infosec

Threat Intelligence Report

# EQST INSIGHT

2024

04

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

infosec

# Contents

# Headline

## AI 기반 보안관제 고도화 전략 및 발전 방향

MSS 사업그룹/Secudium 고도화팀 김종현 팀장

### ■ 개요


한국인터넷진흥원(KISA)에 따르면, 지난해 상반기 침해사고 신고 건수는 664 건으로 전년 동기대비 40% 증가한 것으로 나타났다. 사물인터넷과 커넥티드 기기 사용의 증가, 클라우드 도입과 하이브리드 근무 모델 등을 비롯한 디지털 전환의 가속화로 '공격 표면(Attack Surface)'이 확대되면서 새로운 취약점이 늘고 있다.

보안관제 서비스는 24 시간 365 일 위협 모니터링을 지원한다. 실시간으로 쏟아져 들어오는 수많은 보안 위협에 대한 정확한 판단과 빠른 대응이 필요한만큼, 다양한 사이버 보안 영역 중 특히 힘들고 고단한 업무로 꼽힌다. 무엇보다 해커는 불특정 국가에서 IT 자산을 타깃으로 다양한 방식으로 공격을 시도하고 있으며, 해킹 기술 또한 날로 지능화되고 있기 때문에 밤낮으로 긴장을 늦출 수 없다.

## ■ 기존 보안관제의 어려움

24 시간 365 일 위협을 모니터링하는 관제 특성상 근본적인 어려움이 존재한다. 이번 보고서를 통해 크게 3 가지 어려움에 대해 살펴보도록 한다.

### 질문 1. 모든 수집/로그 이벤트를 분석하고 있는가?

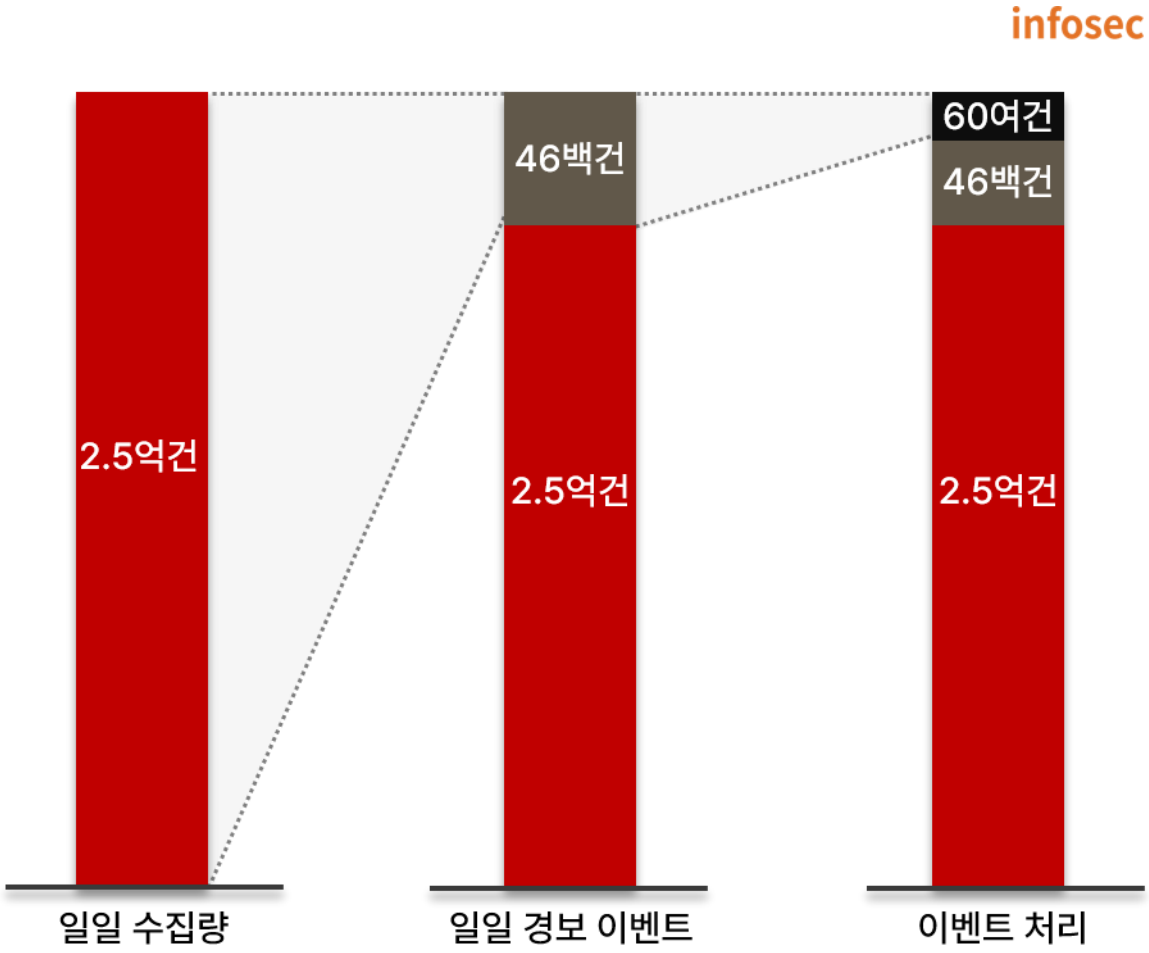



그림 1. 위협 이벤트 현황

위 그림은 A 기업 관제센터에서 수집 및 처리된 위협 이벤트 현황을 나타낸 그래프다. 일일 약 2.5 억 건을 수집하여 관제 플랫폼에서 46 백 건의 경고를 발생시키고 있으며, 이 중 우선순위에 따라 60 여 건의 위협을 분석/대응하고 있다. 분석되지 않은 경고 45 백여 건은 정말로 안전한 것인지, 경고로 발생되지 않은 2.5 억 로그에 보안위협은 없는 것인지 의문을 가질 수 있다.

### 질문 2. 침해위협 탐지/분석 일관성은 유지되고 있는가?

보안관제사는 위협을 판단하기 위해 수집한 로그의 원본 데이터(Raw-Data)를 확인하거나 바이러스토탈(VirusTotal)과 같은 Reputation DB 또는 Threat Intelligence 등을 활용하고 있다.


그림 2. 위협 판단 시 활용하는 자료

1) Raw-Data 가 난독화 되어 있어 즉시 확인이 안되거나, 복호화 하여도 기술의 난이도에 따라 판단이 어렵다면? 2) VirusTotal 의 91 개 분석 엔진 중 89 개가 정상이고, 2 개의 엔진에서만 의심스럽다고 탐지한다면, 이것은 위협으로 봐야 할까? 정상으로 판단해야 할까? 3) Threat Intelligence 에서 조회결과 C&C IP 로 확인을 했지만, 최종 활동 날짜가 2~3 년 전이라면? 이것을 위협이라고 판단할 수 있을까?

위 3 가지 사항에 대해서는 보안관제사마다 모두 다른 판단을 할 수 있으며, 이에 대해서 문제가 있다고 하기도 어려울 것이다.

질문 3. 새로운 공격, 늘어나는 공격 표면, 이를 탐지하기 위한 신규 보안장비, 늘어나는 보안 로그들에 대해서는 어떻게 대응하고 있는가?

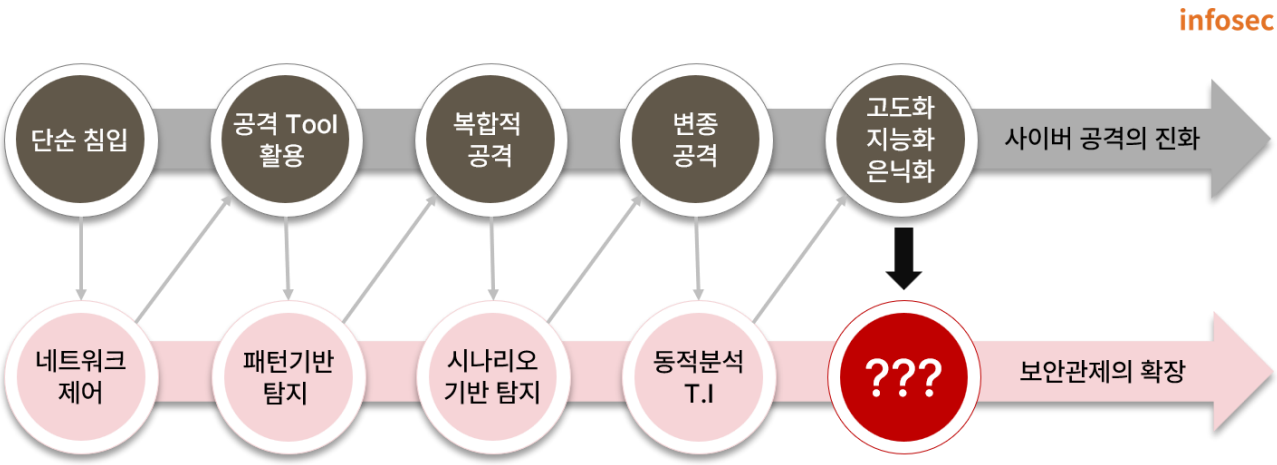



그림 3. 사이버공격 진화 및 보안관제

초기 단순 공격은 방화벽 IP 차단만으로 방어가 가능했다. 자동화 Tool 사용시 IDS/IPS/WAF 에 탐지 패턴을 등록해 방어를 수행했으며, 좀 더 다양한 공격 시도에는 보안 로그 상관분석으로 대응이 가능했다.

최근의 악성 파일 기반 공격에 대해서는 APT 탐지 솔루션을 통해 동적분석/T.I 탐지,분석,대응을 할 수 있다. 그렇다면 향후 AI 를 활용한 고도화/지능화/은닉화 된 공격은 어떻게 대응할 것인지에 대한 고민이 필요하다.

'23 년 마지막 발표 취약점은 CVE-2023-24151 로 일일 평균 66 개의 취약점이 새로 발표됐으며, 보안 대상도 Cloud, OT/ICS 로 확대되고 있다. 또한, 이를 대응하기 위해 Micro-Segmentation, ASM, SASE 등의 새로운 보안 장비들이 보안관제 대상으로 확대되고 있다.

이렇듯 보안관제는 늘어나는 보안로그를 분석해 새로운 위협에 대한 대응이 필요하다. 보안관제에서 모두 커버할 수 있을지에 대한 우려도 존재한다. 공격자는 한번의 공격만 성공하면 되지만, 보안관제는 한번의 실수도 있어서는 안되기 때문이다.

## ■ AI 기반 보안관제

지금까지 보안관제가 가지고 있는 한계에 대해 알아보았다. 한계를 보완하기 위해서는 머신의 도움을 받아 “모든 수집 이벤트에 대해 실시간으로 빠르게 분석하고 판단해 대응”하는 것이 중요하다. 특히 AI 를 결합한다면 보안관제가 가지고 있는 많은 한계를 극복하는 데 도움을 받을 수 있다.

앞서 제기된 첫 번째 질문인 “모든 수집/로그 이벤트를 분석하고 있는가?”와 세 번째 질문인 “새로운 공격의 증가”를 좀 더 요약하면, Unknown 위협을 탐지할 수 있는가? 라는 질문이 될 수 있다. 이미 알고 있는 위협이라면 탐지 패턴을 생성하거나 상관분석 Rule 을 만들어 Threat Intelligence 를 통해 탐지할 수 있기 때문이다. 즉, Unknow 위협을 효과적으로 탐지하기 위해서는 전체 수집 로그에서 다른 특성을 가지는 로그가 포함되어 있는지를 모니터링하는 것이 중요하다.

