SK 쉴더스

EQST Annual Report

2025 보안 위협 전망 보고서

Contents

EQST insight

2024 년 보안 이슈와 2025 년 5 대 보안 위협 전망

■ 2024 년 5 대 보안 위협 리뷰

2024 년은 AI 기술이 빠르게 발전하는 만큼 이를 악용하는 사이버 공격 또한 심화되어 기술 발달의 양면성이 여실히 드러나는 해였다. 해커뿐만 아니라 전문적인 지식이 없는 일반인들조차 보편화된 AI 기술을 통해 랜섬웨어를 제작하거나 불법 합성물을 만들어내는 사례가 있었다.

매년 반복되는 위협인 랜섬웨어와 공급망 공격은 공격자들의 전략 변화 및 피해 규모 확대 등의 방식으로 점차 고도화됐다. 랜섬웨어 그룹은 보안 솔루션 탐지 회피를 위해 피해 서버의 정상적인 시스템이나 도구로 위장하는 방식을 택했으며, 공급망 공격의 경우 유명 플랫폼과 서비스를 타깃으로 다수의 사용자를 노리는 공격이 발생했다.

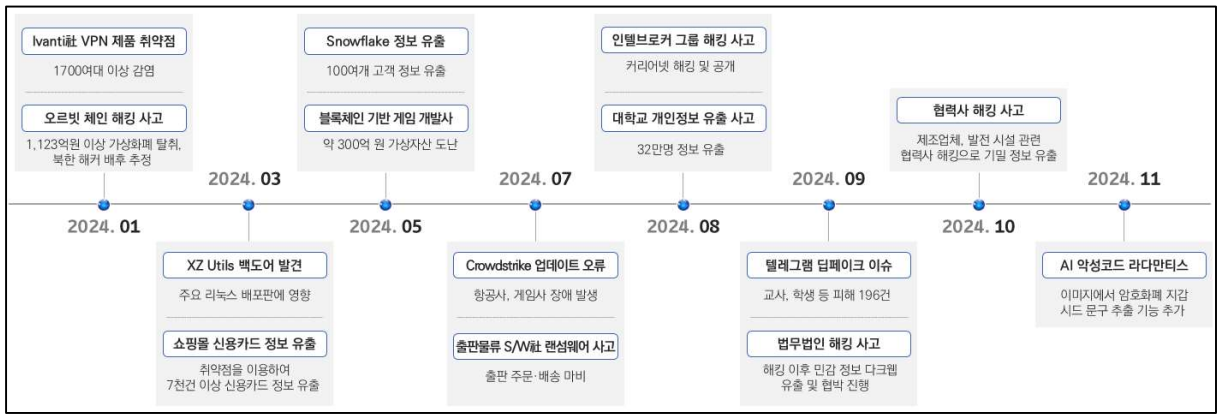
개인과 기업을 겨냥한 정보 유출 사고 역시 여전히 끊이지 않고 있다. 그러나 공격자들은 이를 단순 유출/협박/판매에 그치는 것이 아닌 활용하는 형태로 진화했다. 공격자들은 다크웹을 통해 크리덴셜을 구매하거나 외부에 노출된 크리덴셜을 수집해 이를 공격에 활용했다. 특히 클라우드 자격증명을 활용한 공격이 성행했으며, 공격자들은 이를 활용해 클라우드 환경 내부에 침투해 데이터를 탈취하거나 다크웹에 판매했다.

클라우드 보안 사고는 공격자들의 클라우드 리소스 탈취로 이어졌다. 공격자들은 피해 대상의 클라우드 서버를 장악한 후, 클라우드 리소스에 접근해 대규모 공격을 위한 스캐너로 사용하거나 암호화폐 채굴에 활용하는 등 피해의 범위를 확대시켰다.

이처럼 공격 전략이 다각화 되고 피해가 연쇄적으로 발생하고 있어 최신 위협을 이해하고 이에 대응하기 위한 보안 전략을 세우는 것이 중요하다. 이에 SK쉴더스의 화이트해커 그룹 EQST(이큐스트)는 2024년 주요 보안 이슈를 분석하고, 2025년 5대 보안 위협을 전망한다.

24 년 보안 트렌드 리뷰

■ 2024년 주요 보안 이슈



[2024 년 주요 보안 이슈 타임라인]

1 월에는 Ivanti 의 VPN 장비인 Ivanti Connect Secure 및 Ivanti Policy Secure 에서 제로데이 취약점이 공개됐으며, 현재까지도 공격자들로부터 활발히 악용되고 있다.

특히 인증 우회 취약점(CVE-2023-46805), 명령 주입 취약점(CVE-2024-21887), SSRF 취약점(CVE-2024-21893)은 권한 획득 후 원격 명령 실행을 통해 다수의 내부 서버에 대한 제어권을 획득할 수 있어 공격자들로부터 널리 악용됐다.

Ivanti 취약점으로 인해 전 세계 정부/방산/금융 기관 등 다양한 분야의 1,700 여개 이상의 기업이 피해를 입었으며, 국내에서도 항공사 및 간편결제 관련 기업 2 곳이 피해를 입었다.

국내 2,000 여 개 기관과 기업에서 Ivanti 제품을 사용 중인 만큼 각별한 주의가 필요하다. 이에 SK 쉴더스의 침해사고전문팀 Top-CERT 는 각 기관 및 기업에서 활용할 수 있는 'Ivanti VPN 취약점 공격 동향 및 대응방안' 리포트를 발간했다.

또한, 국내 블록체인 기업 O 社의 크로스 체인[1] 플랫폼에서 신원 불명의 공격자에게 총 여섯 차례에 걸쳐 가상자산을 탈취당하는 사고가 발생했다. O 社는 전 최고정보보호책임자(CISO)가 퇴사 전 임의로 변경한 방화벽 주요 정책이 가상자산 탈취 사고의 발생원인으로 의심된다며 내부자 연루 가능성을 제기했다.

[1] 크로스 체인(Cross Chain): 하나의 블록체인 네트워크에서 다른 블록체인 네트워크로 가상자산, NFT 등을 교환하는 것

공격 수법은 북한 해킹 그룹 라자루스와 유사하다고 분석됐다. 거래 내역을 추적한 결과 해킹 직후에는 별다른 자산 이동이 없었으나, 지난 6 월 약 660 억 원(4,800 만 달러)의 가상자산이 토네이도 캐시[2]로 이동된 정황이 드러났다.

이 해킹 사고로 인해 디지털 자산 거래소 공동협의체(DAXA)는 O 社가 발행한 토큰의 거래소 퇴출을 결정했으며, 해당 거래는 3 월 19 일 종료됐다.

3 월에는 모든 GNU/리눅스 운영체제에서 데이터 압축에 사용되는 오픈소스 'XZ Utils'의 특정 버전(v5.6.0, v5.6.1)에서 백도어가 발견됐다. 해당 취약점(CVE-2024-3094)은 XZ Utils 의 liblzma 라이브러리에 삽입된 백도어를 통해 인증 과정을 우회하여 보안체계를 무력화하고 시스템에 접근할 수 있었다.

공격자는 프로젝트 관리자 권한을 확보하기 위해 2022 년부터 XZ Utils 프로젝트에 활발히 참여하며, 프로젝트 관계자들과 신뢰 관계를 쌓았다. 프로젝트 관리 권한을 획득한 후, 공격자는 프로젝트의 소스코드에 백도어 악성코드를 삽입해 유포한 것으로 밝혀졌다.

XZ Utils 는 리눅스 운영체제에서 필수 패키지로 제공되기 때문에 피해가 클 것으로 예상됐으나, 일반적으로 리눅스 운영체제는 최신 버전이 아닌 안정화된 이전 버전을 사용하기 때문에 큰 피해를 막을 수 있었다. 그러나 오픈소스 기여자가 이를 악용할 수 있다는 점에서 오픈소스 생태계의 보안 취약점을 보여준 사례가 됐다. 기존의 소프트웨어 공급망 공격에 사회공학적 기법이 더해진 진화된 공급망 공격이라는 특징을 보였다.

4 월에는 50 여개의 국내 중소규모 온라인 쇼핑몰에 피싱 페이지를 삽입해 사용자의 카드 정보를 탈취한 뒤, 이를 이용한 부정 결제로 현금화하는 공격 그룹이 발견됐다. 공격자들은 주로 2 차 인증이 없는 관리자 페이지나 FTP 서비스가 노출된 취약한 쇼핑몰을 타깃으로 삼았으며, SQL Injection 과 같은 웹 취약점과 쇼핑몰 플랫폼 취약점을 이용해 피싱 페이지를 삽입했다. 이들은 총 7,089 건의 신용카드 정보와 개인정보를 탈취했으며, 이를 이용해 온라인에서 상품을 구매한 뒤 중고거래 플랫폼에 판매하는 수법으로 현금화를 진행했다.

특히 많은 취약점과 공격코드가 공개된 오래된 버전의 PHP 를 사용하는 곳이 상당수 발견되어, 국내 중소규모 온라인 쇼핑몰의 취약한 보안 실태가 여실히 드러났다.

5 월에는 블록체인 기반의 게임 플랫폼인 '갈라 게임즈(Gala Games)'가 약 300 억 원(2,200 만 달러) 이상의 가상자산을 도난당하는 해킹 사고가 발생했다. 갈라 게임즈는 침해사고 발생 45 분 만에 공격자의 계좌를 확보한 뒤 동결하여 피해를 최소화할 수 있었다.

공격자의 신원이나 구체적인 공격 방법은 공식적으로 확인되지 않았지만, 갈라 게임즈 창립자는 이번 해킹 사건이 플랫폼 내부 통제의 취약성 때문임을 인정했다. 이후 공식 SNS 를 통해 투명하게 상황을 공유하고 대응 조치를 취했으며, 법 집행 기관의 개입으로 사고 발생 이후 대부분의 토큰을 동결시켰다.

한편 5 월 21 일, 공격자는 해킹으로 탈취한 이더리움 전액을 반환했으며, 이는 갈라 게임즈의 신속하고 효과적인 대응과 법 집행 기관의 개입이 심리적으로 작용한 것으로 추정된다.

[2] 토네이도 캐시(Tornado Cash): 범죄자들이 자금 출처를 숨기기 위해 사용하는 암호화폐 믹싱 서비스

6 월에는 미국의 클라우드 기반 데이터 관리 전문 기업인 '스노우플레이크(Snowflake)'의 고객사의 데이터가 탈취되는 사고가 발생했다. 티켓 예매사이트인 '티켓마스터(Ticketmaster)'는 5 억 6 천만 건의 고객 정보를 탈취당했으며, 유럽 최대 은행인 '산탄데르 은행(Banco Santander S.A.)'은 3 천만 건, 미국의 자동차 부품 공급업체 '어드밴스 오토 파츠(Advance Auto Parts)'에서는 3 억 8 천만 건이 탈취 당하는 등 165 개 고객사에서 수억 단위의 데이터가 탈취 됐다.

공격을 감행한 조직은 UNC5537[3] 로 추정되며, 인포스틸러(정보 탈취 악성코드)를 통해 대량으로 수집한 자격증명을 활용했다. 다중인증(MFA)이 설정되지 않은 계정이 주요 표적이었으며, 오래된 자격증명을 사용하거나 네트워크 허용 목록이 미설정 되어있는 등 피해 기업 대부분의 클라우드 보안이 취약한 것으로 확인됐다. 따라서 클라우드 및 하이브리드 환경에서의 사용자 식별 등 접근 통제 보안에 대한 중요성이 부각되는 사례가 되었다.

공격에 활용된 자격증명 중 일부는 2020 년부터 유출된 것으로 파악되며, 공격자들은 스노우플레이크의 웹 기반 사용자 인터페이스(SnowSight), 명령줄 인터페이스 도구(SnowSQL) 등을 통해 피해 조직의 스노우플레이크 인스턴스에 접근했다. 이후 공격자들은 탈취한 데이터를 사이버 범죄 포럼에 판매하거나 피해 조직을 협박하여 금전을 요구했다.

7 월에는 미국의 엔드포인트 보안 기업 '크라우드스트라이크(CrowdStrike)'의 보안 S/W 업데이트 오류로 인해 전세계 약 850 만 대의 윈도우 장비에 장애가 발생했다. 오류가 발생한 S/W 는 'Falcon Sensor'로, 새로운 패치를 적용하는 과정에서 메모리 상의 잘못된 참조로 인해 MS 윈도우와 충돌이 발생하여 사용자 PC 에 블루 스크린을 유발했다. 이로 인해 전세계 2 만 9 천여 개에 달하는 고객사가 피해를 입었으며, 특히 항공/금융/언론사 등의 서비스 운영에 영향을 미쳤다.

국내에서는 저가 항공사의 항공권 예매/발권 시스템 오류, 게임사의 서버 장애 등이 발생했으며, 피해 기업은 총 10 곳으로 파악됐다. 크라우드스트라이크 제품의 사용 비율이 적어 국외에 비해 상대적으로 피해가 적었지만, 2022 년 국산 보안 소프트웨어 오류로 인해 1,600 만대의 PC 에 장애가 발생한 사례가 있어 이번 사고는 소프트웨어 공급망 보안에 대한 중요성과 사이버 복원력에 대한 논의의 필요성을 다시 한 번 부각시키는 계기가 됐다.

