨어에 대한 공격과 피해를 경감하기 위해서는 지속적인 관심과 보안 대책이 필요하다.

Medical Industry 부분에서는 피싱 메일을 통해 계정을 획득하여 의료 시스템에 접근하는 공격이 발생했다. 공격자는 내부 서버에 접근한 뒤 개인 정보뿐만 아니라 의료 정보, 연구 자료 등을 빼돌려 블랙마켓에 판매했다. 또한, 내부서버 침투 및 의료 시스템에 악성코드를 배포해 의료 인프라를 마비시키고, 의료 서비스가 원활하게 제공되지 못하도록 했다.

## 스마트 팩토리 공격 시나리오




[스마트 팩토리 공격 시나리오]

최근 디지털 전환이 가속화됨에 따라 시설 관리를 효율화하고 있고, 생산력을 극대화하기 위한 스마트 팩토리가 늘어나고 있다. 올해도 이를 노린 사이버 공격이 꾸준히 발생했으며, 대표적인 공격 사례는 다음과 같다.

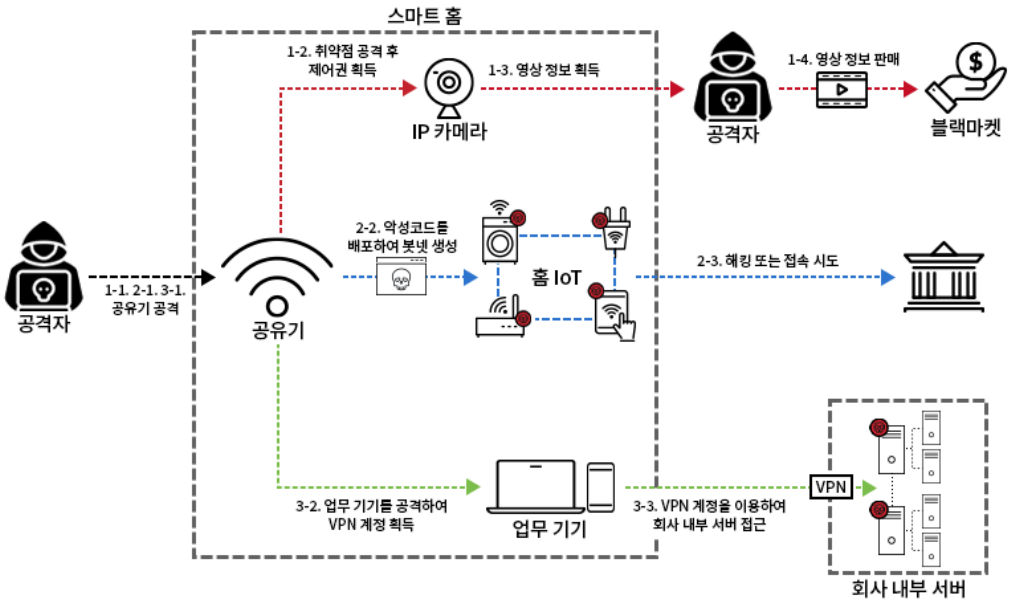
첫 번째 시나리오는 PLC 컨트롤러 제어를 통한 산업 기반 시설 마비 시나리오이다. 공격자는 취약한 인증정보를 이용하는 산업 제어 시스템 관리자 서버에 접속을 시도한다. 이후, 관리자 서버에 연결되어 있는 PLC 제어권을 획득하고, 이를 악용하여 산업 기반 시설에 물리적인 손상을 일으켜 화재나 인재 사고 등을 유발시킨다.

두 번째는 악성코드 감염을 통한 데이터 시스템 마비 시나리오이다. 공격자는 내부 직원의 단말기를 감염시키고 인증정보를 탈취하여 메일 서버에 접속하는 것으로 시작한다. 메일 서버를 통해 연결된 내부 서버에 접속한 공격자는 악성코드를 감염시켜 데이터 시스템 마비 및 공장 시스템 중단 등의 피해를 발생시킨다.

단순히 시스템 내 취약점을 이용한 사이버 공격에서 그치지 않고, 공장 내 기기에 물리적 손상을 일으켜 직접적인 사고로 이어질 수 있다.