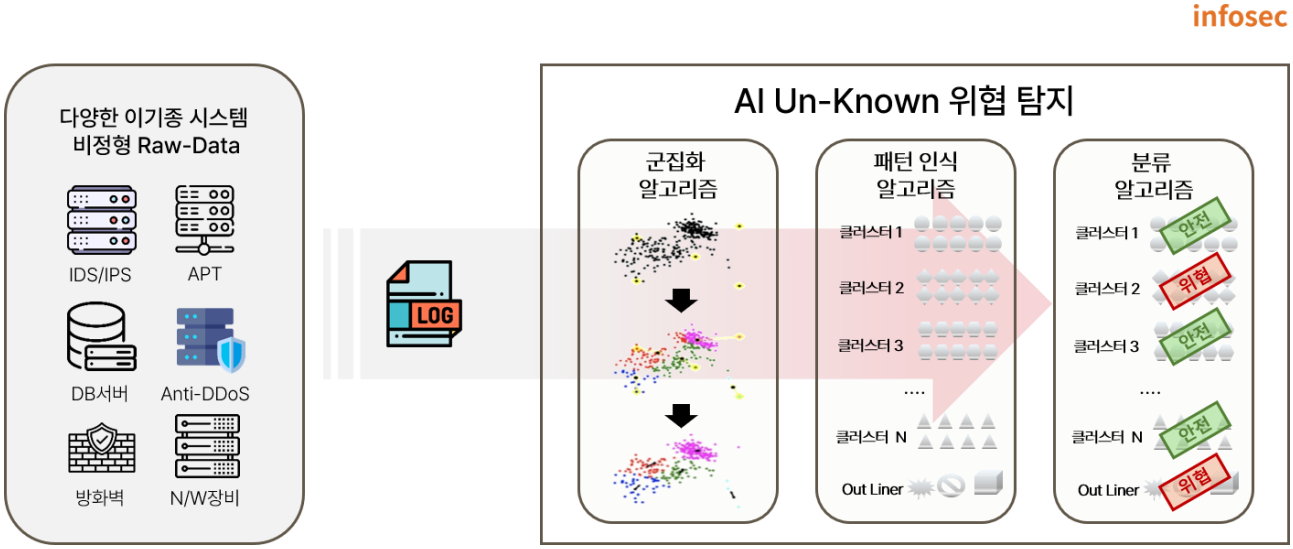



그림 4. AI 기반 Unknown 위협 탐지

AI 는 유사한 항목별로 구분하는 ‘군집화’ 기능이 뛰어나다. 이를 위해서는 아래와 같이 단계를 거쳐 AI 학습 및 활용이 가능하다.

- 초기에는 일정 기간 동안 데이터를 모아 초기 학습 모델을 수행한다. 분류된 각 군집에 대해서 안전한지, 위협인지를 파악하는 Labeling 을 수행한다.
- 이후에는 labeling 을 통해 위협이 될 수 있는 로그를 분석한다.
- 지속적으로 학습을 진행하게 되면, 초기에 어느 군집에도 포함되지 않던 Out-Liner 가 계속적으로 축소된다. 이후 모니터링에서는 “Labeling 된 위협”과 “Out-Liner”를 탐지/분석함으로써 Un-Known 위협을 탐지할 수 있다.

두 번째 질문인 **"침해위협 탐지/분석에 대한 일관성은 유지되고 있는가?"**는 관제사들의 정·오탐 판단에 대한 부분이다. 위협 판단에 경험이 필요하기 때문에 신입관제사와 3~4 년 이상의 경력을 가진 관제사의 판단은 서로 다를 수 있다.

이러한 경험에 의한 판단은 어디 있을까? 기존에 판단했던 정·오탐 결과들이 경험을 반영하고 있다. 정·오탐 판정은 기본적으로 개와 고양이를 구분하는 AI 와 동일하다.

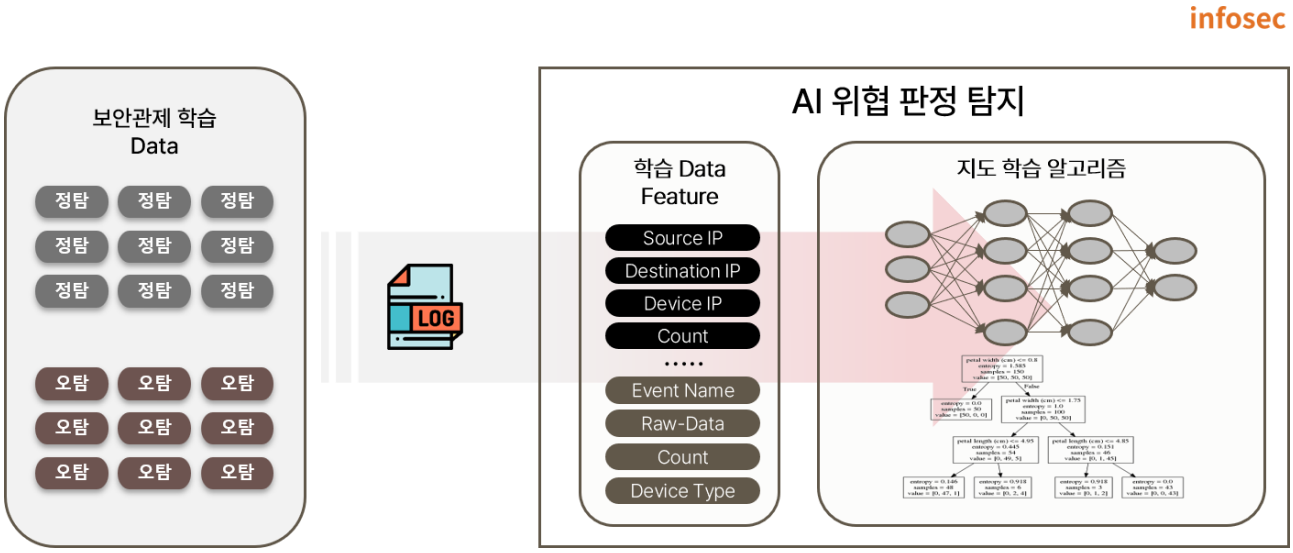



그림 5. 데이터 학습을 통한 AI 위협 판정 탐지

- AI 학습을 위한 Data 를 확보하는 게 가장 중요하다. 정확한 정·오탐 판정 결과 Data 를 확보해 학습을 진행한다.
- 과대적합[1], 과소적합[2]이 발생되지 않도록 다양한 Data 에 대한 학습을 진행한다.
- Training Data 와 TEST Data 의 준비
  - Training Data 와 TEST Data 는 동일한 비율의 정·오탐 분포를 가져야 한다.
  - Training Data 와 TEST Data 는 중복되는 데이터가 없어야 한다.

지금까지 앞에서 언급한 보안관제의 한계와 AI 를 통해 이를 해결할 수 있는 방안에 대해 살펴봤다. 위협을 탐지하는 관점에서 살펴본 것으로 실제 보안관제는 탐지 이후에 **위협 분석, 긴급 대응, 결과 보고 등의 업무**가 진행된다. 특히, 최근 주목받고 있는 생성형 AI 가 많은 도움이 될 것으로 기대한다.

[1] 과대적합: 지나치게 학습 데이터에 최적화되어, 새로운 데이터에 대한 판단을 하지 못하는 현상

[2] 과소적합: 학습이 부족하여 데이터의 구조/패턴을 반영하지 못하는 현상

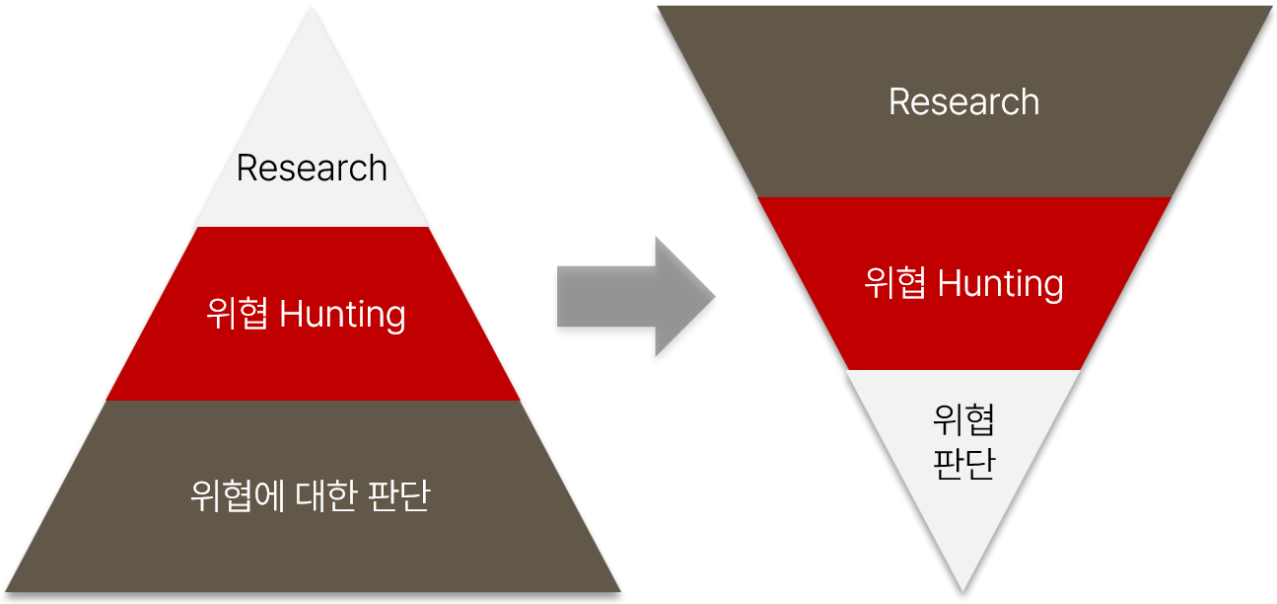
생성형 AI 는 자연어를 인식해 다양한 행위를 할 수 있다. 분석 과정에서는 다양한 조회, 검증을 위한 코드 작성 등을 수행할 수 있고, 대응 과정에서는 SOAR 와 연계해 실시간 위협 대응 조치 수행, 대응 전략 수립 및 위협도를 평가할 수 있다. 또, Chat 을 통한 고객 소통 및 문의 대응과 결과 보고를 위한 보고서 작성 등을 수행할 수 있을 것으로 기대하고 있다.


그림 6. 보안관제에서의 AI 활용

SK 쉴더스 Secudium 센터는 과탐 및 오탐 최소화를 위한 목적으로 AI 를 개발한 뒤 '22.06 이후 플랫폼에 적용해 운영 중이다. 전체 탐지 위협 중 47%를 AI 를 활용해 자동으로 업무를 수행하고 있으며, 이를 위해 7,800 만 건의 Data 가 학습에 사용됐다.

## ■ 맺음말

infosec




지금까지 보안관제 업무의 어려움과 AI 기반 보안관제의 고도화 전략 및 발전 방향에 대해 알아봤다. AI 를 보안관제에 적용 시 '효율화'를 가장 먼저 떠올릴 수 있다. AI 를 활용하는 만큼 관제센터의 인력과 비용을 줄이는 게 가능해질 것이라는 기대감 때문이다.

하지만, AI 는 관제사의 업무 수행을 돕는 보조적인 도구다. AI 를 활용하더라도 최종 결정은 관제사가 수행해야 한다. 현재 관제사는 반복적인 '위협 정·오탐 판단' 업무를 가장 많이 수행하고 있다. 이와 같이 반복적이고 단순한 업무는 이제 AI 에게 맡기고, 관제사는 고도화된 위협을 분석하기 위한 Threat Hunting 과 셀 수 없이 쏟아지는 최신 위협에 대한 연구를 진행해야 한다. 이를 통해 보안관제의 level 을 한단계 끌어올리고 안전한 사이버 세상이 될 수 있도록 노력해야 될 것이다.

국내 정보보안 1 위 기업인 SK 쉴더스는 기업의 비즈니스 환경을 24 시간 365 일 안전하게 보호하고 있는 정보보안관제 서비스를 제공하고 있다. 원격 보안관제 서비스를 통해 다양한 보안 시스템에서 발생하는 로그와 이벤트를 수집해 지능화된 사이버 위협을 탐지/대응하고 있다.

특히, 자체 보유한 글로벌 수준의 보안관제센터 Secudium 센터를 통해 기업의 보안 솔루션 및 시스템 설치/연동에서부터 침해 예방 활동, 모니터링 및 분석, 대응, 보고 등 종합적인 보안관제 서비스를 원격으로 제공한다. SK 쉴더스 보안관제를 도입하면 별도의 전문인력이나 시스템 구축 등 번거로운 절차 없이 합리적인 비용으로 쉽고 빠르게 사이버 위협에 대응할 수 있다.

SK 쉴더스는 업계 최다 전문 보안관제 및 침해사고 대응 인력을 보유하고 있다. 또한, 보안관제 프레임워크와 검증된 자체 보안관제 방법론 ISMM 을 보유하고 있다. 보안관제와 관련한 자세한 내용은 SK 쉴더스 홈페이지에서 확인할 수 있다.

# Keep up with Ransomware

## 늘고 있는 Play 랜섬웨어 공격 위협

### ■ 개요

2024 년 3 월 랜섬웨어 공격으로 인한 피해 사례 발생 건수는 전월(418 건) 대비 약 3% 감소한 405 건으로 나타났다. LockBit 랜섬웨어 그룹은 인프라 압수 후 복귀해서 폭발적인 공격력을 드러냈으나 3 월에는 다소 주춤한 모습을 보이고 있다. 한편, BlackCat(Alphv) 랜섬웨어 그룹은 활동을 잠정 중단하고 엑시트 스캠(Exit scam)[3]으로 추측되는 여러 정황이 포착되기도 했다. 즉, 3 월 랜섬웨어 공격 피해 사례 발생 건수가 전월 대비 소폭 감소한 데에는 LockBit 랜섬웨어 그룹과 BlackCat(Alphv) 랜섬웨어 그룹의 활동이 줄어든 상황이 영향을 미친 것으로 풀이된다.

