SK 쉴더스

EQST Annual Report

2024 보안 위협 전망 보고서

Contents

01 **2023년 5대 보안 위협 리뷰**

02 **2023년 보안 Trend 리뷰**

19 **2024년 5대 사이버 위협 전망 및 대응 전략**

인공지능을 악용한 사이버 공격
제로데이를 악용한 전략 고도화
연쇄적인 공급망 공격
다양한 형태의 자격 증명 탈취
타깃이 되는 클라우드 리소스

EQST insight

2023 년 보안 이슈와 2024 년 5 대 보안 위협 전망

■ 2023 년 5 대 보안 위협 리뷰

2023 년에도 국내/외를 가리지 않고 랜섬웨어 공격이 지속적으로 발생했다. 랜섬웨어의 경우 제로데이를 악용한 공격이 주를 이뤘다. 해외의 경우 대표적으로 'Cl0p'랜섬웨어 그룹에서 'MOVEit' 취약점을 악용해 대량의 공격을 진행했다. 국내는 구버전의 MagicLine4NX 취약점을 악용한 공격이 다수 발견됐다.

작년 대규모 피싱 공격에 사용된 'Caffeine'과 비슷한 역할을 하는 'PhaaS' 서비스인 'Greatness'가 등장했다. 특히 이 서비스는 다중 요소 인증(MFA)을 탈취하는데 용이해 해커들의 주목을 받았다. 이러한 피싱 서비스 외에도 '큐싱(Qshing)[1]' 범죄가 증가하고 있다.

또한 모바일 애플리케이션에 대한 지속적인 위협이 증가했다. 2023 년에도 NSO 그룹이 새로운 제로 클릭 스파이웨어를 유포해 화제가 됐다.

IIoT(산업용 사물 인터넷)분야에서는 주로 방화벽 취약점을 악용하는 공격이 진행되었고, 이스라엘-팔레스타인 전쟁의 여파로 인해 주요 기반시설인 에너지, 국방, 통신 조직을 대상으로 한 공격이 다수 발생했다.

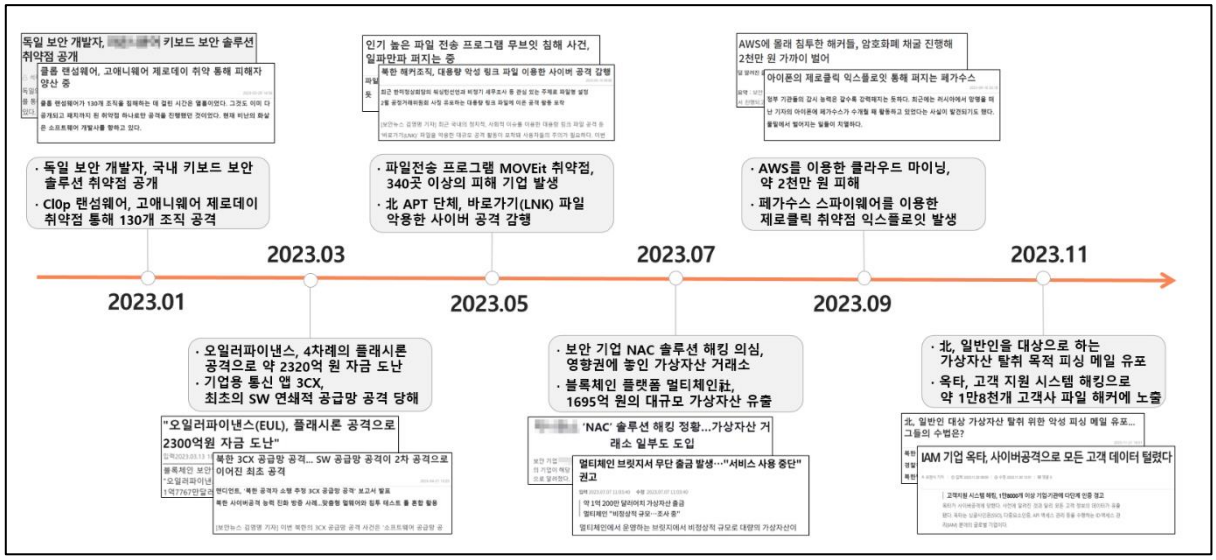
블록체인의 경우 2023 년에도 작년에 비해 피해 규모가 약간 줄었지만, 여전히 큰 피해가 보고되고 있다. 주로 크로스 체인 브릿지의 취약점을 악용한 범죄가 발생했다.

SK 쉴더스의 화이트 해커 그룹 EQST(이큐스트)는 2023 년 주요 이슈를 분석하고, 2024 년 5 대 보안 위협을 전망했다.

[1] 큐싱(Qshing): QR 코드와 피싱(Phishing)의 합성어로 공격자의 QR 코드로 피해자를 피싱 페이지로 유도하는 공격 기법

2023 년 보안 Trend 리뷰

■ 2023 년 주요 사이버보안 사고 리뷰



[2023 년 주요 사이버보안 사고]

올해 1 월에는 독일의 보안 소프트웨어 개발자인 블라디미르 팔란트(Wladimir Palant)가 자신의 블로그에 한국 인터넷 환경의 취약점에 대한 글을 게재하여 이슈가 됐다. 국내 주요 은행/금융 사이트에서 사용하는 보안 솔루션의 취약점을 차례로 공개했으며, 그 중 국내 키보드 보안 솔루션에 대한 취약점이 공개되어 파장이 일었다. 이후, 관련 솔루션들에 대한 대대적인 보안 패치가 이뤄졌다.

또한, 올해는 기업용 솔루션 취약점을 악용한 랜섬웨어 그룹의 공격이 성행했다. 그중 2 월에는 파일 전송 소프트웨어인 고애니웨어(GoAnywhere)의 제로데이 취약점(CVE-2023-0669)을 악용한 Cl0p 랜섬웨어 그룹의 공격이 있었다. Cl0p 랜섬웨어 그룹은 130 개가 넘는 조직들을 공격했으며 피해 기업의 정보를 다크웹에 공개하기도 했다. 핀테크 플랫폼인 해치뱅크(Hatch Bank)는 139,493 명의 고객 개인정보를 탈취당했으며, 이외에도 히타치 에너지(Hitachi Energy), 루브릭(Rubrik) 등의 기업이 Cl0p 랜섬웨어 그룹의 고애니웨어 취약점을 활용한 공격에 피해를 입은 것으로 밝혀졌다.

3 월에는 이더리움 기반의 가상자산 담보 대출 서비스를 제공하는 DeFi 프로토콜인 오일러 파이낸스(Euler Finance)가 플래시론(Flash Loan) 공격을 받았다. 오일러 파이낸스는 이 공격으로 인해 약 2,320 억 원(1 억 9,700 만 달러)의 자금을 도난당했다. 플래시론은 무담보로 받은 대출을 의미하며 거래가 끝나기 전에 상환해야 하는 특징이 있다. 이를 악용한 플래시론 공격은 대출받은 가상자산을 이용해 거래소에 시세 조작 공격을 수행하거나, DeFi 서비스의 스마트 컨트랙트 취약점을 공격하여 이득을 취한 뒤 바로 담보를 갚아버리는 방식으로 이뤄진다. 해당 공격을 통해 공격자는 수백만 개의 스테이블코인 다이(DAI)를 비롯해 USD 코인(USDC), 스테이킹 이더리움(StETH), 랩트 비트코인(WBTC)을 탈취했다. 공격자는 훔친 자산의 약 90% 이상을 피해자들에게 반환했으나, 이를 반환하는 과정에서 일부 자산이 북한의 라자루스 그룹에게 전송된 기록이 발견되어 공격자와 라자루스 간의 연관성이 제기되기도 했다.

또한, 기업용 통신 소프트웨어인 3CX 의 DesktopApp 을 통해 북한 배후의 공격 그룹이 공급망 공격을 수행한 것으로 드러났다. 3CX 의 DesktopApp 은 Windows 와 MAC 환경에서 구동이 가능하고 전 세계 190 개국 60 만개 이상의 고객사에서 사용 중이며, 1 일 사용자는 1200 만 명 수준인 것으로 알려져 있다. 이번 3CX 공급망 공격이 주목받는 이유는 소프트웨어 공급망 공격이 또 다른 소프트웨어 공급망 공격으로 이어진 최초의 연쇄적 공급망 공격 사례이기 때문이다. 3CX 직원이 소프트웨어 제공 업체인 트레이딩 테크놀로지스(Trading Technologies)에서 금융 거래용 소프트웨어인 엑스트레이더(X_Trader)를 다운받았는데, 이는 멀웨어에 감염된 소프트웨어였다. 해당 멀웨어를 통해 해커는 3CX 직원의 PC 권한을 탈취했으며, 자격 증명에 악용해 3CX 시스템에 관리자로 접속한 뒤, 빌드 서버에 침투했다. 그 후 해커는 3CX 의 소프트웨어에 멀웨어를 삽입했고, 이는 공식 홈페이지를 통해 설치 파일 형태로 배포됐다. 1 차 공격으로 감염된 엑스트레이더에서 라자루스가 사용하는 백도어인 베일드시그널(VEILEDSIGNAL)이 발견됐고, 2 차 공격인 3CX 공급망 공격에서 고푸람(Gopuram) 멀웨어가 발견된 것을 근거로 이번 사건의 배후를 북한의 라자루스로 추정하고 있다.

5 월에도 기업용 솔루션의 제로데이 취약점을 활용한 랜섬웨어 그룹의 공격이 이어졌다. 공격자들은 파일 전송 프로그램인 MOVEit 의 SQL Injection 취약점(CVE-2023-34362)을 이용했으며, 공격의 배후는 지난 2 월 고애니웨어 취약점을 이용했던 Cl0p 랜섬웨어 그룹인 것으로 밝혀졌다. 영국의 BBC, 브리티쉬 에어웨어 등 글로벌 대기업을 비롯해 미국 정부와 공공기관, 세계 주요 금융기관이 가장 큰 피해를 입었다. 특히 올해 5 월부터 11 월까지 MOVEit 취약점을 이용한 공격으로 약 2,620 개의 조직과 7,720 만 명이 피해를 입은 것으로 알려졌다.

또한, 북한의 해킹 단체인 APT37 이 Windows 의 바로가기(LNK) 파일[2]을 통해 악성코드 록랫(RokRAT)[3]을 유포한 정황이 포착됐다. 주요 공격 대상은 한국 정부 혹은 관련 단체이며, 기존에 사용하던 매크로 방식이 아닌 바로가기(LNK) 파일을 이용했다. 공격자들은 LNK 파일을 PDF 파일로 변경했으며, 해당 파일을 정상적인 파일과 함께 ZIP 아카이브에 포함하여 피해자에게 전송했다. 피해자가 ZIP 아카이브 압축 해제 후 LNK 파일을 실행하면 파워쉘 스크립트[4]가 실행되고 이 스크립트는 또다른 파워쉘 스크립트를 실행한다. 해당 스크립트는 공격자의 드라이브에서 악성 페이로드를 다운로드하게 되고 이로 인해 피해자의 시스템에 록랫이 설치된다. 해당 악성코드를 유포한 APT37 은 '금성 121', '스카크러프트', '레드아이즈' 등 다양한 이름으로 불리고 있으며, 국내 대북 단체와 국방 분야 관계자를 대상으로 공격을 감행하고 있다. 지난 3 월에는 국내 금융 기업의 보안 메일을 사칭한 CHM 파일[5]을 이용한 악성코드를 유포하기도 했다. MS 오피스의 매크로 기능은 공격자에 의해 활발히 사용됐으나, 지난 2022 년 MS 에서 인터넷을 통해 다운로드 된 오피스 문서 파일의 매크로가 자동 실행되지 않도록 정책을 바꾼 이후 매크로를 이용한 공격이 거의 사라진 추세다. 하지만 공격자들은 여전히 LNK 파일과 같이 새로운 기법을 통해 공격을 이어가고 있는 만큼 주의가 필요하다.

