SK 쉴더스

EQST Annual Report

2022 보안 위협 전망 보고서

Contents

EQST insight

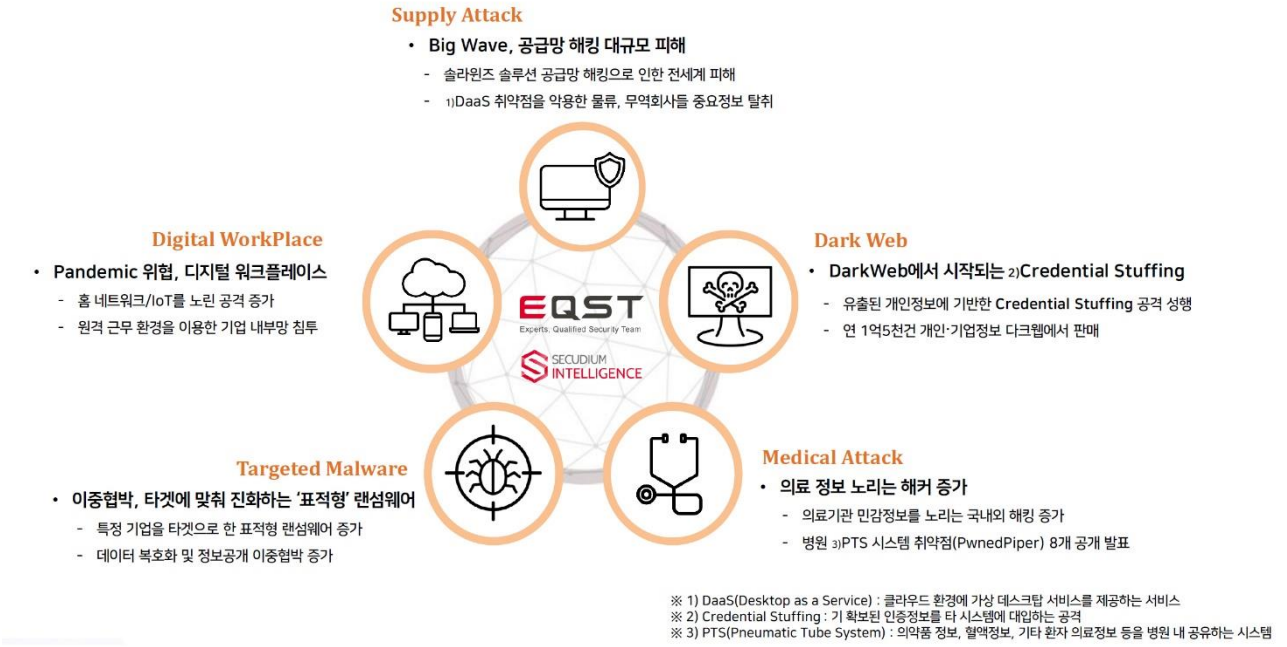
2021년 5대 보안 위협 리뷰

2021 년은 코로나 19 장기화에 따라 디지털 워크플레이스와 관련한 위협이 부각되는 해였다. 원격/재택근무가 활성화되면서 기업들은 외부에서 회사망을 접속할 수 있는 VPN(가상사설망)이나 DaaS(Desktop as a Service)와 같은 가상 데스크탑 서비스를 도입하기 시작했고, 해커들의 관심 또한 이러한 시스템에 집중되면서 관련 취약점을 이용한 공격 사례가 늘어났다.

또한, 중앙관리형 소프트웨어 취약점을 악용한 공급망 공격도 대두되었다. 작년 12 월 솔라윈즈에서 시작된 공급망 해킹은 미국의 각 정부부처 및 Major IT 기업까지 피해를 발생시켰고, 우리나라에서도 병원/대학/기관 등에서 관련 취약점을 이용하는 공격이 유행하였다.

이 외에도 의료 정보를 노리는 해커의 증가, DarkWeb 에 유출된 개인 정보를 활용한 Credential Stuffing, 고객 정보를 다량으로 가진 대기업이나 정부 기관에 대한 표적형 랜섬웨어 공격이 주를 이뤘다. 특히 랜섬웨어 공격의 경우 이전의 양상과는 다르게 데이터 몸값 외에 탈취한 정보 공개를 빌미로 추가 협박하는 이중 협박 사례가 증가되고 있다.

SK 쉴더스 인포섹의 화이트해커그룹 EQST(이큐스트)는 2021 년 발생한 정보 보안 이슈 및 침해사고 데이터, 고객사 컨설팅 수행 내역 등을 분석하여 2022 년 5 대 보안 위협을 전망하였다. 공격 현황 및 유형, 해킹 사고 사례 등을 통해 2021 년 주요 이슈를 상세히 알아보자.



[2021년 보안 이슈 Review]

먼저 첫 번째 주제로 **"Big Wave, 공급망 해킹 대규모 피해"**를 선정했다. 가장 큰 피해를 입힌 공급망 해킹 사례는 2020 년 12 월에 솔라윈즈 솔루션에서 시작된 해킹 사고로, MS 사를 포함한 전세계 30 만 고객 중 1 만 8 천 개 고객사가 피해를 입었다. 美정부 및 각 부처 대부분의 시스템도 공격을 피해갈 수 없었고, 미국 핵무기 비축량을 관리하는 NNSA 또한 피해 기관으로 지명되었다. 우리나라도 병원/대학/기관등에서 관련 취약점 스캔이 성행하였다.

이러한 공급망 해킹으로 카세야, 코드코브와 같은 여러 솔루션을 이용한 공격이 지속되었고, DaaS 취약점을 이용한 물류 및 무역회사들의 중요정보 탈취 사고로도 이어졌다. 관련 공격들은 연중 꾸준히 이슈가 되었으며, 피해 회사가 랜섬웨어 유포 경로로 악용되는 등 다수의 해킹 사고가 발생하였다.

두 번째는 **"DarkWeb 에서 시작되는 Credential Stuffing"**이다. DarkWeb 에서 유통되는 개인 정보, 기업 정보는 연 1 억 5 천 건으로, 개인이 사용하는 포탈이나 쇼핑몰 외에도 회사에서 사용하는 내부 시스템 침투에 활용하는 사례가 증가하고 있다. 회사 시스템 접속 이후에는 AD 나 SSO 등으로 통합 인증을 하기 때문에 별도의 추가 인증 없이 회사 내 주요 시스템에 접근이 가능하고, 이를 이용해 주요 기밀정보 탈취가 가능하다. 따라서 외부에서 회사 시스템에 접속할 경우 Two Factor 인증(이중 인증)을 도입하여 위협을 보완하는 추세다.

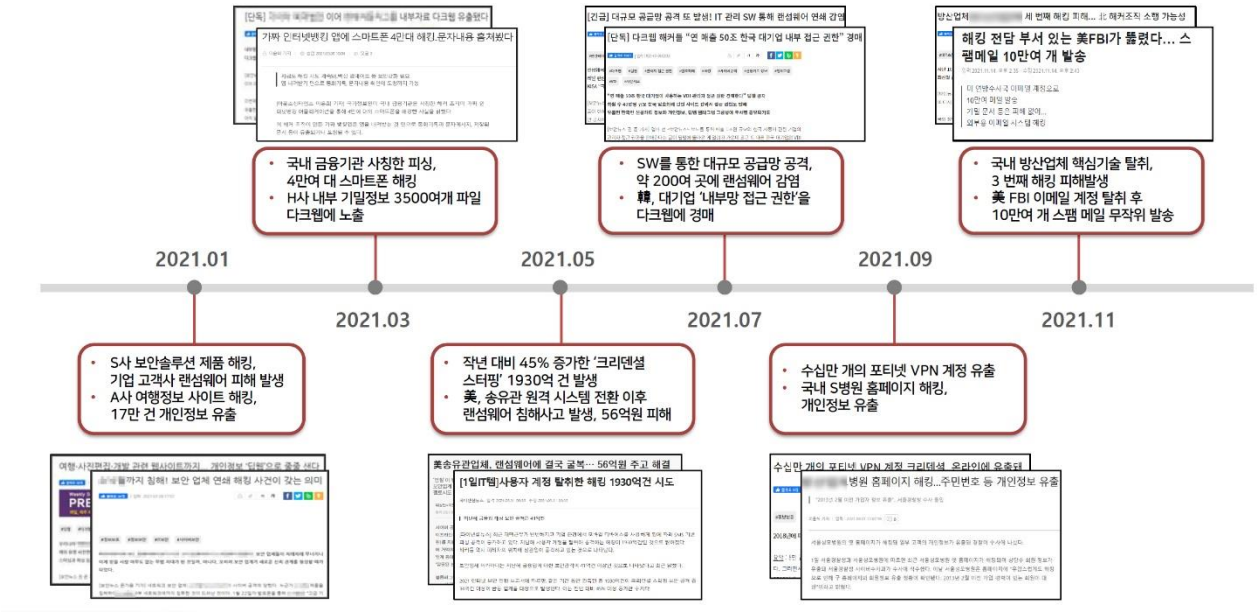
세 번째는 **"의료 정보를 노리는 해커 증가"**이다. 올해 8 월, 전세계 3000 여 개가 넘는 대형병원에서 표준처럼 사용되고 있는 PTS 에서도 취약점이 발견되었다. PTS 란 병원 내 의료정보(의약품 정보, 혈액정보, 기타 환자 의료정보 등)를 기압튜브로 공유하는 시스템으로, PwnedPiper 라는 취약점을 이용하면 비인가자가 다른 사람의 의료정보를 탈취할 수 있고 PTS 에 DDoS, 랜섬웨어 공격 등이 가능하다.