'notchy' 계열사로 추정되는 사용자가 BlackCat(Alphv)으로부터 수수료를 받지 못했다고 주장하는 글을 러시아 해킹 포럼 램프(RAMP)에 게시한 게 이슈가 되기도 했다. 헬스케어(Healthcare) 기업을 공격하고 약 350BTC(한화 약 352 억 원)를 받았으나 BlackCat(Alphv) 그룹의 운영진은 해당 가상 화폐를 모두 다른 주소로 옮기고 수수료를 계열사에 지불하지 않았다는 것이다. 게시글이 업로드 된 이튿날 다크웹 데이터 유출 사이트의 화면은 국제 수사기관에 의해 폐쇄된 것으로 변경됐다. 그러나 해당 웹 사이트는 수사기관이 아닌 BlackCat(Alphv) 그룹에 의해 변경된 것으로 확인됐다. 또, BlackCat(Alphv) 그룹은 연락 수단 중 하나인 Tox 메신저의 상태 메시지를 'GG', 'Selling source code 5kk'로 변경하는 등 수상한 움직임을 보였다. 이는 전형적인 엑시트 스캠의 정황으로, 이후 다크웹 사이트와 포럼 등에서도 종적을 감추며 사실상 운영을 중단한 것으로 추측된다.

반면 Play, Medusa, RansomHub 그룹은 지난 2 월 대비 피해를 게시하는 글을 늘리며, 타 랜섬웨어 그룹에 비해 왕성한 모습을 보였다. 먼저, Play 랜섬웨어 그룹은 IT 서비스 업체 Xplain 을 공격해 스위스 정부와 관련된 약 6 만 5 천 건의 문서를 탈취한 이력이 있다.

[3] 엑시트 스캠(Exit scam): 계열사에게 수수료를 지급하지 않거나 랜섬웨어 피해자에게 돈을 지불받고 파일 복구를 해주지 않은 채 사라지는 사기 행위

해당 사건은 지난해 5 월 발생했으나 관련 조사는 지난달 마무리되었으며, 약 10 개월이라는 상당한 시간과 자원이 소모되었다. 해당 사건은 랜섬웨어 공격으로 인한 피해가 단발성으로 끝나지 않는다는 교훈을 안고 있다.

또한, Play 랜섬웨어 그룹이 커넥트와이즈(ConnectWise)의 스크린커넥트(ScreenConnect) 취약점 CVE-2024-1708[4], CVE-2024-1709[5]를 악용한 공격을 시도한 정황이 확인되기도 했다. 해당 취약점은 LockBit, BlackCat(Alphv), BlackBasta, Bloody 그룹 등 최근 다양한 랜섬웨어 그룹에서도 활발하게 악용 중인 공격 방식이다. 구체적으로 1-day 취약점[6]을 악용한 랜섬웨어 공격을 수행한다. 이는 비교적 쉽게 공격 대상을 지정 후 침투하기 용이하다. 공격 대상은 Shodan, Censys 등 인터넷에서 액세스할 수 있는 장치를 검색, 모니터링 및 분석하는 데 도움이 되는 플랫폼을 악용해 취약점이 존재하는 서버를 선별해 정한다.

이외에도 젯브레인(JetBrains)의 팀시티(Teamcity)에서 발견된 CVE-2024-27198 인증 우회 취약점과 CVE-2024-27199 디렉토리 순회 취약점을 악용한 사례도 있었다. BianLian 그룹과 오픈소스로 제작된 Jasmin 랜섬웨어가 이를 악용해 데이터 탈취 및 파일 암호화를 수행한 것이다. 해당 취약점을 통해서 랜섬웨어 뿐만 아니라 암호화폐 채굴기 악성코드인 XMRig, 침투 테스트 도구인 Cobalt Strike, 백도어 악성코드 SparkRAT 등을 유포해 악의적인 작업을 수행할 수 있는 것으로 확인됐다.

앞서 언급된 ScreenConnect 와 Teamcity 취약점 모두 CVSS[7] 점수가 9.8(CVE-2024-27198), 7.3(CVE-2024-27199), 8.4(CVE-2024-1708), 10.0(CVE-2024-1709)으로 상당히 높은 위협을 나타내고 있다. 또한, 노출되어 있는 서버 대부분이 취약점이 패치되지 않은 채 운용되고 있어 여전히 해당 모듈과 서버를 운영하고 있을 경우 빠른 조치가 필요하다.

마지막으로, MS-SQL 데이터베이스 서버 취약점을 통해 유포되는 Mallox(Fargo) 랜섬웨어를 복호화 할 수 있는 툴이 공개됐다. 비록 최신버전을 제외한 2022 년 10 월부터 2024 년 2 월까지 유포된 Mallox 랜섬웨어 변종만 지원하나, 많은 버전을 지원하는 만큼 피해를 경감시킬 수 있을 것으로 보인다.

---

[4] CVE-2024-1708: ConnectWise 의 ScreenConnect 에서 발생하는 디렉토리 순회 취약점

[5] CVE-2024-1709: ConnectWise 의 ScreenConnect 에서 발생하는 인증 우회 취약점

[6] 1-day 취약점: 발견된 취약점에 대하여 패치가 발표되었지만, 아직 적용되지 않은 취약점

[7] CVSS (Common Vulnerability Scoring System): 사이버 보안에 미치는 취약점의 위험성을 나타내는 수치

## ■ 랜섬웨어 뉴스

infosec

### BlackCat(Alphv), Exit Scam 정황 포착

- 3월 3일, RAMP 포럼에 계열사 유저가 BlackCat(Alphv)으로 부터 수수료를 받지 못했다는 글 게시
- 2월 21일 발생한 HealthCare 기업 공격과 관련. 이를 통해 BlackCat(Alphv)이 받은 수익은 350BTC
- BlackCat(Alphv)은 수수료를 지불하지 않고 350BTC 모두 8개의 다른 주소로 전송
- BlackCat(Alphv) Tox 메신저 상태 메시지 변경 (GG → Selling source code 5kk)
- 다크웹 유출 사이트를 국제 수사 기관에 의해 폐쇄된 것처럼 FAKE 페이지 게시
- 다크웹 포럼에서도 모습을 감추며 사실상 운영 중단한 것으로 추정

### JetBrains 社 TeamCity 취약점을 악용하는 랜섬웨어 그룹

- 인증 우회 취약점인 CVE-2024-27198과 디렉토리 순회 취약점인 CVE-2024-27199가 해당
- URL 조작을 통해서 TeamCity 엔드포인트에 접근이 가능하며, 이를 통해서 관리자 생성이 가능
- 3월 4일 취약점 완전 공개와 패치가 동시에 이루어 지면서 공격에 악용될 가능성 발생
- BianLian 그룹과 오픈소스로 제작된 Jasmin 랜섬웨어가 공격에 활용한 정황 포착
- 랜섬웨어 그룹 뿐만 아니라 채굴 악성코드와 백도어 등 다양한 악성코드 공격에 활용

### Play, IT 서비스 업체 통해 스위스 연방 정부 데이터 유출

- 2023년 5월 발생한 공격으로, 같은 해 8월부터 행정 조사를 실시하여 2024년 3월까지 조사 진행
- 약 6만 5천건의 스위스 연방 정부 데이터가 유출되어 다크웹에 게시

### aiohttp Python 라이브러리, 랜섬웨어 공격에 활용 의심

- aiohttp는 Python의 비동기 http 클라이언트/서버 프레임워크로, 디렉토리 순회 취약점인 CVE-2024-23334 발견
- 랜섬웨어 공격자 ShadowSyndicate가 2월부터 3월까지 해당 취약점에 취약한 서버를 스캔한 정황 발견
- 1월 28일 3.9.2 버전 출시로 패치 완료 및 2월 27일 GitHub*에 POC 익스플로잇 코드*공개

* GitHub : 웹 기반 소스코드 버전 관리 및 협업 플랫폼
* PoC (Proof of Concept) 익스플로잇 코드 : 취약점을 이용한 공격이 가능함을 보여주는 시현 소스코드

### Mallox 랜섬웨어 복호화 도구 업데이트

- 키 생성을 통해서 복구하는 방식으로, 2022년 10월부터 2024년 2월까지의 변종 복호화 가능
- Mallox 그룹은 최신 변종에 대해서도 복호화 도구를 만들어보라는 포럼 글 게시

## 복호화 키를 포함한 CryptoWire 유포

- 2018년 유행하던 오픈 소스 기반 랜섬웨어로, 주로 피싱 메일을 통해 유포
- Autoit 스크립트로 제작되었으며, 스크립트에 복호화 키가 포함되어 있거나 복호화 키를 공격자 서버로 전송

## Qillin, 영국 출판 및 사회적 기업 Big Issue 공격

- 인사 정보, 계약서 및 파트너 데이터, 재무제표 및 투자 정보 등 550GB의 데이터 탈취 주장
- Big Issue는 공격 인지 이후, 시스템 액세스를 제한하는 등 즉각적으로 조치 및 시스템 복구 진행
- 잡지 발행 및 배포에는 영향이 없다고 발표

## Rust 버전 Qillin 랜섬웨어 변종 발견

- PowerShell Script를 활용하여 Rust 변종을 VMware vCenter* 및 ESXi 서버에 유포
- RMM 도구 및 Cobalt Strike, PsExec, SecureShell, SYS 드라이버 등 다양한 도구 및 시스템 활용

* VMware vCenter : 다수의 ESXi 및 가상 시스템을 중앙 집중 관리하여 모니터링 기능을 제공하는 서비스

## KillSec 랜섬웨어 그룹 다크웹 유출 사이트 신규 개설

- 2023년 10월부터 텔레그램 채널 통해서 활동하던 랜섬웨어 그룹으로, 같은 해 11월 루마니아 경찰 공격 이력존재
- 2024년 3월, 다크웹 유출 사이트를 개설하여 피해자를 게시하기 시작

## BlackByte와 RA Group 랜섬웨어 그룹 활동 재개

- BlackByte, 5개월 만에 다크웹 유물 사이트(DLS) 개편과 함께 신규 유출 1건 게시하며 활동 재개
- RA Group, RA World로 그룹명 변경 및 3개월 만에 유출 7건 게시하며 활동 재개

## DarkRace 계열의 신규 랜섬웨어, Donex 등장

- DarkRace 랜섬웨어는 유출된 LockBit 빌더를 기반으로 개발
- 5월에 발견된 DarkRace 계열의 랜섬웨어를 사용하며, 신규 유출 5건 게시

## Medusa, US #1364 Federal Credit Union 공격

- 미국의 금융 기관으로 대출, 투자, 저축, 카드 등 다양한 금융 서비스 제공
- 2월 21일 발생한 서비스 이용 장애와 연관된 것으로 추정
- 3월 7일 다크웹 유출 사이트에 게시

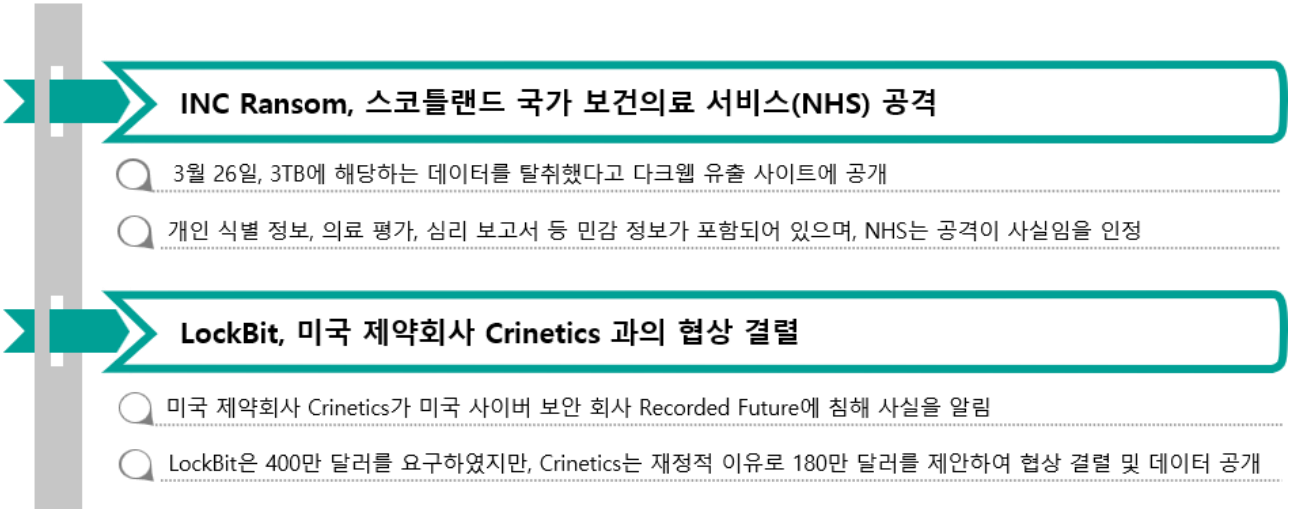

INC Ransom, 스코틀랜드 국가 보건의료 서비스(NHS) 공격
3월 26일, 3TB에 해당하는 데이터를 탈취했다고 다크웹 유출 사이트에 공개
개인 식별 정보, 의료 평가, 심리 보고서 등 민감 정보가 포함되어 있으며, NHS는 공격이 사실임을 인정
LockBit, 미국 제약회사 Crinetics 과의 협상 결렬
미국 제약회사 Crinetics가 미국 사이버 보안 회사 Recorded Future에 침해 사실을 알림
LockBit은 400만 달러를 요구하였지만, Crinetics는 재정적 이유로 180만 달러를 제안하여 협상 결렬 및 데이터 공개