따라서 스마트 팩토리를 겨냥한 보안 위협이 확대되는 만큼 보안솔루션 구축, 지속적인 모니터링 등 OT/ICS 영역 보안에 신경 써야 한다.

## 스마트 홈 공격 시나리오




[스마트 홈 공격 시나리오]

첫 번째 시나리오는 해커가 홈 내부 IP 카메라의 취약점을 공격해 제어권을 탈취하는 시나리오다. 공격자는 제어권을 획득한 IP 카메라를 이용하여 개인의 사생활 영상을 획득한 후 이를 블랙마켓에서 금전을 받고 판매한다.

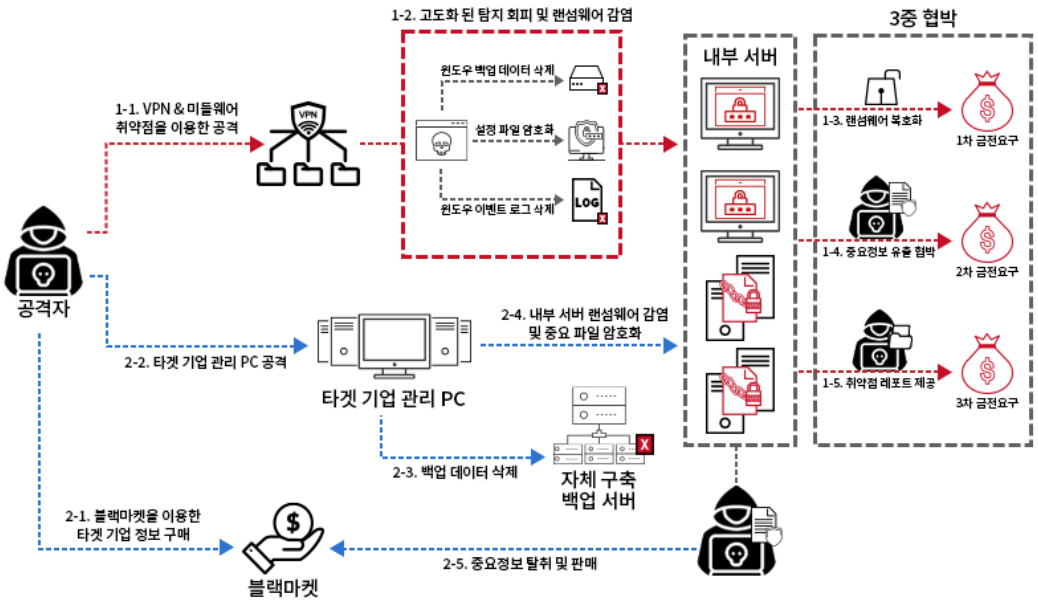
두 번째 시나리오는 홈 내부의 IoT 기기들에 악성코드를 배포해 봇넷을 생성하는 시나리오다. 2021 년 하반기부터 현재까지 IoT 기기들을 대상으로 악성코드를 배포하여 봇넷으로 만든 정황이 지속적으로 발견되었다. 공격자는 봇넷에 감염된 IoT 기기들을 이용하여 DDoS 등의 공격을 수행할 수 있다.

세 번째는 홈 내부의 업무 기기들을 대상으로 한 공격 시나리오다. 원격 근무지의 공유기를 해킹한 후, 연결된 업무 기기들을 대상으로 공격을 진행해 회사 VPN 계정을 탈취한다. 이후 해당 계정을 이용하여 회사 내부 서버로 2 차 공격을 수행한 뒤 기밀정보를 탈취한다.

스마트 홈의 공격 거점은 공유기가 되는 경우가 많으므로, EOS[5]가 된 공유기들은 최신 기기로 교체하고, 주기적인 펌웨어 업데이트를 통해 공격에 미리 대비해야 한다.

[5] EOS(End Of Service): 업데이트 서비스가 종료된 제품

## 랜섬웨어 공격 시나리오




[랜섬웨어 공격 시나리오]

랜섬웨어는 다양한 전략과 회피 기법을 사용하여 고도화되고 있으며, 지능화된 공격으로 진화하고 있다.