8 월에는 국내 출판사에서 사용하는 출판물류 소프트웨어 개발사의 전산망이 랜섬웨어에 감염되는 사고가 있었다. 해당 기업은 출판사와 출판물류기업 간의 주문·배송 네트워크 솔루션을 제공하는 업체로 도서 출고 지시를 일괄 처리하는 시스템이 랜섬웨어에 감염됐다. 이로 인해 해당 솔루션을 사용하는 1,000 여개의 출판사와 100 여개의 물류사 간의 네트워크가 마비되어 도서 배송에 차질이 발생하는 등의 피해가 있었다.

랜섬웨어 감염 이후 데이터 복구 전문 업체를 통해 공격자와 협상을 진행하고 복구 비용을 지불했으나, 공격자는 작동하지 않는 복구 키를 보내며 추가로 돈을 지불할 것을 요구했다. 이후 해당 기업은 구 서버에 존재하는 백업 자료를 활용해 긴급 서버를 운영했지만, 최신 버전인 프로그램과 구 버전인 데이터베이스 간의 구조적 불일치 문제가 발생하여 프로그램 안정화에 오랜 시간이 소요됐다.

[3] UNC5537: 금전 탈취를 목적으로 공격을 감행하는 단체로 추정되며, 조직적으로 스노우플레이크 고객 인스턴스를 침해함

해당 기업은 사고 이후, 오래된 방화벽 사용, 해킹사고 대응 매뉴얼 부재 등 안일한 보안 인식에 대한 사과문을 게재했다.

또한, 글로벌 유명 기업을 대상으로 공격을 진행해온 '인텔브로커(IntelBroker)'가 다수의 국내 기관 및 기업을 대상으로 데이터 침해 공격을 감행해 화제가 됐다. 인텔브로커는 데이터 침해 후 데이터 샘플을 공개하며 협박 및 판매하는 공격 그룹 사이버니거스(CyberNiggers)를 이끄는 주요 인물로, 지난 6 월에는 미국의 반도체 기업인 AMD 와 전자제품 제조사인 애플(Apple)을 해킹하기도 했다.

인텔브로커는 진로 및 진학 정보를 제공하는 '커리어넷'을 해킹한 뒤 다크웹을 통해 개인정보 샘플을 공개하고 판매 글을 업로드했다. 이에 커리어넷은 160 만 건 이상의 회원정보가 유출된 사실을 인정하며 사과문을 게재했다. 또한, 이들은 경찰청을 포함한 정부 기관 3 곳의 중요 문서 탈취 성공을 주장했으며, 국방부와 해양경찰청의 내부 자료로 추정되는 데이터 샘플을 다크웹에 공개했다. 공개된 정보는 재난안전통신망 테스트보드에서 사용되는 정보였지만, 이외에도 외부로 공개되지 않은 군 조직 정보 등이 포함된 기밀정보가 유출된 것으로 확인됐다.

이후에도 인텔브로커는 시스코(CISCO), 노키아(Nokia), MIT 테크놀로지리뷰(MIT Technology Review) 등 다양한 기업을 대상으로 데이터 침해 공격을 활발히 이어가고 있다.

국내 기관 및 기업뿐만 아니라 국내 대학에서는 대량의 개인정보 유출 사고가 잇따라 발생했다. 올해 1 월부터 8 월까지 대학에서 발생한 개인정보 유출 사고는 총 22 건으로 집계됐으며, 2022 년에는 7 건, 2023 년에는 23 건인 것으로 보아 해를 거듭할수록 대학을 타깃으로 한 정보 유출 사고가 증가하고 있음을 알 수 있다.

올해 국내 대학에서 발생한 개인정보 유출 사고는 다양한 형태로 나타났다. 시스템과 홈페이지의 보안취약점을 이용한 해킹은 물론, 위탁업체와 내부자의 실수로 인한 개인정보 노출 사례도 있었다.

A 대학의 경우 소스코드 취약점으로 인해 통합정보시스템이 해킹 당해 학생 및 졸업생 등 32 만 명의 개인정보가 유출됐으며, B 대학에서는 학사정보관리시스템이 해킹 당해 졸업생 8 만 명의 개인정보가 유출됐다. 또한, C 대학에서는 홈페이지 개발·운영 위탁업체의 S/W 업데이트 과정에서 9,700 여 명의 개인정보가 홈페이지에 노출됐으며, D 대학에서는 내부자의 실수로 인해 1 만 9 천 명 이상의 개인정보가 담긴 파일이 홈페이지에 노출되는 사례가 있었다.

동일한 대학에서 3 년간 4 건의 정보 유출이 발생하는 등 개인정보 유출 사고가 반복적으로 일어나는 대학들이 여럿 존재했으며, 개인정보 유출 사고가 발생한 대학 중 일부는 정보보호수준 진단에서 우수로 평가받거나, ISMS[4] 인증을 취득한 것으로 알려져 문제가 됐다.

대학을 비롯한 여러 교육기관은 재학생은 물론 졸업생의 개인정보까지 다루고 있는 만큼 구체적인 보안 대책과 개인정보에 대한 보안 인식 제고가 필요하다.

[4] ISMS(Information Security Management System): 정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

9 월에는 전국 초·중·고교 및 대학 등 전국 학교를 중심으로 딥페이크 기술을 악용한 디지털 성범죄 이슈가 확산되어 사회적으로 큰 파장이 있었다.

교육부가 실시한 '학교 딥페이크 허위 영상물 피해 현황' 10 차 조사 결과, 올해 1 월부터 11 월 기준 딥페이크 피해 신고 건수는 총 561 건에 달했다. 초등학교 18 건, 중학교 243 건, 고등학교 300 건으로 집계됐으며, 피해자의 96%가 학생인 것으로 드러났다. 또한, 경찰청에서 발표한 '딥페이크 관련 경찰 신고 건 수'는 2021 년 156 건에서 2024 년 11 월 1,094 건으로 급증한 것으로 나타났다.

딥페이크는 주로 정치, 선거 분야의 허위 영상물 제작에 악용됐으나, 최근에는 불특정다수의 일반인에게까지 그 피해가 확산되고 있다.

가해자는 대부분 온라인 커뮤니티 및 SNS 에 업로드 된 타인 또는 지인의 사진을 무단 도용했으며, 텔레그램과 같은 SNS 를 통해 허위영상물 제작을 의뢰했다. 뿐만 아니라 오픈소스나 딥페이크 제작 앱 등을 통해 손쉽게 제작하는 사례도 존재했다. 이들은 제작된 허위영상물을 SNS 를 통해 유포하거나 이를 빌미로 피해자에게 금전을 요구했다.

AI 기술이 보편화됨에 따라 불법 콘텐츠 제작이 간단해지고, 디지털 성범죄 특성상 유포 및 재확산이 빠르게 진행되는 만큼 추적에 어려움이 있어 사회적으로 큰 문제가 되고 있다.

이에 대응하기 위해 2024 년 10 월 16 일, 국회는 딥페이크 성범죄를 방지하고 피해자를 보호하기 위한 '딥페이크 성범죄 방지법'을 시행했다. 제작·유포시 징역 5 년에서 7 년으로 법정형이 상향됐으며, 소지·구입·저장·시청할 경우, 징역 3 년 또는 3,000 만원 이하의 벌금에 처하는 규정 등이 신설됐다. 처벌 강화뿐만 아니라 플랫폼 사업자의 책임성 제고, 신속하고 확실한 피해자 보호, 맞춤형 예방 교육·홍보 등 딥페이크 성범죄 근절을 위한 노력이 이어지고 있다.

이와 함께 최근 법안 심사에 통과한 'AI 기본법'에서는 AI 기술로 생성된 컨텐츠에 대해 워터마크 삽입을 의무화하고 있지만, 워터마크 만으로는 AI 불법 컨텐츠를 제재하기 쉽지 않아 실시간 모니터링 및 삭제 등 추가적인 대책 논의가 필요하다. 무엇보다 디지털 성범죄 예방 교육과 더불어 딥페이크로 제작된 허위영상물을 제작·유포하는 것뿐만 아니라, 소지하고 시청하는 것 역시 명백한 범죄라는 인식 개선이 필요하다.

또한, 금전적 이득을 목적으로 국내 법무법인을 타깃으로 한 공격이 발생했다. 데이터를 탈취한 해킹 그룹은 'Trustman0'이며, 이들은 탈취한 개인정보와 민감 소송 정보, 사업체 법률자문 정보 등을 다크웹에 판매해온 것으로 파악됐다. 또한, 국내 법무법인을 대상으로 금전 협박을 진행하기도 했다.

‘Trustman0’과 공모한 A 씨는 국내 유명 B 법무법인을 대상으로 1.4TB 분량의 기밀자료를 탈취했다는 사실을 주장하며, 유포를 빌미로 협박하고 30BTC 를 요구했다. 하지만, B 법무법인의 해킹 피해는 없었으며, A 씨가 건넨 외장하드에는 직접적인 연관이 없는 자료가 담겨있던 것으로 알려졌다. 이후 9 월에는 ‘Trustman0’이 다크웹을 통해 C 법무법인의 샘플 데이터를 공개한 후 2TB 분량의 데이터를 5BTC 에 판매한다는 글을 게시했으며, 데이터 공개 협박을 빌미로 10BTC 를 지불할 것을 요구했다. 이에 C 법무법인은 이 사건을 경찰에 신고했으며, 현재 사이버수사대에서 조사 중이다.

10 월에는 국내 제조업체와 발전 시설의 협력사에서 해킹 사고가 발생하여 대량의 기밀정보가 유출됐다. 이외에도 국내 유명 골프장의 협력사 문자발송 시스템에 사이버 공격이 발생해 이용객의 개인정보가 유출되는 사례가 있었다. 또한 국내 게임사에 제공되는 보안 솔루션 공급 업체의 유효한 인증서를 탈취한 뒤 악성 보안 솔루션에 서명해 게임 서비스에 배포하는 사례도 있었다.

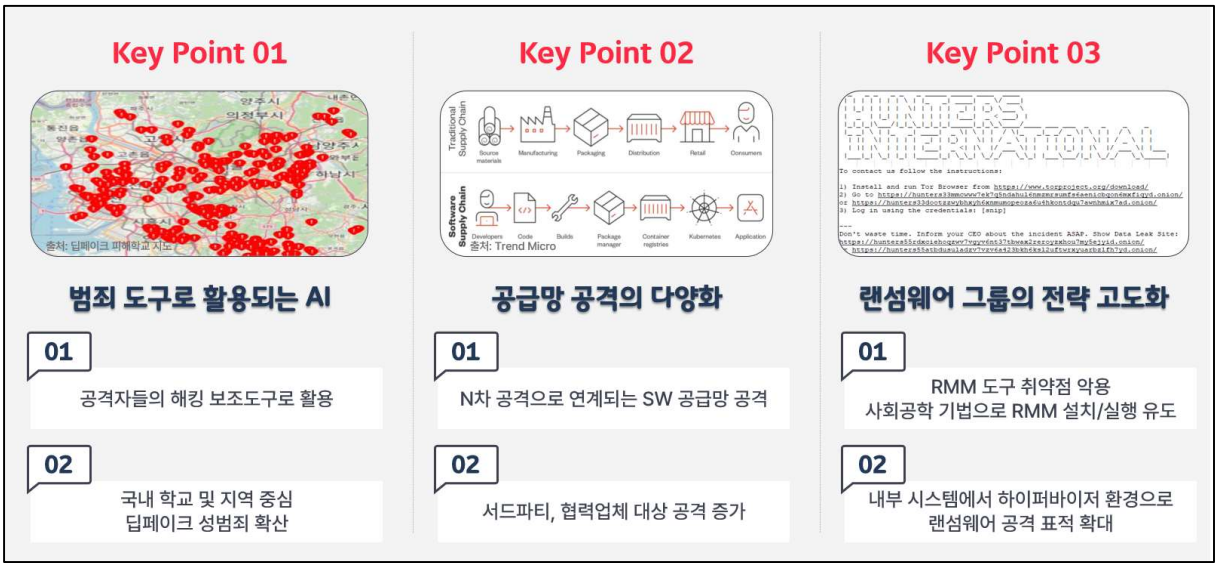
국외 사례로는 프랑스의 의료 보험 지급 관리 대행업체 두 곳에서 침해사고가 발생하여 3,300 만 명의 개인정보가 유출됐다. 이 중 한 곳은 대행업체 직원의 피싱 공격에 의해 발생한 것으로 단 한 명의 부주의로 인해 수천만 명의 개인정보가 유출된 사례이기도 했다.

이처럼 최근에는 기업 본사가 아닌 협력사를 비롯한 대행업체, 서드파티 등을 대상으로 하는 공격이 늘어나고 있다. 협력사의 경우 상대적으로 보안에 대한 투자가 적거나 보안 담당자가 부재하는 경우가 많아 공격자의 주요 타깃이 되고 있다. 협력사의 중요 정보를 탈취하여 2 차 공격을 시도하거나, 협력사를 경유하는 공급망 공격을 통해 원청사와 본사를 협박하는 등 연쇄적 피해가 발생할 수 있어 주의가 필요하다.

11 월에는 악성코드에 AI 기능을 탑재한 '라다만티스(Rhadamanthys)'가 등장했다. 라다만티스는 2022 년에 처음 공개된 정보 탈취형 멀웨어로, 올해 4 월에는 공격에 사용되는 PowerShell 스크립트가 LLM 으로 제작되었을 가능성이 있는 것으로 분석됐다. 해당 악성코드는 빠른 속도로 발전하고 있으며, 최근에는 광학 문자 인식(OCR)[5]을 위한 AI 기능이 추가되어 탈취한 이미지에서 암호화폐 지갑 시드 문구를 자동으로 추출해 공격자의 서버로 전달한다. 이는 현재 다크웹을 통해 활발히 거래되고 있으며, 암호화폐 지갑 정보와 사용자 자격증명 탈취를 목적으로 하는 공격자들에게 큰 호응을 얻고 있다.