7 월에는 블록체인 플랫폼 멀티체인에서 운영하는 팬텀 브릿지에서 약 1,695 억 원에 달하는 대량의 토큰들이 예고 없이 인출되는 사고가 발생했다. 멀티체인은 공격 사실을 인지한 후 서비스를 중단했으며, 대규모 인출과 관련한 지갑을 블랙리스트에 올리고 자금을 동결시키는 등의 후속 조치를 취했다. 하지만 며칠 뒤 1,309 억 원 규모의 가상자산이 추가 탈취된 정황이 드러났다. 이에 블록체인 데이터 플랫폼 체이널리시스(Chainalysis)는 멀티체인의 대규모 가상자산 유출은 외부 해커가 멀티체인의 특정 키에 대한 통제권을 탈취했을 가능성이 있지만, 내부자 소행 또는 러그풀(Rug Pull)[6]일 가능성이 높다고 분석했다.

또한, 국내 가상자산 거래소에 설치된 네트워크 접근제어(NAC) 서버에 대한 침해 사고 의심 정황이 나타났다. 해당 제품을 제공하는 보안 기업의 업데이트 서버에서 일부 고객사의 NAC 정책 서버로 악성 프로그램이 전송된 것을 확인했으며, 이를 토대로 NAC 제공 업체에서는 자사의 업데이트 서버가 침해된 것으로 판단했다. 사건 발생 2 개월 후, 해당 기업은 추가 공지사항을 통해 침해사고 조사 결과 공격자 및 침투 경로 등에 대해서는 밝혀진 바가 없다고 발표했으며, 자체 조사를 통해 발견한 취약점을 보완하여 NAC 제품에 대한 업데이트를 제공했다.

---

[2] 바로가기(LNK) 파일: Windows 에서 원본 파일, 폴더 등에 대한 바로가기를 제공하는 파일로 해당 파일을 클릭하면 대상 파일을 호출할 수 있음

[3] 록랫(RokRAT): 사용자 정보를 수집하고 추가 악성코드를 다운로드 할 수 있으며, 한글 및 워드 문서를 통해 유포된 이력이 존재하는 악성코드

[4] 파워쉘 스크립트: 관리 및 작업을 수행할 때 사용하는 명령 프로그램 powershell 에서 실행하는 명령 스크립트

[5] CHM 파일: HTML 로 작성된 콘텐츠, 이미지, 스크립트 등을 포함할 수 있는 Windows 에서 사용되는 도움말 파일 형식

[6] 러그풀(Rug Pull): 가상자산 시장에서 팀이나 회사가 진행하던 서비스나 프로젝트를 중단하고 투자금을 가로채는 행위

9 월에는 AWS(Amazon Web Services)에서 제공하는 서비스[7] 중 덜 알려진 클라우드 서비스를 악용하는 새로운 암호화폐 채굴 캠페인이 발견됐다. 앰버스퀴드(AMBERSQUID)라는 이름으로 불리는 이 캠페인은 공격에 사용된 스크립트나 사용자 이름을 통해 인도네시아의 해커들이 배후에 있는 것으로 의심하고 있으며, 사용된 지갑 주소를 분석한 결과 9 월까지 공격자들이 올린 수익은 1 만 8300 달러인 것으로 추정하고 있다. 이처럼 일반 PC 나 기업 서버를 대상으로 한 암호화폐 채굴이 클라우드 자원을 훔치는 것으로 변화되는 추세이므로 주의가 필요하다.

또한, 이스라엘의 NSO 그룹에서 만든 스파이웨어인 페가수스(Pegasus)[8]의 새로운 익스플로잇이 공개됐다. 페가수스는 iOS 의 제로데이 취약점을 통해 진행되는 제로 클릭[9]이 적용된 대표적인 스파이웨어다. 이번 페가수스 스파이웨어에 악용된 제로데이 취약점은 블라스트패스(BLASTPASS)로 2023 년 7 월 25 일 공개된 iOS 16.6 버전에서 발견됐다. 공격자는 해당 취약점으로 iMessage 를 통해 패스킷(PassKit)[10] 첨부파일을 보내며 공격을 진행한다. 공격에 성공할 경우 사용자의 음성 정보, 시스템 정보, 통화 기록 등 민감 정보가 공격자에게 전송될 수 있다.

11 월에는 북한 해킹 조직 김수키(Kimsuky)의 활동으로 인해 내국인 1,468 명의 이메일 계정이 탈취된 사실이 밝혀졌다. 경찰청 국가수사본부의 추적·수사 결과에 따르면, 김수키는 국내외 서버 576 대를 경유하며 IP 주소를 바꾼 뒤 정부기관, 기자 등을 사칭해 피싱 메일을 발송했다. 메일 수신자가 첨부된 파일을 열람하거나 URL 을 클릭하면 PC 의 내부 정보가 유출될 수 있는 악성 프로그램을 설치하거나 실행시키는 수법을 사용했다. 특히 김수키의 공격 대상이 외교·안보 분야의 공무원과 전문가뿐만 아니라 일반인까지 확대된 것으로 나타났다. 일반인 피해자의 다수는 가상자산거래소를 이용하고 있으며, 공격자는 실제로 피싱 메일 피해자 중 19 명의 가상자산거래소 계정에 접속해 가상자산 절취를 시도했다. 해킹으로 장악한 경유 서버 147 대에 가상자산 채굴 프로그램을 관리자 몰래 실행한 정황도 밝혀졌다.

---

[7] AWS 앰플리파이(AWS Amplify), AWS 파게이트(AWS Fargate), 아마존 세이지메이커(Amazon SageMaker) 등

[8] 페가수스(Pegasus): 아이폰의 보안 취약점을 활용해 사용자의 기기에서 정보를 탈취하는 이스라엘의 NSO 그룹에서 만든 스파이웨어

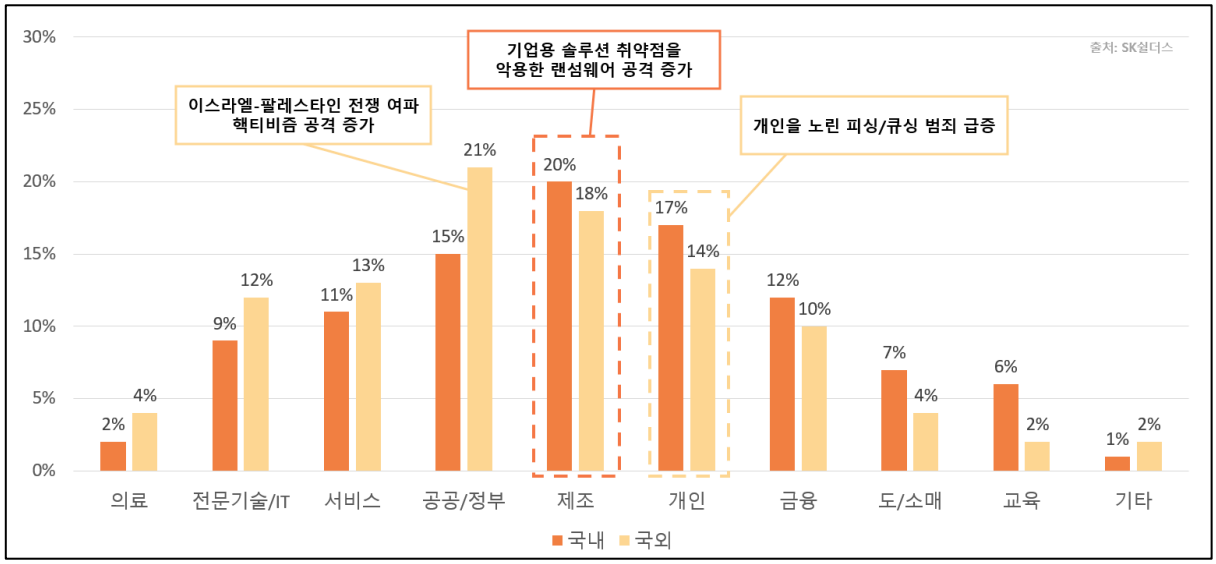
[9] 제로 클릭(Zero-Click): 사용자가 첨부파일이나 링크를 누르는 상호작용을 하지 않아도 기기에 침투할 수 있는 공격

[10] 패스킷(PassKit): Apple 기기의 Wallet 에 서명을 추가하거나 인증이 필요할 때 시간, 장소를 화면에 표시하거나 푸시 알람 기능 등이 가능하도록 구현한 파일

또한, 보안 기업 옥타(Okta)는 자사의 고객 지원 시스템 업로드 파일에 외부 해킹 그룹이 접근했다고 밝혔다. 해당 시스템은 옥타에서 제공하는 서비스 이용 중 발생한 오류를 해결하기 위한 고객 지원 서비스로 고객이 해당 시스템을 통해 업로드 하는 파일에는 세션 토큰, 쿠키 등을 포함한 고객의 인증 데이터가 담겨있다. 해당 침해 사고에 대한 최초 발표에서는 공격자가 134개의 고객사 파일에 액세스한 것으로 알려졌지만, 조사 결과 옥타의 서비스인 Workforce Identity Cloud(WIC), 고객 신원 확인 솔루션(CIS)을 이용하는 모든 고객들의 데이터가 도난당한 것으로 드러났다.

로그인 및 아이덴티티 관리 시스템을 제공하는 IAM(Identity and Access Management) 분야에서 글로벌 기업인 옥타는 공격자들의 주요 공격 대상이 되고 있다. 지난해에는 해킹 그룹 랩서스(LAPSUS$)의 공격을 받았으며, 옥타의 자격 증명과 인증 코드를 노린 '0ktapus'라는 대규모 피싱 캠페인이 4 건이나 벌어진 바 있다. 올해 9 월에는 옥타의 관리자 계정을 탈취하기 위한 소셜엔지니어링 공격이 유행했고, 10 월 고객 지원 시스템 침해 사고 이후 11 월에는 옥타와 관련 있는 서드파티 업체가 해킹 공격을 당해 옥타의 전·현직 직원 및 가족 5,000 여 명 정도의 개인정보가 유출되기도 했다.

■ 업종별 침해사고 발생 통계



[2023 년 업종별 침해사고 발생 통계]

2023 년 업종별 침해사고 발생 통계를 살펴보면, 국내 기준 제조분야에서 20%, 개인 대상 17%로 가장 많은 사고가 발생했다. 또한 공공/정부 15%, 금융 12%, 서비스 11%, 전문기술/IT 11%, 도/소매 7%, 교육 6%를 차지했다. 국외 기준으로는 공공/정부 분야에서 21%로 가장 높은 수치를 보이며, 제조, 개인, 서비스가 뒤를 이었다.