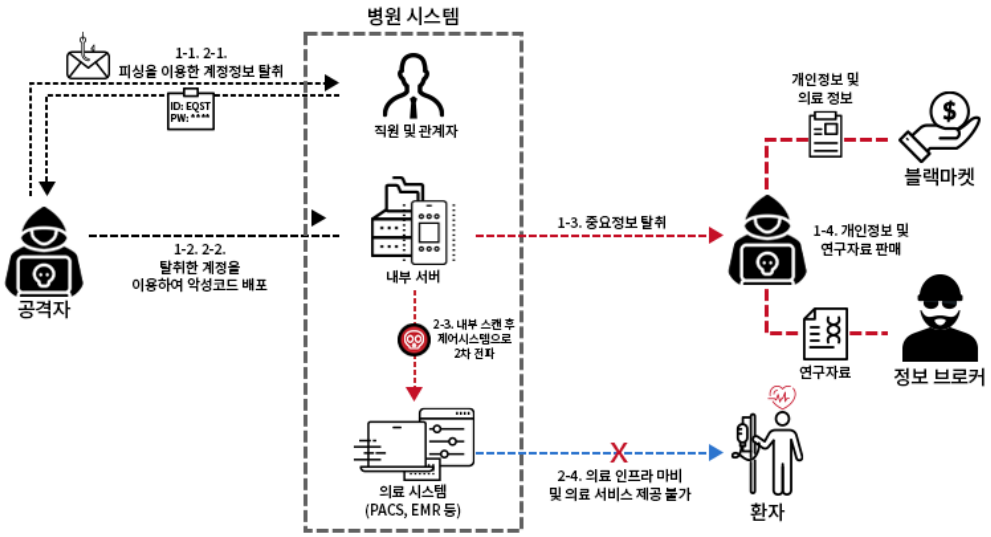
첫 번째 시나리오는 VPN, 미들웨어 등의 취약점을 이용해 내부 서버에 랜섬웨어를 감염시킨다. 탐지를 회피하기 위해 설정 파일 암호화, 이벤트 로그 삭제 등 다양한 기법을 이용하며, 복호화 키를 대가로 금전을 요구하는 데서 그치지 않고, 탈취한 중요 정보 유출 협박, 취약점 리포트 제공, 총 3 단계에 걸쳐 협상을 진행하는 3 중 협박 전략을 통해 피해자를 협박한다.

두 번째 시나리오는 최근에 성행했던 기업, 기관을 타깃으로 한 표적형 랜섬웨어 공격 시나리오다. 블랙마켓, 피싱 등을 통해 타깃 기업을 공격하기 위한 사전 정보를 수집하고, 이를 이용하여 타깃 기업의 관리 PC 에 접근한다. 공격자는 일차적으로 암호화된 데이터의 복구를 막기 위해 백업 데이터를 파괴시키고, 이후 내부 서버에 랜섬웨어를 유포해 감염된 서버 내 중요 정보들을 탈취 및 암호화한다. 탈취한 중요정보는 블랙마켓에 다시 판매하여 악순환이 반복된다.

계속해서 진화하는 랜섬웨어에 대한 공격과 피해를 경감하기 위해서는 내부 네트워크와 인프라 자산에 대한 관리가 체계적으로 이뤄져야 하며, 망 분리가 적용된 보안 백업 솔루션을 이용해 정기적으로 데이터를 백업하면서 내부 데이터를 보호해야 한다.

또한, 랜섬웨어 최신 트렌드와 공격 동향을 이해하고 이에 맞는 적극적인 사전 예방이 필요하다. 랜섬웨어 대응 민간 협의체 KARA 에서는 최신 랜섬웨어 트렌드를 분석하고 공격 전략과 대응 방안을 담은 랜섬웨어 동향 보고서를 발표하고 있다.

## 의료시설 공격 시나리오




[의료시설 공격 시나리오]

2021 년에 이어 2022 년에도 피싱을 통해 의료산업 관계자들의 계정을 탈취하고 내부망으로 접속해 악성코드를 배포하는 방식의 공격이 성행했다.

첫 번째 시나리오는 의료 정보 및 연구 자료를 탈취해 블랙마켓에 판매하는 시나리오다. 해커는 피싱을 통해 획득한 내부 관계자 계정을 이용하여 내부 서버를 공격한다. 서버 제어권을 획득한 공격자는 환자들의 개인정보 및 의료 정보를 탈취하여 블랙마켓에 판매하고, 연구 자료를 탈취한 후 정보 브로커에게 판매해 수익을 챙긴다.