그림 1. 랜섬웨어 동향

## ■ 랜섬웨어 위협

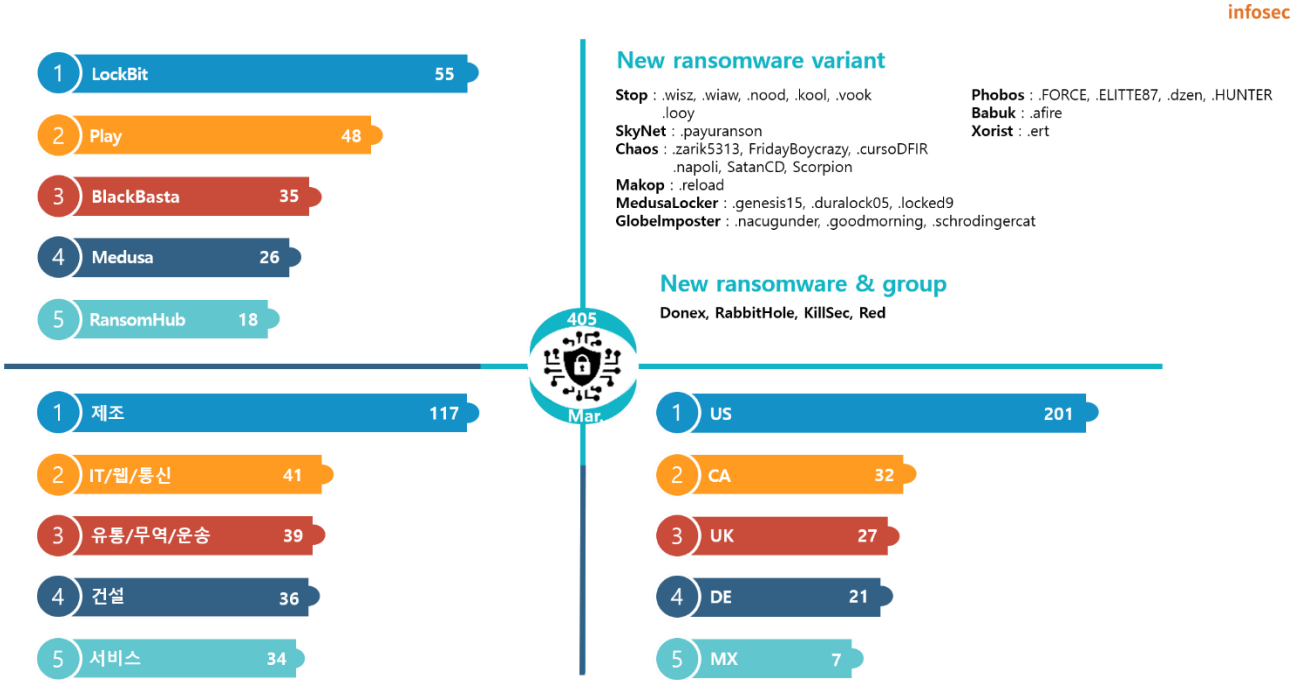



그림 2. 2024 년 3 월 랜섬웨어 위협 현황

### 새로운 위협

3 월에는 활동을 재개하는 그룹이 다수 발견됐다. 악명 높은 해킹 범죄 포럼인 브리치포럼(BreachForums)에서 활동하던 판매자 인텔브로커(IntelBroker)는 3 월에 계정을 복구하여 활동을 이어 나갔으며, BlackByte 랜섬웨어 그룹은 약 5 개월만에 데이터 유출 사이트를 개편하며 신규 유출 데이터를 게시했다. 마지막으로 라그룹(RA Group)은 2023 년 12 월 이후 3 개월만에 라월드(RA World)라는 이름으로 7 건의 데이터를 게시하며 활동을 재개했다.

Donex 그룹은 2023 년 5 월에 발견된 DarkRace 계열의 랜섬웨어를 사용하고 있으며, 현재까지 5 개의 조직에 대한 데이터를 유출시켰다. DarkRace 랜섬웨어는 유출된 LockBit 빌더의 코드를 기반으로 랜섬노트 형태, 파일 아이콘 변경, 변경되는 확장자 등 LockBit 랜섬웨어의 기술을 통합해 개발한 것으로 분석된다.

Rabbit Hole 그룹은 다크웹 데이터 유출 사이트가 발견됐다. 다만, 아직 어떠한 피해도 게시하지 않고 있어 인프라 구축 또는 공격을 준비하고 있는 것으로 보인다. KillSec 그룹은 2023 년 10 월부터 텔레그램을 통해 활동을 시작한 것으로 보이며, 최근 다크웹에 데이터 유출 사이트를 개설해 피해자를 게시하기 시작했다. 텔레그램의 유출 이력을 살펴보면 2023 년 11 월 루마니아 경찰 20 만 건의 데이터를 게시해 1,500 유로(한화 약 220 만 원)를 지불했다고 주장하고 있지만 사실 여부가 확인되지는 않은 상태다.

Red 그룹은 등장과 함께 총 12 건의 피해 유출을 게시했다. 발견 초기에는 유출 데이터의 모든 샘플 파일 다운로드 링크가 정상적으로 작동하지 않거나 일부 유출 대상이 이미 영업 정지된 곳을 나타내며 Scam 의혹이 존재했다. 하지만 4 월 1 일을 기준으로 모든 다운로드 링크가 정상적으로 작동하는 것이 확인되면서 이들이 Scam 그룹인지 여부는 더 지켜봐야 할 것으로 보인다.

Top5 랜섬웨어

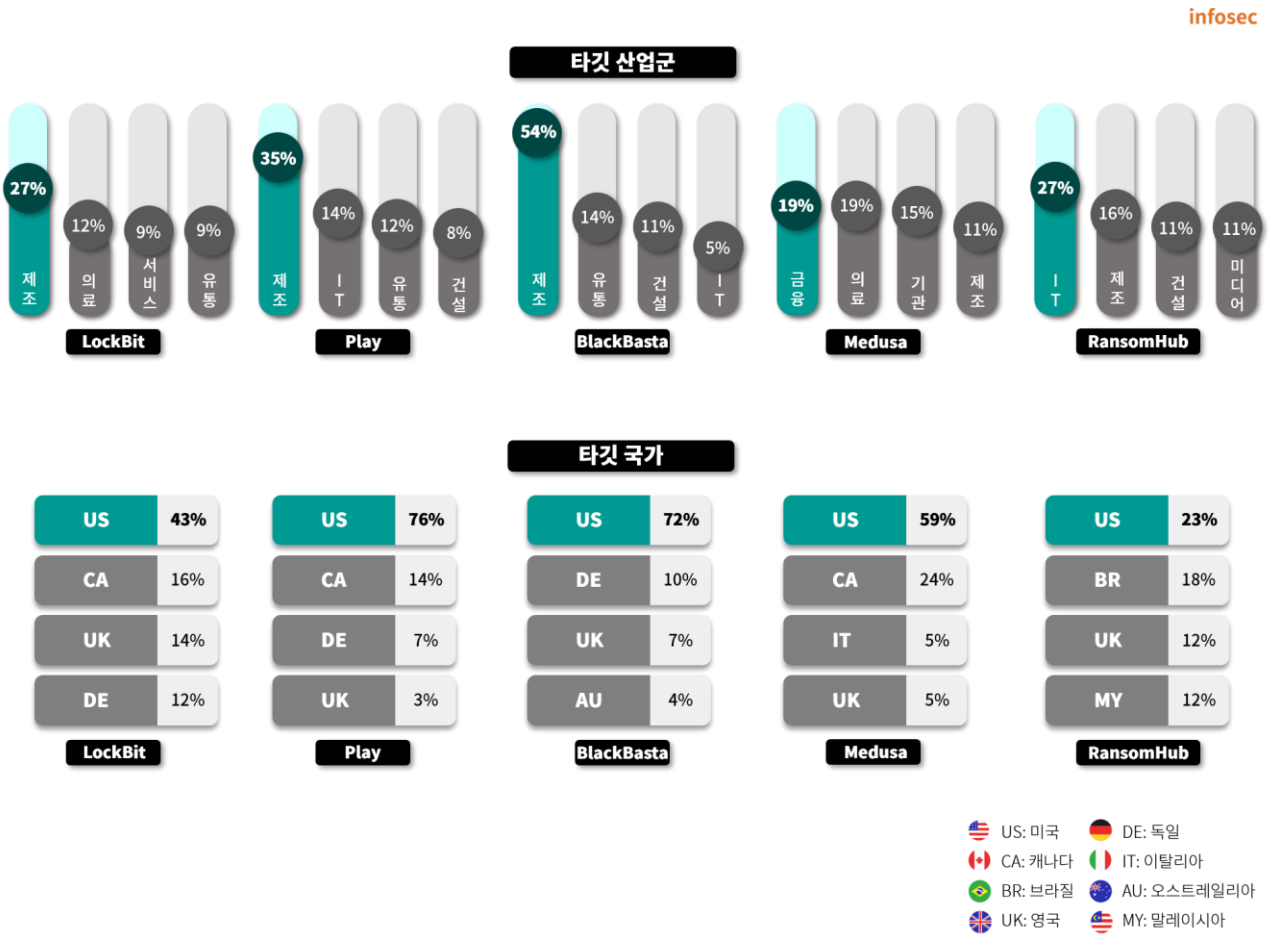



그림 3. 산업/국가별 주요 랜섬웨어 공격 현황

LockBit 랜섬웨어 그룹은 활동을 재개한 이후, 활발한 공격을 수행하며 가장 많은 피해자를 양산하고 있다. 이 가운데 '금전적인 부분을 타협하지 않는' 독특한 전략을 사용하고 있는 모습이 포착됐다.

지난 3 월 18 일 미국의 스타트업 제약 회사인 크리네틱스(Crinetics)를 다크웹 데이터 유출 사이트에 게시했다. 공개된 내용은 Crinetics 가 비밀 유지를 위반하고 미국 보안 회사인 레코디드 퓨쳐(Recorded Future)에 침해 사실을 공유했다는 것이다. 또한, LockBit 랜섬웨어 그룹은 Crinetics 에게 400 만 달러(한화 약 55 억 원)를 지불하지 않으면 데이터를 공개하겠다고 통보했으나, Crinetics 는 재정상황의 이유로 180 만 달러(한화 약 25 억 원)를 제시했다고 밝혔다. 결국 LockBit 은 이를 받아들이지 않고 데이터 공개를 통보하고 대화를 종료했다. 이러한 행보는 다른 기업들에게 협상 금액을 타협하지 않는다는 경고성 메시지를 보낸 것으로 풀이된다.

Play 랜섬웨어 그룹은 2022 년부터 꾸준하게 활동을 이어왔다. 올해 초 잠시 주춤하는 모습을 보였지만, 근래 다시 공격 사례가 증가하고 있다. 최근 랜섬웨어 트렌드와 일치하는 취약점을 악용한 공격을 수행하고 있지만, RaaS[8] 운영이 다수를 차지하는 다른 그룹과는 달리 서비스형 랜섬웨어 운영을 하지 않는 폐쇄적인 그룹으로 알려져 있다.

BlackCat(Alphv) 랜섬웨어 그룹의 활동 중단과 강세를 보였던 다른 랜섬웨어 그룹이 주춤하는 사이, Medusa, BlackBasta, RansomHub 그룹은 많은 랜섬웨어 공격을 수행하며 Top5 랜섬웨어로 급부상했다. BlackBasta 그룹은 지난 1 월 다크웹 유출 사이트가 약 10 일 동안 오프라인으로 변경되며 활동이 주춤한 모습을 보였지만, 최근 지속적으로 악용되고 있는 ScreenConnect 취약점 공격 수행 정황이 발견되면서 꾸준히 피해자를 게시하고 있는 것으로 파악된다.