[5] 광학 문자 인식(OCR): 이미지나 문서에서 텍스트를 인식하고 추출하는 기술

■ 2024년 주요 보안 이슈 Key Point



[2024 년 주요 보안 이슈 Key Point]

2024 년 주요 보안 이슈 Key Point 는 다음 3 가지로 분류할 수 있다.

범죄 도구로 활용되는 AI

AI를 활용한 직접적인 공격 수행이 아직 어렵지만, AI는 피싱 메일 작성, 악성 스크립트 제작, 악성코드에 AI 기능 탑재 등 사이버 공격의 보조 수단으로 활발히 활용되고 있다. 특히 딥페이크/딥보이스 기술을 악용한 디지털 성범죄가 심각한 사회문제로 떠올랐다. AI 기술이 빠르게 발전하면서 일반인도 쉽게 악용할 수 있게 되었고, 이로 인해 누구나 피해자가 될 수 있는 상황이다. 따라서 AI 관련 법제도 마련과 함께 사회적 인식 개선이 시급하다.

공급망 공격의 다양화

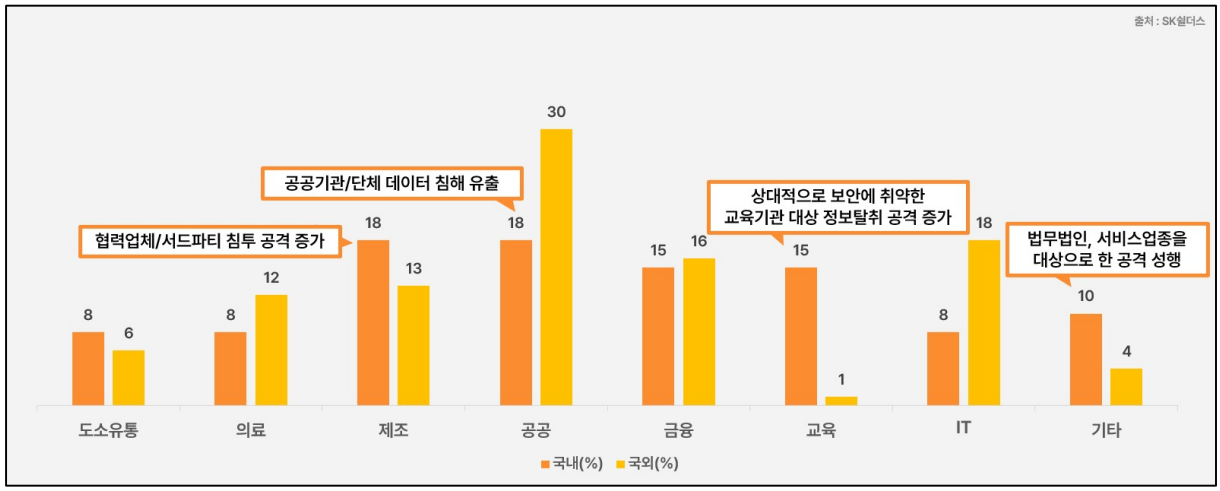
오픈소스 플랫폼과 패키지 매니저 등 다양한 소프트웨어를 노린 공급망 공격이 지속되었고, 이는 다수의 사용자를 대상으로 N 차 공격으로 이어졌다. 또한, 기업 본사보다는 상대적으로 보안이 취약한 서드파티, 협력사 등을 대상으로 하는 공격이 성행했다. 협력사 침해사고 발생 시 협력사를 공격 통로로 활용하는 등 추가 피해가 발생할 수 있어, 1~2 차 협력사에서도 강도 높은 보안대책 수립이 필요하다.

랜섬웨어 그룹의 전략 고도화

랜섬웨어 그룹은 초기침투에 상용 RMM(Remote Monitoring and Management, 원격 모니터링 시스템) 도구를 악용하거나 사회공학적 기법으로 피해 서버에 RMM 설치 및 실행을 유도하고 있다. 이들은 합법적인 툴을 활용해 내부 침투 후 랜섬웨어를 배포하는 형태로 전략을 고도화하고 있으며, 내부시스템에서 하이퍼바이저 환경으로 랜섬웨어 공격 표적이 확대되고 있다. 이와 같이 고도화되고 있는 랜섬웨어 공격에 선제적으로 대응하고 탐지할 수 있는 보안 체계를 구축해야 한다.

주요 보안 이슈와 관련된 자세한 공격 시나리오는 **'24 년 보안 이슈 리뷰**에서 이어진다.

■ 업종별 침해사고 발생 통계



[2024 년 업종별 침해사고 발생 통계]

2024 년 국내 업종별 보안 사고 통계를 살펴보면 제조업과 공공 분야가 각각 18%로 가장 높은 비중을 차지하며 주요 타깃이 된 것으로 나타났다. 금융과 교육 분야가 각각 15%를 기록하며 상위권에 속했고, IT, 의료, 도소유통 분야가 8%로 뒤를 이었다.

국내 제조업의 경우 설계 도면이나 생산 현장 사진 등 기업의 핵심 자산이 유출되는 사고가 발생했으며, 이는 접근 권한 관리의 미흡과 보안이 약한 협력사를 통해 유입된 악성코드 공격 때문인 것으로 밝혀졌다. 특히 서드파티를 통한 공격이 증가하면서 공급망 보안이 중요한 과제로 부상하고 있다.

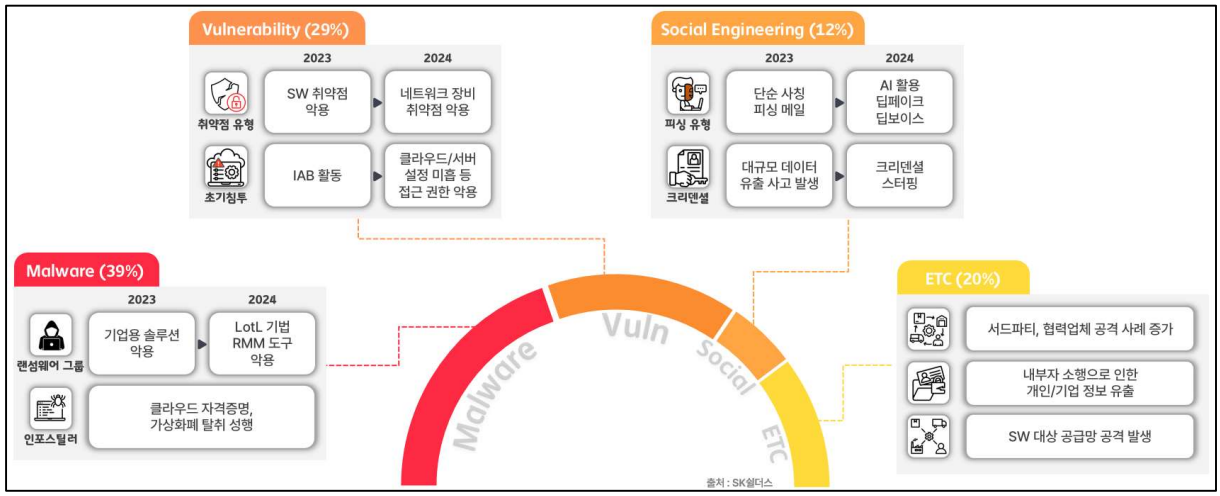
공공기관과 군 관련 기관, 지방자치단체에서는 개인정보 유출 사고가 지속적으로 발생했다. 주로 내부 접근 권한 관리 미흡과 보안 설정이 불완전한 서버를 대상으로 한 공격에서 비롯됐다.

대량의 개인정보를 가진 교육기관도 주요 공격 대상이 되고 있으며, 상대적으로 보안이 취약한 점이 사고의 주요 원인으로 지목되고 있다. 특히 웹 서버의 취약점을 악용하거나 접근 제어가 제대로 이루어지지 않는 환경에서 데이터 유출 사고가 발생했다.

또한, 올해는 서비스 업종에서의 보안 사고가 두드러졌으며, 특히 법무법인과 같이 중요정보를 다루는 업체를 대상으로 한 공격이 활발히 이뤄졌다. 랜섬웨어와 웹 해킹이 주된 공격 수단으로 활용됐고, 탈취한 정보를 빌미로 금전을 요구하거나 다크웹에 BTC 로 판매하는 사례가 있었다.

해외에서는 공공 분야가 전체 보안 사고의 21%를 차지하며 가장 높은 비중을 보였고, IT, 금융, 제조 분야가 뒤를 이었다. 특히 데이터 관리 업체인 NPD(National Public Data)에서 약 29 억 건, 통신 기업 AT&T 에서 1 억 여 명에 달하는 개인정보가 유출됐다. 국가 배후 해킹 그룹에 의한 공격도 여전히 활발했으며, 국가 간 긴장이 고조되는 가운데 주요 인프라와 공공기관에 대한 해킹 시도가 끊이지 않았다.

■유형별 침해사고 발생 통계



[2024 년 유형별 침해사고 발생 통계]

2024 년 유형별 침해사고 발생 통계를 살펴보면 멀웨어 공격이 39%, 취약점 악용 공격이 29%, 소셜 엔지니어링이 12%를 차지했으며, 서드파티 공격, 내부자 정보 유출, 공급망 공격 등 기타 유형이 20%로 뒤를 이었다.

먼저, 멀웨어 공격이 39%로 가장 높은 비율을 차지했으며, 랜섬웨어 공격 유형의 변화가 눈에 띄었다. 2023 년에는 기업용 솔루션을 악용하는 사례가 많았지만, 2024 년에는 LotL[6] 기법이나 RMM 도구 등을 악용한 탐지 회피 전략을 보였다. 또한 클라우드 자격증명이나 가상화폐 탈취 등 정보 탈취를 목적으로 하는 인포스틸러도 함께 성행했다.

두번째로, 취약점을 악용한 공격이 29%의 비율을 차지했다. 2023 년에는 소프트웨어 취약점을 악용하는 공격이 많았던 반면, 2024 년에는 네트워크 장비 취약점을 통한 공격이 대량으로 발생했다. 또한 시스템 초기 침투를 위해 IAB[7]를 통해 정보를 구매하는 대신 클라우드나 서버의 설정 미흡 등 취약한 접근 권한을 악용하는 형태로 변화했다.

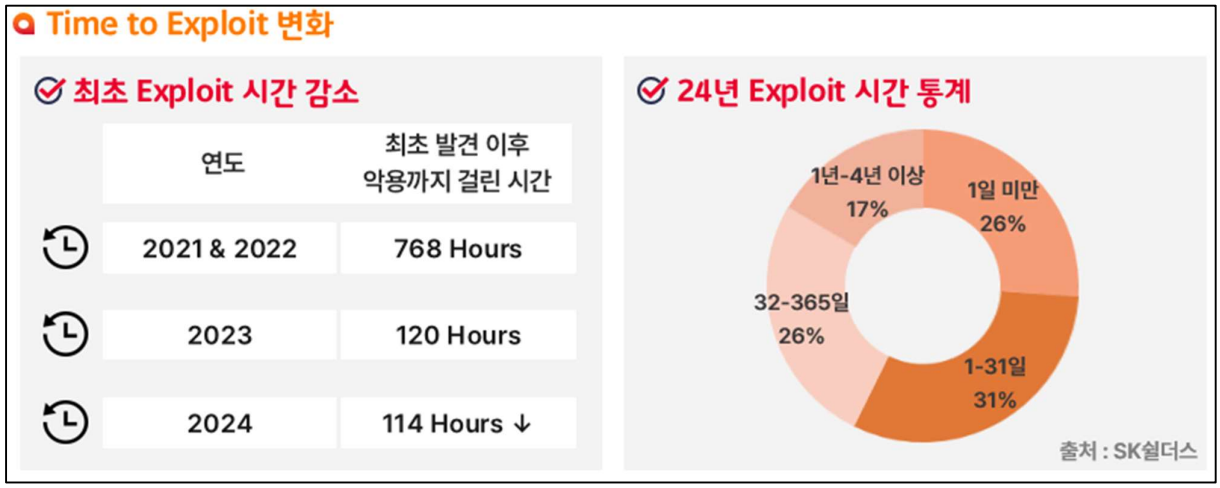
소셜 엔지니어링은 12%를 차지했는데, 피싱 유형이 단순 사칭 메일에서 AI 를 활용한 딥페이크/딥보이스 피싱으로 변화한 것이 눈에 띄었다. AI 기술의 발전으로 정교해진 딥페이크/딥보이스는 사실 여부 판단이 어렵기 때문에 각별한 주의가 필요하다. 더불어 2023 년에 발생한 대규모 데이터 유출 사고의 영향으로 탈취한 계정정보를 다른 사이트에 대입해보는 크리덴셜 스터핑이 성행했다.

이외에도 협력사나 서드파티를 공격하는 사례가 나타났으며, 내부자 소행으로 인한 정보 유출이 활발히 발생했다. 또한 S/W 공급망 공격이 지속되고 있어 기업 내/외부로 각별한 주의가 필요하다.

[6] LotL(Living off the Land): 탐지 및 차단 회피를 위해 시스템의 기본 도구와 프로세스를 악용하는 공격

[7] IAB(Initial Access Broker): 시스템에 대한 무단 접근 권한을 얻은 후 판매하는 위협 행위자

■ 취약점 동향



[Time to Exploit 변화]

2024 년 취약점 동향은 크게 두 가지의 특징을 보이고 있다.