두 번째 시나리오는 의료 시스템 악성코드 감염 시나리오다. 내부 서버에 접근한 공격자는 내부 스캔을 통해 PACS, EMR 등의 의료 시스템에 악성코드를 감염시킨다. 악성코드로 인해 의료 시스템이 마비되고, 이로 인해 환자들에게 의료 서비스를 제공하지 못하게 된다.

의료 산업의 경우 악성코드 감염이 환자들의 생명과 직결될 수 있으므로, 직원 및 관계자들은 피싱 메일이나 메세지에 특히 주의하여 계정 노출 및 악성코드 감염을 예방해야 한다.

# 2023년 5대 사이버 위협 전망 및 대응 전략


[2023년 사이버 위협 전망]

## 지능화/다변화하는 랜섬웨어 공격과 전략

- 3 중 협박, 유포 방식의 다양화, 국내 타깃형 랜섬웨어, 데이터 파괴형 랜섬웨어

서비스형 랜섬웨어(Ransomware-as-a-Service)의 출현 이후 랜섬웨어 이슈는 좀처럼 수그러들지 않고 있다. 대부분의 공격자 그룹은 기존에 사용하던 전략과 본인들의 노하우, 기술, 경험을 바탕으로 타깃을 모색해 공격을 진행하는 것이 일반적인 공격과 전략이다.

그러나 올해 랜섬웨어 그룹들의 양상을 살펴보면, 국내 기업을 타깃으로 한 귀신(GWISIN) 랜섬웨어를 비롯해, 데이터 파괴를 통해 목적을 이루고자 하는 Azov, BlackCat(Alphv) 그룹의 ExMatter 정보 유출 툴의 변화, 데이터 베이스 서버의 취약점을 노린 Globelmposter, Mallox(Fargo), Masscan 랜섬웨어 등 생존을 위해 기존과는 다른 전략과 공격 방식을 선택한 랜섬웨어 그룹들이 증가하고 있다. 이로 인해 피해를 입는 기업 역시 증가하고 있다.

또한, 국내에서 유포 중인 Magniber 랜섬웨어는 짧은 기간 동안 '.msi', '.cpl', '.jse', '.js', '.wsf' 등 다양한 포맷으로 유포 방식을 빠르게 변경하고 인젝션, UAC 우회 등 탐지를 우회하여 더 많은 피해를 입히기 위해 다양한 변화를 시도하고 있다.

2023 년에는 이보다 더욱 진화한 전략과 공격 방식을 선택하는 랜섬웨어 그룹들로 인해 피해가 증가될 것으로 전망된다.

## PhaaS(서비스형 피싱 공격, Phishing-as-a-Service)의 유행

- 새로운 형태의 피싱 플랫폼으로 범죄의 진입장벽이 낮아졌다.

다크웹에서 'Caffeine'이라고 불리는 피싱 판매 사이트가 발견되면서 최근 PhaaS(Phishing-as-a-Service)가 유행하고 있다. 'Caffeine'은 다크웹이 아니더라도 일반적인 검색 엔진을 통해 쉽게 접근이 가능하고, 서비스 이용에 이메일만 요구되고 있어 피싱 범죄에 대한 진입 장벽이 현저하게 낮아졌다.

또한 다크웹을 통해 맞춤형 피싱 사이트를 제작할 수 있다. 판매자는 제작에 필요한 세부정보를 받아 구매자가 원하는 형태의 피싱 사이트를 제작한다. 이는 기존과 달리 타깃층을 선정하거나 특정 서비스를 사칭할 수 있다는 점에서 더욱 위험성이 있다.

위와 같은 사례 외에도 피싱에 사회적 이슈를 통한 사회 공학적 기법을 응용하고, AI 를 통한 스팸 메일 필터링 우회 등 AI 기술을 활용한 고도화된 피싱이 등장하고 있어 내년에도 다양한 피싱 공격이 지속적으로 발생할 것이라고 전망된다.