Medusa 랜섬웨어 그룹은 최근 텍사스 정부 기관인 Tarrant Appraisal District(TAD)를 공격해 70 만 달러(한화 약 9 억 6000 만 원)의 몸값을 요구했지만 협상에 실패한 것으로 보인다. 또, 금융 기관인 US #1364 Federal Credit Union 을 공격해 서비스 장애를 일으킨 바 있다.

RansomHub 그룹은 CIS[9], 쿠바, 북한, 중국, 루마니아 국가 및 비영리단체에 대한 공격을 시도하지 않겠다고 밝혔다. 다만, 다크웹 유출 사이트에 공개된 내용에 따르면 공격 제외 대상에서 루마니아가 빠져 있는 모습을 확인할 수 있다. 또한, 랜섬웨어에 재감염 되지 않도록 규칙을 설정했다. 이와 함께 RaaS 제휴 프로그램을 러시아 해킹 포럼인 RAMP 에 게시하며 홍보를 진행하고 있다. 해당 랜섬웨어는 x25519 알고리즘을 사용해 대칭키를 보호하고 하드웨어에 따라 AES256, chach20, xchacha20 대칭키 알고리즘으로 파일을 암호화하여 빠른 암호화 속도를 지원한다. Go 언어[10] 기반으로 작성되어 윈도우, 리눅스, ESXi[11], ARM/MIPS[12] 등 다양한 플랫폼을 지원하며, 계열사의 가상화폐 지갑을 협상에 사용해 지불이 확인되면 10%의 수수료만 제공하는 전략을 사용한다. 이는, BlackCat(Alphv) 그룹의 Exit scam 에 따라 금전적 손실을 입을 수 있는 상황을 방지하기 위한 전략으로 보인다.

---

[8] RaaS (Ransomware-as-a-Service): 랜섬웨어 그룹들이 계열사나 공격자에게 대가를 받고 랜섬웨어를 제공해주는 형태

[9] CIS (Commonwealth of Independent States): 소련의 해체로 독립한 국가들의 국제기구. 러시아, 몰도바, 벨라루스, 우즈베키스탄, 카자흐스탄 등이 포함됨

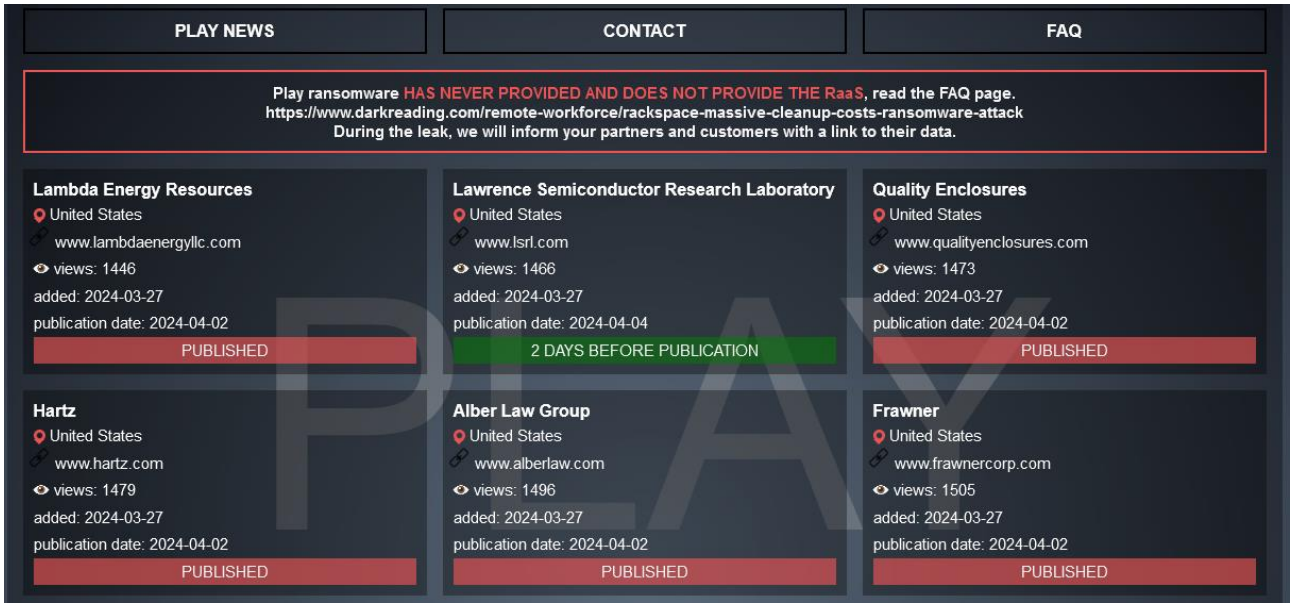
[10] Go 언어: Google 에서 생산성을 높이기 위해 개발한 오픈소스 프로그래밍 언어

[11] ESXi: VM 웨어에서 개발한 호스트 컴퓨터에서 다수의 운영체제를 동시에 실행시킬 수 있는 UNIX 기반 논리적 플랫폼

[12] ARM/MIPS: CPU 아키텍처의 한 종류. ARM 은 주로 Mac 이나 모바일에서 사용되며 MIPS 는 주로 임베디드 시스템에 사용됨

## ■ 랜섬웨어 집중 포커스

Play 랜섬웨어 개요




출처: Play 랜섬웨어 그룹 데이터 유출 사이트

Play 랜섬웨어 그룹은 2022 년 6 월부터 활동을 시작했으며 현재까지 약 410 여 건의 피해자를 다크웹 데이터 유출 사이트에 게시했다. 특히, Play 그룹은 일정 주기마다 다수의 피해자를 동시에 게시하는 특성을 보이고 있는데, 이번 3 월에만 48 건의 피해자를 게시했다. 다소 활동이 주춤했던 1 월 이후 꾸준히 공격 사례가 증가하고 있어 주의가 필요하다.

최근 다수의 랜섬웨어 공격에서 동일한 전략을 사용한 정황이 확인되며 Play 그룹이 RaaS 를 제공한다는 보고서가 공개됐다. 그러나 Play 그룹은 타 랜섬웨어 그룹들과 달리 RaaS 를 제공하지 않는다고 다크웹 유출 사이트에 밝혔다. Play 그룹의 발표를 100% 확신할 수는 없다. 이들이 RaaS 를 제공하지 않는다고 밝힌 이유는 실제로 서비스를 하고 있지 않거나 수사망을 좁히지 못하도록 하는 전략 등으로 볼 수 있다.

Play 랜섬웨어는 Hive, Nokoyawa 랜섬웨어와 상당히 유사한 전략을 구사한다. ▲권한 상승을 위한 Nekto, PriviCMD, WinPEAS ▲Cobalt Strike 를 통한 공격 도구 다운로드 ▲원격 제어가 가능한 Coroxy, SystemBC 악성코드 사용 ▲원격으로 프로그램을 실행할 수 있게 도와주는 도구인 PsExec 등을 사용해 이미 일부 연관성이 확인된 바 있다. 이외에도 독자적으로 개발한 Grixba 데이터 탈취 도구를 사용하거나 네트워크 상의 액티브 디렉터리 정보를 수집해 주는 도구인 AdFind 를 사용하는 등 차별화된 전략도 펼치고 있다.

Play 그룹은 다크웹 유출 사이트에 유출된 자료를 게시할 때 '?' 문자를 사용해 이름을 숨겨 일정 기간 피해자를 특정하지 못하도록 보호하는 전략도 사용하고 있다. 이 경우 피해 사실을 알리지 않고 조용히 금전적 이득을 취할 수 있다. 다만, 이 전략은 모든 피해자가 아닌 협상의 여지가 있는 기업에 한해서만 사용하는 것으로 보인다.

분석결과, Play 랜섬웨어의 침투방식은 노출된 RDP[13] 서버, 탈취한 계정 사용, Fortinet VPN[14] 서버 취약점(CVE-2018-13379 [15] , CVE-2020-12812 [16] ), MS Exchange Server [17] ProxyNotShell 취약점(CVE-2022-41040[18], CVE-2022-41082[19]), ConnectWise 의 ScreenConnect 취약점 CVE-2024-1708, CVE-2024-1709 등을 사용하는 것으로 밝혀졌다. 또한, 침투와 랜섬웨어 공격이 탐지되지 않도록 하는 회피 전략 중 하나인 RMM[20] 도구를 주로 악용하는 것으로 발견됐다. 해당 전략은 Play 뿐 아니라 다수의 랜섬웨어 그룹에서도 사용 중이다.

[13] RDP (Remote Desktop Protocol): 다른 컴퓨터를 원격으로 제어할 수 있도록 해주는 프로토콜

[14] VPN (Virtual Private Network): 인터넷 상에서 개인 정보를 보호하고 지역 제한을 우회하기 위해 사용하는 가상의 보안 네트워크

[15] CVE-2018-13379: FortiOS 시스템 파일을 다운로드할 수 있는 웹 경로 탐색 취약점

[16] CVE-2020-12812: 인증 요소인 FortiToken 입력 메시지가 표시되지 않고 로그인할 수 있는 부적절한 인증 취약점

[17] MS Exchange Server: 마이크로소프트에서 개발한 메시지, 협업 소프트웨어 제품

[18] CVE-2022-41040: 서버 측 요청 위조(SSRF, Server-Side Request Forgery) 공격 취약점

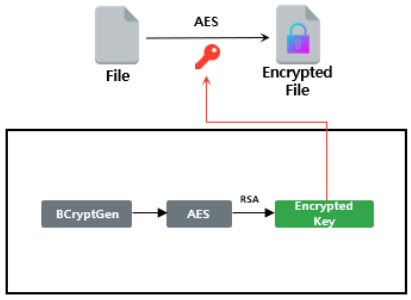
[19] CVE-2022-41082: 원격 코드 실행 취약점

[20] RMM (Remote Monitoring and Management): 원격 모니터링 및 관리를 제공하는 상용 프로그램

## Play Ransomeware

**암호화 키**

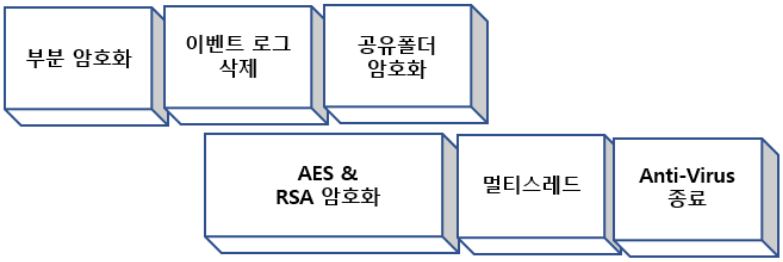
AES 알고리즘으로 파일 암호화를 하고, 해당 키를 RSA로 보호




**암호화 방식**

256MB 이하 : 전체 암호화
256MB 초과 4GB 이하 : 일정 비율마다 1MB씩 부분 암호화, 총 2MB만 암호화
4GB 초과 16GB 이하 : 일정 비율마다 1MB씩 부분 암호화, 총 3MB만 암호화
16GB 초과 : 일정 비율마다 1MB씩 부분 암호화, 총 4MB만 암호화