첫 번째는 TTE(Time to Exploit)가 눈에 띄게 감소했다는 점이다. 취약점 공개 이후 최초 악용까지 걸리는 시간을 TTE 라고 하는데, 2018-2019 년 평균 1512 시간(63 일)에서 2021-2022 년 768 시간(32 일)으로 단축됐고, 2023 년에는 큰 폭으로 감소하여 평균 120 시간(5 일)을 기록했다. 2024 년 11 월을 기준으로 평균 114 시간(4.75 일) 이하로 더욱 감소해, TTE 는 계속 짧아지고 있다.

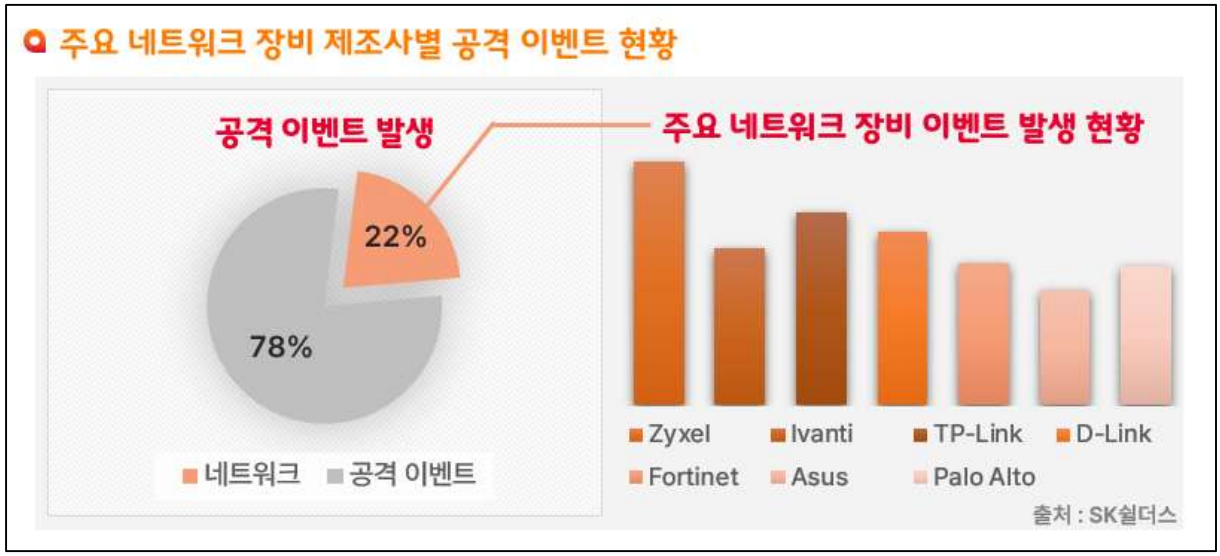
2024 년 11 월을 기준으로 취약점 공개 이후 최초 악용까지 걸리는 시간을 살펴보면, 취약점 공개 후 1 일 미만에서 악용된 사례가 26%, 1 일 이상 31 일 이하가 31%, 32 일 이상 365 일 이하가 26%, 1 년 이상이 17%로 나타났다. 이를 통해 과반수 이상의 취약점이 공개 후 1 개월 이내에 악용되며, 이 중 절반은 1 일 이내에 악용되는 것을 알 수 있다.

[Time to Exploit 사례]

실제로 2024 년 공개된 취약점 중 악용 시간이 1 일 미만인 사례가 다수 존재했다. TeamCity 인증 우회 취약점은 공개 후 24 시간 이내에 Jasmin 랜섬웨어 변종 배포에 악용됐다. PHP CGI Command Injection 취약점 또한 공개 후 24 시간 이내에 TellYouThePass 랜섬웨어 그룹으로부터 악용됐으며, 하반기에는 WhatsUp Gold 의 SQL Injection 취약점이 공개 후 단 5 시간 이내에 악용되어 다수의 RAT[8] 설치에 악용된 사례가 있었다.

이처럼 TTE 가 급격히 감소함에 따라 방어자는 실시간으로 위협을 탐지하고 대응할 시간이 부족해지고 있다. 따라서 전체 시스템과 네트워크를 대상으로 발생 가능한 위협을 선제적으로 조치하고, 취약점 발생 시의 영향도를 고려하여 접근 제어를 구현하는 것이 필요하다. 패턴 기반 탐지 보다는 행위 기반 탐지 솔루션을 통해 비정상적인 행위를 실시간 탐지하고, 위협 초기 단계에서 공격 체인을 끊어내는 것이 중요하다.

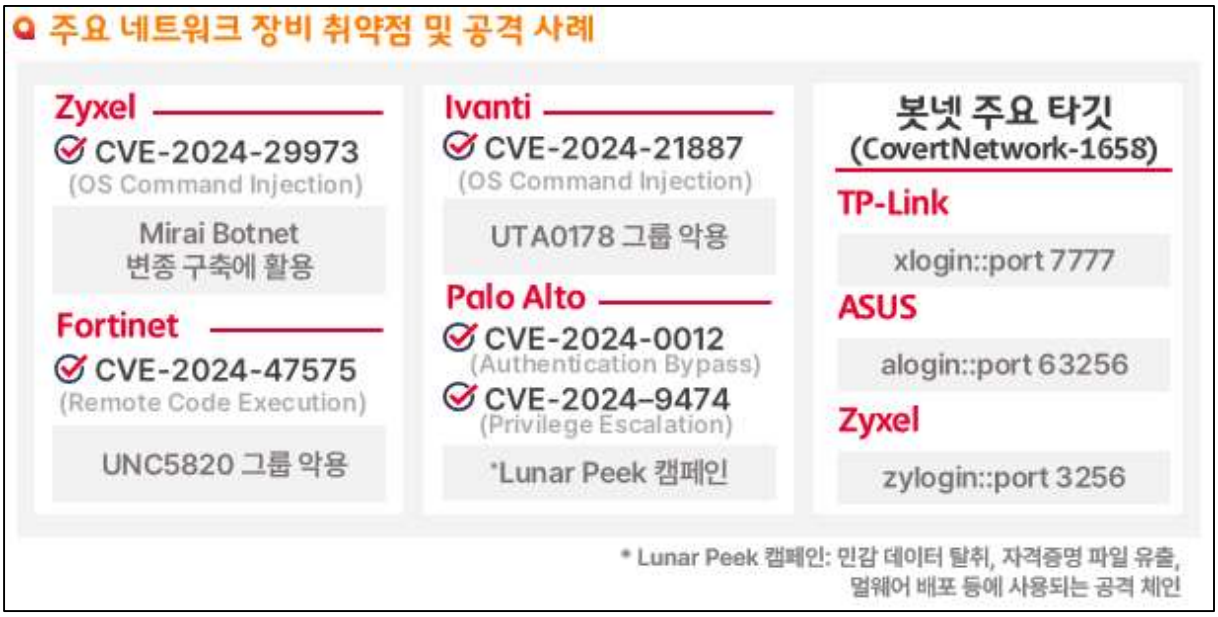
[8] RAT(Remote Access Tool, Remote Administrator Tool): 원격에서 시스템에 물리적 접근권한이 있는 것처럼 시스템을 제어하게 해주는 S/W 및 프로그래밍 모음으로 해당 사례에서는 Atera Agent, Radmin, SimpleHelp Remote Access, Splashtop Remote가 활용되었음



[2024 년 주요 네트워크 장비 공격 이벤트 현황]

두 번째 특징은 네트워크 공격 비율이 높게 나타났다는 것이다. 네트워크 장비를 대상으로 한 신규 취약점들이 지속적으로 발견되고, 공격자들로부터 활발히 악용되어 2024 년 전체 공격 이벤트 발생 비율 중 네트워크 공격 비율이 22%로 높은 비중을 차지했다.

Zyxel, Ivanti, Fortinet, Palo Alto 등 다양한 제조사별 네트워크 장비에 대한 공격 이벤트가 꾸준히 발생했으며, Zyxel 제품을 대상으로 한 공격은 작년에 이어 지속적으로 발생했다. 올해 1 월과 9 월에는 Ivanti 제품에 대한 파급력 높은 취약점들이 발견되면서 Ivanti 제품을 타깃으로 한 공격이 성행했으며, 이외에도 TP-Link, D-Link, ASUS 등 다수의 취약한 네트워크 장비가 Botnet 구축에 활용되거나 멀웨어 배포 확산에 악용됐다.



[주요 네트워크 장비 취약점 및 공격 사례]

공개된 주요 네트워크 장비의 취약점과 공격 사례는 다음과 같다.

Zyxel 의 NAS 제품 취약점(CVE-2024-29973)은 공격자가 인증 없이 원격으로 임의의 운영체제 명령을 실행할 수 있으며, 이는 Mirai Botnet 변종 구축에 악용됐다. 또한, 랜섬웨어 그룹 'HellDown'은 Zyxel 의 방화벽 취약점(CVE-2024-42057)을 악용해 기업 네트워크에 침투하고 데이터 탈취 및 암호화를 하는 것으로 나타났다.

Fortinet 의 FotriManager 에서 발견된 취약점(CVE-2024-47575)은 인증 누락으로 인해 공격자가 임의의 코드나 명령을 실행할 수 있으며, 이는 새로운 위협 그룹인 UNC5820 에 의해 50 개 이상의 조직을 공격하는데 악용됐다.

Ivanti VPN 제품의 Command Injection 취약점(CVE-2024-21887)은 다른 취약점들과 연계해 인증되지 않은 공격자가 원격 코드를 실행할 수 있었고, 이외에도 파급력 높은 추가 취약점이 연달아 공개되며 UTA0178, Volt Typhoon, UNC5330, UNC5337 등 다양한 공격 그룹에서 악용했다.

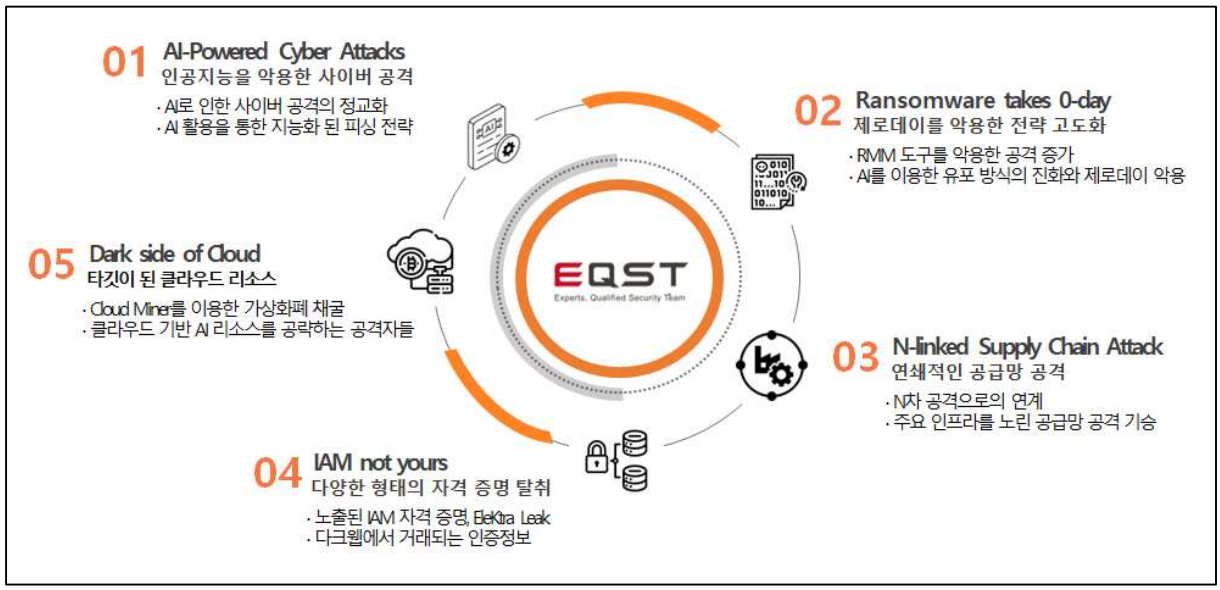
Palo Alto 의 방화벽 펌웨어에서 발견된 인증 우회 취약점(CVE-2024-0012)과 권한 상승 취약점(CVE-2024-9497)은 제로데이 공격 캠페인 'Lunar Peek'에 악용됐다. 공격자는 해당 취약점을 통해 방화벽 관리 웹 인터페이스에 대한 관리자 권한을 획득하고, 민감 데이터 탈취, 자격증명 파일 유출, 멀웨어 배포 등을 진행했다. 이에 따라 미국, 인도 등 여러 나라에서 해당 캠페인을 통한 피해 사례가 보고됐다. 이후 11 월, 해당 취약점에 대한 상세 기술 분석 보고서가 공개된 후 C2 도구 및 암호화폐 채굴기 설치와 같은 위협 활동이 증가한 것으로 보아 취약한 네트워크 장비를 대상으로 하는 공격은 지속될 것으로 보인다.

이외에도 중국 위협 그룹 Storm-0940 이 운영하는 Botnet 인 'Quad7(CovertNetwork-1658)'의 활동이 성행했다. 기존에는 TP-Link 라우터를 대상으로 공격을 진행해왔으나, 최근에는 ASUS 라우터, Zyxel VPN, Ruckus Wireless 장비 등 다양한 네트워크 장비로 타깃을 확장해 현재까지 175,000 대 이상의 기기를 손상시켰다. 주로 제조사 지원이 중단되거나 패스워드 설정이 취약한 네트워크 장비를 대상으로 공격을 감행했으며, 각각의 Botnet 은 익명 프록시를 설치해 피해자들의 MS 365 계정 정보 탈취에 활용됐다.