추가로 이전에는 사용자의 ID, PW, 주민등록번호가 해커의 주요 타깃이었다면 최근에는 개인의 의료기관 민감 정보까지 그 타깃이 확장되었다. 이를 반증하듯이 상급 종합병원 45 곳 중 38 곳의 계정 정보가 DarkWeb 에 판매되고 있고, 관련 해킹사고도 끊임없이 일어나고 있다.

네 번째는 **"이중협박, 타깃에 맞춰 진화하는 '표적형' 랜섬웨어"**이다. 과거 불특정 다수를 노린 랜섬웨어와 달리 특정 기업이나 기관을 타깃으로 한 표적형 랜섬웨어가 증가하고 있다. 주로 많은 고객 정보를 가진 대기업이나 정부 기관을 중심으로 제조업, 서비스업, 의료 분야 등 전방위 산업에 걸쳐 공격이 확대되고 있다. 대상을 타깃화하여 공격하는 랜섬웨어는 오랜 기간 기업에서 사용하는 시스템을 분석하여 해당 기업에 특화된 악성코드를 개발한다. 이를 이용하여 내부 시스템에 침투한 후 랜섬웨어를 내부망에 대량 유포하게 된다. 추가로 올해부터는 데이터 몸값만 요구하는 것이 아니라 탈취한 정보 공개를 빌미로 추가 협박하는 이중 위협 사례가 증가하고 있다.

다섯 번째는 **"Pandemic 위협, 디지털 워크플레이스"**이다. 코로나 19 장기화로 인해 재택근무로 전환한 기업이 늘어남에 따라 근무환경의 변화가 발생하였다. 기업들은 외부에서 회사망을 접속할 수 있는 VPN(가상사설망)이나 DaaS 시스템을 도입하였고, 해커들 관심 또한 이런 시스템에 집중되면서 관련 취약점을 이용한 공격사례가 늘어났다. 또한, 홈네트워크 및 IoT 를 노린 공격이 전년보다 3 배 폭증함에 따라 회사뿐만 아니라 개인 홈 네트워크 보안이 필요한 시대로 변화하고 있다.

2021 년 주요 보안 사고 리뷰



[2021년 주요 보안 사고]

올해 1 월, 네트워크 보안 업체를 비롯하여 IT 분야의 주요 보안 기업들이 연쇄적으로 해킹 피해를 입었다. 앞서 언급한 공급망 해킹기법을 이용해 내부 네트워크에 침투한 것으로 확인되었으며, 1 만 8 천 개의 고객사가 해킹 피해를 입으면서 엄청난 파급효과를 불러왔다. 이 사고 이후 카세야, 코드코브를 통한 추가 공급망 해킹이 발생하였다.

또한 여행 사이트를 비롯해 사진편집, 개발 분야 웹사이트들까지 해킹을 당해 개인 정보가 꾸준히 DarkWeb 에 유출되고 있는 것으로 나타났다. 유출된 정보는 연간 1 억 5 천 건이고 해당 정보를 사용하여 다른 웹사이트에 접속 시도하는 Credential Stuffing 공격이 이어지므로, 국내 인터넷 사용자의 계정이 매년 3~4 번씩은 유출된다고 볼 수 있다. 따라서 앞으로 중요 서비스들은 Two Factor 인증을 설정해서 보안을 강화시켜야 한다.

3 월에는 국내 이동통신사에 가입된 스마트폰 4 만여 대가 해킹 당한 사실이 포착됐다. 해커 조직은 국내 금융기관을 사칭한 가짜 인터넷뱅킹 앱을 통해 해킹을 진행했으며 악성앱이 설치된 사용자들의 통화기록, 문자메시지, 저장 문서 등을 가로채거나 통화를 도청한 정황도 포착됐다.

또한 국내 H 사 내부 기밀정보 3500 여 개 파일이 DarkWeb 에 노출되었다. 유출 자료에는 그룹 계열사들과 관련된 내부망 구조도와 보안 점검 보고서 등이 포함되어 있다. 이렇듯 국내 대기업들이 랜섬웨어 해커조직의 주요 타깃이 되면서, 이를 빌미로 돈을 요구하는 협박 행위가 끊임없이 이어지고 있어 국내 기업들의 핵심기술 유출 가능성도 커지고 있다.

5 월에는 美송유관업체가 해킹 당일 해커들에게 약 56 억을 지불한 것으로 드러났다. 보안업계 등에서는 "대형 인프라 시설을 타깃으로 한 추가 사이버 공격을 불러올 수 있는 '잘못된 선례'"라는 지적이 나왔다. 이와 같이 글로벌 해킹 범죄 조직의 랜섬웨어 공격은 갈수록 거세지고 있다.

이외에도 Credential Stuffing 공격으로 전 세계가 몸살을 앓고 있는 것으로 나타났다. 우리나라에서는 DarkWeb 에서 유통되는 개인 정보가 1 억 5 천만 건이지만, 전 세계적으로는 1930 억 건에 달한다. 이 중 금융업에서만 작년 대비 45% 증가한 34 억 건 이상의 Credential Stuffing 공격이 발생하였다. Credential Stuffing 공격의 증가 추세는 금융 서비스 업계를 위협하는 피싱 공격과 직접적인 관련이 있다. 범죄자들은 다양한 방법을 사용해 개인 정보를 조합하고 있으며, 이를 이용해 뱅킹 서비스 직원을 타깃팅하여 침투하는 스피어 피싱 메일이 성행하고 있다.

7 월에는 IT 관리 SW 를 통한 대규모 공급망 공격이 추가로 발생하였다. 약 200 여 곳의 기업에서 랜섬웨어 피해 사례가 발생하였는데, IT 관리용 서버를 통해 랜섬웨어가 업데이트 되어 파일이 암호화되는 피해를 입은 것으로 드러났다. 특히 일부 슈퍼마켓 체인 기업의 경우 이번 공격으로 인한 전산망 마비때문에 점포 800 여 곳이 문을 닫은 것으로 알려졌다. 이번 공격은 랜섬웨어를 실행할 때 MS 윈도우 백신인 윈도우 디펜더의 정상 파일을 사용해서 랜섬웨어를 감염시키는 DLL 사이드 로딩 기법을 사용했다. DLL 사이드 로딩 기법은 정상적으로 보이는 애플리케이션을 사용해 보안 솔루션들을 속임으로써 악성 DLL 을 로딩하는 기법이다.

또한, 연 매출 50 조에 달하는 국내 대기업의 '내부망 접근 권한'을 DarkWeb 에 경매로 판매하는 일이 발생했다. 해커들의 주장에 의하면 해당 기업의 Citrix VDI(Virtual desktop Infrastructure)의 접근 권한을 확보했으며 자신들의 주장이 사기가 아니라는 점을 입증하기 위해 VDI 에 접속해 PC 정보, 그룹웨어 접속 화면, 내부문서 열람 정보를 증거로 올렸다. 이렇듯 한국 기업의 기밀 정보와 관리자 접근 권한 탈취를 노린 공격이 잇달아 발생하고 있어 기업들의 보안 관리에 비상이 걸렸다. 특히 재택근무가 많아진 상황에서 원격으로 회사 내부망에 접속이 가능한 가상 데스크톱 인프라(VDI)나 가상사설망(VPN)의 계정 탈취를 노린 공격들이 빈번해지고 있어 각별한 주의가 요구되고 있다.