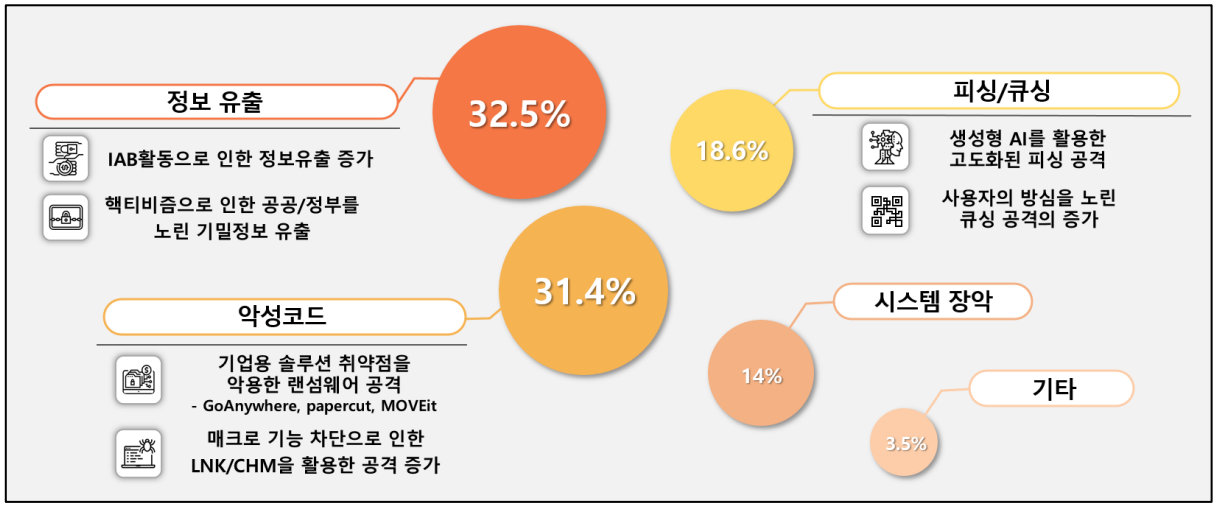
올해 상/하반기에 걸쳐 기업용 솔루션 취약점을 악용한 랜섬웨어 공격이 증가했다. 국내의 경우 MagicLine4NX 의 구버전에 존재하는 취약점과 PaperCut 의 취약점을 악용한 공격이 제조, 공공 등의 분야에서 증가했다. 해외의 경우 MOVEit, GoAnywhere 파일관리 솔루션과 프린터 관리 솔루션인 PaperCut 취약점을 노린 랜섬웨어 공격으로 수많은 제조기업과 공공/정부, 의료 등의 분야에서 데이터 탈취가 이뤄졌다.

또한 하반기에는 개인을 노린 큐싱 범죄가 등장하여 피싱 공격에 사용됐고, 큐싱 공격 외에도 스미싱과 이메일 피싱 공격이 꾸준히 이어져 개인을 대상으로 한 침해사고가 높은 비율을 차지했다.

국외의 경우 이스라엘-팔레스타인 전쟁의 여파로 핵티비즘[11] 활동이 증가하여 공공/정부 분야를 대상으로 한 사이버 공격이 증가하면서 가장 높은 비율을 차지했다.

[11] 핵티비즘(Hacktivism): 해킹과 액티비즘의 합성어로 해킹을 통해 사회적, 정치적 목적을 추구하는 활동

■ 유형별 침해사고 발생 통계



[2023 년 유형별 침해사고 발생 통계]

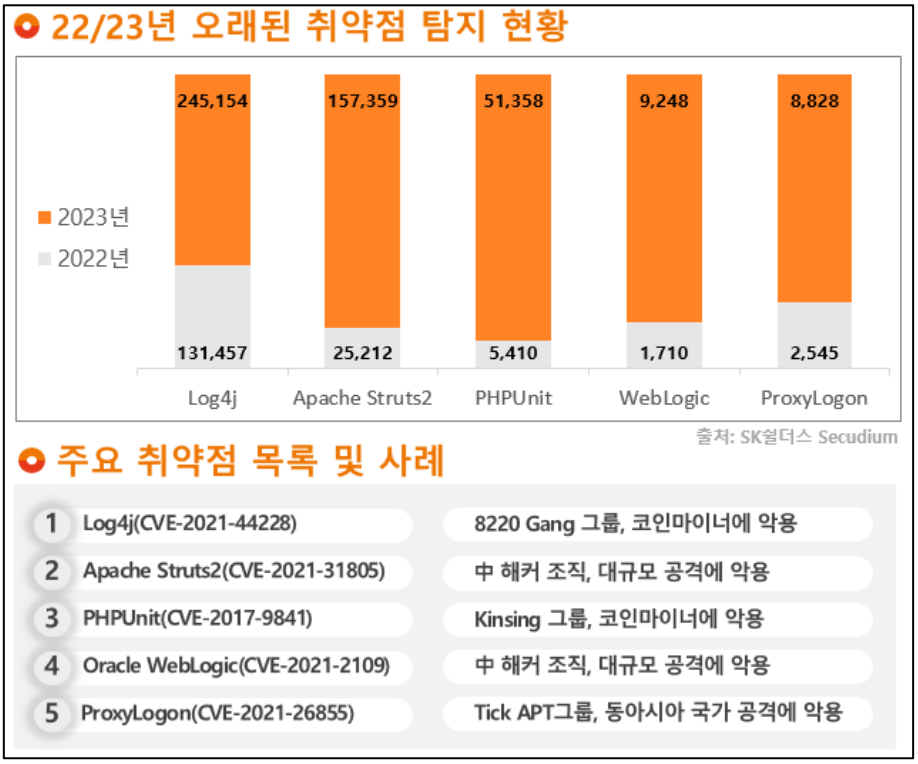
2023 년 유형별 침해사고 발생 통계를 살펴보면 정보 유출 32.5%, 악성코드 감염 31.4%, 피싱/스캠 공격이 18.6%를 차지했다. 그 외 시스템 장악 14%, 기타 공격이 3.5%로 뒤를 이었다.

먼저, 중요 정보 유출이 32.5%로 가장 높은 비율을 차지했다. 올해 IAB 활동으로 인해 공격자들이 시스템에 접근할 경로를 구하는 것이 수월해져 정보유출 사례가 증가했고, 핵티비즘으로 인한 공공/정부 기관을 노린 기밀정보 유출 사건 또한 큰 영향을 미친 것으로 보인다.

두번째로, 악성코드 감염으로 인한 피해는 31.4%의 비율을 차지했다. 국내/외 모두 기업용 솔루션의 취약점을 악용해 다양한 분야를 대상으로 대규모 랜섬웨어 공격을 진행한 사건이 큰 비중을 차지했다. 국외의 경우 MOVEit, GoAnywhere 등의 취약점을 악용했고, 국내의 경우 MagicLine4NX 취약점을 사용해 공격을 시도했다. 또한, MS Office 의 매크로 기능을 이용한 악성코드 배포에 대응하기 위하여 최근 MS 에서 오피스 매크로 차단 정책을 적용했고, 이를 우회하기 위한 LNK/CHM 형식의 악성코드가 증가했다.

마지막으로, 피싱/스캠으로 인한 침해사고에서 주목할 점은 AI 챗봇 서비스인 ChatGPT 를 비롯해 많은 AI 서비스들이 대중화되면서 이를 악용한 정교한 피싱 메일 제작이 가능해졌다는 것이다. 또한, 일반적인 피싱 외에도 최근 QR 코드 사용의 증가로 큐싱(Qshing)이라 불리는 공격 방식이 증가하고 있다. 이는 공격자가 조작된 QR 코드를 원본 위에 붙여 피해자를 피싱 페이지로 유도하는 공격 기법으로 개인 및 기업은 출처가 불분명하거나 QR 코드가 의심스러운 페이지를 가리킬 시 주의가 필요하다.

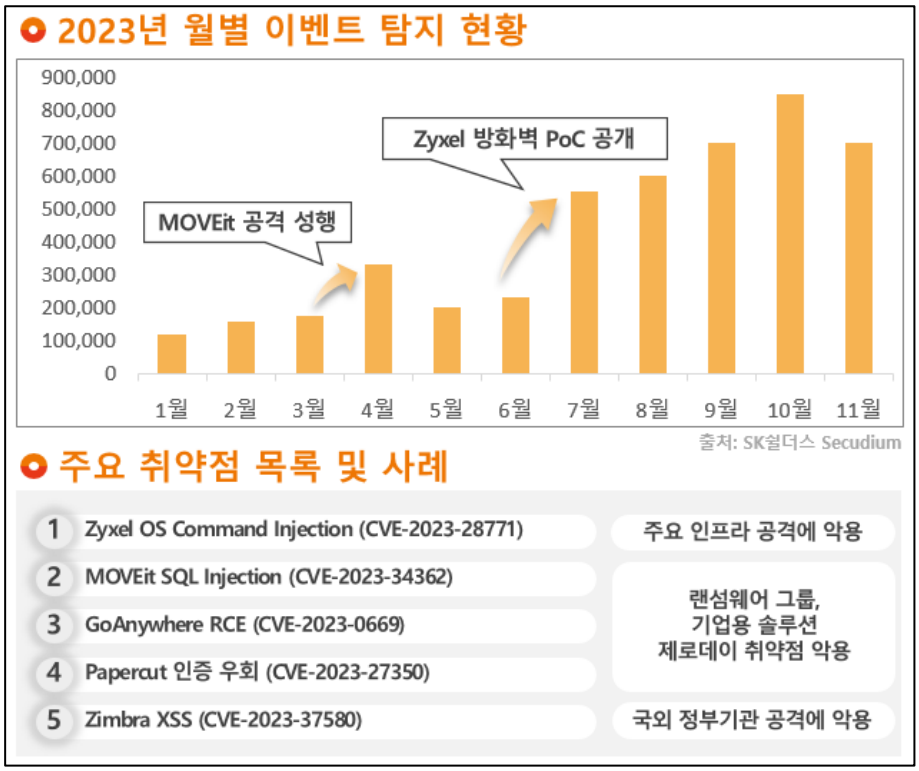
■ 취약점 동향



[2022/23 년 오래된 취약점 통계]

올해에도 여전히 다양한 해킹 그룹에서 오래된 취약점을 이용한 공격시도가 꾸준히 이루어지고 있다. 주요 취약점인 'Log4j', 'Apache Struts2', 'PHPUnit', 'WebLogic', 'ProxyLogon' 공격은 전년도 대비 전반적으로 증가했으며 'Log4j' 약 24 만건, 'Apache Structs2' 약 15 만건으로 높은 수치가 집계됐다. 특히 'PHPUnit'의 경우 2017 년에 공개된 취약점임에도 불구하고 작년대비 약 10 배 이상의 이벤트가 발생한 것으로 보아 현재까지도 이러한 오래된 취약점들이 활발하게 공격에 이용되고 있음을 알 수 있다.

실제로 올해 상반기에 중국 해킹 그룹인 판다정보국(PIB), 1937cN, 샤오치잉에서 'Apache Struts2', 'WebLogic' 등 오래된 취약점을 이용한 대규모 공격을 수행했다. 국내에서는 기업의 인프라 서버, 공공기관 웹사이트, 교육부 산하 기관 홈페이지에 대한 공격이 확인됐으며, 이 과정에서 일부 개인정보가 유출되는 사고도 발생했다. 이외에도 'Log4j', 'PHPUnit'을 코인 마이너암호화폐 채굴 공격(코인 마이너)에 악용한 국외 사례가 보도됐으며, 많은 기업에서 사용하고 있는 'Exchange Server'를 타깃으로 하는 'ProxyLogon' 취약점도 여전히 APT 그룹의 공격도구로 악용되고 있다. 이처럼 오래된 취약점이 꾸준히 발생되고 있는 만큼 보안 담당자 및 관련부서의 지속적인 관심과 모니터링이 요구된다.