올해는 네트워크 장비를 대상으로 하는 신규 취약점들이 지속적으로 등장했고, 공격자들은 이를 Botnet 구축과 멀웨어 배포 등에 적극 악용했다.

따라서 네트워크 장비에 대한 엄격한 접근 통제를 수행해야 하며, 지속적인 모니터링을 통한 보안 취약성 검토 및 대응책 마련이 중요하다. 또한, 제조사의 지원이 종료된 제품의 경우, 보안 위협을 고려하여 안전하게 폐기하거나 대체 제품의 도입을 고려해야 한다.

24 년 보안 이슈 리뷰



[2024 년 보안 이슈 Review]

AI-Powered Cyber Attacks 영역에서는 LLM으로 제작한 악성 스크립트와 AI 기능이 탑재된 악성코드가 다크웹에서 활발히 거래됐다. 또한, 딥페이크 기술을 악용해 성 착취물을 제작하고 유포하거나, 피해자에게 금전적 협박을 하는 디지털 성범죄가 확산됐다. AI 기술의 발달로 사이버 공격이 더욱 정교해졌으며, 일반인들도 쉽게 접근가능해 AI 기술의 양면성이 드러나는 계기가 됐다.

이에 대비하기 위해 국가 및 기업에서는 AI를 악용한 사이버 공격에 대한 선제적이고 종합적인 대응 방안을 마련해야 한다. 기업에서는 AI 기반 보안 솔루션, 제로 트러스트 등 고도화된 AI 공격에 대응하기 위해 보안 체계를 강화해야 하며, 정부에서는 AI 기술의 오남용을 방지하기 위한 법적 대응책을 마련하고, 딥페이크와 같은 신기술 악용 사례에 대한 엄격한 규제 도입이 필요하다.

Ransomware takes 0-day 부분에서는 원격 모니터링 및 관리 시스템(RMM)을 악용한 다양한 형태의 공격 전술이 확인됐다. RMM 솔루션의 손상된 계정이나 취약점을 이용해 초기 침투하거나, 고객 지원 센터로 위장해 RMM 설치를 유도하는 등 다방면으로 RMM을 공격에 활용하는 모습을 보였다.

또한, 랜섬웨어 그룹의 제로데이 악용 사례가 다수 확인됐다. 'BlackBasta' 그룹은 2024년 2월 Windows 권한 상승 취약점을 악용했으며, 6월에는 Windows 운영체제 취약점을 악용했다. 뿐만 아니라, 가상 환경 플랫폼인 ESXi 하이퍼바이저 취약점이 'BlackBasta', 'Akira' 그룹에 의해 악용됐으며, 최근에는 'PSAUX' 랜섬웨어가 웹 호스팅 제어판 CyberPannel 취약점을 악용해 공격을 수행했다.

이처럼 상용 RMM 솔루션과 제로데이가 점차 지능화된 방식으로 공격에 악용되고 있어 개인 및 기업에서는 최신 동향을 이해하고 적극적으로 사전 예방책을 준비해야 한다.

N-linked Supply Chain Attack 부분에서는 다양한 영역에서 공급망 공격이 활발했다. 오픈소스 플랫폼의 패키지 매니저를 변조하거나 게임사에 제공되는 보안 솔루션 및 설치 파일 등에 악성코드를 삽입하여 다수의 사용자 또는 기업을 대상으로 하는 공급망 공격이 발생했다.

이러한 공급망 공격에 대응하기 위해 SBOM[9]을 활용해 전반적인 소프트웨어 위험을 식별해야 하며, SBOM 의 주기적인 업데이트와 검증을 통해 실시간으로 올바른 대응을 할 수 있도록 해야 한다. 새로운 모듈 및 소프트웨어 개발의 경우, SAST(Static Application Security Testing), DAST(Dynamic Application Security Testing)를 통해 개발 및 운영 단계에서 발생할 수 있는 취약점을 1 차적으로 탐색하고 예방해야 한다.

IAM not yours 부분에서는 네트워크 장비 취약점을 통해 시스템에 침투한 후 IAM(Identity and Access Management, 클라우드 환경에서 사용자와 권한을 관리하는 시스템) 정보를 수집하거나 다크웹에 판매하는 사례가 있었으며, 수집한 IAM 정보를 활용한 연계 공격이 발생했다. 공격자는 Github, 웹 Application 등 외부에 노출되거나 멀웨어를 통해 탈취한 IAM 정보를 통해 클라우드 리소스를 장악했다.

IAM 정보를 활용한 공격은 서비스 무단 액세스 및 데이터 탈취 등의 연쇄적인 공격이 가능하기 때문에 계속해서 공격자들의 타깃이 될 것으로 보인다. 따라서 사용자는 외부 접근 가능 여부, 최소 권한 원칙 적용 여부, 다중인증(MFA) 적용 여부 등 IAM 정보에 대한 보안 점검에 주의해야 한다. 또한 시스템 내부에 존재하는 IAM 정보에 접근하는 것을 예방하기 위해 운영 환경에 대한 취약점을 사전에 식별하고 보완하는 노력이 필요하다.

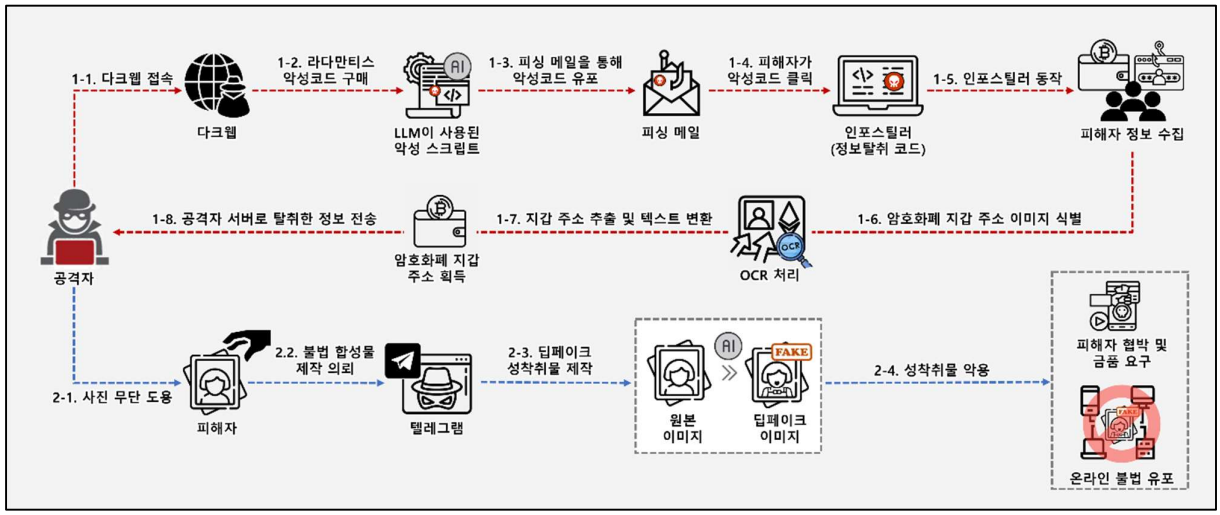
Dark side of Cloud 부분에서는 클라우드 리소스를 활용해 암호화폐를 채굴하는 다양한 사례가 존재했다. 공격자들은 허위 기업을 등록해 클라우드 서비스 제공 업체를 속여 그래픽 카드가 장착된 대규모 컴퓨팅 자원에 대한 액세스 권한 획득 후 약 13 억 원 상당의 암호화폐를 채굴했다.

뿐만 아니라 클라우드 및 컨테이너 환경을 주요 타깃으로 삼는 'TeamTNT' 그룹의 공격 사례가 있었다. 이들은 노출된 Docker 데몬을 표적으로 삼아 사이버 웜과 암호화폐 채굴기를 배포하고, 감염된 서버와 Docker Hub 를 통해 멀웨어를 확산시켰다.

이러한 클라우드 관련 위협에 대응하기 위해 정기적인 취약점 점검을 진행해야 하며, 클라우드 공급업체와 협력해 보안 인증 절차를 강화하는 것이 중요하다. 또한, 클라우드 서비스의 접근 권한을 최소한으로 제한하고, 다단계 인증을 도입해 계정 탈취로 인한 추가 피해를 방지하기 위한 대비가 필요하다.

[9] SBOM(Software Bill of Materials): 버전, 라이브러리 등 사용하는 S/W에 대한 상세 정보를 기술한 목록

■ AI 공격 시나리오



[AI 공격 시나리오]

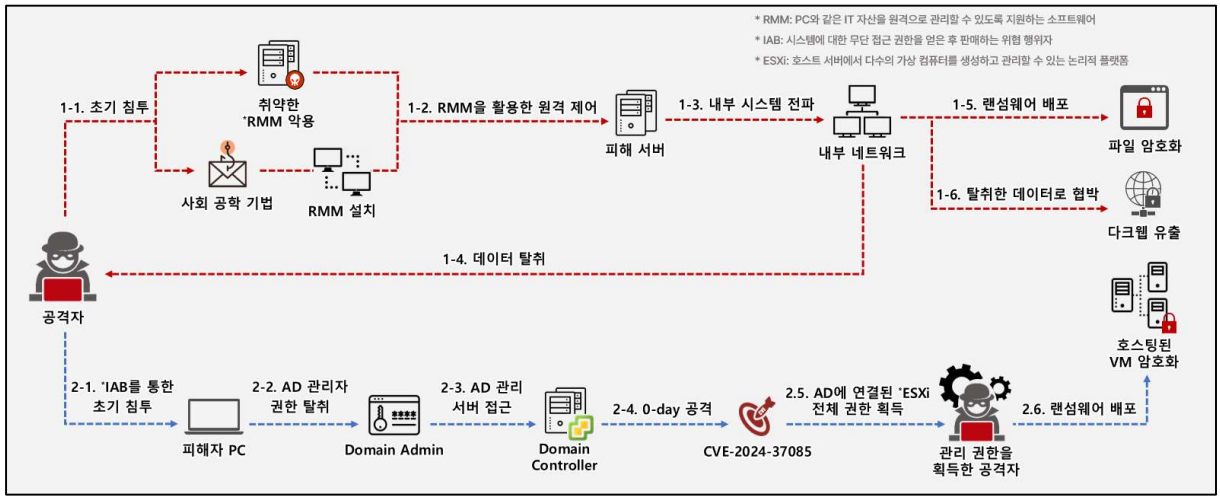
AI 기술의 발전으로 다양한 분야에서 활용도가 높아지는 동시에, 이를 악용한 사이버 공격의 고도화가 진행되고 있다.

첫 번째 시나리오는 AI 기능을 탑재한 라다만티스 악성코드 공격 사례이다. 공격자는 다크웹을 통해 라다만티스 악성코드를 구매한 뒤, 피싱 메일을 통해 피해자에게 발송한다. 피해자가 메일을 열거나 링크를 클릭하면 악성코드가 실행되어 피해자 PC 에서 정보를 수집한다. 수집한 정보들 중 암호화폐 지갑 이미지를 선별한 뒤, OCR 기능을 통해 시드 문구를 자동 추출한 뒤 공격자 서버로 전송한다.

두 번째 시나리오는 딥페이크 기술을 악용한 디지털 성범죄 사례이다. 공격자는 온라인 커뮤니티 및 SNS 에 공개된 사진을 무단 수집해 텔레그램과 같은 비밀 채널이나 다크웹을 통해 불법 합성물 제작을 의뢰한다. 이후 딥페이크를 통해 성 착취물을 생성하고, 이를 금전 협박 수단으로 활용하거나 온라인에 불법 유포한다.

위 두 시나리오는 AI 기술을 악용한 새로운 사이버 공격 방식의 등장을 보여주며, 악성코드의 고도화나 딥페이크 악용이 더욱 확대될 가능성을 시사한다.

■ 랜섬웨어 공격 시나리오



[랜섬웨어 공격 시나리오]

랜섬웨어 그룹은 다방면으로 RMM 을 활용하고 있으며, 내부 시스템에서 가상환경으로 표적을 확대하고 있다.

첫 번째 시나리오는 RMM 을 악용한 랜섬웨어 공격 사례이다. 공격자는 주로 내부 시스템에 존재하는 RMM 의 취약점을 악용하거나, 사회공학 기법을 이용해 RMM 설치를 유도한다. 이후, 취약한 RMM 을 활용해 내부 시스템에 침투하고, 데이터를 탈취하거나 랜섬웨어를 배포한다. 탈취한 데이터는 다크웹에 판매하거나, 데이터 유출을 빌미로 금전을 요구하는 등 피해자 협박으로 이어진다.