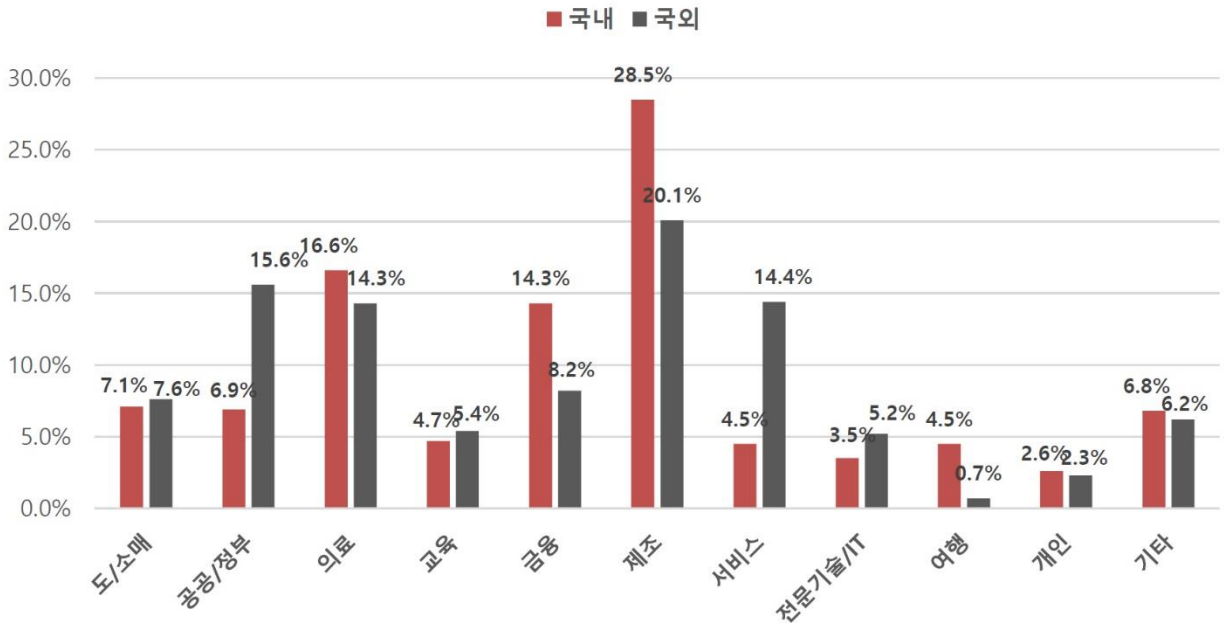
9 월에는 8 만 7 천여 개의 포티넷 SSL-VPN 이 패치 되지 않은 상태로 실행되고 있어 VPN 사용자의 ID, PW 가 대량 노출되었다. 이 취약점은 2018 년에 발견되었으며 아직까지 패치가 되지 않은 업체가 주요 타깃이 된다. 전 세계적으로 가장 많이 익스플로잇 되는 취약점 30 개 중 하나로 9 월에 다시 한번 공격이 유행하면서 이슈가 되었다. 현재 포티넷 VPN Credential 약 50 만 개가 온라인에 올라왔고, 2 만 2500 여 개 조직들이 피해를 입은 것으로 나타났다.

또한, 국내 S 병원에 해킹을 통한 개인정보 유출 사고가 발생했다. 병원 측에 따르면 (구)홈페이지 해킹으로 2013 년 2 월 이전 가입한 회원정보가 유출됐으며 유출된 개인 정보는 ID, PW, 이름, 주민등록번호, 우편번호, 휴대전화번호 등 총 10 개 항목에 달한다. 병원 정보를 노리는 해커들의 공격이 더욱 증가하고 있어 병원 경영진들의 인식변화와 정보보호에 대한 투자가 시급한 상황이다.

11 월에는 美 FBI 의 외부용 이메일 시스템이 뚫려 해킹 공격을 받았다. 해커들이 FBI 의 이메일 계정을 탈취한 후 일반인에게 최소 10 만여 개의 스팸 메일을 무작위로 발송하였다. 해당 메일은 악성코드가 첨부되지 않았으며 명성을 훼손하거나, FBI 에 전화가 쇄도하도록 만들기 위한 의도로 보인다.

그외에도 국내 방산업체 핵심기술 탈취를 위한 선박/해양 분야의 해킹이 지속적으로 일어나는 것으로 드러났다. 지난 2016 년에도 잠수함 관련 핵심기술 등 1~3 급 군사기밀 60 여 건을 포함한 4 만여 건의 내부자료를 탈취당한 바 있는데, 이번 해킹은 내부 전산망까지 침투하여 유출 문서나 피해 규모가 더 클 것으로 보고 기관에서 조사하고 있는 것으로 알려졌다.

업종별 침해 사고 발생 통계



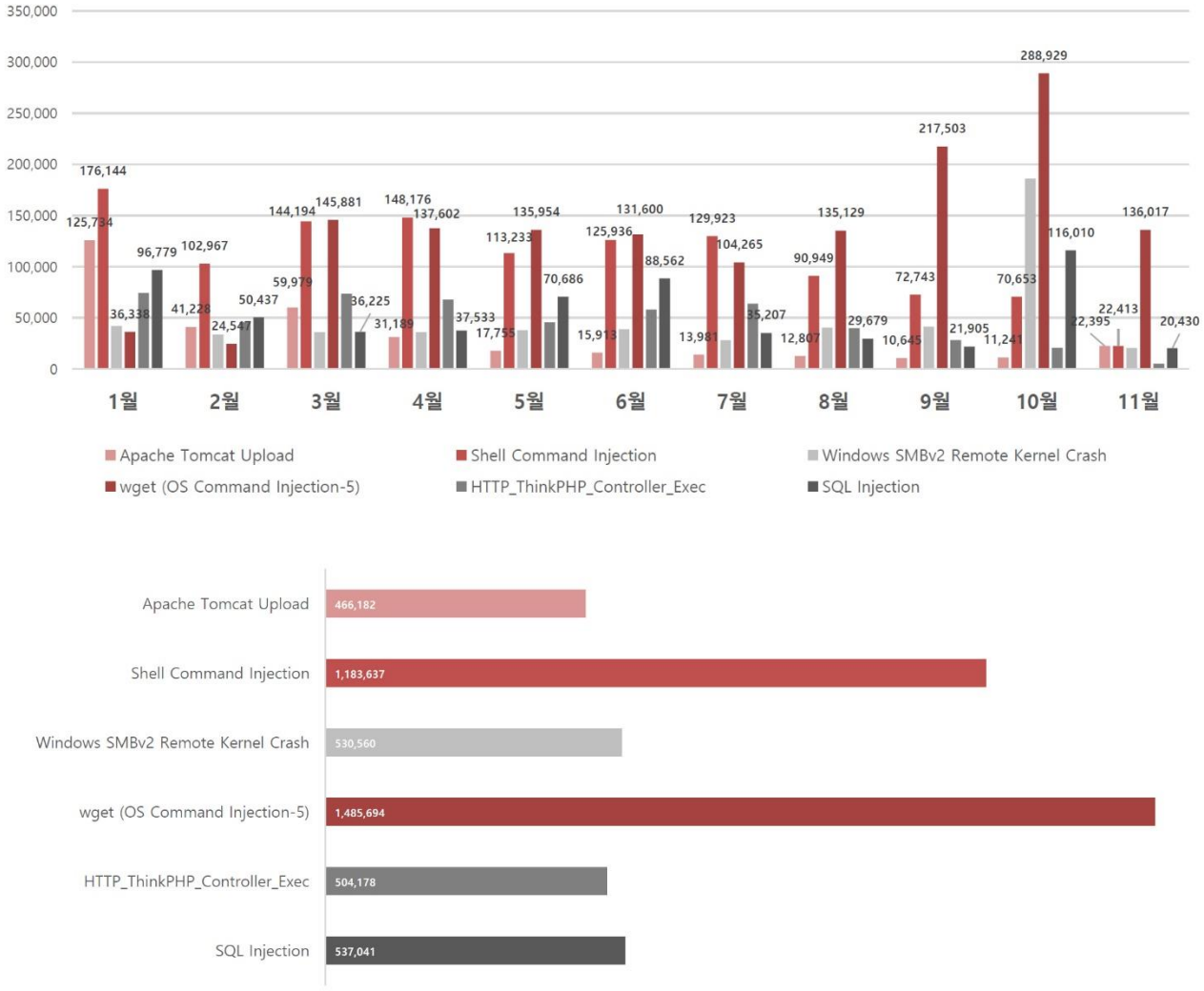
[2021년 업종별 침해 사고 발생 통계]

2021 년 업종별 침해 사고 발생 건수를 살펴보면 국내 기준 제조와 의료에서 28.5%, 16.6%로 가장 많은 사고가 발생했고, 뒤이어 금융 14.3%, 도/소매 7.1%, 공공/정부 분야가 6.9%를 차지했다. 국외 기준으로는 제조, 공공/정부 분야에서 20.1%, 15.6%로 큰 비율을 차지했으며, 뒤이어 서비스는 14.4%, 의료는 14.3%를 기록했다.