## 슈퍼앱 활성화를 악용한 모바일 대상 공격 증가

- 모바일 위협의 고도화

일상생활에서 모바일 기기는 더 이상 떼어놓을 수 없을 만큼 사용 영역이 넓어지고 기능이 다양해졌다. 은행, 메신저, SNS 등의 서비스를 각각의 앱으로 이용했던 이전과 달리, 슈퍼앱의 등장으로 한 개의 앱으로 다양한 서비스를 한 번에 이용할 수 있게 되었다. 그러나, 한 개의 앱에 여러 기능을 합치는 과정에서 검증 프로세스가 누락되거나 권한 관리에 허점이 생기면서 침해사고가 발생할 수 있다. 또한, 같은 기능을 하는 기존의 앱들을 삭제하고, 슈퍼앱을 새로 설치하는 과정을 노리는 슈퍼앱을 가장한 악성 앱들이 기승을 부릴 수 있다.

슈퍼앱 뿐만 아니라 제로클릭 공격과 같이 기존의 방어 전략을 무너뜨리는 고도화된 모바일 위협이 등장함에 따라 모바일 기기를 노린 공격은 계속될 것이라고 전망된다.

제로클릭 공격은 일반적인 피싱 공격과 다르게 이메일 또는 문자 메시지에 포함된 링크를 클릭하지 않아도 악성코드에 감염될 수 있는 공격이다. 제로클릭 공격의 예시로는 문자메시지에 GIF 파일로 위장한 악성코드를 전송해 피해자가 문자메시지를 읽기만 해도 코어그래픽스 라이브러리에 의해 악성코드가 실행되는 방법이 있다.

## OT/ICS 를 비롯한 산업 전반에 걸친 무인화

- 무인화/자동화만이 능사는 아니다.

임금 문제, 안전 문제를 포함한 다양한 이유로 업종을 불문하고, 산업 전반에 걸쳐 자동화와 무인화가 이뤄지고 있다. 또한, 2019 년에 발생한 코로나로 인해 언택트(Un-tact) 문화가 확산되면서, 키오스크를 사용하는 무인 매장이 늘어나고 있다. 우후죽순 생겨나는 무인화/자동화 기기는 언제든지 공격자의 타깃이 될 수 있으므로, 관심과 주의가 필요하다.

무인화 기기는 일반적으로 경량화된 하드웨어를 사용하며, 그만큼 사용 가능한 운영체제에 제한이 생겨 취약한 버전의 운영체제를 사용할 가능성이 높다. 업데이트를 지원하지 않는 EOS(End of Service) 운영체제를 사용하거나, 보안 업데이트가 되어 있지 않은 취약한 버전의 운영체제를 사용할 경우 개인정보 유출 피해를 입거나 봇넷으로 사용될 위험이 있다.

산업 시설에서는 다양한 장비를 사용하기 때문에 일원화되지 않은 프로토콜 사용 및 자산 관리의 미흡, 24 시간 365 일 운영되는 설비 등의 이유로 버전을 최신으로 유지하는 것이 쉽지가 않다. 따라서 공격자는 이를 이용해 취약한 산업 시설에 접근해 랜섬웨어 감염 등의 공격을 진행할 수 있다.

위와 같이 최신 업데이트가 쉽지 않은 곳들이 다수 존재한다. 이러한 문제들이 해결되지 않으면, 2023 년에도 피해가 지속적으로 이루어질 것이라고 전망된다.