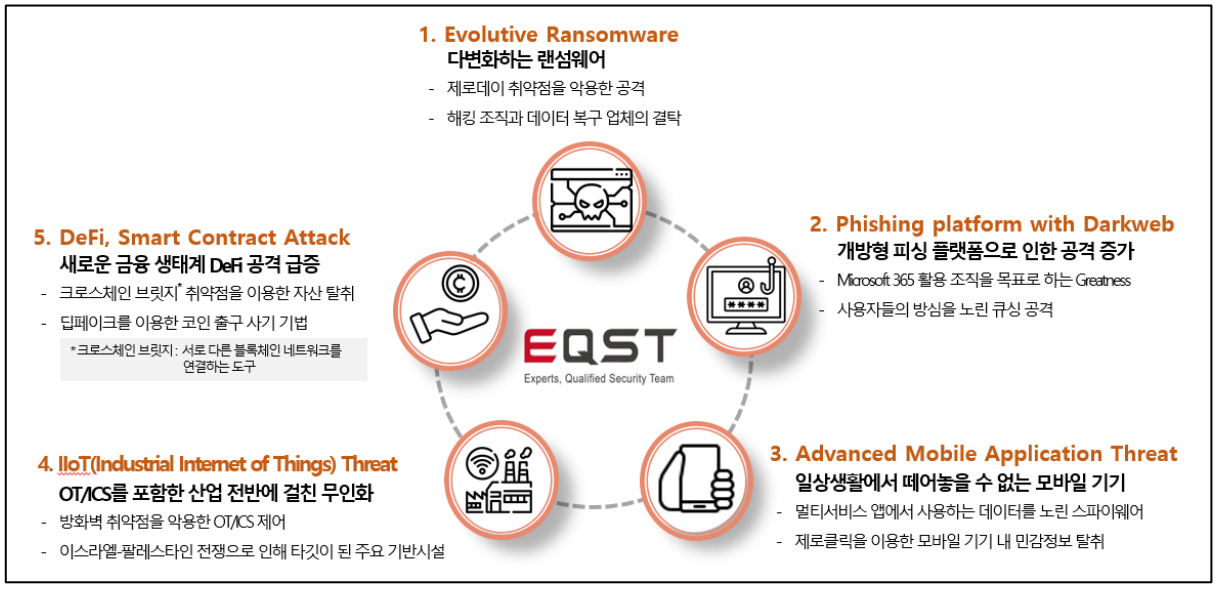


[2023 년 신규 취약점 통계]

올해 주요 신규 취약점인 GoAnywhere(2 월), PaperCut(4 월), MOVEit(5 월), Zyxel(6 월), Zimbra(7 월)는 상반기에 주로 발견됐고, 그로 인해 하반기에 많은 이벤트가 탐지됐다. 이 중 4 월과 7 월에 높은 상승폭을 나타내고 있는데, 이는 MOVEit 과 Zyxel 취약점의 영향을 받았기 때문이다. 4 월에는 SQL Injection 을 사용하는 MOVEit 공격이 성행하여 SQL Injection 이 탐지된 전체 이벤트의 높은 비중을 차지했다. 6 월에 공개된 Zyxel 취약점은 방화벽 제품 관련 취약점으로, 다른 취약점보다 공격 조건이 까다롭지 않아 PoC 가 공개된 이후 7 월부터 전반적인 네트워크 대역에 대한 공격이 이뤄졌다.

Zyxel 방화벽 제품에서 발생한 취약점은 주요 인프라를 공격하는데 사용됐으며, 실제 국외의 에너지 기반 시설이 공격당해 피해를 입고 봇넷의 거점으로 사용되는 사례도 보도됐다. MOVEit, GoAnywhere, PaperCut 과 같이 기업에서 많이 사용하는 솔루션들의 제로데이 취약점을 이용한 랜섬웨어 그룹의 공격이 성행했으며, 기존의 방식과는 달리 신규 취약점을 이용하여 기존보다 많은 대상들에게 피해를 입혔다. 이메일, 캘린더, 채팅 및 비디오 서비스를 제공하는 플랫폼인 Zimbra 에서 발생한 취약점은 국외의 정부기관을 대상으로 공격한 사례가 많이 발생했다. 다양한 방면에서 제로데이 취약점이 발생하고 있으며, PoC 공개 이후 패치가 되지 않은 타깃을 목표로 한 대규모 공격이 이루어지고 있으므로, 해당 위협에 대한 꾸준한 관심과 주기적인 패치 활동이 필요하다.

2023 년 보안 이슈 리뷰



[2023 년 보안 이슈 리뷰]

Evolutive Ransomware 부분에서는 제로데이를 악용한 랜섬웨어 그룹의 활동이 활발했다. 2023 년 1 월 말 'Cl0p' 랜섬웨어 그룹의 'GoAnywhere' 취약점을 이용한 랜섬웨어 공격을 시작으로, 4 월에는 'PaperCut', 6 월에는 'MOVEit' 취약점을 이용한 랜섬웨어 그룹의 활동이 대거 포착됐다. 해당 취약점들은 인쇄 관리 소프트웨어와 파일 전송 소프트웨어의 취약점이며, 특히 해외 기업에서 많이 사용하는 파일 전송 소프트웨어 'MOVEit'은 랜섬웨어 그룹의 주요 타깃이 됐다. 또한, 최근에는 'Cl0p' 랜섬웨어 그룹에서 11 월에 발견된 'SysAid' 제로데이를 이용한 랜섬웨어 공격을 수행하고 있는 것으로 확인돼, 해당 취약점을 이용한 랜섬웨어 공격에 각별한 주의가 필요하다.

이뿐만 아니라 국내 데이터 복구 업체와 북한 해킹 조직 'Lazarus'가 결탁하여 랜섬웨어를 유포하고, 피해자로부터 금전을 갈취한 정황이 포착됐다. 데이터 복구 업체는 해킹 조직으로부터 복호화 키를 사전에 전달받은 후, 복호화 서비스를 홍보했다. 해킹 조직에게 랜섬웨어 피해를 받은 피해자들은 데이터 복구 업체에게 복호화를 위한 금전을 지불했고, 데이터 복구 업체와 해킹 조직은 수익을 분배하여 가져가는 형태였다.

제로데이 취약점을 악용한 사례가 증가하고 있고, 체계화/지능화된 방향으로 공격 트렌드가 변모하고 있으므로 개인과 기업에서는 최신 동향을 이해하고 적극적으로 사전 예방책을 준비해야 한다.

Phishing platform with Darkweb 부분에서는 'PhaaS(Phishing-as-a-Service)'를 이용한 피싱 공격이 발생했다. 'PhaaS'란 서비스형 피싱 플랫폼으로 금전적 보상을 받고 피싱 키트를 판매하는 조직화된 사이버 범죄를 뜻한다. 작년 대규모 피싱 캠페인에 이용된 'Caffeine'에 이어 올해에는 Microsoft 365 를 사용하는 기업을 표적으로 한 'Greatness'라는 'PhaaS' 플랫폼이 사용됐다. 'Greatness'는 Microsoft 365 계정에 액세스하기 위한 자격 증명과 쿠키를 얻는 데 사용되며, 특히 다중 요소 인증(MFA)이 활성화된 계정도 처리할 수 있어 주목받았다. 해당 캠페인은 주로 미국, 영국, 호주 등 해외에 위치한 제조, 의료 기업을 대상으로 발생한 것으로 확인된다.

또한, 피싱에 대한 사람들의 대응 능력이 향상되고, 금융서비스, 공공자전거 등 QR 코드를 이용하는 플랫폼이 증가함에 따라 QR 코드를 이용한 '큐싱(Qshing)' 범죄가 증가하고 있다. 최근 국내에서도 뱅킹 입금을 유도하거나 가상화폐를 노린 큐싱 사례가 등장해 국내에서도 각별한 주의가 필요하다.

Advanced Mobile Application Threat 부분에서는 멀티서비스를 제공하는 앱을 노린 스파이웨어 공격이 발견됐다. 채팅, 금융, 쇼핑 등 다양한 서비스를 하나의 플랫폼에서 제공하는 앱 특성 상 수집 및 이용되는 다양한 데이터는 해커들의 좋은 먹잇감이 되고 있다. 올해 중국 해킹 단체 'APT-41'에서는 모바일 내 민감 정보 탈취를 목표로 'LightSpy'라는 스파이웨어를 활용하여 캠페인을 진행했다. Pay, SNS, 항공예매 등 다양한 서비스를 제공하는 'WeChat'이 타깃 중 하나였으며, 'WeChat Pay'의 결제 데이터를 비롯하여 'WeChat'의 오디오 기능을 악용한 피해자의 대화 녹음 등 'WeChat'에서 이용되는 다양한 데이터가 공격 대상이 됐다.

작년에 이어 올해에도 어김없이 제로 클릭 취약점을 이용한 공격들이 발생했다. 4 월에는 'QuaDream [12] '에서 'ENDOFDAYS'라는 제로 클릭 취약점을 이용하여 'Reign' 스파이웨어를 유포했다. 해당 취약점은 iCloud Calendar 초대 기능을 통해 발생하는 익스플로잇으로, 2021 년에 공개된 취약점이지만 업데이트 되지 않은 기기들을 대상으로 여전히 사용되고 있는 것을 알 수 있다. 또한, 9 월에는 'NSO' 그룹이 제로데이 취약점을 이용하여 'Pegasus' 스파이웨어를 유포했다. 해당 그룹은 지난 해 'FINDMYPWN', 'PWNYOURHOME', 'LATENTIMAGE' 익스플로잇을 이용하여 iMessage 를 타깃으로 한 제로 클릭 공격을 수행했다. 올해에는 'BLASTPASS'라는 신규 익스플로잇을 이용해 제로 클릭 공격을 수행한 것으로 밝혀졌다.

취약한 기기들을 타깃으로 오래된 제로 클릭 익스플로잇을 이용함과 동시에 꾸준히 신규 제로 클릭 익스플로잇을 활용한 새로운 공격이 발견되고 있다. 사용자들은 지속적으로 최신 보안 업데이트를 수행하고, 각별한 주의를 기울여야 한다.

[12] QuaDream: iPhone 해킹 툴을 판매했던 이스라엘 기업으로 현재는 운영을 중단함

IIoT(Industrial Internet of Things) Threat 부분에서는 이스라엘-팔레스타인 전쟁으로 인한 주요 기반시설을 타깃으로 한 공격이 주요 이슈가 됐다. 공격자들은 주로 방화벽 및 라우터 취약점을 이용하여 공격을 하고, 내부망 접근 권한을 획득하여 산업 시스템을 제어하는 것을 목표로 했다. 뿐만 아니라 한 해커 그룹에서는 'Zyxel' 방화벽 취약점을 이용하여 덴마크의 주요 에너지 기반 시설을 공격해 해당 시설을 봇넷에 감염시킨 후, 이를 거점으로 미국 및 홍콩 등 다른 국가에 DDoS 공격을 수행한 것으로 밝혀졌다. 단순히 국가의 주요 인프라를 제어하는 것에서 그치지 않고, 해당 인프라를 거점으로 다른 국가를 타깃으로 하여 추가 공격을 수행한 사례라고 볼 수 있다.

작년 러시아-우크라이나 전쟁에 이어 올해 이스라엘-팔레스타인 분쟁이 발발하면서, 국가 간 사이버 전쟁이 지속되고 있다. 국가 간 사이버 전쟁에 있어 산업 기반 시설이 주요 타깃이 되고 있는 만큼 산업 기반 시설 시스템의 보안 취약성 검토와 지속적인 공격 모니터링을 통해 대비책을 마련해야 할 것으로 보인다.