국내외 업종별 침해사고 발생 통계에서 보듯이 공급망 공격을 통한 금전 취득, 정보 유출 등을 노리는 공격으로 인해 제조 업종에서 침해 사고가 가장 많이 확인됐다.

제조업 특성 상 생산이 중단될 경우 납기 지연에 따른 피해가 크기 때문에 이를 악용하여 몸값을 요구하는 사례가 늘어나고 있다. 또한 노후화된 장비나 윈도우 95 를 쓰는 공장도 많아 해커들의 관심 및 위협이 증가하고 있어 운영기술(OT) 및 산업제어시스템(ICS) 등 제조업 전반적으로 보안이 더욱 요구되고 있다.

월별 주요 공격 이벤트 통계

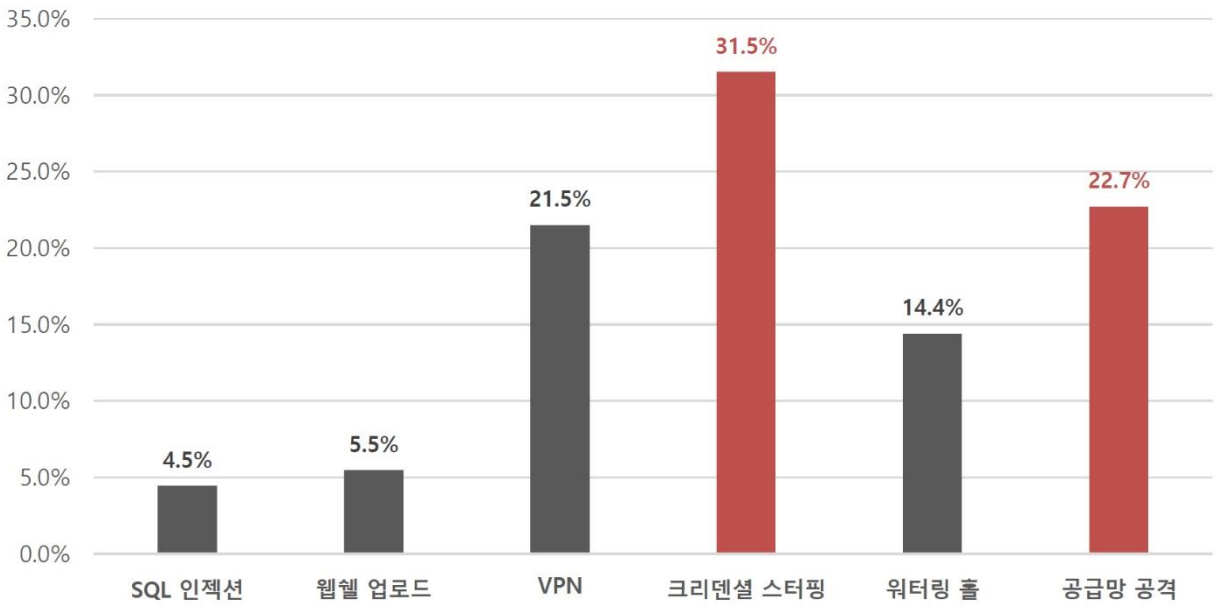


[2021년 월별 공격 발생 이벤트 통계]

2021 년 월별 주요 공격으로는 악성코드 다운로드를 위한 wget 공격이 148 만 건으로 가장 많았다. 외부에서 원격 명령을 삽입하는 Shell Command Injection 공격이 118 만 건으로 확인되었고, SMBv2 취약점 공격 시도가 53 만 건, PHP 프레임워크인 ThinkPHP 원격 코드 삽입 공격이 50 만 건으로 확인되었다. 뒤이어 웹 상의 근본적인 취약점인 SQL Injection 이 54 만 건, File Upload 취약점이 46 만 건에 달했다.

작년에 이어 올해도 웹서버 권한을 탈취할 수 있는 Shell Command Injection 과 OS Command Injection 을 이용한 공격이 가장 많았고, 특히 9~11 월에는 해양/선박 및 국내 주요 상급병원을 공격하는 이벤트가 다수 발생하였다. 방산에 대한 해킹은 꾸준히 이어져왔지만 개인 정보에서 한층 더 나아가 의료기관의 민감 정보가 활발하게 거래되는 추세인 만큼, 국내 상급병원의 보안 인식이 빠르게 개선되야 될 것으로 보인다.

침해사고 원인



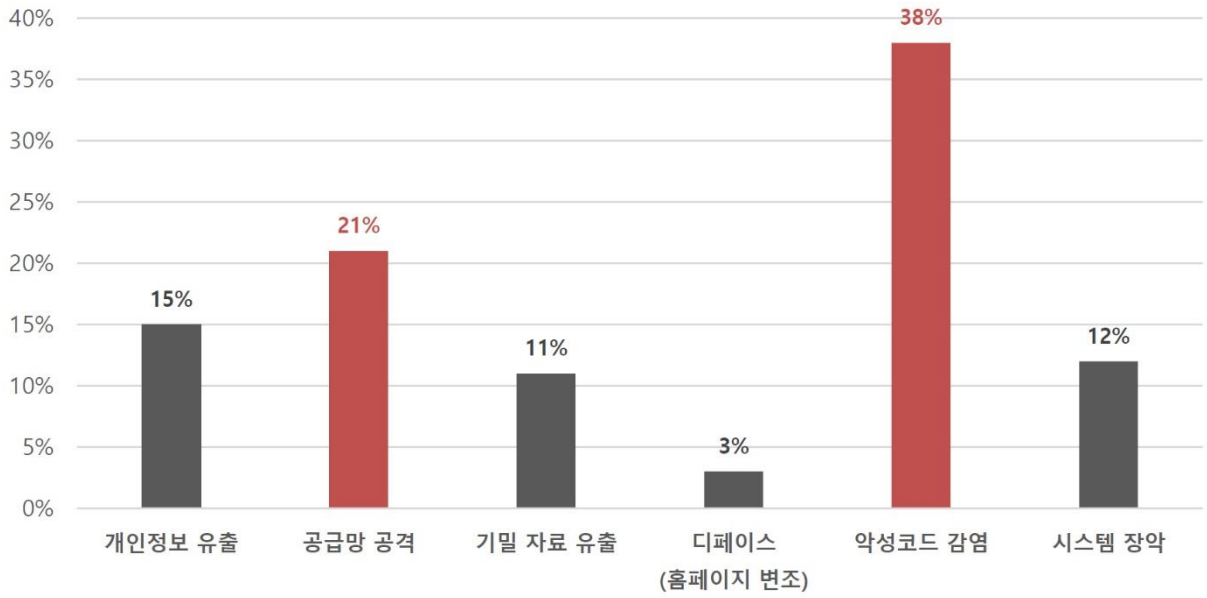
[2021년 침해 사고 원인]

2021 년 침해 사고 원인을 분석한 결과 Credential Stuffing 이 31.5%로 가장 많은 비율을 차지했다. 뒤이어 공급망 공격과 VPN 공격이 각각 22.7%와 21.5%를 차지했다.

상반기에 이어 DarkWeb 을 활용한 개인정보 거래가 활발하게 이뤄지면서 하반기에도 Credential Stuffing 으로 인한 피해는 꾸준히 발생하였다. DarkWeb 에 개인 정보를 판매하는 행위는 해커들에 가장 기본적인 금전화 수단이기 때문에, 앞으로도 개인 정보를 사고 팔고 이를 악용하여 Credential Stuffing 공격을 하는 악순환은 지속될 것으로 보인다. 사용자들은 사이트별로 다른 ID 혹은 다른 PW 를 사용하고, 주기적으로 PW 를 변경하는 등 개인 계정관리에 주의가 요구된다.