**특징**




**랜섬노트**


ReadMe.txt

**변경 확장자**

.PLAY

**제작 언어**

C/C++

그림 4. Play 랜섬웨어 개요

Play 랜섬웨어 전략

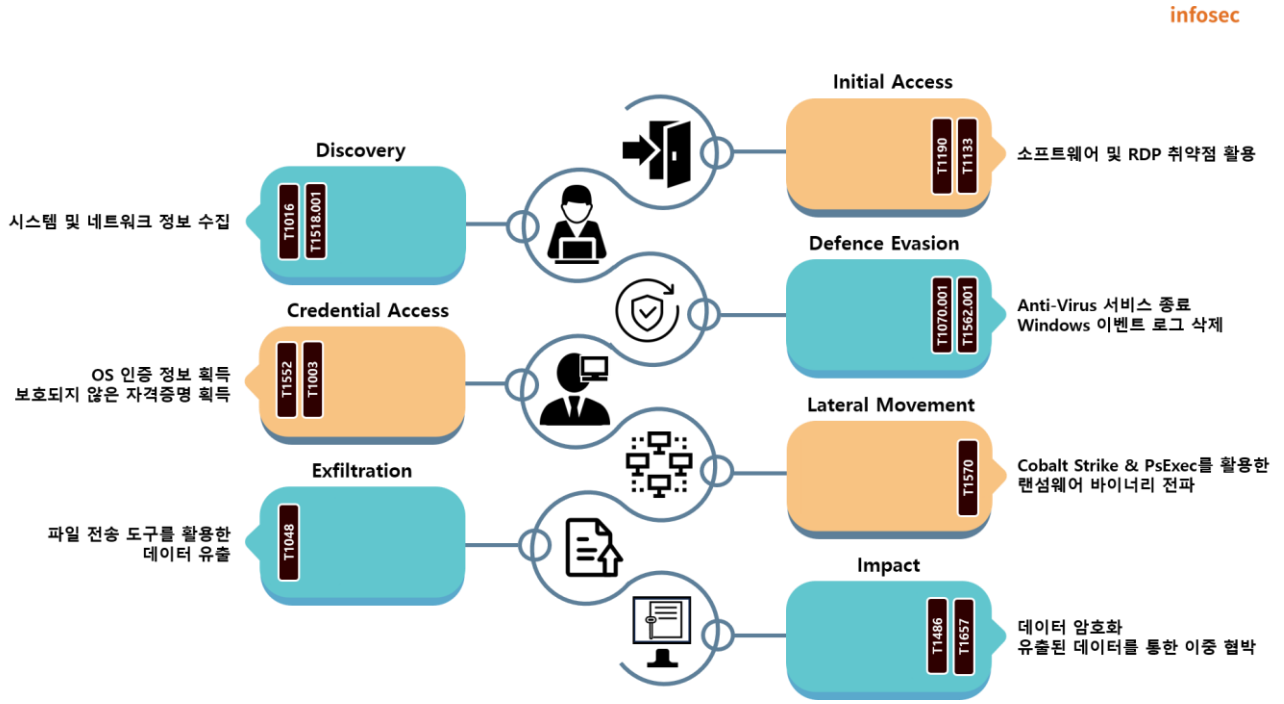



그림 5. Play 랜섬웨어 공격 전략

Play 랜섬웨어는 노출된 원격 데스크톱 프로토콜(RDP)이나 소프트웨어 취약점을 활용해 초기 침투를 시도한다. 포티넷(Fortinet) VPN 서버 취약점, MS Exchange Server ProxyNotShell 취약점, ConnectWise 의 ScreenConnect 취약점 등과 같은 RMM 취약점을 주로 활용했다. 이외에도 탈취한 계정 정보를 활용해 초기 침투를 시도한 이력도 존재한다.

초기 침투에 성공하면 자격 증명 탈취, 시스템 데이터 수집, 내부 전파, 원격 접속, 데이터 유출을 위한 도구들을 다운로드 받아 사용한다. 권한 상승을 위해 ▲Nekto ▲PriviCMD ▲WinPEAS 를 사용하며, 내부 전파를 위해 Cobalt Strike 와 PsExec 를 다운로드 한다. 또한 데이터 유출을 위해 자체 개발한 데이터 탈취 도구 Grixba 를 사용하거나, 압축 도구 WinRAR 과 파일 전송 프로그램 WinSCP 등 다양한 도구를 활용한다.

이처럼 Play 랜섬웨어는 다양한 도구를 활용하기 때문에 랜섬웨어 파일 자체에는 파일 암호화와 랜섬노트 생성 기능만 존재한다. 대신 랜섬웨어 파일의 분석을 어렵게 하기 위해 문자열을 난독화해 저장하고 프로그램 실행 흐름과 전혀 상관없는 가비지 코드를 사용하는 방식을 보이고 있다. 또한 프로그램 실행에 필요한 API 를 동적으로 불러오며, 해시 알고리즘 중 하나인 xxHash32 를 통해서 API 의 주소를 확인하는 방식도 사용한다.

파일 암호화는 대상 PC 의 드라이브뿐만 아니라 공유 폴더도 암호화한다. 파일마다 랜덤하게 생성된 AES 키를 통해서 파일을 암호화하며, 암호화에 사용된 키는 RSA 를 통해서 보호해 파일의 끝에 추가한다. Play 랜섬웨어는 빠른 암호화를 위해서 멀티스레드 방식과 부분 암호화 방식을 사용한다. 파일의 크기가 256MB 이하인 경우 파일 전체를 암호화하지만, 256MB 를 초과하면 파일의 일정 비율마다 1MB 씩만 암호화한다.


그림 6. Play 랜섬웨어 부분 암호화 방식

Play 랜섬웨어는 암호화를 위해서 파일을 1MB 크기의 Chunk 로 구분하며, 크기가 큰 파일의 경우 파일의 전체 Chunk 중에서 극히 일부 Chunk 만 암호화한다.

256MB 초과 4GB 이하의 파일은 첫번째와 마지막 Chunk 만 암호화하며, 4GB 초과 16GB 이하의 파일은 첫번째와 마지막 Chunk 뿐만 아니라 전체 Chunk 중 1/2 지점에 위치한 Chunk 까지 암호화한다. 마지막으로 16GB 보다 큰 파일은 첫번째와 마지막 Chunk 를 암호화하며, 1/3 지점과 2/3 지점에 위치한 Chunk 도 암호화한다. 만약 6,000 개의 Chunk 로 이루어진 파일이라면 첫번째와 마지막 Chunk 를 암호화하며, 1/2 지점인 3,000 번째 Chunk 또한 암호화한다.

Play 랜섬웨어 대응방안

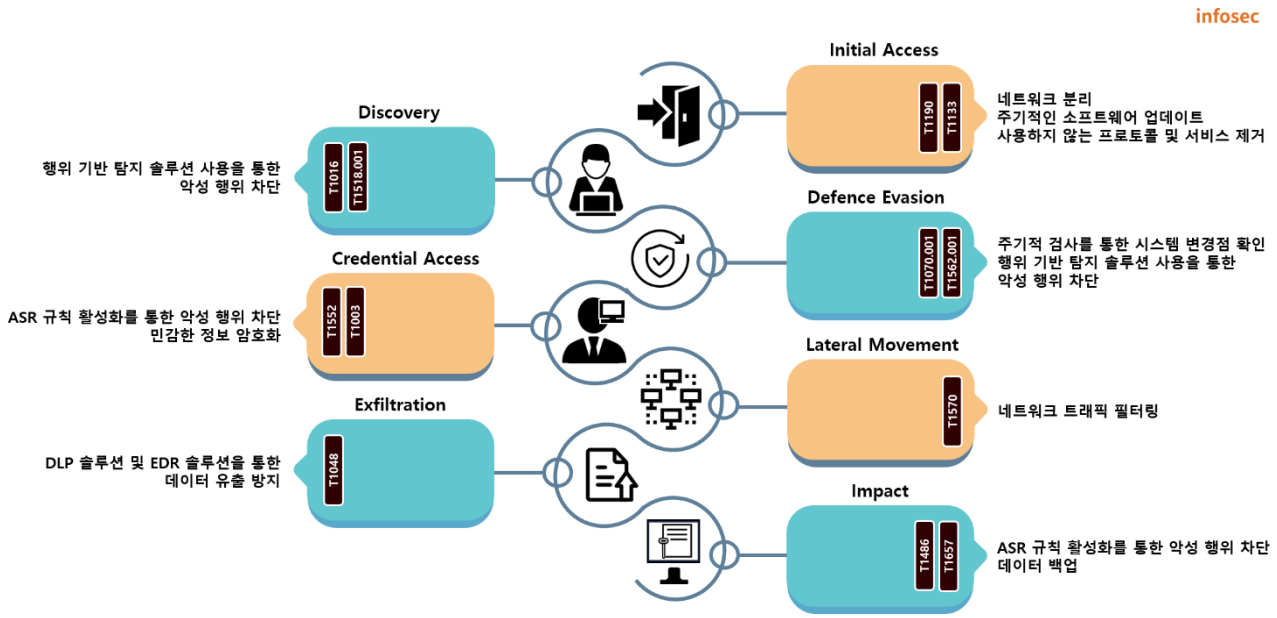



그림 7. Play 랜섬웨어 대응방안

Play 는 주로 소프트웨어의 취약점이나 프로토콜 취약점을 이용해 직접적으로 배포하기 때문에 소프트웨어나 운영체제를 취약하지 않은 버전으로 주기적으로 업데이트 하는 것이 중요하다. 또한, 사용하지 않는 프로토콜과 서비스는 비활성화 하거나 제거해 악용을 방지해야 한다. 이와 함께 네트워크를 세분화하여 분할하거나 가상 사설망을 사용하는 등 네트워크 분리를 통해 피해를 최소화할 수 있다.

다음은 Play 랜섬웨어 그룹에서 악용한 것으로 확인된 취약점이며 영향을 받는 서버 혹은 솔루션을 사용하고 있다면 취약점이 패치된 버전으로 업데이트가 필요하다.

| CVE | 설명 | 영향 버전 | 패치 버전 |
|---|---|---|---|
| CVE-2018-13379 | Fortinet 의 보안 OS FortiOS 에서 SSL VPN 을 사용하는 경우, 시스템 파일을 다운로드 받을 수 있는 파일 경로 탐색 취약점 | 5.4.6 ~ 5.4.12<br>5.6.3 ~ 5.6.7<br>6.0.0 ~ 6.0.4 | 5.6.8 이상<br>6.0.5 이상 |
| CVE-2020-12812 | Fortinet 의 보안 OS FortiOS 에서 SSL VPN 을 사용하는 경우, 이중 인증(2FA)이 제대로 수행되지 않는 부적절한 인증 취약점 | 6.0.9 이하<br>6.2.0 ~ 6.2.3<br>6.4.0 | 6.0.10 이상<br>6.2.4 이상<br>6.4.1 이상 |
| CVE-2022-41040 | MS Exchange Server 에서 발생하는 서버 측 요청 위조(SSRF) 공격 취약점 | 업데이트 이전의 Exchange Server 2013, 2016, | KB5019758 업데이트 |
| CVE-2022-41082 | MS Exchange Server 에서 발생하는 원격 코드 실행 취약점 | 업데이트 이전의 Exchange Server 2013, 2016, | KB5019758 업데이트 |
| CVE-2024-1708 | 원격 데스크톱 솔루션 ScreenConnect 취약점으로, 임의의 파일이나 디렉토리에 접근할 수 있는 경로 탐색 취약점 | 23.9.7 이하 | 23.9.8 이상 |
| CVE-2024-1709 | 원격 데스크톱 솔루션 ScreenConnect 취약점으로, 원격 데스크톱에 시스템 관리자 계정을 생성할 수 있는 인증 우회 취약점 | 23.9.7 이하 | 23.9.8 이상 |

표 1. Play 랜섬웨어가 악용한 소프트웨어 취약점

초기 침투 이후 데이터 수집, 랜섬웨어 배포 등 악성행위를 위해서 Anti-Virus 서비스를 종료시킨다. 또한 OS 인증 정보와 보호되지 않은 각종 자격 증명을 획득하여 공격에 추가적으로 활용한다. 따라서, ASR 규칙 활성화를 통해 악성 행위를 차단하거나 계정 정보와 같이 민감한 정보는 암호화하여 안전하게 보관해야 한다.

코발트 스트라이크(Cobalt Strike)와 PsExec 를 사용해 원격지에 랜섬웨어를 전파하고 실행한다. 따라서 이를 방지하기 위해 네트워크 모니터링 도구를 통해 지속적으로 트래픽 흐름과 액세스를 제어하고, 알 수 없거나 신뢰할 수 없는 출처가 내부 시스템에 접근하는 것을 막는 네트워크 트래픽 필터링을 해야 한다.

데이터 탈취와 파일 암호화에 대해서도 대비가 필요하다. 이는, DLP[21] 솔루션이나 EDR[22] 솔루션을 활용해 데이터 유출을 방지할 수 있다. 데이터 유출 과정에서 정상 도구들을 사용하는 경우도 있어 사전에 인지할 수 있도록 조치가 필요하다.

특히, 대용량 파일일 경우 더욱 주의가 필요하다. 이외에도 파일 복구를 위해 정기적으로 백업을 생성해 관리해야 하며, NAS[23]와 백업 저장소의 데이터를 삭제하는 경우도 존재하므로 별도의 네트워크나 저장소에 데이터를 소산 백업[24]해 관리하는 것을 권장한다. Play 랜섬웨어의 경우, 백업 복사본을 삭제하는 기능이 확인되지 않았기 때문에, 별도의 복원 지점을 생성해 일부 파일을 복구할 수 있다.