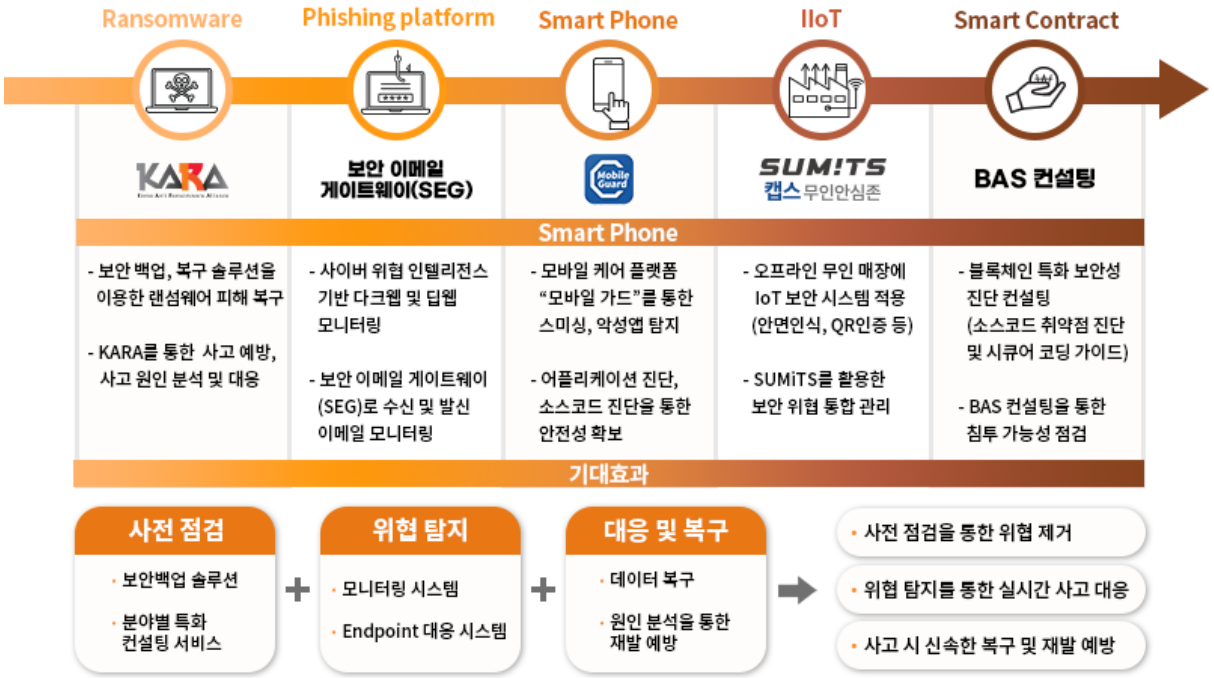
## DeFi 의 등장으로 가상자산 타깃 공격 급증

- 21 년 대비 피해 건수는 줄었으나, 피해액은 비슷한 규모로 나타났다.

2022 년 현재까지 가상자산은 약 130 건 총 4 조 3 천억 원 규모의 피해를 입었다. 또한, 세계 최대 가상화폐 거래소인 B 社에서도 약 8 천억 가량의 피해를 입은 것으로 파악되었다. 2022 년 10 월 기준 총 피해액이 작년과 비슷한 것으로 보아 올해 피해액은 역대 최대를 기록할 것으로 보인다.

이러한 피해가 발생한 원인으로는 Decentralized Finance, 줄여서 DeFi(탈중앙화 금융)의 등장이 원인인 것으로 파악된다. 블록체인 분석 기업 체이널리시스(Chainalysis)에 따르면 2022 년 8 월 10 일 기준 올해 발생한 가상자산 피해 중 69%가 DeFi 플랫폼에서 사용하는 크로스체인 브릿지에서 발생한 것으로 파악했다. 또한, 올해 발생한 상위 5 개의 크로스체인 브릿지 피해액이 전체 규모의 대부분을 차지한다는 점이 DeFi 로 인해 피해가 발생했다는 의견을 뒷받침해 준다.

## EQST 5 대 위협 대응 전략




[EQST그룹 사이버 위협 대응 전략 및 서비스]

랜섬웨어는 사전 점검을 통해 감염되지 않도록 예방해야 하며, 관제 및 모니터링 솔루션을 통해 실시간으로 대응할 수 있어야 한다. 또한, 사고 시 침해사고 분석, 보안 백업을 통한 데이터 복구, 협상 등 적절한 대응이 필요하다.

SK 쉴더스에서는 랜섬웨어 대응 센터(1600-7028)와 KARA 협의체를 통해 사전/사후 랜섬웨어 대응 서비스를 제공하고 있다.

다크웹 및 딥웹 모니터링을 통한 위협 대비, 보안 이메일 게이트웨이(SEG)를 사용한 수신/발신 모니터링으로 피싱 공격을 예방할 수 있다. SK 쉴더스는 악성 이메일 모의 훈련을 통해 임직원들의 피싱 예방 훈련을 제공하고 있다.

스마트폰 해킹 분야의 보안대책으로는 자사 모바일 케어 플랫폼 '모바일가드'를 통해 스미싱, 악성 앱을 탐지할 수 있다. SK 쉴더스 화이트해커 그룹인 'EQST'는 어플리케이션 및 소스코드 진단을 통한 컨설팅을 제공하고 있다.