이외에도 올해 오픈 소스 기반 시스템의 증가, 원격 근무 환경 확대 등으로 공급망과 VPN 에 대한 공격이 증가한 것을 알 수 있다. 앞서 공격 발생 이벤트에서도 확인하였듯이, 관련 공격 시도가 꾸준히 증가하며 실제로 솔라윈즈, 카세야, 포티넷 취약점을 이용한 대규모 침해 사고가 발생하였다.

침해 사고 유형별 발생 통계



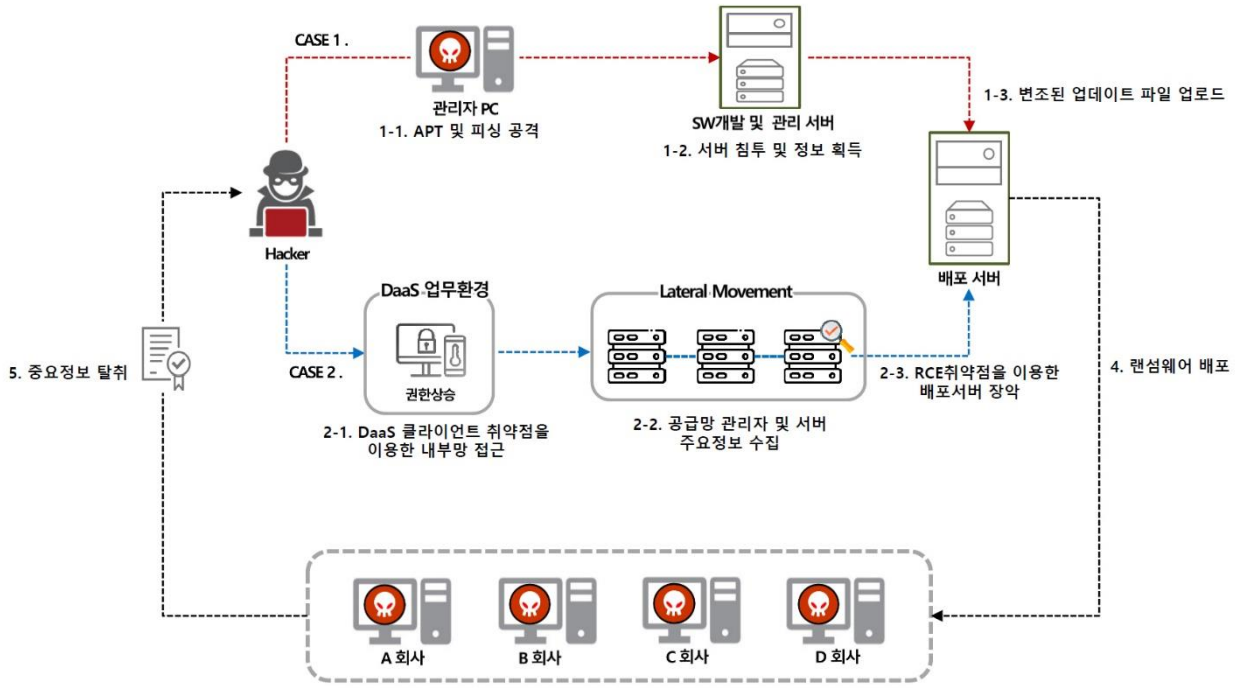
[2021년 침해 사고 유형별 발생 통계]

2021 년 침해 사고를 유형별로 나눠보면 개인/기업 데이터 복구 비용, 시스템 마비 등을 노린 악성코드 감염 사고가 38%로 가장 많이 발생했다. 뒤이어 다수의 기업을 노린 공급망 공격이 21%를 차지했고 개인 정보 유출로 인한 사고가 15%, 기밀 자료 유출 목적의 공격은 11%를 차지했다.

최근 악성코드 감염 사고는 대부분 대기업, 금융, 의료 등 자금 능력이 있는 회사를 공격하여 금전을 갈취하려는 목적으로 발생하고 있다. 특히 올해는 사용자나 시스템을 악성코드로 감염시켜 회사 내부망을 침투하는 APT 공격이 가장 많았다. 개인 정보+내부 기밀정보는 탈취 후 DarkWeb 에 판매하고, 랜섬웨어 배포 후 데이터 몸값을 요구하는 이중 협박 사례가 증가하였다.

산업군별로 정부 차원에서 보안 책임자 지정을 의무화하거나 보안에 소요되는 예산을 적정 수준 이상으로 규제하는 등의 조치를 취할 필요가 있다.

공급만 공격 시나리오



[공급망 공격 시나리오]

매년 발생하는 공급망 공격은 단시간 안에 많은 피해를 줄 수 있기 때문에 해커가 좋아하는 해킹방식이다. 올해도 다수의 공급망 공격이 발생했으며, 두 가지 사례를 알아보려고 한다.

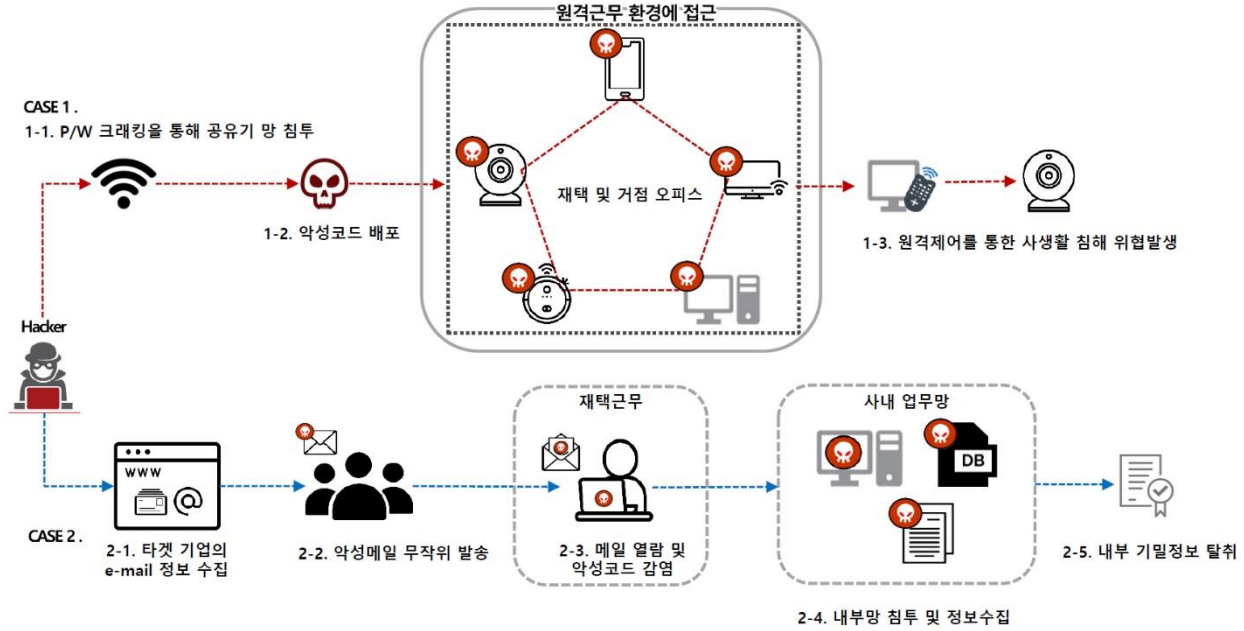
첫 번째는 일반적인 공급망 공격 방식으로, 해커가 APT 및 피싱 공격으로 PC의 관리자 권한을 획득한다. 이후 내부망에 있는 소프트웨어 개발 및 관리 서버와 배포서버를 공격하고 배포서버에 있는 업데이트 파일을 변조한다.

두 번째는 해커가 DaaS 클라이언트 취약점 공격으로 내부망에 접근한다. 이후 내부 확산 공격으로 공급망 관리자 및 주요정보를 수집한다. 수집한 정보를 바탕으로 원격 코드 실행(RCE, Remote Code Execution) 취약점을 이용해 배포서버를 장악한다.

위의 두 가지 방법을 이용하면 정상파일을 악성코드로 변조할 수 있다. 소프트웨어의 업데이트 시 변조된 악성코드를 다운로드해서 실행하기 때문에 여러 회사에 랜섬웨어를 동시에 배포할 수 있다.