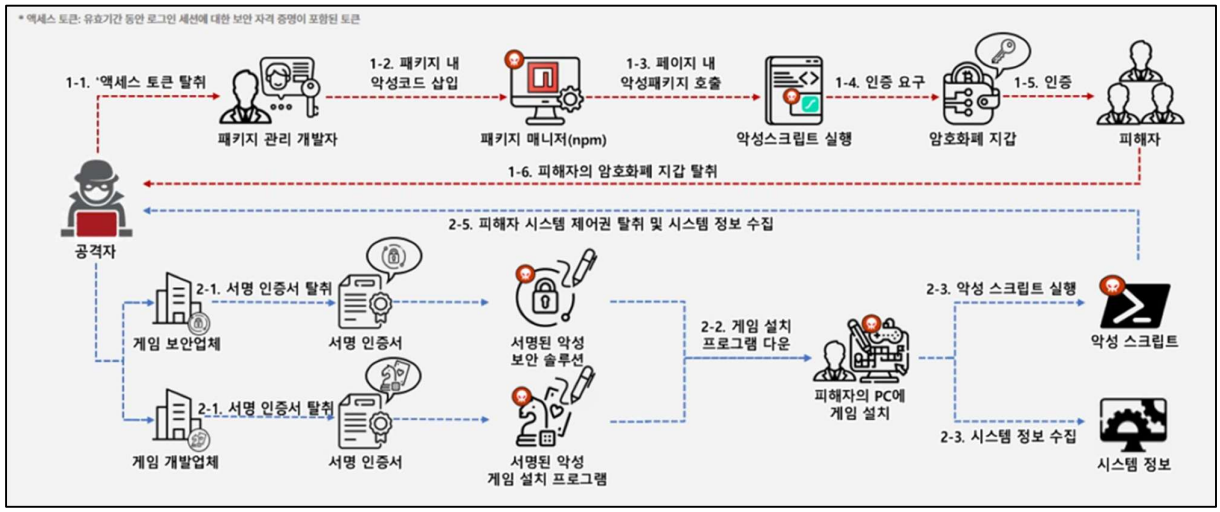
실제로 'BlackBasta', 'BI00dy', 'Play', 'Qillin' 등 다양한 랜섬웨어 그룹들이 RMM 취약점을 악용해 내부 시스템에 침투했으며, 'Mad Liberator' 그룹과 'BlackBasta' 그룹은 사회공학기법을 사용해 초기 침투를 시도하기도 했다.

두 번째 시나리오는 제로데이 취약점을 악용한 랜섬웨어 공격 사례이다. 공격자는 IAB 를 통해 초기 침투를 수행하고, 침투한 시스템에서 AD(Active Directory)[10]의 관리 권한을 가진 Domain Admin 의 자격증명을 탈취한다. 이후 탈취한 권한으로 AD 관리 서버인 Domain Controller 에 접근한 뒤, ESXi 인증 우회 취약점(CVE-2024-37085)을 악용해 호스팅된 ESXi 의 전체 권한을 획득한다. 공격자는 전체 권한을 이용해 랜섬웨어를 배포하며, ESXi 의 파일 시스템뿐만 아니라 호스팅된 모든 VM(Virtual Machine, 가상 컴퓨터 시스템)을 암호화한다.

최근 랜섬웨어 그룹들은 악성 행위가 탐지되거나 차단될 가능성을 낮추기 위해 RMM 과 제로데이를 악용하는 등 공격 방식을 고도화하고 있으므로, 적극적인 사전 예방과 대응이 필요하다.

[10] Active Directory: Windows에서 제공하는 IT 자산 통합 관리 서비스

■ 공급망 공격 시나리오



[공급망 공격 시나리오]

유명 오픈소스 플랫폼의 패키지 매니저를 변조하거나, 공급업체 및 개발업체를 대상으로 한 다양한 유형의 공급망 공격이 발생하고 있다.

첫 번째 시나리오는 오픈소스 플랫폼의 패키지 매니저를 변조한 공급망 공격 사례이다. 공격자는 패키지 관리 개발자의 액세스 토큰을 탈취한 후 패키지 내 악성코드를 삽입한다. 악성코드가 포함된 패키지가 사용자에게 배포되고 실행되면, 정상 서비스로 위장한 암호화폐 지갑 인증 팝업이 표시된다. 피해자는 의심없이 암호화폐 지갑 인증 정보를 입력하고, 공격자는 피해자의 암호화폐 지갑 정보를 탈취할 수 있다.

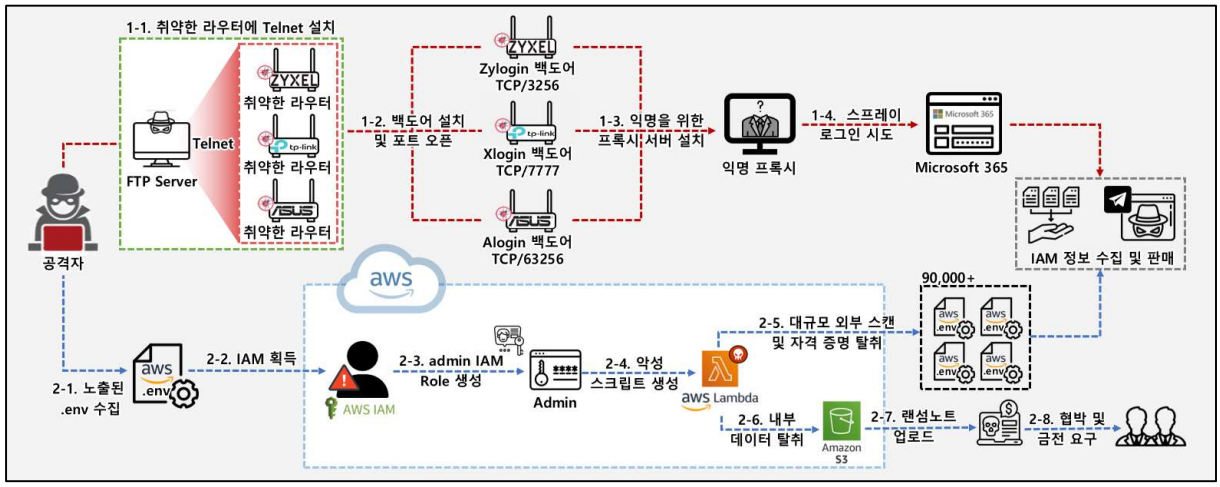
두 번째 시나리오는 국내 게임 보안 솔루션 공급업체 및 게임 개발업체를 대상으로 발생한 공급망 공격 사례이다. 공격자는 게임 보안 솔루션 공급업체의 서명 인증서를 탈취한 후 악성 보안 솔루션에 서명을 진행한다. 이후 해당 솔루션이 게임사에 배포되고, 이를 다운 받은 피해자의 PC 에서 악성 보안 솔루션이 동작한다. 해당 보안 솔루션은 악성스크립트를 실행해 공격 대상의 IP 주소를 판별하고, 특정 IP 주소에 해당할 경우 Remcos RAT[11]을 다운로드 한다.

또한, 공격자는 게임 개발업체의 서명 인증서를 탈취한 후 게임 설치 파일에 악성코드를 삽입한다. 이후 악성코드가 삽입된 설치 파일이 배포되면, 이를 다운 받은 피해자의 PC 에서 악성코드가 동작하여 피해자의 하드웨어 및 Windows 버전 정보를 수집해 공격자 서버로 전송한다.

최근 공급망 공격에서 오픈소스 플랫폼, 패키지 매니저 등 다수의 사용자가 이용하는 시스템을 변조하는 사례가 증가하고 있다. 이에 따라 사용자는 오픈소스 플랫폼 이용 시 각별한 주의가 필요하다. 또한, 단순히 서비스 제공업체를 직접 공격하는 것이 아닌 공급업체와 같은 협력사 등을 통한 공격이 활발히 발생하고 있어, 서드파티에 대한 보안관리와 주의가 더욱 중요해지고 있다.

[11] Remcos RAT: 원격제어, 키로깅, 백도어 설치, 정보 탈취 등 다양한 악성 행위를 수행하는 악성코드로, 본래 시스템 원격 관리를 위해 개발된 합법적인 도구이나 시스템 권한을 탈취하기 위한 목적으로 다양한 해킹 캠페인에 악용되고 있음.

■ IAM 공격 시나리오



[IAM 공격 시나리오]

IAM 정보 수집 및 판매를 목적으로 하는 공격과 노출된 IAM 정보를 악용한 공격 사례가 증가하고 있다.

첫 번째 시나리오는 취약한 네트워크 장비를 통한 IAM 정보 유출 사례이다. 공격자는 취약한 네트워크 장비를 타깃으로 원격 코드 실행 공격을 시도한다. 공격 성공 시, 원격 FTP 서버를 통해 Telent 바이너리와 각 네트워크 장비에서 활용할 백도어를 설치한 후 포트를 연다. 이때 공격자는 추적을 피하기 위해 익명 프록시 역할을 하는 SOCKS5[12] 프록시를 설치하며, 이를 통해 MS 365 계정을 획득하기 위해 슬로우 스프레이 공격[13]을 시도한다. 이후 수집한 로그인 정보를 피싱 메일에 악용하거나 다크웹에 판매한다.

두 번째 시나리오는 외부에 노출된 .env 파일을 수집해 획득한 IAM 을 악용하는 사례이다. 공격자는 Github 또는 웹 Application 등 외부에 노출된 AWS .env 파일을 수집한다. 해당 파일 정보를 기반으로 클라우드 환경에 대한 초기 액세스 권한을 획득한다. 이때 탈취한 클라우드 환경은 권한 설정을 제한하고 있지 않아, 공격자는 이를 악용해 관리자 권한 획득이 가능했다. 이후 관리자 권한의 공격자는 Lambda 함수를 생성해 대규모 공격을 위한 자격증명 스캐너로 악용하고, S3 스토리지의 내부 데이터를 탈취해 비트코인을 요구하는 랜섬노트를 업로드한다.

IAM 정보는 다른 서비스의 공격에도 악용할 수 있어 파급력이 크다. 따라서 사용자는 철저한 IAM 관리와 함께 클라우드 환경 전반의 취약점을 사전에 식별하고 보완해야 한다.

[12] SOCKS5(Socket Secure 5): 클라이언트와 서버 간 트래픽을 중계하는 프록시 기능을 제공하는 네트워크 프로토콜

[13] 슬로우 스프레이 공격: 다량의 계정에 로그인 시도를 수행할 때, 발각될 위험을 줄이기 위해 하루에 한 번 정도의 매우 느린 속도로 로그인 시도를 반복하는 고도화된 크리덴셜 공격 방식

25 년 5 대 사이버 위협 전망

[2025 년 사이버 위협 전망]

■ Escalating AI Threat in AX

- AX 시대를 파고드는 AI 보안 위협

'모든 것이 디지털'인 시대였던 'DX(Digital Transformation)' 넘어 'AX(AI Transformation)'를 향해 나아가고 있다. 검색엔진 대신 ChatGPT 를 사용하는 사람들이 생겨났으며, 다수의 기업들은 기존과 신규 나눌 것 없이 AI 를 접목한 서비스를 제공하고 있어 AI 는 사용자들의 일상에 빠르게 녹아들고 있다.

그러나 AI 기술이 급속도로 성장하는 만큼 이를 악용하는 사례도 증가하고 있다. 고도화된 딥페이크와 딥보이스 기술이 피싱과 스미싱에 악용돼 큰 피해를 일으켰으며, 나아가 성 착취물 제작에까지 사용되면서 그 피해가 더욱 확산되고 있다

실제로 간편 금융 거래와 본인 인증, 로그인 등에서 활용되는 안면 인식 기술이 고도화된 딥페이크로실시간 우회가 가능해졌다. 특히, 노이즈를 추가해 딥페이크 탐지를 우회하는 기술도 등장하면서, 이를 악용한 공격이 증가할 것으로 예상된다. 뿐만 아니라 딥보이스를 악용해 기업 임원을 사칭한 뒤, 내부 인력으로부터 민감 데이터를 유출하거나 금전적인 손실을 초래할 가능성도 존재한다.

또한 많은 기업들이 sLLM(Small Large Language Model)을 이용한 기업 내부 시스템을 구축하는 사례가 증가함에 따라 이를 타깃으로 하는 공격도 발생할 것으로 전망된다. LLM 으로 구축된 시스템은 AI 가 최종 권한을 판단하고 실행하기 때문에, 이를 교묘하게 속여 관리자만 접근가능한 내부 중요 정보나 고객 데이터에 무단으로 접근하는 등의 공격이 발생할 수 있다.

■ The Changing Ransomware Landscape

- 다면적인 공격 기법과 협박 전략을 사용하는 Ransomware

기존의 랜섬웨어 그룹은 피해자의 파일을 암호화하고 랜섬노트를 통해 비용을 요구하는 전형적인 형태를 띄고 있었으나, 기업들의 사전 대비 및 사후 대응 등 보안 수준이 높아짐에 따라 수익성이 줄어들자 다면적인 공격 기법과 협박 전략을 사용하기 시작했다.

데이터 탈취 후 유포를 빌미로 하는 이중 협박을 넘어, 피해 기업과 연관된 협력사나 고객사를 추가로 협박하거나 디도스 공격을 병행해 기업의 핵심 업무 수행을 방해하는 다중 협박 전략이 등장하고 있다. 이러한 전략은 피해 규모를 확대하고 협상 압박을 강화해 금전적 수익성을 늘리는 방식으로 2025 년도에도 지속될 것으로 보인다.

또한 공격 기법은 각종 보안 솔루션을 우회하거나 비활성화하는 방식으로 변화하고 있다. 보안 솔루션탐지 회피를 위해 운영체제에서 기본적으로 제공하는 기능이나 사용자가 직접 시스템에 설치한 도구를 활용하거나, BYOVD(Bring Your Own Vulnerable Driver) 기법[14]을 활용해 시스템 권한으로 보안 솔루션을 비활성화하는 공격의 빈도가 증가하고 있다. 실제로 2024 년동안 489 건의 침해사고를 발생시킨 'RansomHub' 그룹에서 BYOVD 를 악용해 EDR(Endpoint Detection and Response) 프로세스를 무력화시킨 것으로 보아, 내년에도 많은 랜섬웨어 그룹에 의해 지속적으로 악용될 것으로 전망된다.