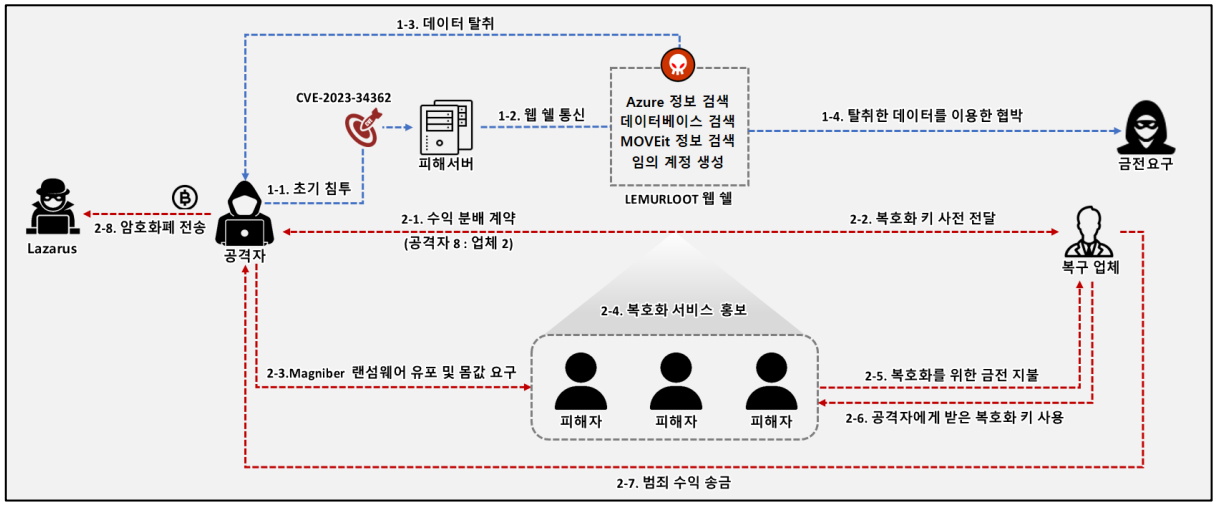
DeFi, Smart Contract Attack 부분에서는 지속적으로 암호화폐를 노린 공격이 발생하고 있다. 올해 상반기 DeFi 프로토콜인 '오일러 파이낸스'에서 2 억 달러에 달하는 큰 규모의 해킹이 발생했다. 이어 7 월에는 크로스체인 브릿지 프로토콜인 '멀티체인' 브릿지 해킹으로 약 1 억 2500 만 달러, 11 월에는 'HECO' 브릿지 해킹으로 약 8660 만 달러 규모의 손실이 발생했다.

뿐만 아니라 가상화폐 투자자를 타깃으로 한 '출구사기(exit scam)'가 발생했다. '출구사기'란 사기를 목적으로 코인을 설계하고, 해당 코인을 홍보하여 투자를 유도한 후 피해자들의 투자로 인해 코인 가치가 상승했을 때 코인을 환전하여 수익을 내는 기법이다. 배우 섭외를 통한 홍보를 진행했던 기존과 달리, 최근 AI 기술의 발전으로 인해 정교해진 딥 페이크를 악용하여 투자자들을 대상으로 고도화된 공격을 수행하고 있는 추세다.

따라서, 개발사 측에서 상용 딥 페이크 관련 모델에 악용이 불가능하도록 변조가 불가능한 워터마크를 삽입해야 하며, 일반 사용자들은 딥 페이크를 판별하기 위해 디지털 리터러시[13] 교육과 보안 의식 제고가 필요하다.

[13] 디지털 리터러시: 다양한 미디어로부터 명확한 정보를 찾고 평가하며 조합할 수 있는 개인의 능력

■ 랜섬웨어 공격 시나리오



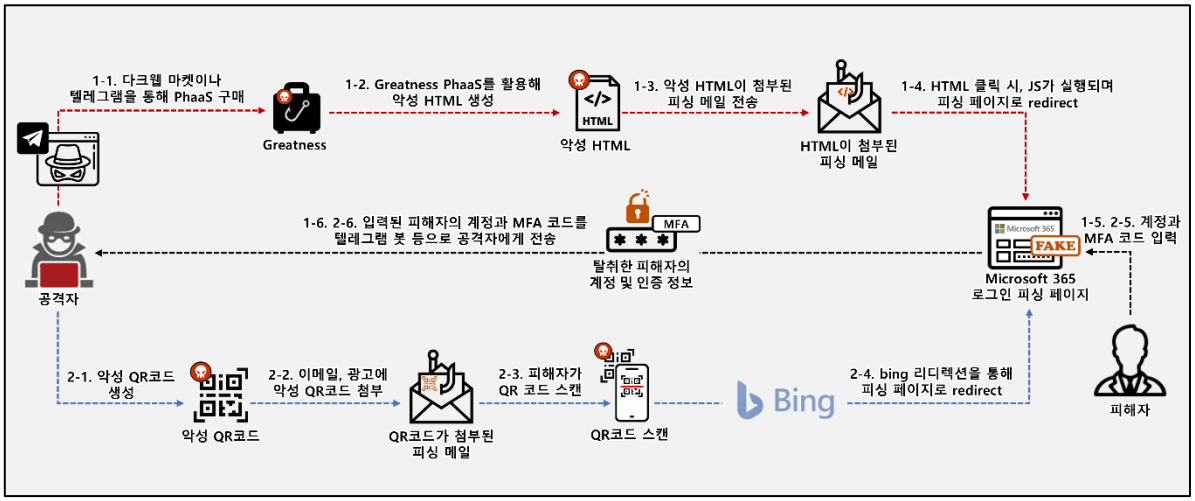
[랜섬웨어 공격 시나리오]

첫 번째 시나리오는 'Cl0p'의 'Progress MOVEit Transfer' 취약점을 악용한 공격 시나리오다. SQL Injection 취약점 CVE-2023-34362 를 통해 MOVEit 서버에 'LEMURLOOT'라는 이름의 웹 쉘을 업로드한 후 공격이 이뤄졌다. LEMURLOOT 는 일종의 백도어 역할을 수행하는데, 피해 서버의 Microsoft Azure 정보를 포함한 자격 증명을 탈취하고 임의의 계정을 생성하여 관리자 권한을 탈취하는 데 사용됐다. 주요 정보를 탈취한 후 다크웹에 게시하여 협박을 시도했으며, 비교적 쉬운 방법으로 공급망 공격이 가능해 대규모 공격 시나리오 중 하나에 해당된다.

두 번째 시나리오는 국내에서 발생한 데이터 복구 업체와 결탁한 북한 해킹 조직 'Lazarus'의 'Magniber' 랜섬웨어 공격 시나리오다. 공격자는 국내 데이터 복구 업체와 결탁하여 랜섬웨어를 유포하고, 미리 복호화 키를 전달받은 데이터 복구 업체는 랜섬웨어에 감염된 피해자를 대상으로 복호화 서비스를 홍보하여 피해자들을 유인한다. 복구 업체는 미리 공격자에게서 전달받은 복호화 키를 통해 복호화를 수행하고 몸값과 동일한 비용의 복호화 대금을 요구하여 공격자와 8:2 로 수익을 분배한다. 이렇게 분배된 범죄 수익이 Lazarus 측에 암호화폐로 송금된 정황으로 보아 Lazarus 의 소행으로 추측된다. 730 건에 걸쳐 발생한 해당 범죄는 약 26 억 원의 범죄 수익을 올려, 결국 데이터 복구 업체 대표와 직원이 구속됐다.

랜섬웨어 그룹의 대규모 공급망 공격과 취약점을 악용한 공격 사례가 증가하고 있고, 복구 업체와 범죄 단체가 결탁하여 랜섬웨어를 감염시키는 등 랜섬웨어 트렌드가 지속적으로 변화하고 있다. 이를 예방하기 위해서는 랜섬웨어 최신 트렌드와 공격 기법에 발맞춰 효과적인 대응책을 수립해야 한다.

■ 피싱 공격 시나리오



[피싱 공격 시나리오]

일반적인 피싱 방법과 다르게 PhaaS(Phishing-as-a-Service)와 QR 코드 등을 악용한 공격 사례가 증가하고 있다. 상세 시나리오는 다음과 같다.

첫 번째 시나리오는 피싱 키트를 통해 피해자의 계정을 탈취하는 공격 방식이다. 공격자는 우선 다크웹이나 텔레그램을 통해 구매한 PhaaS(Phishing-as-a-Service) 키트인 'Greatness' 활용해 견적서, 명세서 등 피해자의 실행을 유도하는 악성 HTML 을 생성하고, 메일에 첨부하여 전송한다. 피해자가 해당 피싱 메일의 HTML 파일을 클릭할 경우, 공격자가 작성한 JS 코드[14]가 실행되면서 피싱 페이지인 가짜 Microsoft 365 의 로그인 페이지로 redirect 된다.

두 번째 시나리오는 악성 QR 코드를 활용한 피싱 공격 방식이다. 공격자는 악성 QR 코드를 생성한 뒤 메일, 광고 등을 통해 전송한다. 피해자가 첨부되어 있는 QR 코드를 스캔하면, 피싱 URL 로 접속되며 해당 사이트에서는 악성 앱 다운로드 또는 개인정보 입력 등을 유도한다. 해당 시나리오는 Bing Redirection URL[15]을 악용한 시나리오이며, 악성 QR 코드 스캔 시 신뢰할 수 있는 URL 인 bing.com/ck/a 형태로 연결되어 피해자의 의심을 최소화할 수 있다.

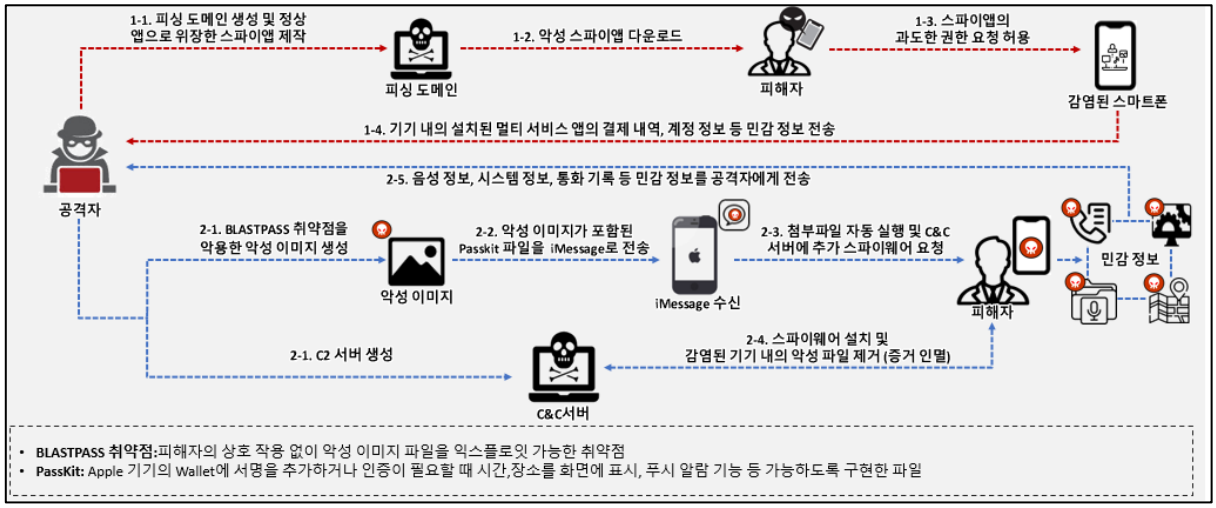
최종적으로 공격자는 피해자가 피싱 페이지에 입력한 계정과 MFA 코드를 탈취한 후, Microsoft 365서비스에 로그인하여 피해자의 권한을 가질 수 있게 된다. 피싱 공격은 피해자의 상황과 심리를 이용하여 계속해서 발전하고 있다. 사용자는 악성 링크나 파일로 인한 피해를 최소화하기 위해 메일 열람 시 발신자 신원 확인에 주의를 기울여야 한다.