공급망 공격에 대비하기 위해서는 기업에서 사용하고 있는 솔루션에 대한 취약점 동향에 대해 상시 모니터링하며 최신 패치를 유지할 수 있도록 해야 한다.

디지털 워크플레이스 공격 시나리오



[디지털 워크플레이스 공격 시나리오]

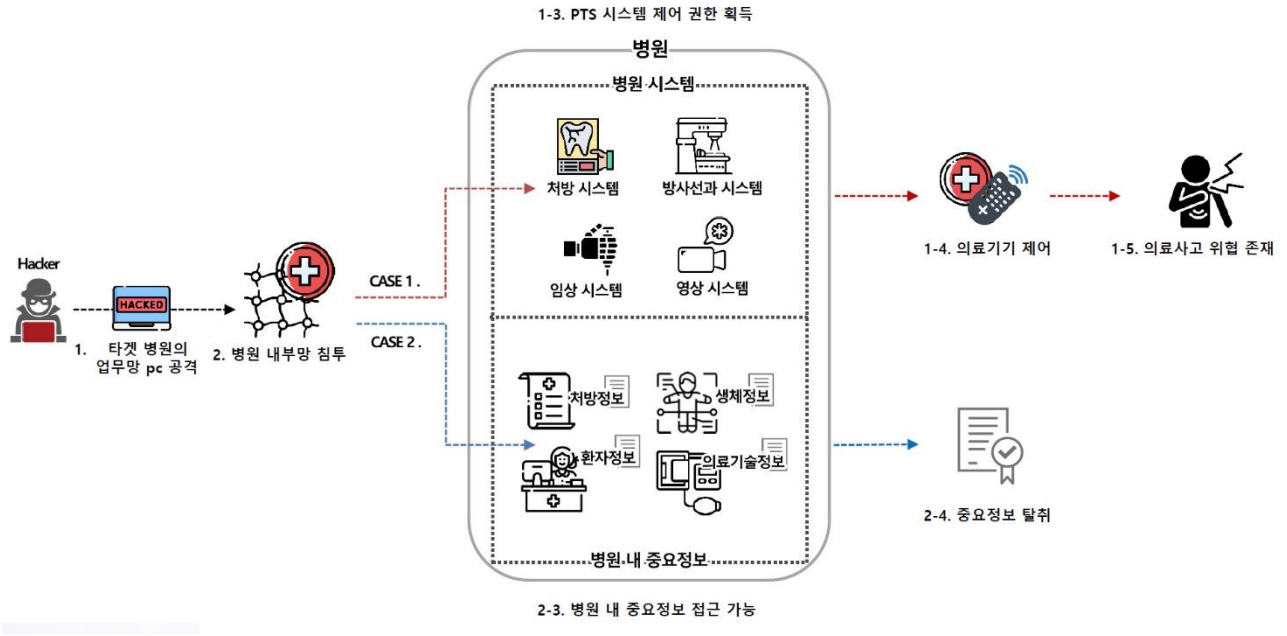
코로나 장기화로 인해 근무환경이 원격 근무로 변화하면서 보안홀이 발생했고 해커의 타깃이 되었다. 원격 근무 환경에서의 사생활 침해 위협이 늘었고, 재택근무자 대상으로 피싱 메일을 배포하여 업무망 침투 및 기밀정보를 탈취하는 상황이 발생했다.

첫 번째 사례는 해커가 재택 및 거점 오피스에서 사용 중인 공유기의 원격코드 실행 취약점을 이용해서 관리자 권한을 획득했다. 이후 DNS 조작으로 공유기와 연결된 업무용 PC에 악성코드를 유포했다. 추가로 같은 공유망을 사용하고 있는 화상채팅용 캠을 이용해서 사생활 녹화하고 유출했다.

두 번째 사례는 인터넷에서 임직원들의 이메일 정보를 수집하고, 악성코드가 첨부되어 있는 메일을 발송한다. 원격 근무를 하고 있는 사용자가 악성 메일을 열람할 경우 악성코드에 감염되고, 해커는 사내 업무망 침투에 성공한다. 이후 회사 기밀정보를 수집 및 탈취할 수 있다.

이처럼 원격 근무 환경에서는 다양한 방식의 피해 사례가 지속적으로 발생할 수 있으므로 주의가 요구된다.

병원 PTS 시스템 공격 시나리오



[병원 PTS 시스템 공격 시나리오]

과거에는 홈페이지를 해킹하거나 이메일로 피싱 메일을 보내서 내부 PC를 장악하는 사례가 많았다. 최근 전 세계 3000개가 넘는 병원에서 사용 중인 PTS 시스템[1]에서 취약점이 발견되면서 병원을 해킹하는 방식이 변화하고 있다.

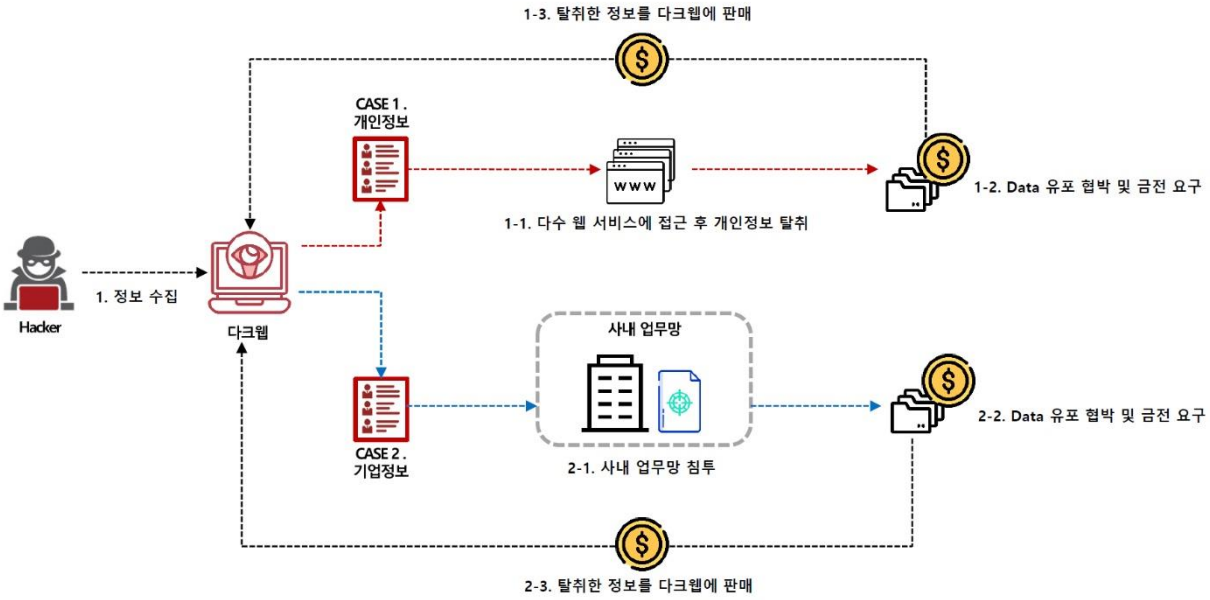
해커는 외부에 공개되어 있는 이메일 주소로 악성코드를 보낸다. 악성코드에 감염된 업무망 PC로 내부망을 스캐닝 하고, PTS 시스템의 취약점을 이용해서 관리자 권한을 획득할 수 있다.

병원 내에서 PTS로 공유되는 혈액, 약물 공급 차단하거나 투입양을 변조해서 의료사고 피해를 입힐 수 있고 병원 내 처방 정보, 환자 정보, 의료기술 정보 등 민감정보를 외부로 탈취하는 공격도 가능하다.

따라서 단기적으로는 홈페이지, 모바일 앱, 네트워크 장비에 대한 모의해킹, 피싱메일 훈련이 필요하고 장기적으로는 망분리를 하여 내부의 중요시스템을 안전하게 보호해야 한다.