뿐만 아니라 주로 제로데이 취약점을 악용하던 기존의 방식과 달리, 최근에는 아직 패치를 적용하지 않은 시스템들을 대상으로 1-Day 취약점을 악용하고 있다. 1-Day 취약점은 제로데이보다 훨씬 악용하기 쉬울 뿐만 아니라, 위협에 노출된 시스템을 쉽게 찾아낼 수 있기 때문에 이를 악용한 랜섬웨어 공격이 증가할 것으로 보인다.

[14] BYOVD(Bring Your Own Vulnerable Driver): 합법적 서명이 적용된 드라이버의 취약점을 악용한 공격 기법

■ Deregulation and IAM Threat

- 망분리 규제 완화에 따른 IAM 위협 증가

2024 년 8 월, 금융위원회에서 금융권의 망분리 규제를 완화하고 개선하겠다는 로드맵을 발표했다. 외부 침입으로부터 자원을 보호하기 위해 네트워크를 나누던 망분리 규제는 하이브리드 클라우드, AI 등 외부 서비스 사용에 제약이 있어 디지털 금융의 장애물로 여겨졌다.

이러한 망분리 규제가 완화됨에 따라 금융권에서는 가명처리 된 고객데이터에 한해서 SaaS, AI, 빅데이터, MS 365 등의 협업 서비스를 활용할 수 있게 되었으며, 이를 통해 업무 생산성과 비즈니스 속도 향상 등 긍정적인 효과를 기대하고 있다. 하지만 가명처리 되지 않은 중요 정보의 유출, 랜섬웨어 공격 등과 같은 데이터 보안 위험과 데이터 마이그레이션[15]과 관련된 보안 위협 요소들도 함께 등장할 것으로 전망된다.

IAM 자격증명 관련 문제로 매년 크고 작은 사고들이 발생하고 있으며, 모든 해킹 공격의 시작이 IAM 을 타깃으로 한다고 할 수 있을 만큼 영향력이 커져가고 있다. 금융권 망분리 규제 완화에 따라 도입될 서비스들이 IAM 자격증명을 사용할 확률이 높고, 공격자들은 IAM 을 New Perimeters 로 여기는 경향이 많아져 피해사례가 증가할 것으로 예상된다.

[15] 데이터 마이그레이션: 운영에 미치는 영향을 최소화하면서 대량의 데이터를 다른 스토리지 시스템으로 이동하는 것

■ Chain Reaction of Cyber Incidents

- 협력사의 보안사고에 따른 연쇄 피해 위협

대기업 혹은 원청 기업들은 자체적인 정보보안팀을 꾸려 침해사고에 대비·대응하거나 ISO27001, ISMS-P 와 같은 국내외 정보보호 인증을 받으며 내부 자원을 보호하고 있다. 그러나 해당 기업들의 협력사들은 비교적 규모가 작고 보안담당자가 존재하지 않는다는 점을 악용해, 이들을 원청사의 공격 벡터로 삼는 경우가 많아질 것으로 전망된다.

특히, 2,3 차 협력사처럼 더 하위단계로 내려가게 되면 제품의 안정성 외에 시설보안이나 OT 보안은 투자하지 않는 경우가 많고, 보안팀이 없거나 소수의 보안담당자가 많은 업무를 하는 경우가 많아, C 레벨 임원의 적극적인 관심이 없다면 보안투자를 진행하기 어려운 게 현실이다. 따라서 원청사의 데이터 혹은 원청사 내부로 접근할 수 있는 정보를 탈취하기 위해 협력사를 대상으로 하는 공격시도가 계속될 것으로 보인다.

단순히 하나의 협력사의 피해로 끝나는 것이 아니라 관련된 다른 원청사와 협력사까지 피해가 번져, 협력사 보안사고 발생 시 연쇄적으로 N 차 피해가 발생할 것으로 전망된다.

■ Cryptocurrency exchange Target

- 암호화폐 거래소 해킹 공격 위협 증가

암호화폐 자금 세탁에 사용되는 믹서 서비스에 대한 제재가 철회되고, 재취임을 앞둔 트럼프의 암호화폐 지지로 가격이 상승하면서 암호화폐를 타깃으로 하는 공격이 확대될 것으로 보인다.

특히, 대량의 암호화폐를 다루고 있는 거래소의 경우 한 번의 공격 성공으로 많은 수익을 얻을 수 있어 공격자들에게 더없이 좋은 공격 타깃이 될 것이다. 실제로 올해 5 월 일본 DMM 거래소에서는 4,500 억원 상당의 비트 코인이 유출되는 사례가 있었다.

또한 암호화폐의 가치 상승은 개인을 대상으로 하는 탈취 캠페인으로 이어질 수 있다. 개인 투자자들을 대상으로 투자 전문가 혹은 관련 분야의 교수 등을 사칭해 암호화폐 지갑을 탈취하거나, 인터넷에 코인 마이너가 심어진 파일들을 배포한 후 피해자의 컴퓨터 자원을 이용해 코인을 채굴하는 등의 많은 피해가 발생할 것으로 전망된다.

대응 전략

■ 2025 년 보안 위협 대응 전략

[SK 쉴더스 대응 서비스]

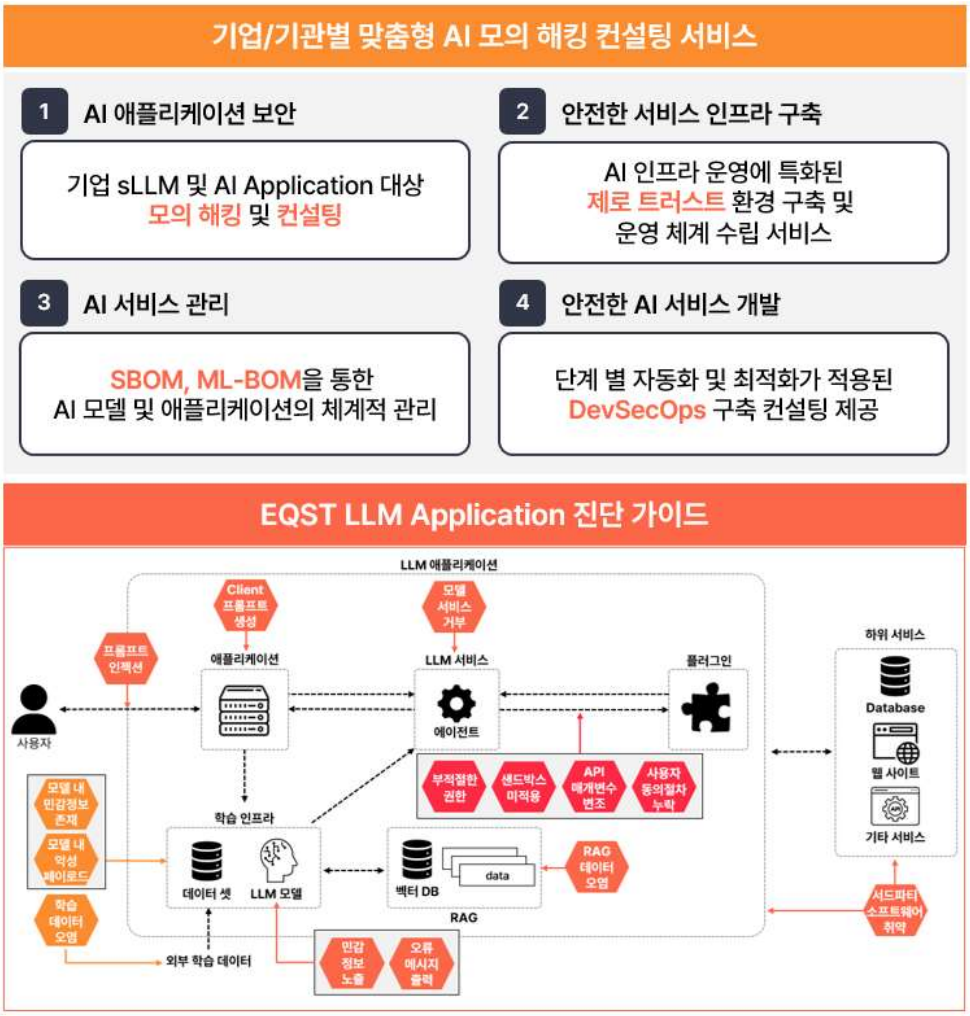
SK 쉴더스에서는 발전과 진화를 거듭하는 여러 보안 위협에 대응할 수 있도록, 지속적으로 정보보안 서비스를 고도화 및 강화하고 있다. SK 쉴더스의 다양한 서비스 중 앞서 전망한 위협들에 대응할 수 있는 맞춤형 서비스는 다음과 같다.

안전한 AI 서비스 구축 및 사용

AI 기술의 성능과 최적화 속도가 향상되면서 여러 기업에서 AI 를 적용해 활용하고 있다. 특히, 최근 sLLM 을 활용해 AI 서비스 플랫폼을 구축하는 기업들이 증가하면서, 개발 단계에서부터 운영까지 여러 관점에서 발생 가능한 보안 위협에 선제적 대응과 조치가 중요시되고 있다.

개발 단계에서는 DevSecOps 를 적용해 AI 서비스 플랫폼의 전체 개발 과정에 보안을 통합하고, 보안 테스트와 취약점 평가 등을 통해 보안 위협을 조기에 발견해 신속하게 대응해야 한다. 또한, 대부분 오픈소스 패키지와 클라우드 환경을 활용하여 AI 인프라를 구성하기 때문에 정기적인 보안 점검을 통해 사용 중인 소프트웨어에 존재하는 취약점을 제거하고 안전한 인프라 환경을 유지하는 것이 좋다. 특히, AI 서비스 플랫폼을 구성하고 있는 소프트웨어의 보안 관리에는 ML-BOM(Machine Learning Bill of Materials, 머신러닝 모델에 개발된 모든 구성요소를 문서화한 상세 목록)을 활용해 AI 구성 요소와 데이터 소스를 파악하고 위험 관리를 하는 것이 효과적이다.

개발이 완료되어 운영 중인 AI 서비스의 경우 사용자와 직접 상호 작용을 하는 인터페이스와 더불어 AI 모델, 학습 데이터, 서드 파티 패키지 등 다양한 아키텍처에 발생 가능한 보안 위협이 존재한다. 따라서, 기업에서는 운영중인 AI 서비스를 대상으로 각 아키텍처 별 발생 가능한 위협을 분류하고 사전에 대응해야 한다.



[AI 모의 해킹/컨설팅 서비스]

SK 쉴더스에서는 기업의 안전한 AI 서비스 플랫폼 구축을 위해 AI 모의 해킹/컨설팅 서비스를 제공하고 있으며, 각 기업에서 내부적으로 활용할 수 있는 LLM Application 취약점 진단 가이드[16]를 공개했다. 해당 가이드는 'OWASP Top 10 for LLM Application 2025'가 포함된 14 개의 세부 항목으로 구성되어 있으며, 항목 별 점검 방법과 상세 대응 방안이 담겨있다.

또한, 최근 AI Labs 를 신설해 내부적으로 AI 학습을 위한 위협 정보 전처리와 모델 평가를 위한 AI 분석 플랫폼을 구축했으며, EQST, Secudium 센터 등 유관 부서와 협업해 Red Team, Blue Team 각각의 관점에서 활용할 수 있는 AI 보안 연구를 진행하고 있다. 연구 결과를 바탕으로 사이버 보안 전반에 화두가 되고 있는 AI 기반의 지능화된 위협과 기업 내 AI 서비스 보안 위협들에 선제적 대응을 할 수 있도록 고도화된 보안 서비스를 제공할 예정이다.

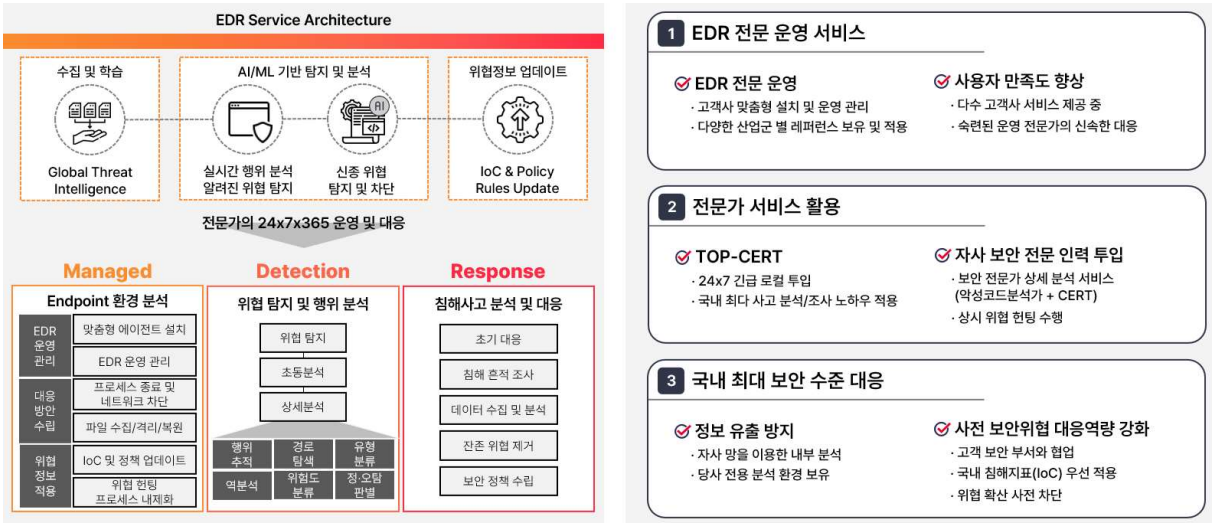
[16] EQST LLM Application 취약점 진단 가이드: https://www.skshieldus.com/kor/media/newsletter/insight.do

실시간 위협 탐지/분석/대응

랜섬웨어를 비롯하여 다양한 사이버 공격을 탐지 및 대응하기 위해서는 EDR, 안티바이러스, 방화벽 등 엔드 포인트 보안 솔루션을 적용하는 것이 중요하다. 특히, 오늘날 EDR 은 AI 를 활용해 알려진 위협 뿐만 아니라 다양한 침해 및 공격 지표를 학습해 지능화된 공격 행위 패턴을 탐지하기 때문에 엔드 포인트 보안에 많이 사용된다.