[21] DLP (Data Loss Prevention): 데이터의 흐름을 감시하여 중요 정보 유출을 감시/차단하는 데이터 유출 방지 솔루션

[22] EDR (Endpoint Detection and Response): 컴퓨터와 모바일, 서버 등 단말기에서 발생하는 악성 행위를 실시간으로 감지하고 분석 및 대응하여 피해 확산을 막는 솔루션

[23] NAS (Network Attached Storage): 네트워크에 연결되어 여러 사용자가 데이터를 공유하고 접근할 수 있는 저장 장치

[24] 소산 백업: 백업된 데이터를 일정거리 떨어진 장소에 분리 보관하는 방식

## Indicator Of Compromise

**Play : SHA256**

5a0a4e5379e1f0bc9bdd42f5c638c601a0068da4b19b063e5276a01494ae116e
2d01ddc075b48db3ba69b036f9f5977f3607edba5dec6799e4fae7ccd4f1ba75
50d72707eb0a9b7f4ecaa8e0242675e3349b9d67901ac020635ae2ec0eb328e4
64087027f0c727a807c8b6ccf602398adc9d346fe518cbd3b589348702dc39ed

**File Name**

LkToXG.exe
Thimble pulverization
P137.exe

## ■ 참고 사이트


• Symantec 공식 홈페이지(https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy)

• BleepingComputer 공식 홈페이지(https://www.bleepingcomputer.com/news/security/play-ransomware-gang-uses-custom-shadow-volume-copy-data-theft-tool/#google_vignette)

• CISA 보안 권고문(https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a)

• The Register 뉴스레터(https://www.theregister.com/2024/03/08/swiss_government_files_ransomware/)

• SOCRadar 공식 홈페이지(https://socradar.io/dark-web-profile-play-ransomware/)

• Trend Micro 공식 홈페이지(https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play)

• Malwarebytes 공식 홈페이지(https://www.malwarebytes.com/blog/news/2023/12/fbi-issues-advisory-over-play-ransomware)

• CISA 합동 권고문(https://www.cisa.gov/news-events/alerts/2023/12/18/fbi-cisa-and-asds-acsc-release-advisory-play-ransomware)

• DarkReading 뉴스레터(https://www.darkreading.com/cloud-security/-play-ransomware-group-targeting-msps-worldwide-in-new-campaign)

• MS 보안 대응 센터(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082)

• MS 보안 대응 센터 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040)

• NIST 국가 취약점 데이터베이스(https://nvd.nist.gov/vuln/detail/CVE-2018-13379)

• NIST 국가 취약점 데이터베이스(https://nvd.nist.gov/vuln/detail/CVE-2024-12812)

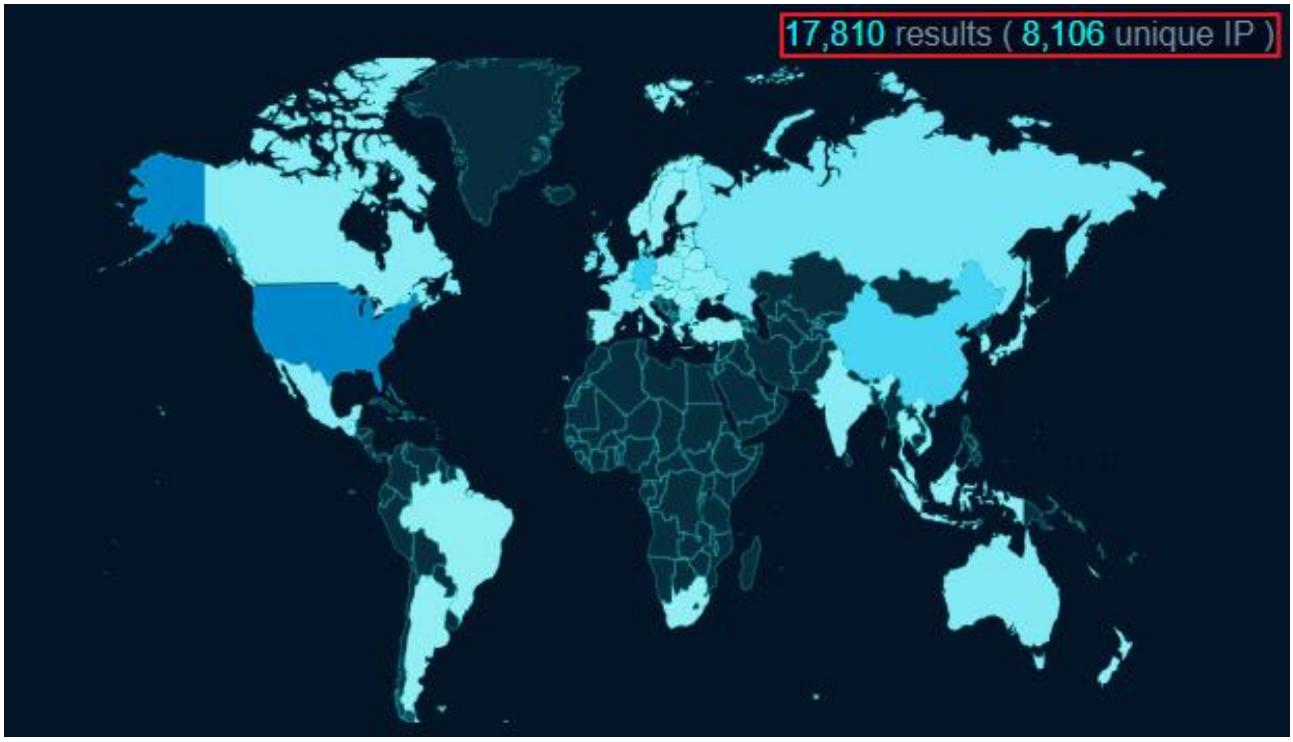
• NIST 국가 취약점 데이터베이스(https://nvd.nist.gov/vuln/detail/CVE-2024-1708)

• NIST 국가 취약점 데이터베이스(https://nvd.nist.gov/vuln/detail/CVE-2024-1709)

# Research & Technique

## Jetbrains TeamCity 인증 우회 취약점(CVE-2024-27198)

### ■ 취약점 개요




출처: fofa.info

그림 1. TeamCity 사용 통계

2024 년 3 월 4 일, 글로벌 CI/CD 소프트웨어인 JetBrains 의 TeamCity 제품에서 인증 우회 취약점(CVE-2024-27198)이 공개됐다. 해당 취약점은 임의의 경로에 접근할 수 있는 특정 파라미터의 안정성 검증 로직이 미흡하여 이를 우회할 수 있기 때문에 발생한다. 공격자는 특정 경로에 비정상적인 접근을 통해 임의의 관리자 계정을 등록하거나 access token 을 발급받을 수 있다.

CVE-2024-27198 로 인하여 인증되지 않은 사용자의 임의 관리자 계정 및 access token 생성이 가능하며, 악성 Plugin 업로드를 통한 원격 코드 실행도 가능하다. 2024 년 3 월 기준 해당 취약점을 이용한 Jasmin 변종 랜섬웨어 유포, XMRig 암호화폐 채굴기 배포, SparkRAT 백도어 배포 등 다양한 공격이 활발하게 이루어지고 있어 각별한 주의가 요구된다.

위와 같이 OSINT 검색 엔진을 통해 인터넷 상에 공개된 TeamCity 를 조회한 결과, 우리나라를 비롯한 전 세계적으로 많은 기업에서 TeamCity 를 CI/CD 툴로 사용하고 있었다. 특히, 이번 취약점이 발생한 TeamCity 는 Samsung, Tesla, Citybank, Amazon games 등 다수의 기업에서 사용하는 CI/CD 툴이기 때문에 현재 사용 중인 TeamCity 버전이 취약한지 확인하는 것이 필요하다.

## ■ 공격 시나리오

CVE-2024-27198를 이용한 공격 시나리오는 다음과 같다.

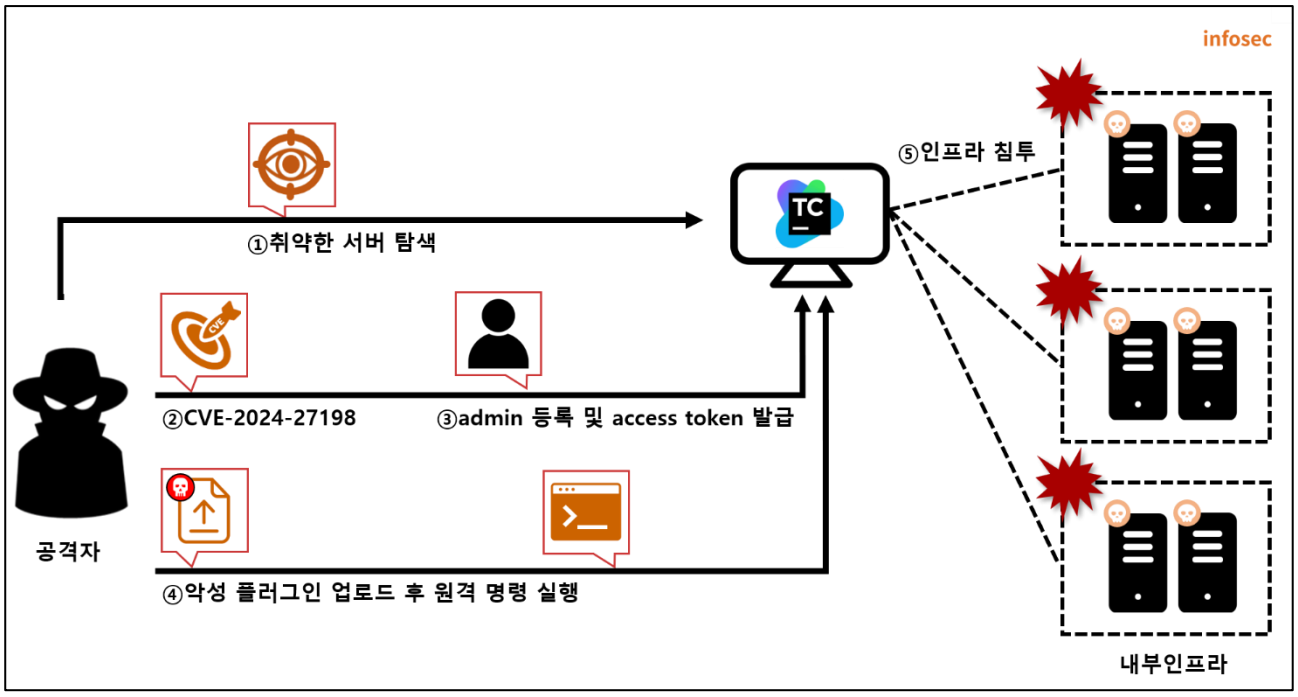



그림 2. CVE-2024-27198 공격 시나리오

① 공격자는 기업 내 사용중인 취약한 TeamCity 서버를 탐색
② 공격자는 CVE-2024-27198 취약점을 이용하여 피해자 서버에 접근
③ 공격자는 임의의 admin 계정을 등록하고 새로운 access token을 발급
④ 공격자는 악성 Plugin을 업로드하여 원격 명령 실행
⑤ 공격자는 내부 인프라에 침투하여 랜섬웨어, 암호화폐 채굴기 등 유포

## ■ 영향받는 소프트웨어 버전

CVE-2024-27198 에 취약한 소프트웨어는 다음과 같다.

| S/W 구분 | 취약 버전 |
|---|---|
| **JetBrains TeamCity** | 2023.11.3 이전 버전 |

## ■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2024-27198 의 동작 과정을 살펴본다.

| 이름 | 정보 |
|---|---|
| **피해자** | Ubuntu 22.04.6 LTS<br>TeamCity Professional 2023.11.3<br>(192.168.102.74) |
| **공격자** | Kali Linux<br>(192.168.219.129) |

## ■ 취약점 테스트

### Step 1. 환경 구성

피해자 PC 에 CVE-2024-27198 취약점이 존재하는 TeamCity 서버를 구축한다. 다음 명령어를 통해 취약한 서버를 구축할 수 있다.

| 명령어 | # docker pull<br>docker pull jetbrains/teamcity-server:2023.11.3<br># docker run<br>docker run –it –d –name teamcity –p 8111:8111 jetbrains/teamcity-server:2023.11.3 |
|---|---|

설치한 TeamCity 서버(192.168.102.74:8111)에 접근하면, 아래와 같이 CVE-2024-27198 취약점이 존재하는 2023.11.3 버전의 서버를 확인할 수 있다.