[1] PTS(Pneumatic Tube System): 의약품 정보, 혈액정보, 기타 환자 의료정보 등을 병원 내 공유하는 시스템

DarkWeb 내 유출정보를 통한 공격 시나리오



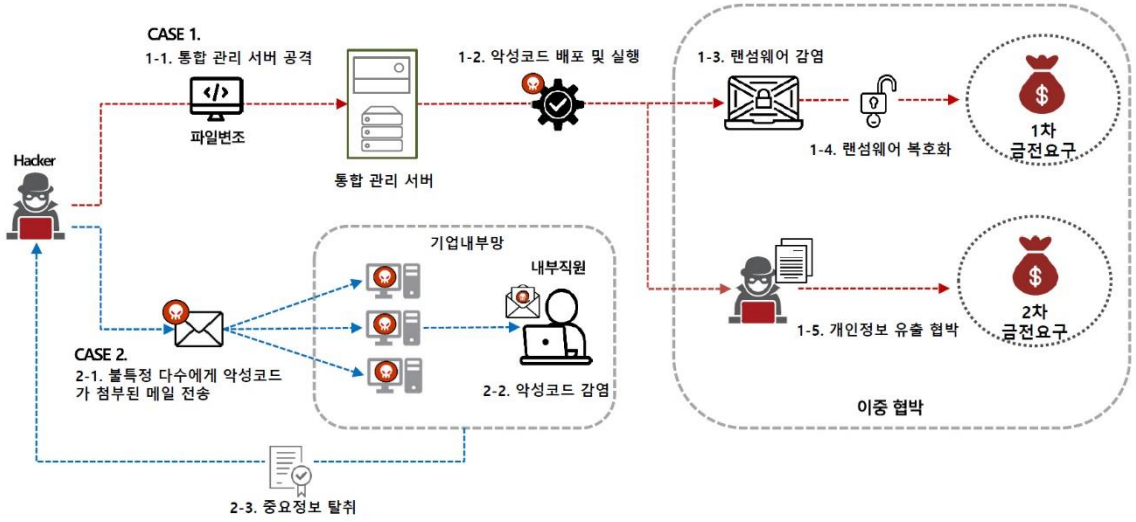
[DarkWeb 내 유출정보를 통한 공격 시나리오]

DarkWeb에서는 연 1억 5천 건의 개인 정보와 기업 정보가 거래되고 있다. 거래에 그치지 않고 수집된 개인 정보로 다수의 웹서비스에 계정 정보(ID/PW)를 대입하여 접속한다. 접속에 성공한 웹서비스에서 추가적인 개인정보나 문서, 영상, 사진 등의 개인 Data를 탈취하고, 탈취한 정보 유포 협박 및 금전 요구 또는 DarkWeb에 재판매하는 등 2차 피해를 입힐 수 있다.

또한 수집된 기업 정보로 사내 업무망에 침투해서 임직원 정보, 고객 정보를 탈취한 후, 마찬가지로 탈취한 정보 유포 협박 및 금전 요구 또는 DarkWeb에 재판매하는 2차 피해를 입힐 수 있다.

사용자는 가입되어 있는 웹사이트 별로 패스워드 설정을 다르게 하여 만약 유출이 되더라도 추가적인 피해가 발생하지 않도록 주의해야 한다.

표적형 악성코드 공격 시나리오



[표적형 악성코드 공격 시나리오]

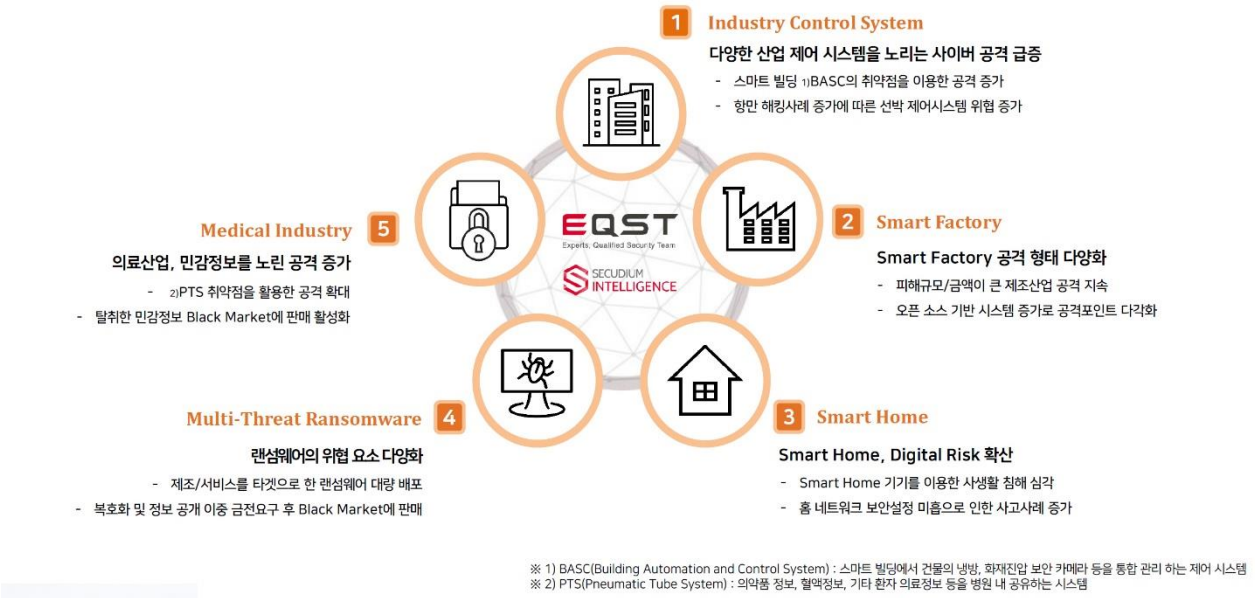
최근 특정 기업이나 기관을 타깃으로 하는 표적형 랜섬웨어가 증가되고 있다. 오랜 기간 기업의 정보를 수집하여 취약점을 분석한 후 고객사 환경에 특화된 랜섬웨어를 개발하고 유포하여 시스템 장악 후에 탈취한 정보를 유출하거나, '이중 협박'으로 DarkWeb에 정보를 팔기도 한다.

첫 번째 사례는 해커가 통합 관리 서버 공격을 통해 악성코드를 유포한다. 랜섬웨어를 감염시킨 해커는 복호화를 빌미로 1차적으로 금전을 요구한다. 데이터 복구 비용을 지불하면 사전에 유출한 개인 정보 유포로 2차 금전요구를 한다.

두 번째 사례는 기업의 내부 직원에게 악성코드가 첨부된 메일을 발송한다. 내부 직원이 해당 메일을 열람하면 악성코드에 감염되고, 기업 내부망에 침투하여 중요 정보 탈취가 가능하다.

이러한 피해를 막기 위해 취약점 및 보안 업데이트의 주기적인 모니터링을 통해 피해를 최소화하고, 출처가 불분명한 파일은 다운로드 받거나 실행하지 말아야 한다.

2022년 5대 보안 위협 전망



[2022년 보안 위협 전망]

다양한 산업 제어 시스템을 노리는 사이버 공격 급증

- 스마트 빌딩, 해운항만 해킹 사례 증가

2022년도에는 빌딩과 해운항만 분야에서 ICT 기술이 적용되면서 보안 위협이 증가하고, 이를 타깃으로 한 공격이 더 늘어날 전망이다.

폐쇄적으로 운영되어 오던 빌딩과 항만분야가 ICT 기술의 적용으로 외부에 공개되면서 해킹 공격에 손쉽게 노출되고 있다.

특히, 위드코로나 사회에 접어들고 세계 경제가 급속도로 회복하면서 물류의 중요성이 부각되고 있다. 올해 내내 글로벌 해운 기업들은 꾸준히 공격을 받았고, 국내 최대 H해운사도 6월에 이메일 접속 불가 및 노트북 포맷 등의 해킹 공격을 받은 것으로 나타났다.

돈이 있는 곳에는 항상 해커가 있다. 따라서 해커가 보안에 취약한 산업제어시스템을 지속적으로 공격하고, 이를 빌미로 금전적인 요구가 늘어날 것으로 예상된다.

Smart Factory 공격 형태 다양화

- 피해 규모/금액이 큰 제조산업 공격 지속

폐쇄적인 환경에서 운영하던 공장 시스템에 사물인터넷(IoT), 사이버-물리시스템(CPS) 등 첨단 ICT 기술이 적용되면서 제조업이 변화하고 있다. 설비와 공정의 자동화, 모니터링, 관리 시스템화와 코로나로 인한 반도체 수요의 폭발적인 증가 및 공급을 위한 제조업의 성장, 그 중심에는 5G, AI, 사물인터넷(IoT), 플랫폼, 클라우드가 있다.