---

[14] JS 코드: 웹 페이지를 만들기 위해 사용하는 프로그래밍 언어 Javascript 로 작성된 코드

[15] Bing Redirection URL: Microsoft 에서 제공하는 서비스로, 판매 또는 제휴 페이지에 연결하기 위해 Bing 으로 Redirect 하는 URL 을 생성할 수 있음

■ 모바일 공격 시나리오



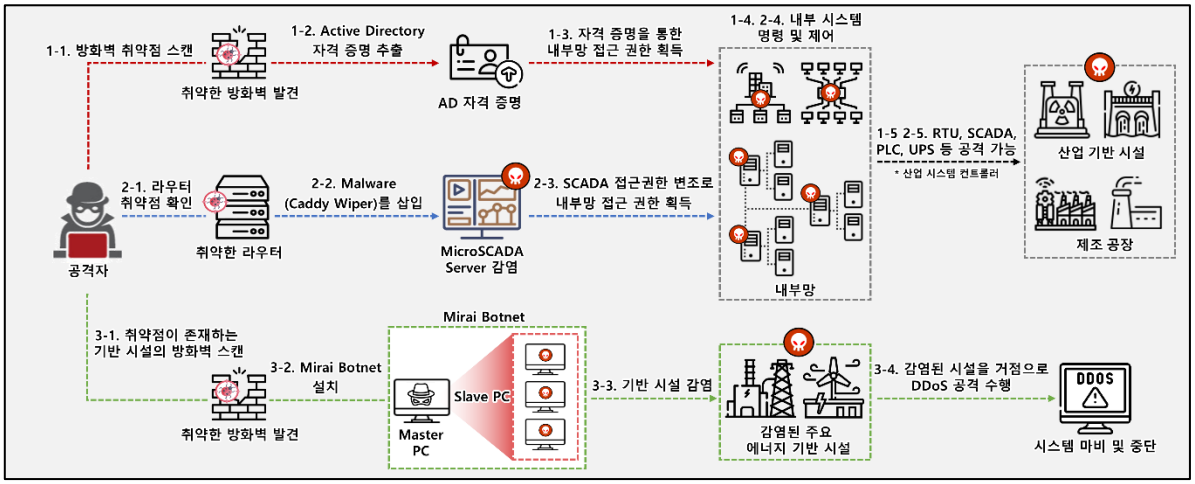
[모바일 공격 시나리오]

하나의 앱에서 멀티 서비스를 지원하는 앱들이 유행하면서 이를 타깃으로 한 공격들과 기존의 대응 전략을 무너뜨리는 제로 클릭 공격이 성행했다.

첫 번째 시나리오는 멀티 서비스 앱을 타깃으로 한 스파이앱 설치 시나리오다. 공격자는 피싱 사이트와 정상 앱으로 위장한 스파이앱을 제작하여 피해자에게 혼동을 준다. 피해자가 피싱 사이트에서 스파이앱을 다운로드 후 실행하면 필요한 범위 이외의 권한도 허용하도록 피해자에게 요청을 강요한다. 이렇게 감염된 스마트 폰은 기기 내의 설치된 목록 중 멀티 서비스를 지원하는 앱의 결제 내역, 통합 로그인 정보 등 중요 정보를 탈취하여 공격자에게 전송한다. 멀티 서비스를 지원하는 점 때문에, 더욱 피해가 커질 수 있어 앞으로도 공격의 타깃이 될 가능성이 높다. 따라서 출처가 불분명한 앱을 다운받지 않도록 주의해야 하며, 여러 사이트 마다 계정을 동일하게 사용하는 것 또한 위협 요인이 될 수 있으므로 주의해야 한다.

두 번째 시나리오는 제로 클릭 공격 시나리오다. 공격자는 상호 작용 없이 익스플로잇이 가능한 악성 이미지와 피해자에게 명령을 전달할 C&C(Control & Command) 서버를 생성한다. 이후 공격자는 PassKit 파일에 악성 이미지를 포함시켜 피해자에게 iMessage 를 전송한다. 피해자가 iMessage 를 열람 시, PassKit 파일이 자동으로 실행되며 악성 이미지에 포함된 취약점이 동작한다. 피해자의 모바일 기기에서는 공격자의 C&C 서버에서 스파이웨어를 설치한 뒤, 증거 인멸을 위해서 악성 파일을 제거한다. 따라서 피해자는 자신의 모바일 기기가 감염됐는지 파악하기 어렵다. 이후에 공격자는 피해자의 음성 정보, 시스템 정보, 통화 기록 등 민감 정보를 지속적으로 탈취할 수 있다.

■ OT/ICS 시나리오



[OT/ICS 공격 시나리오]

산업 시설의 디지털화로 OT/ICS 사이버 공격이 증가하고 있다. 상세 시나리오는 다음과 같다.

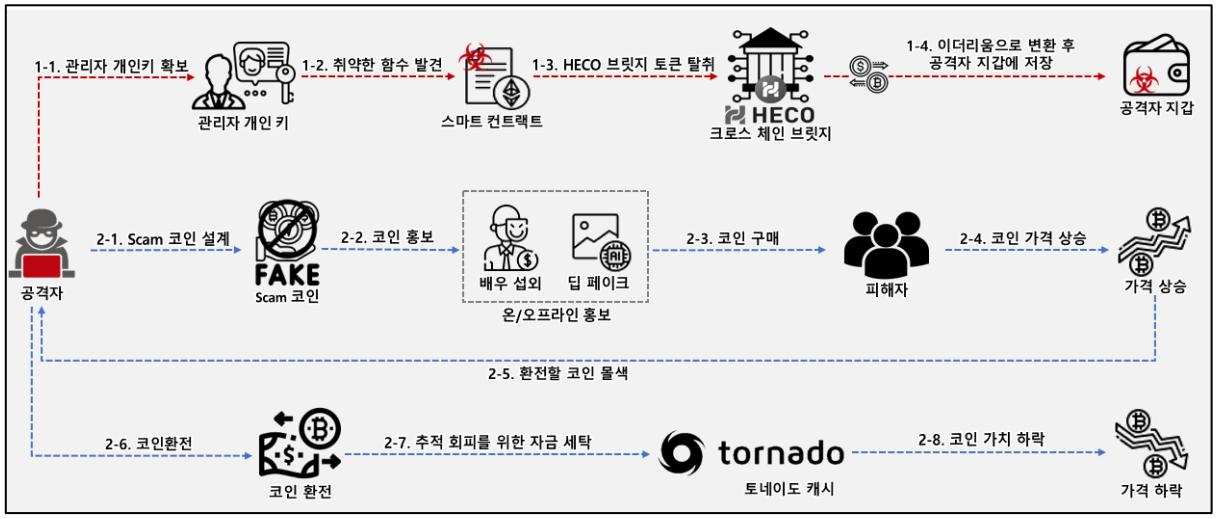
첫 번째 시나리오는 방화벽 취약점을 공격해 산업 시스템 컨트롤러의 제어권을 탈취하는 공격 방식이다. 공격자는 취약한 방화벽을 통해 추출해 낸 AD 자격 증명을 통해 내부망에 접근할 수 있는 권한을 획득한다.

두 번째 시나리오는 라우터 취약점을 공격해 산업 시스템 컨트롤러의 제어권을 탈취하는 공격 방식이다. 공격자가 라우터의 취약점을 통해 'Caddy Wiper'라는 Malware 를 MicroSCADA Server 에 삽입하면, SCADA 의 접근 권한을 변조해 내부망에 접근할 수 있는 권한을 획득한다. 두 시나리오 모두 획득한 내부망 접근 권한을 통해 내부 시스템을 제어하고 명령을 내릴 수 있다. 이를 통해 RTU, SCADA, PLC, UPS 등 산업 시스템을 제어할 수 있는 컨트롤러를 공격해 산업 기반 시설이나 제조 공장의 데이터를 변조하거나 서비스 중단을 시킬 수 있다.

마지막 세 번째 시나리오는 주요 기반 시설의 방화벽 취약점을 공격해 산업 시스템 컨트롤러의 제어권을 탈취하는 공격 방식이다. 공격자가 스캔한 시설 방화벽 취약점을 통해 Mirai Botnet(미라이 봇넷)을 설치한다. Botnet(봇넷)으로 인해 악성 프로그램에 감염된 주요 에너지 기반 시설들을 거점으로 삼아 DDoS(디도스) 공격을 수행해 해당 시설과 연결된 시스템을 마비시키거나 중단할 수 있다.

감염이 발생하면 공장 생산 중단으로 인한 손실과 복구비용에 대한 문제, 시설 오작동으로 인한 안전 사고 발생, 데이터 변조로 인한 제품 신뢰성 감소 등의 심각한 문제를 초래할 수 있으며, 더 나아가 기업의 안정성과 지적재산에 대한 위협으로 이어질 수 있다. 따라서 이를 대비하기 위해 강력한 사이버 보안 대책을 마련해야 하고 주기적인 감사가 필요하다.

■ 가상자산 공격 시나리오



[가상자산 공격 시나리오]

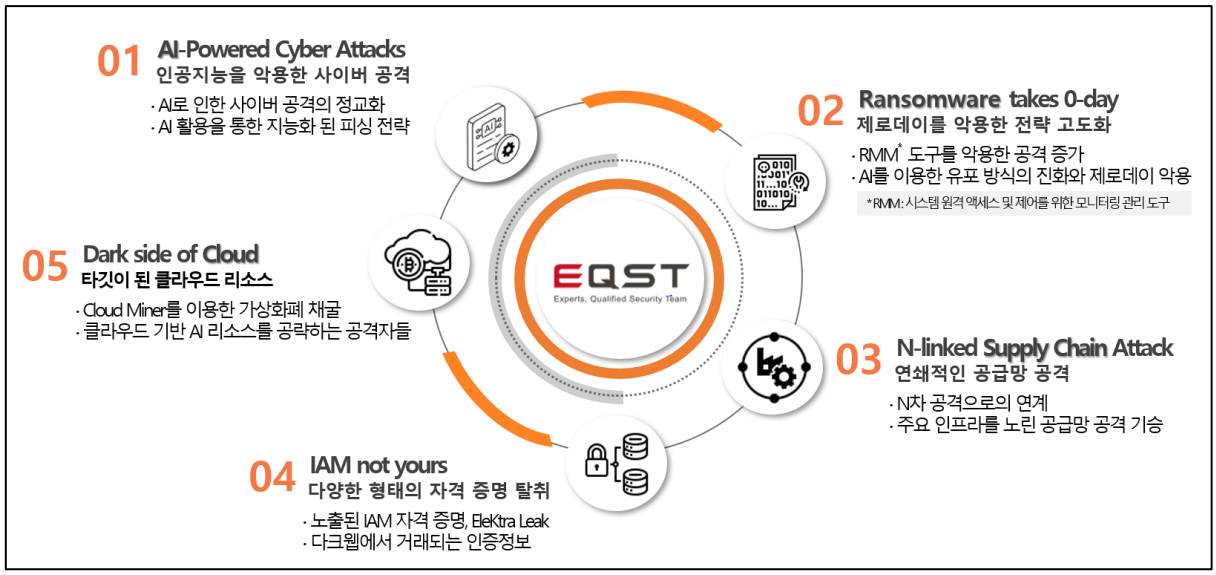
가상 자산 기반의 공격은 피해 발생 시 피해의 규모가 크기 때문에, 공격자들이 여전히 주목하는 분야 중 하나이다.