IIoT 위협의 보안대책으로는 보안 플랫폼(안면 인식, QR 인증 등)이 있다. 이를 통해 무인 매장에 대한 보안을 더욱 강화할 수 있다. SK 쉴더스는 무인 경비로 24 시간 영상 보안을 제공하고 있으며 무인 매장에 필요한 솔루션들을 통합 제공하는 '캡스 무인안심존'도 제공하고 있다.

또한, SK 쉴더스가 자체적으로 개발한 '써미츠(SUMiTS)'는 사이버보안 및 물리보안 역량이 결합된 지능형 융합보안 플랫폼으로, 산업안전/건물관리 등의 분야에 활용된다. 사업장 특성에 따라 복합적으로 발생될 수 있는 위협 요소를 제거하고 EQST 에서 검증한 전문적인 보안 가이드 컨설팅을 제공한다.

가상자산의 경우 소스코드 진단 및 시큐어 코딩 가이드를 통한 블록체인 특화 보안성 진단 컨설팅으로 피해를 예방할 수 있으며, BAS(Breach Attack Simulation) 시나리오 해킹 시뮬레이터를 통해 침투 가능성을 점검할 수 있다.

기업들은 SK 쉴더스가 제시한 2023 년 5 대 보안위협에 대한 보안대책을 참고하여, 사전 점검, 위협 탐지, 대응 및 복구 프로세스를 통한 체계적인 관리를 함으로써 피해를 최소화할 수 있다. 다가오는 사이버 위협에 대비해 보안성을 강화하는 데 도움이 될 수 있을 것이다.

## KARA (Korea Anti Ransomware Alliance)


[랜섬웨어 대응 협의체 KARA]

SK 쉴더스에서는 24 시간 365 일 랜섬웨어 대응센터를 운영 중이며, 사고 접수부터 원인 파악, 피해 복구, 협상 배상, 재발방지 대책 등 랜섬웨어에 대응하기 위한 모든 절차를 컨설팅하고 있다.

그리고, SK 쉴더스의 주도로 트렌드마이크로코리아, 지니언스, 베리타스코리아, 맨디언트코리아, 에스투더블유(S2W), 캐롯손해보험, 법무법인 화우, 총 8 개사가 협력하여 랜섬웨어 대응 협의체 KARA 를 구성했다. KARA 는 각 분야 전문 기업들이 랜섬웨어 최신 트렌드 및 피해 실태와 관련하여 정기적인 정보를 공유하고, 이를 통해 사고 접수와 대응, 복구, 대책까지 원스톱으로 대응하는 프로세스를 제공하고 있다.

또한, 계속해서 고도화되고 있는 랜섬웨어의 공격 동향을 이해하고 적극적인 사전 예방을 할 수 있도록 최신 랜섬웨어 트렌드를 분석하고 공격 전략과 대응 방안을 담은 랜섬웨어 동향 보고서를 발간하고 있다.

KARA 는 앞으로도 분석 내용을 바탕으로 정기적인 세미나, 대외 홍보활동을 이어 나갈 예정이며, 랜섬웨어 그룹 및 최신 랜섬웨어를 주기적으로 분석하여 랜섬웨어 통합 대응 프로세스를 고도화해 나갈 예정이다.

※ SK 쉴더스 랜섬웨어 대응센터 : kara@sk.com, 1600-7028

## 맺음말

SK쉴더스에서는 IoT, 클라우드, 스마트 컨트랙트 등 새로운 ICT 분야 기술을 비롯해 지능화/다변화되고 있는 랜섬웨어에 대한 연구까지 지속적으로 진행하고 있다. 이러한 연구 결과를 바탕으로 보안 이슈를 분석하고, 발생 가능한 보안 위협에 대하여 대응 전략을 제시함으로써 급변하는 지능형 사이버 위협에 민첩하게 대응해 나갈 것이다.

랜섬웨어처럼 지속적으로 진화하는 사이버 공격 방식에 대응하기 위해서는 각자의 위치에서 적극적인 관심과 대처 또한 필요하다.

# EQST Annual Report

# 2022.12

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST그룹
제　작 : SK쉴더스 커뮤니케이션그룹