폐쇄적이었던 공장들이 인터넷과 연결되면서 이를 노린 공격도 더욱 거세질 전망이다. 보다 정교해진 공격이 증가할 것이기 때문에 운영체제나 소프트웨어의 보안 관리가 꼭 필요한 시점이다.

Smart Home, Digital Risk 확산

- 개인까지 확대되는 위협

지난달 전국 여러 아파트의 월패드 카메라가 해킹 되면서 사생활이 노출되었다.

2007년 정부가 '홈네트워크 건물 인증 제도'를 통해 스마트홈 기술을 장려하면서 아파트, 오피스텔, 빌라 등 건물을 신축할 때 스마트홈을 적극 도입하고 있다. 스마트홈 증가에 따라 CCTV, 월패드, 무선공유기 등 여러 장비들이 앞다투어 도입되고 우리 생활을 편리하게 했지만 일반인도 해킹 가능한 수준의 취약점들이 발견되면서 해킹으로 인한 사생활 노출 위협은 증가하게 되었다.

전국에 사전 보안점검 없이 무분별하게 설치된 스마트홈 기기의 취약점 조치 및 대책이 준비되지 않아 당분간 이슈는 계속될 것으로 예상된다.

랜섬웨어의 위협 요소 다양화

- 복호화, 정보 공개로 금전 요구 후 판매

랜섬웨어 공격은 보다 지능화되고 다양한 위협 형태로 진화할 것으로 전망한다.

기존의 랜섬웨어 공격은 데이터를 암호화하거나 시스템을 사용하지 못하게 한 후 대가를 요구했다. 여기서 더 나아가 Maze 랜섬웨어는 탈취한 개인 정보 및 기밀정보를 외부에 공개하겠다고 협박하며 금전을 요구했다. 앞으로도 더 많은 피해를 입히기 위해서 랜섬웨어 기법이 고도화될 것이다.

또한 위드코로나 시대로 세계 경제가 급속히 회복되면서 제조/서비스를 타깃으로 한 랜섬웨어가 등장할 것으로 예상된다. 앞서 설명한 것처럼 보안을 적용하면 시스템을 재시작 해야 하고, 이것이 생산성 저하로 이어지게 되는 제조 분야의 특성상 다른 분야보다 보안 위협의 위험이 높다고 말할 수 있다. 이외에도 금융이나 공공에 비해 Compliance 영향이 약한 일반 서비스 기업을 타깃으로 하는 랜섬웨어가 등장할 것으로 예상한다.

의료산업, 민감정보를 노린 공격 증가

- 민감정보로 확대된 개인 정보 탈취 공격

코로나19의 장기화, 디지털 전환의 가속화로 의료산업이 해킹의 타깃이 되고 있다.

편의성을 높이기 위해서 PC, 스마트폰, 웨어러블 기기와 같은 다양한 디지털 플랫폼을 통해서 예약부터 검사, 입원, 퇴원 등 많은 절차에 손쉽게 접근이 가능하다. 누구나 접근할 수 있고, 국민 건강과 관련된 민감한 개인 정보를 가지고 있어서 해킹의 타깃이 되고 있다.

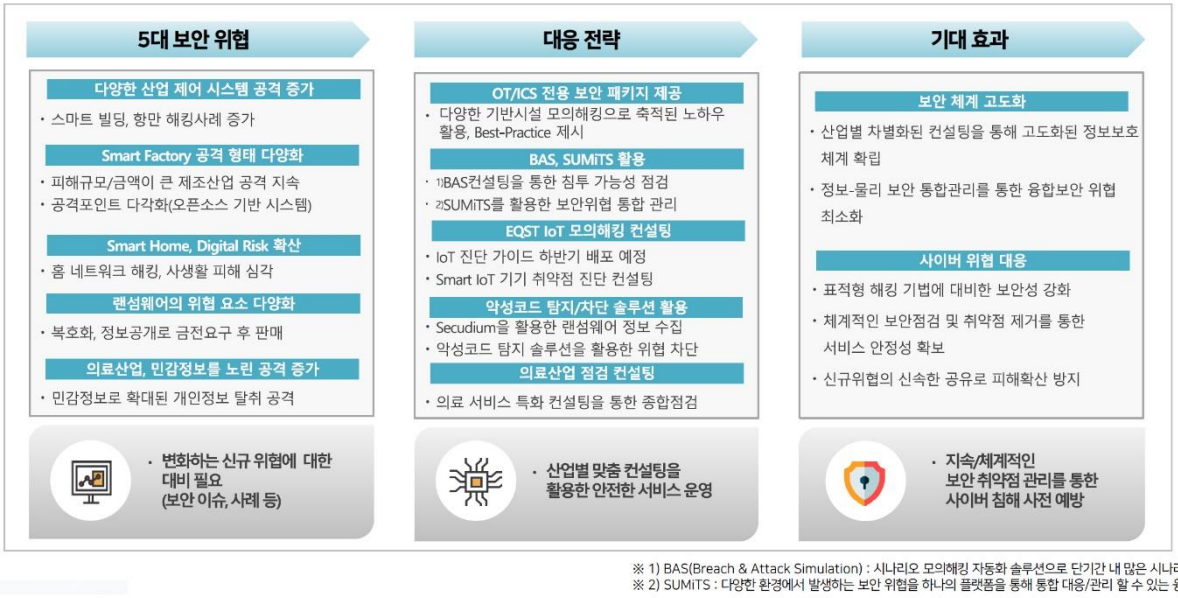
지난 7월에 발생한 모 병원의 해킹 사례를 보면, 악성코드가 담긴 피싱 공격으로 약 7,000여 건의 개인 정보, 진단명, 검사결과 등 민감의료 정보가 유출되었다.

지난 8월에 발생한 모 병원의 해킹 사례에서는 새로운 홈페이지를 개발한 이후에 과거의 홈페이지를 서비스 종료하지 않아서 가입한 사용자의 아이디, 패스워드, 이름, 주민등록번호, 주소 등 총 10개 항목이 유출되었다.

빠르게 디지털로 전환되고 있는 반면, 정보 보안에 대한 인식 및 투자가 부족하여 발생한 사건으로 당분간 의료산업의 민감정보를 노린 공격이 증가할 것으로 예상된다.

또한, 과거에는 홈페이지를 해킹하거나 이메일로 피싱 메일을 보내서 내부 PC를 장악하는 사례가 많았으나 PTS 시스템에서 취약점이 발견되면서 혈액, 약물 공급 차단하거나 투입양을 변조하여 의료사고 피해를 입힐 수 있게 되었다. 이처럼 병원 내 처방 정보, 환자 정보, 의료기술 정보 등 민감정보를 외부로 탈취하는 공격이 증가할 것으로 예상된다.

EQST 보안 위협 대응 전략



[EQST 보안 위협 대응 전략 및 서비스]

앞서 언급한 보안 위협 5대 전망과 최신 보안 이슈에 대응하기 위해 SK쉴더스는 IoT 진단 가이드를 고도화하여 배포할 예정이며, 다양한 기반 시설 모의해킹으로 축적된 노하우를 바탕으로 산업군별 고도화된 정보보호 체계를 확립할 수 있도록 지원할 방침이다.

또한, BAS(Breach Attack Simulation)의 시나리오 해킹 시뮬레이터를 활용하여 현재 구축되어 있는 보안 시스템들을 검증하고, 문제점을 보완할 수 있는 컨설팅을 제공할 예정이다.

추가로 자체 개발한 지능형 융합보안 플랫폼 'SUMiTS'는 물리보안(출동/출입/경비)과 시설관리(시설/환경/주차)에 최신 ICT기술을 접목시켜 통합 관리가 가능하다. 융합보안에서 발생하는 다양한 이벤트를 수집·분석·처리하고 위협 요소를 빠르게 파악하여 통합 관리할 수 있도록 제공할 것이다.

이와 함께 Secudium Intelligence를 활용하여 랜섬웨어 정보를 수집하고 보안성 강화를 실시해 보안 위협 식별 및 맞춤형 보안 대책을 수립하는 데 도움이 되고자 한다.

변화하는 신규 위협에 대비하여 SK쉴더스가 제안하는 산업군별 차별화된 컨설팅과 융합 보안 통합관리를 통한 위협을 최소화한다면, 체계적인 보안 취약점 관리로 사이버 침해를 사전 예방하는 데 도움이 될 것이다.

EQST Annual Report

2021.12

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

발행인 : SK쉴더스 EQST 담당
제 작 : SK쉴더스 PR팀