첫 번째 시나리오는 HECO 브릿지에서 발생한 취약한 함수와 개인키 탈취로 인한 피해 시나리오다. 공격자는 피싱, 트로이 목마 등을 통해 관리자의 개인키를 확보한다. 관리자의 개인키를 획득한 공격자는 HECO 브릿지의 스마트 컨트랙트에서 관리자 권한이 있으면, 자동으로 자금 인출이 가능한 취약한 함수를 발견한다. 따라서 공격자는 관리자 개인키와 취약한 함수를 통해 크로스 체인 브릿지 내의 다수의 코인을 공격자의 지갑으로 인출한다. 크로스 체인 브릿지는 실수가 발생할 수 있는 코드 영역과 복잡한 트랜잭션이 혼합되어 있으므로 더욱 주의해야 하며, 액세스키나 개인키 같은 중요 정보를 유출하지 않도록 주의해야 한다.

두 번째 시나리오는 FSL 토큰의 출구 사기(Exit Scam) 시나리오를 각색한 내용이다. 공격자는 사기를 위해 1 억 개의 Scam 코인을 생성한다. 공격자는 1 억 개의 코인 중 300 만 개를 높은 가격에 피해자에게 판매하기 위해 특정 유명인의 딥 페이크 영상과 배우 섭외 등을 통해 홍보한다. 이후 현혹된 피해자들이 거래소에서 Scam 코인을 구매하면 거래량이 증가하여 Scam 코인의 가격이 상승하게 된다. Scam 코인의 가격이 공격자의 목표 금액에 도달하면 공격자는 나머지 모든 코인을 타 코인으로 환전한다. 이후 환전한 자금의 출처를 세탁하기 위해 코인 믹서(Crypto Mixer)[16] 중 하나인 토네이도 캐시를 통해 자금을 세탁한다. 이로 인해 급격하게 Scam 코인의 가격이 하락하면서 피해자들은 금전적인 피해를 보게 된다.

[16] 코인 믹서(Crypto Mixer): 거래내역을 비공개로 유지하여 탈중앙화를 구현하기 위한 장치이지만 자금 세탁에 악용됨

2024 년 5 대 사이버 위협 전망



[2024 년 사이버 위협 전망]

■ AI-Powered Cyber Attacks

- 인공지능을 악용한 사이버 공격

최근 인공지능(AI) 기술의 발전은 많은 산업 분야에 혁신을 가져왔지만, 사이버 보안 분야에서는 피싱, 악성코드 생성 등 각종 악의적인 수단으로도 악용되고 있다. 특히, 최근 주목받고 있는 LLM(Large Language Model) 모델은 방대한 데이터 세트를 사용하여 훈련되고, 다양한 자연어 처리 작업이 뛰어난 특성으로 인해 정교한 피싱 메일을 작성하는데 유용하다.

실제로 악의적인 용도로 제작된 LLM 모델 기반의 생성형 AI 'WormGPT'가 등장하여 다양한 사이버 공격에 이용되고 있다. 특히, 공개된 데이터를 분석하여 수신자 맞춤형의 설득력 있는 악성 이메일을 생성함으로써 정교한 BEC(Business Email Compromise) 공격[17] 수행이 가능한 것으로 알려졌다.

뿐만 아니라 실제와 구별이 어려울 정도로 높은 완성도를 보이는 딥페이크와 딥보이스 기술은 수많은 피싱 공격에 악용되고 있다. 특히, 딥보이스 기술은 몇 초의 음성만 가지고 있더라도 타인의 목소리를 복제할 수 있을 정도로 발전했으며, 국내에서도 딥보이스 피싱 피해 사례가 빈번하게 발생하고 있다.

AI 기술이 발전함에 따라 사이버 공격 맞춤형 서비스(e.g. WormGPT)를 이용한 고도화된 사이버 공격이 발생할 것으로 보이며, 특히 AI 가 생성한 데이터의 문법 오류, 맥락 결여 문제 등 언어적 한계가 해소되면서 문법적으로 더 자연스러워지고 정교해진 피싱 공격이 성행할 것으로 전망된다.

[17] BEC 공격: 피해자가 평소 신뢰하는 조직 또는 관계자가 보낸 이메일로 가장하여 민감 정보 유출을 유도하는 공격

■ Ransomware takes 0-day

- 제로데이를 악용한 전략 고도화

최근 랜섬웨어 공격의 탐지 우회와 편의를 위해 상용 RMM(Remote Monitoring and Management) 도구 사용 빈도가 증가하고 있다. RMM 은 시스템 원격 액세스 및 제어를 위한 모니터링 관리 도구로, 기업에서는 유지관리 비용을 줄이고 시스템 문제 해결을 위한 액세스 용도로 주로 사용한다. 내부 확산에 악용될 수 있는 기능을 포함하고 있지만, 정상적인 활동으로 분류되어 쉽게 탐지되지 않아 많은 랜섬웨어 그룹이 악용하고 있다.

이와 더불어 AI 기술이 발전함에 따라 랜섬웨어의 유포 방식도 지능적으로 변화할 것으로 보인다. 타깃형으로 제작된 기존의 피싱 형태에서 AI 를 악용한 피싱 제작으로 발전할 것으로 예상되며, 이는 메일을 수신한 사용자가 수상한 점을 더욱 파악하기 어려운 형태로 진화되어 랜섬웨어 공격이 증가할 것으로 보인다.

기존의 랜섬웨어 그룹들은 특정 조직을 대상으로 하는 APT 공격에 주력했으나, 최근 상황은 'MOVEit', 'GoAnywhere', 'PaperCut' 등 상용 솔루션들의 제로데이 취약점을 악용하여 대규모 공격을 수행하는 흐름으로 변화하고 있다. 이러한 솔루션들은 많은 기업 및 조직에서 활용되고 있어 하나의 취약점으로 다수의 공격이 가능해 공격자들의 타깃이 되었으며, 2024 년에도 랜섬웨어 그룹들의 취약점을 악용한 대규모 공격이 지속될 것으로 보인다.

■ N-linked Supply Chain Attack

- 연쇄적인 공급망 공격

공급망 공격의 핵심 위험성은 N 차 공격으로의 연계 가능성에 있다. 이는 단순히 하나의 기업이나 네트워크를 타깃으로 하는 것이 아니라, 해당 기업의 제품을 사용하거나 네트워크가 연결된 다수의 기업들로 공격이 확산되는 현상을 말한다.

이러한 연쇄적 공격은 주로 소프트웨어 공급망, 서비스 공급자 혹은 파트너 네트워크를 통해 이뤄진다. 올해 4 월에 발생한 기업용 소프트웨어 '3CX' 공급망 공격은 1 차 소프트웨어(X_TRADER) 공급망 공격에서 2 차 소프트웨어(3CX) 공급망 공격으로 이어진 최초의 연쇄적 공급망 공격의 예시라고 볼 수 있다.

공급망 공격은 주로 여러 조직에서 사용하는 솔루션을 목표로 공격을 진행하며, 이는 타깃이 된 기업에서 즉시 대응이 불가능하고 단일 공격 지점을 통해 다수의 피해를 유발할 수 있어 매우 위험하다.

또한, 작년 러시아-우크라이나 전쟁에 이어 올해 이스라엘-팔레스타인 분쟁이 발발하면서, 공급망 공격을 통한 주요 인프라 공격이 증가하고 있다. 국가 간 사이버 전이 계속되면서 기업 및 세계 주요 인프라를 노린 새로운 공급망 공격이 지속적으로 발생할 것으로 보인다.

■ IAM not yours

- 다양한 형태의 자격 증명 탈취

자격 증명 관련 문제는 매번 중요하게 다뤄졌던 문제이며, 다양한 형태로 자격 증명이 탈취되고 있다.

대부분의 기업에서 분업을 진행하기 때문에 계정정보, IAM 자격 증명 등을 GitHub, GitLab 등과 같은 협업 플랫폼에 저장하는 경우가 많다. 이때, 관리자의 실수로 자격 증명 정보를 전체 공개로 설정된 리포지터리[18]에 저장하는 경우가 종종 있어 주의가 필요하다. 최근 공격자는 이런 실수를 공략하여 자격 증명을 탈취하는 'EleKtra Leak' 캠페인을 수행하고 있어 각별한 주의가 요구된다.

개발자의 실수뿐만 아니라, 피싱이나 악성코드 등을 통해 개인용 PC 에 저장된 자격 증명 정보가 유출되어 2 차, 3 차적인 피해가 발생할 수 있다. 유출된 정보는 다크웹에서 거래되어 초기 침투에 이용될 수 있으므로 기본 인증 외의 추가적인 인증 요소를 설정하는 것이 중요하다.

로그인 및 아이덴티티 관리 시스템을 제공하는 IAM 플랫폼을 이용하더라도 공격자가 해당 업체의 취약점을 공격하거나, 해당 업체의 관리자 계정을 탈취하는 등 IAM 제공 업체를 타깃으로 한 공격이 지속적으로 발생하고 있으므로 완벽하게 방어할 수는 없다.

비즈니스 환경이 복잡해지고, 자격 증명 노출 경로가 다양해짐에 따라 2024 년에도 자격 증명 탈취와 악용을 노린 사이버 공격은 지속될 것이다.

[18] 리포지터리: 개발자가 프로젝트 코드를 체계적으로 저장하고 작업할 수 있는 저장소

■ Dark side of Cloud

- 타깃이 되는 클라우드 리소스

공격자들의 클라우드에 대한 이해도가 높아짐에 따라 클라우드 인프라나 플랫폼 등을 활용하는 사이버 공격이 증가하고 있다.

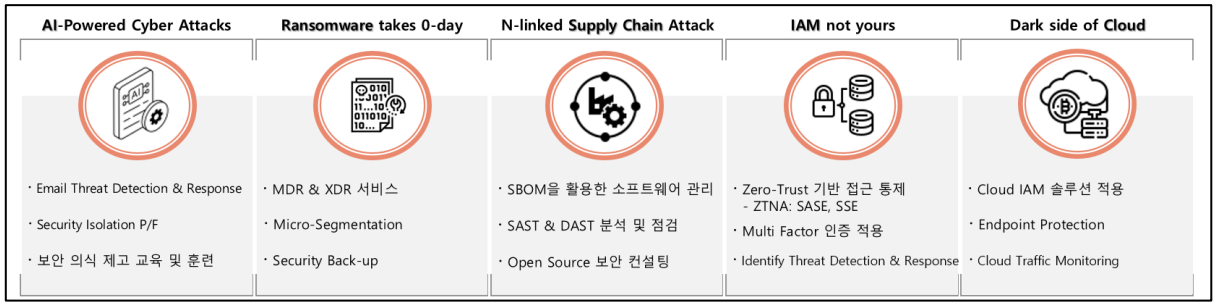
올해에는 클라우드 서비스를 악용해 암호화폐를 채굴하는 '클라우드 마이닝' 공격이 다수 발생했다. 클라우드 마이닝은 클라우드 리소스를 통해 암호화폐를 채굴하는 기법으로, 사용자 PC 에 접근해 마이닝 공격을 했던 기존과 달리 현재는 클라우드 자원을 탈취하여 마이닝 공격을 수행하는 형태로 변화하고 있다.

또한, 기업에서 생성형 AI 서비스를 제공할 때 방대한 데이터를 학습시키거나, 사용자 유입에 따라 실시간으로 빠르게 달라지는 리소스 비용을 효율적으로 관리하기 위해 클라우드 기반 GPU 를 활용하고 있는 추세다.

클라우드 환경을 사용하는 기업들이 점점 더 많아지고 기업별로 사용하는 리소스 형태도 다양해짐에 따라 공격 표면에 노출된 클라우드 리소스는 암호화폐 채굴, 기업 데이터 유출 등 지능적인 공격에 계속해서 악용될 것으로 전망된다. 기업에서는 이에 대응할 수 있도록 Cloud 솔루션, Endpoint protection, Cloud Traffic Monitoring 등 고도화된 클라우드 보안 대책에 대해 논의할 필요가 있다.