EDR 은 탐지된 악성코드의 행위 정보와 영향도를 분석하고, 이를 기반으로 한 주기적인 위협정보 업데이트를 통해 정확도와 성능을 향상시킬 수 있다. 또한, 전문가의 주기적인 위협 헌팅을 통해 알려지지 않은 위협을 탐지하고, 위협 격리 시 원인 분석, 잔존 위협 제거 등 신속한 대응이 더해지면 EDR 을 더욱 효과적으로 활용할 수 있다.

하지만, 전문성이 요구되는 작업이기 때문에 EDR 을 도입해 사용하고 있더라도 보안 전문 인력이 없을 경우 제대로 된 EDR 활용이 이뤄지지 않는 경우가 많다.



[전문가의 MDR 운영 서비스]

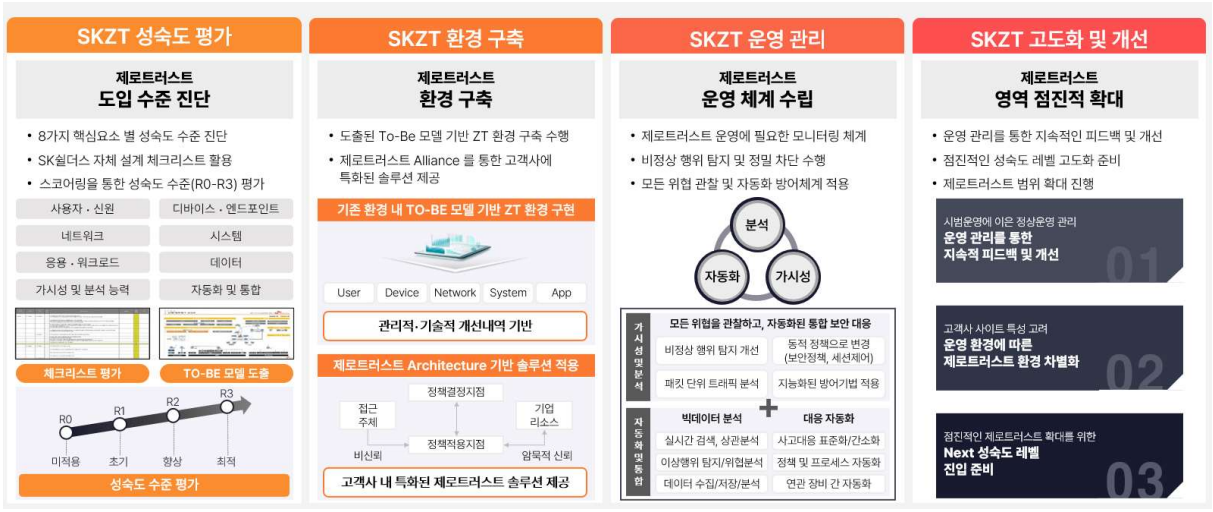
SK 쉴더스에서는 전문 인력의 EDR 운영을 필요로 하는 기업들을 대상으로 MDR[17] 서비스를 제공하고 있다. 다양한 산업군 별 솔루션 운영 레퍼런스를 바탕으로 기업 환경에 알맞은 엔드포인트 보안서비스를 구축하고, 국내 최다 사고 분석 노하우와 최신 국내 침해지표(IoC)업데이트를 통해 효과적인 MDR 운영을 진행하고 있다. 특히, 자사 보안 전문 인력을 24 시간 365 일 투입해 실시간 탐지 및 대응을 진행함으로써 해커의 실시간 공격 Kill-Chain 을 무력화하고, 신속한 사후 대응을 제공함으로써 위협 확산을 사전에 차단 및 대응할 수 있다.

[17] MDR(Managed Detection and Response): EDR 센서를 통해 기업 내 발생한 모든 보안 위협을 모니터링하고 대응하는 서비스

안전한 자격증명 관리 및 접근제어 강화

인포스틸러, 피싱 등 다양한 방법을 통해 자격증명을 탈취한 뒤 다크웹 거래와 무단 액세스를 시도하는 사례가 꾸준히 발생하고 있다. 이에 대응하기 위해서는 가장 기본적으로 자격증명이 외부에 노출되지 않도록 해야 한다. 자격증명의 탈취와 도용 사례가 꾸준히 발생하고 있음에도 불구하고, 미흡한 자격증명 관리로 인해 기업에서 사용하는 코드 저장소(ex. Github, Gitlab)에 노출되어 있거나 소스코드에 하드코딩 되어 있는 경우가 많다. 이러한 경우 공격자들은 손쉽게 자격증명을 획득해 악용할 수 있으므로 자격증명이 외부에 노출되지 않도록 철저하게 관리해야 한다.

또한, 다양한 루트를 통해 이미 탈취된 자격증명의 도용을 방지하기 위해서는 다중인증(MFA)과 더불어 제로 트러스트 도입을 통한 높은 수준의 인증과 접근 제어를 적용해야 한다. 다중인증은 공격자들의 공격 비용을 높일 수는 있지만, 피싱, AiTM 공격[18] 등 다양한 기법을 통해 인증 우회가 가능하기 때문에 최소한의 보안 대책으로 적용해야 한다. 제로 트러스트의 경우 탈취한 자격증명으로 액세스 인증을 하더라도 검증되지 않은 사용자에게는 권한을 부여하지 않아 불필요한 접근을 차단할 수 있기 때문에 가장 강력한 보안 대책이라고 할 수 있다.



[제로 트러스트 구축 (SKZT)]

많은 기업에서 제로 트러스트 도입 필요성에 대해 인지하고 있지만, 제로 트러스트 도입 방법론의 부재와 기존에 사용중인 환경에 맞는 제로 트러스트 구축에 어려움이 있어 구현이 늦어지고 있다. SK쉴더스에서는 SKZT(SK shieldus Zero-Trust)를 기반으로 기업 환경에 맞는 제로 트러스트 구축을 진행하고 있다.

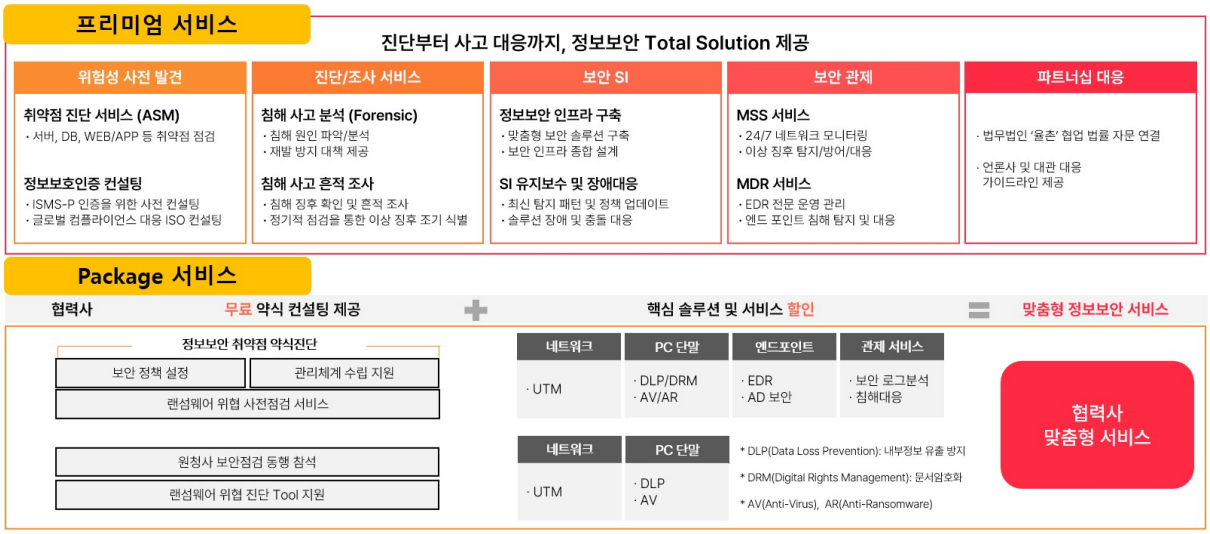
[18] AiTM : 공격자가 사용자와 정상 서버 사이의 중간자 역할을 하여 사용자의 계정 정보, MFA 값 등을 탈취하는 공격 기법

SKZT 는 성숙도 평가, 환경 구축, 운영 관리 세 가지로 나눠진다. 먼저, 195 개 체크리스트 기반의 성숙도 평가를 바탕으로 기업의 기존 환경에 맞는 제로 트러스트 모델을 도출한다. 이후, 도출한 모델을 기반으로 MFA 를 통한 강화된 인증, 마이크로 세그멘테이션[19]등을 적용한 권한 최소화 등 신뢰 기반이 아닌 검증 기반의 맞춤형 제로 트러스트 환경을 구축한다. 운영 관리 단계에서는 모니터링, 비정상 행위 탐지, 위협 관찰 및 대응 자동화 등 구축한 제로 트러스트 환경에서의 운영 체계를 수립하고, 지속적인 피드백 및 개선을 통해 성숙도를 향상시켜 고도화된 제로 트러스트 환경을 운영할 수 있다.

현재, SK 쉴더스에서는 여러 기업들을 대상으로 기업 별 특성에 맞는 제로 트러스트 환경을 컨설팅 및 구축하고 있으며, 제로 트러스트 협의체(ZETIA)를 운영함으로써 국내외 전문 업체들과 협력해 제로 트러스트 시장 활성화를 위한 선도적인 역할을 수행하고 있다.

협력사 정보보안 컨설팅

대부분의 대기업은 보안인증 심사를 의무적으로 받고 있으며, 별도의 보안팀을 구성해 정기적인 보안감사, 전문업체를 통한 모의 해킹 등 지속적으로 보안 체계를 강화하고 있다. 하지만, 대기업과 협력하는 협력사 중에는 상대적으로 보안 투자가 적고, 별도의 보안팀이 없는 경우가 많아 공격자들의 타깃이 되고 있다. 협력사를 초기 침투 지점으로 악용하거나, 협력사 시스템에 있는 원청사의 중요 정보를 타깃으로 한 공격이 주로 발생하기 때문에 원청사가 피해를 받지 않으려면 협력사와 함께 보안 대응 전략을 마련하고 보안 컨설팅, 솔루션 도입 등 보안 조치를 취해야 할 필요가 있다.



[협력사 정보보안 Total Solution]

SK 쉴더스에서는 '사전발견-실시간탐지-사후대응'까지 정보보안 Total Solution 을 제공하고 있으며, 보안 담당자가 없을 경우 정보보안을 위탁할 수 있는 맞춤형 보안 컨설팅을 진행하고 있다. 또한, 약식 컨설팅, 보안 솔루션 할인 등의 패키지 서비스를 통해 보안 투자가 적은 협력사들도 보안 컨설팅을 받고 실시간 위협 탐지/대응에 활용할 수 있도록 협력사 특화 서비스를 제공하고 있다.

[19] 마이크로 세그멘테이션: 데이터 센터 또는 클라우드 환경에서 서버 간 격리를 통해 액세스를 제어하고 제한하는 보안 기술

■ 맺음말

2024 년에도 다양한 산업군을 타깃으로 한 해킹 공격이 지속적으로 발생했다. 특히 생성형 AI 가 일상 생에 보편화되면서, 딥페이크 기술의 악용으로 인한 피해가 크게 증가했다. AI 가 피싱 고도화와 악성 툴킷 개발, 제로데이 취약점 발견 등에 악용되면서 전반적인 공격 기법이 고도화되고 있다. 또한 AI 서비스가 보편화되어 일반인도 쉽게 악용할 수 있게 되면서 사이버 공격의 위험이 더욱 커지고 있다. 각 기업의 담당자와 여러 보안 전문가들은 이에 대응하기 위한 끊임없는 보안 연구와 대책 수립이 필요하다.

SK 쉴더스에서는 AI, 랜섬웨어, 제로데이 등 현재 화두가 되고 있는 다양한 분야의 보안 연구를 진행하고 있다. 연구 결과를 바탕으로 보안 가이드 및 서비스를 제공하고, 앞으로 발생 가능한 보안 위협과 이에 대한 대응 전략을 제시함으로써 국가와 각 기업에서 사이버 위협에 대응할 수 있도록 지속적으로 선도해 나갈 것이다.

EQST Annual Report

2024.12

SK쉴더스

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

발행인 : SK쉴더스 EQST/SI솔루션사업그룹
제　작 : SK쉴더스 마케팅그룹