대응 전략

■ EQST 5 대 위협 대응 전략 및 서비스



[5 대 위협 대응 전략]

사이버 공격은 스피어피싱, 딥 페이크/딥 보이스를 악용한 피싱 공격 등 AI 를 활용하면서 점점 정교화, 지능화되고 있다. 이제는 인공지능을 악용한 사이버 공격이 영화 속의 이야기가 아닌 우리에게 직면한 문제임을 인정해야 한다. 고도화된 피싱 공격에 대응하기 위해서는 ETDR(Email Threat Detection & Response) 솔루션을 통해 실시간 위협 모니터링을 수행하고 악성 메일을 차단함으로써 위협을 최소화하는 것이 중요하다. 또한, 이메일 격리 플랫폼을 구축하면 1 차적으로 이메일에 포함된 악성 링크 및 콘텐츠를 격리하고, 신뢰할 수 있는 콘텐츠만 사용자에게 전달할 수 있어 안전하게 사용할 수 있다. 무엇보다 피싱 공격은 사용자의 상황과 심리를 이용하여 범죄 수법이 교묘해지고 있으므로, 보안 의식 제고 교육 및 훈련을 통해 피싱 공격 위험에 노출되어 있음을 인지하고, 발신자 신원 확인에 주의를 기울여야 한다.

최근 랜섬웨어 그룹에서는 고도화된 전략을 활용한 공격을 수행하고 있다. 이에 대응하기 위해서는 Endpoint, 네트워크, 클라우드 전반에 걸쳐 발생하는 위협을 탐지하고 분석하는 XDR(Extended Detection & Response) 서비스와 전문가의 노하우가 결합되어 실시간으로 침해 지표가 업데이트 되는 등 적은 비용으로 최대한의 효과를 낼 수 있는 MDR(Managed Detection & Response) 서비스를 통해 보안을 강화해야 한다. 추가적으로 작업 환경을 구성할 때, 네트워크를 세분화하여 격리시키는 Micro-Segmentation 기법을 이용해 네트워크 접근을 제어하고 제한하는 것이 필요하다. 이는 각각의 세그먼트별로 보안 제어를 구현할 수 있으며 침해사고 발생 시, 다른 세그먼트에는 영향을 주지 않아 피해 범위를 최소화할 수 있다. 마지막으로 신뢰할 수 있는 시스템에 주기적인 백업을 진행하여 중요 데이터를 보호해야 한다.

공급망 공격은 해킹 그룹에게 좋은 타깃이 되고 있으며, N 차 감염을 통해 더 큰 피해를 낳고 있다. 이를 대응하기 위해 SBOM(Software Bill of Materials)를 참고하여 사용하는 소프트웨어 전반의 잠재적인 위험을 식별해야 한다. SBOM 은 버전, 라이브러리 등 사용하는 소프트웨어에 대한 상세 정보를 기술한 목록을 말하며, 신규 취약점이 공개됐을 때 SBOM 을 참고하여 취약점 영향을 받는 파일을 찾아 분석하고 빠르게 조치할 수 있다. 또한, 실시간으로 올바른 대응을 할 수 있도록 SBOM 의 주기적인 업데이트와 검증이 필요하다. 새로운 모듈 및 소프트웨어 개발 시에는 SAST(Static Application Security Testing), DAST(Dynamic Application Security Testing)를 통해 개발 및 운영 단계에서 발생할 수 있는 취약점을 1 차적으로 탐색하고 예방할 수 있으며, 오픈소스를 이용하는 경우에는 보안 컨설팅을 수행해 안전하게 사용해야 한다.

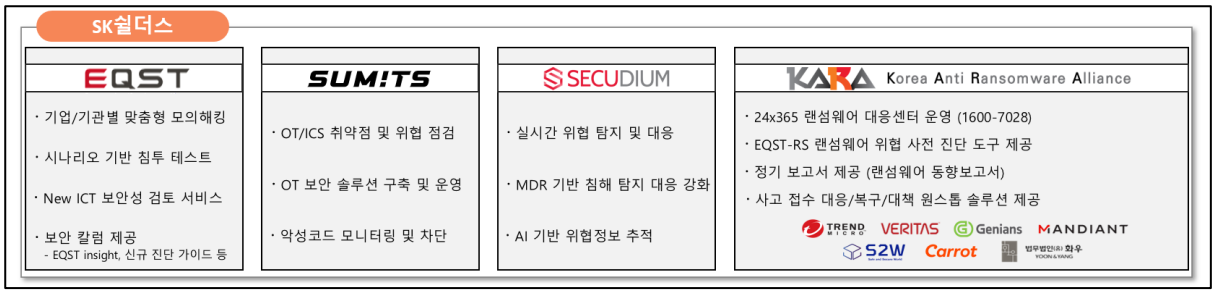
다양한 형태의 자격 증명 탈취에 대한 위협은 '아무것도 신뢰하지 않는다'를 전제로 하는 Zero-Trust 기반의 환경을 구축하여 자격 증명에 대한 접근 제어를 강화해야 한다. Zero-Trust 환경을 구현하는 기술인 ZTNA(Zero-Trust Network Access)를 적용하여 데이터 및 리소스에 대한 불필요한 접근을 차단할 수 있다. ZTNA 는 네트워크 전반의 모든 사용자에게 접근 권한을 제공하도록 설계된 VPN 과 달리 재인증을 자주 요구하며, 승인되지 않은 사용자에게는 권한을 부여하지 않는 특징을 가지고 있다. Zero-Trust 관련 프레임워크인 SASE(Secure Access Service Edge)[19]와 SSE(Security Service Edge)[20]를 통해 ZTNA 구현이 가능하다. 또한, 사용자가 시스템에 접근할 때 두 가지 이상의 인증을 요구하는 Multi-Factor(다중 요소) 인증과 같이 높은 수준의 인증을 요구해 보안을 강화해야 한다. 무엇보다 각 기업 환경에 맞는 엄격한 보안 정책을 수립하고, 세분화된 접근 제어를 적용해 단순히 솔루션에 의존하는 것이 아닌 관리적 측면에서의 지속적인 관심과 모니터링이 필요하다.

클라우드 환경이 보편화되면서 기업에서는 생성형 AI 를 위한 클라우드 기반의 GPU 등 다양하게 클라우드를 활용하는 모습을 보이고 있다. 이에 공격자들도 클라우드 환경에 맞춰 고도화된 전략을 선보이고 있다. 기존에는 IAM 권한 탈취를 통한 데이터 탈취가 주된 목적이었다면, 현재는 더 나아가 데이터 탈취와 채굴을 병행하는 공격으로 진화했다. 이에 대응하기 위해서 클라우드 서비스에서 제공하는 IAM 자격 증명 솔루션을 적용하여 사용자 및 리소스에 대한 접근 권한 관리 등을 통해 보안을 강화해야 한다. 또한, 주기적으로 IAM 자격 증명 솔루션 감사가 필요하다. 자격 증명 외에도 공격자가 클라우드 자원을 직접 공격하는 경우를 대비하기 위해 실시간으로 위협 탐지, 대응 가능한 Endpoint Protection 기능 적용이 필요하며, Traffic Monitoring 기능을 활성화하여 클라우드 환경에서 이상 징후가 탐지될 경우 신속한 조치를 취할 수 있도록 해야 한다.

---

[19] SASE(Secure Access Service Edge): 제로 트러스트 아키텍처를 구현하기 위한 프레임워크 중 하나로 기존의 네트워킹과 클라우드 네이티브 보안 기능의 통합

[20] SSE(Security Service Edge): SASE 프레임워크의 구성 요소로 WAN 을 제외한 보안 정책 결정 및 집행에 대한 정의



[SK 쉴더스 대응 서비스]

SK 쉴더스에서는 앞서 전망한 위협들에 대응할 수 있는 다양한 맞춤형 서비스를 제공하고 있다. 화이트 해커 그룹 EQST 에서는 IoT, 클라우드 등 New ICT 영역을 비롯하여 다양한 산업군별 위협 시나리오와 진단 방법론을 바탕으로 기업/기관별 맞춤형 모의해킹을 수행하고 각 기업 환경에 최적화된 가이드를 제공하고 있다. 또한, 보안 담당자 및 관련 종사자들이 최신 트렌드를 파악하고 선제적 대응을 할 수 있도록, 신규 취약점 분석 및 기술 연구 결과를 담은 다양한 보안 칼럼을 공식 홈페이지를 통해 무료로 제공하고 있다.

지속적인 보안 위협이 발생하고 있는 OT/ICS 분야는 맞춤형 보안 컨설팅을 통해 환경에 맞는 솔루션을 구축 및 운영하여, 실시간으로 위협을 모니터링하고 차단해야 한다. SK 쉴더스에서는 지능형 융합보안 플랫폼 SUMiTS 를 활용하여 OT/ICS 에 특화된 위협 점검 서비스를 제공하고 있다.

또한, 자사의 사이버보안 관제 센터인 Secudium Center 에서는 MDR 을 기반으로 보안 위협을 실시간으로 감지하고 위협을 사전에 차단하고 있으며, AI 기반 위협정보 추적을 통해 지능화된 사이버 위협에 대한 탐지 및 대응 서비스를 제공하고 있다.

랜섬웨어의 위협을 빠르게 식별하기 위해서는 최신 랜섬웨어 공격 트렌드 파악과 빠른 인지가 필요하다. SK 쉴더스에서는 최신 랜섬웨어 동향을 담은 정기 보고서를 제공하고 있으며, 랜섬웨어 위협을 사전에 진단할 수 있는 도구 'EQST-RS'를 무료로 배포하고 있다. 개인 및 기업에서는 이를 활용해 효과적으로 랜섬웨어 초기 대응책을 수립할 수 있다.

또한, 앞서 나온 여러 변화하는 랜섬웨어에 대응하기 위해서는 기업 특성에 맞춘 랜섬웨어 특화 서비스 및 솔루션이 필요하다. SK 쉴더스에서는 빠른 대응과 복구를 위해 랜섬웨어 대응 협의체 KARA(Korea Anti Ransomware Alliance) 운영하여, 랜섬웨어 대응에 필요한 모든 프로세스를 원스톱으로 처리하는 통합 대응 프로세스를 제공하고 있다. 또한 SK 쉴더스는 24 시간 365 일 대응 가능한 랜섬웨어 대응센터(1600-7028)를 운영하고 있다.

■ 맺음말

2023 년 사이버 보안 트렌드를 살펴보면 생성형 AI 의 등장으로 인해 고도화/정교화 되었으며, 오래된 취약점뿐만 아니라 제로데이를 적극적으로 활용하는 랜섬웨어 그룹이 증가했음을 알 수 있다. 또한 기업용 솔루션을 통한 N 차 공급망 공격 등 공격의 유형이 다양해진 것을 볼 수 있다.

EQST 에서는 기존 보안 분야의 연구뿐만 아니라 클라우드를 비롯해 올해 가장 큰 화두가 되었던 생성형 AI 분야에서의 연구를 진행하고 있다. EQST 는 2017 년 창설 이래 '모의해킹', '신기술 연구', '해킹 프로그램 개발 및 구축', '랜섬웨어 대응', '신규 취약점 분석 및 진단', '해킹 교육' 등 다양한 활동을 선도적으로 펼치고 있으며, 새로운 분야의 연구도 지속적으로 이어 나갈 예정이다.

EQST Annual Report

2023.12

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

발행인 : EQST사업그룹
제　작 : SK쉴더스 커뮤니케이션그룹