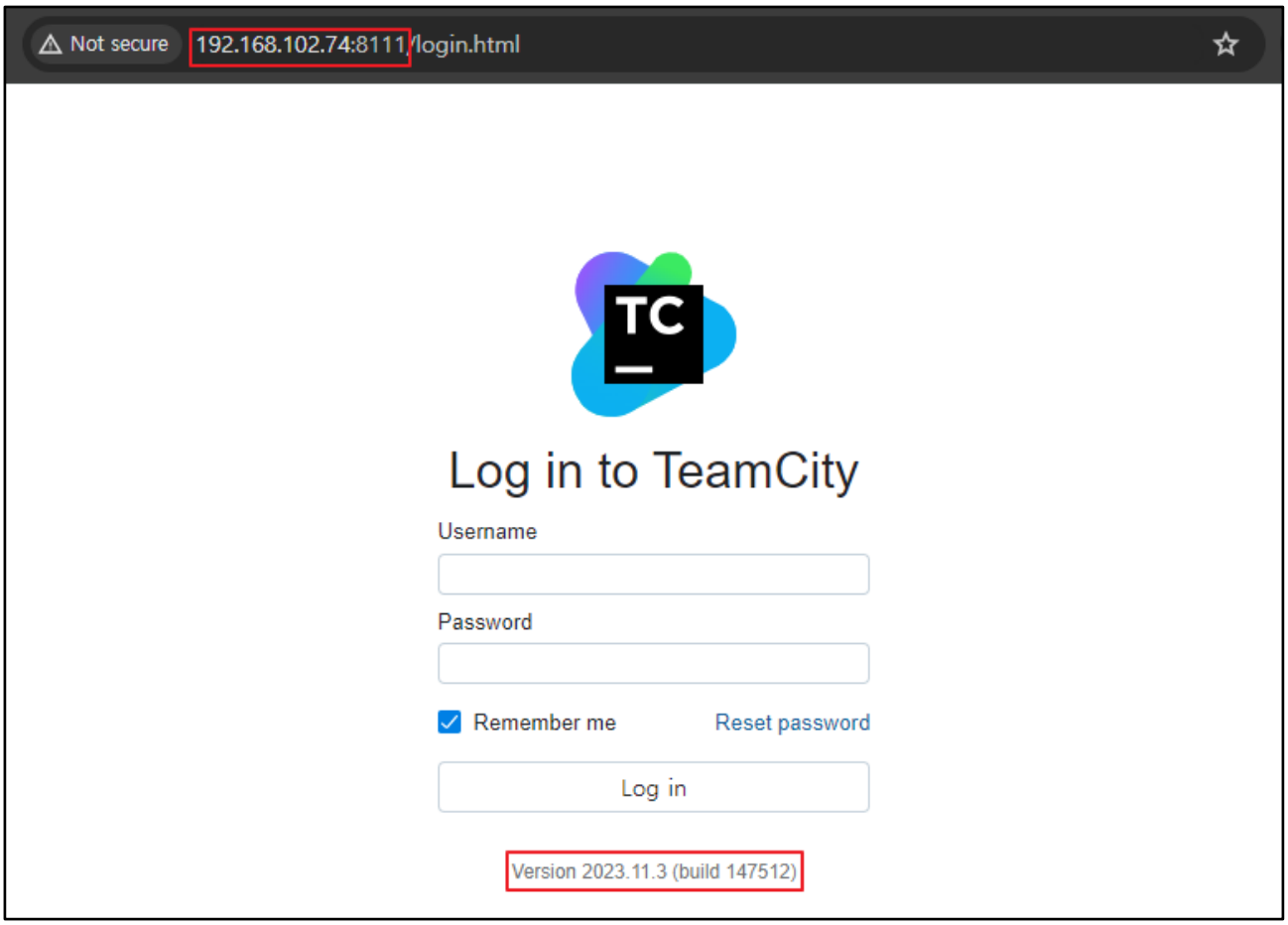



그림 3. 취약 서버 정보 확인

Step 2. 취약점 테스트

CVE-2024-27198 취약점을 이용해 공격자 PC 에서 아래 curl 커맨드로 관리자 계정을 생성한다.

```
$ curl -ik http://192.168.102.74:8111/eqst?jsp=/app/rest/users;.jsp -X POST -H "Content-Type: application/json" --data "{"username": "eqst", "password": "eqst", "email": "eqst@skshieldus.com", "roles": {"role": [{"roleId": "SYSTEM_ADMIN", "scope": "g"}]}}"
```


그림 4. curl 을 통한 관리자 계정 생성 요청

생성한 eqst 관리자 계정으로 로그인한다.

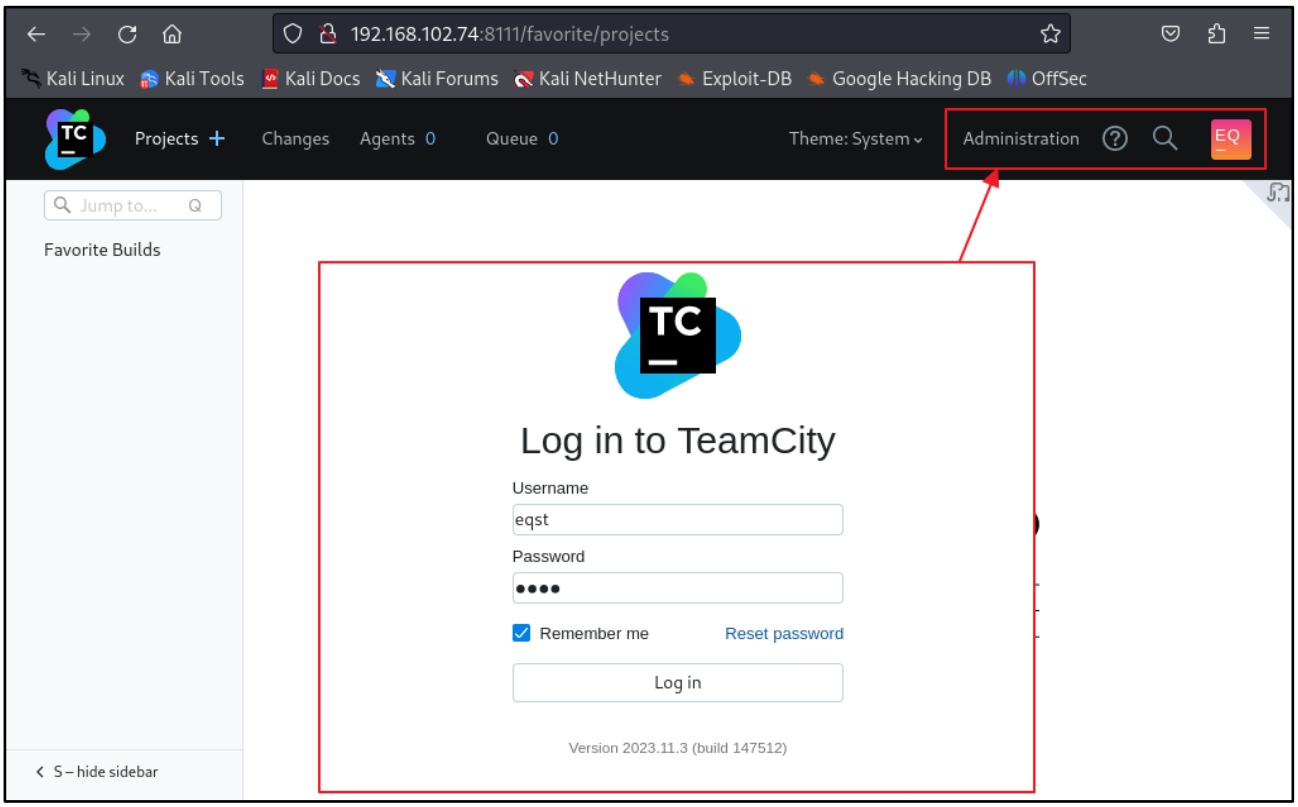



그림 5. 생성한 관리자 계정으로 로그인

Administrator 메뉴에 접근해 악성 Plugin 을 업로드한다.

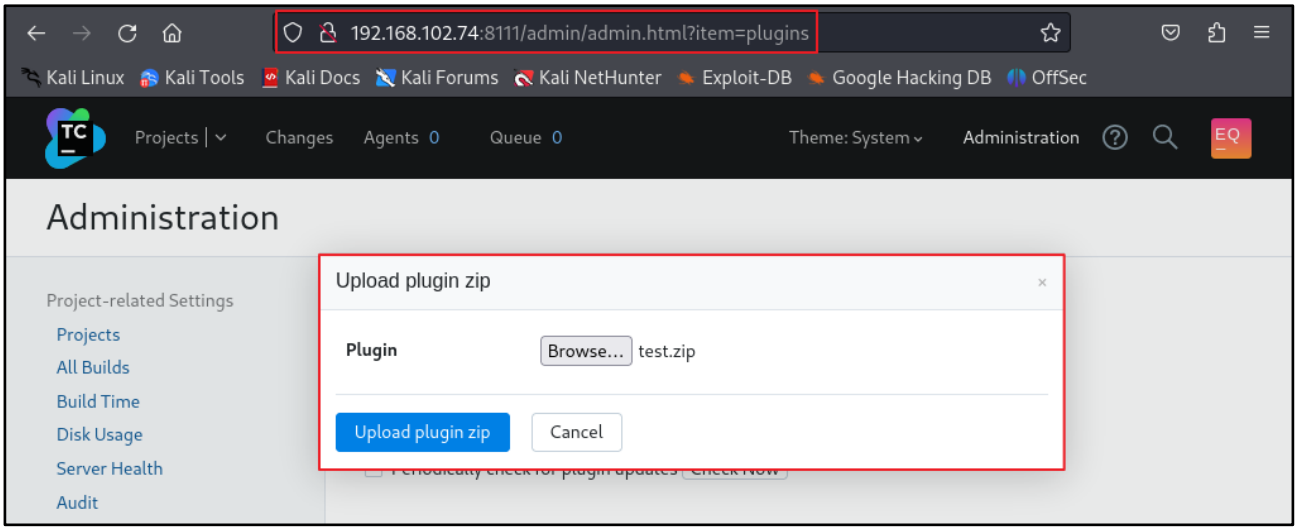



그림 6. 악성 Plugin 업로드

아래의 주소에 접근하면 업로드한 악성 Plugin 을 실행할 수 있으며, 공격자가 전송한 명령어가 피해자의 TeamCity 서버에서 실행된다.

```
http://{TeamCity_서버}/plugins/{plugin_이름}/{악성코드.jsp}?cmd={명령어}
```

아래 그림은 cat /etc/passwd 명령을 실행한 결과로 서버 측에 존재하는 계정들에 대한 정보를 출력하는 것을 확인할 수 있다.

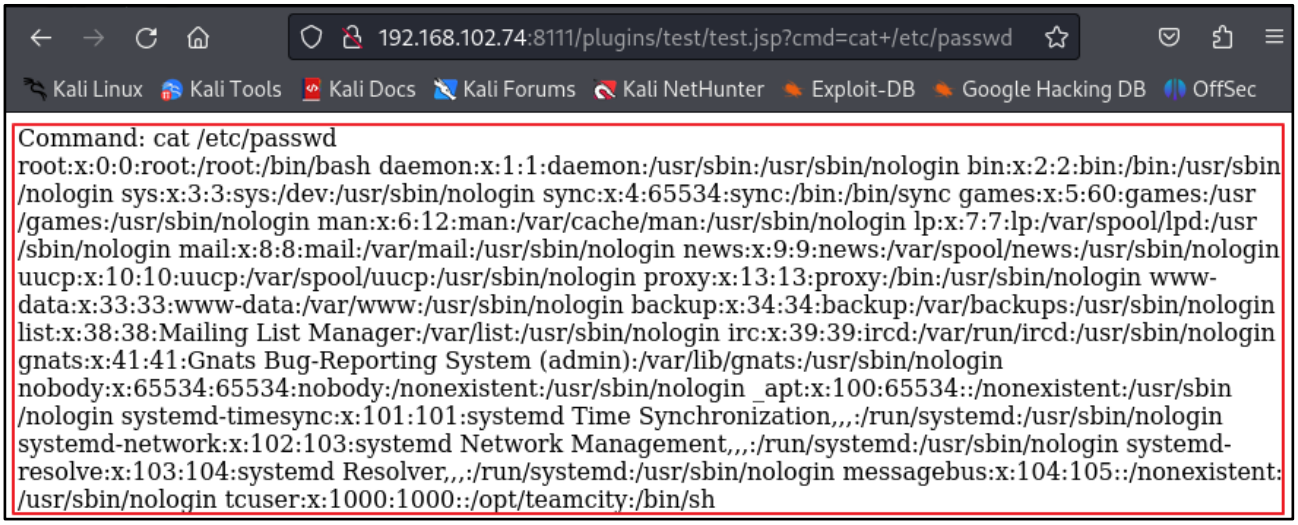



그림 7. 원격 명령 실행

## ■ 취약점 상세 분석

취약점 상세 분석에서는 CVE-2024-27198 취약점의 사용자 요청 검증 과정과 우회 방안, 해당 우회 이후 악성 Plugin 을 업로드하여 원격 코드를 실행하는 과정까지 다룬다.

### Step 1. 소스코드 분석

CVE-2024-27198 취약점은 web-openapi.jar 라는 자바 아카이브 파일(JAR)[25] 에서 구현되는 jetbrains.buildServer.controllers.BaseController 클래스에서 요청에 대한 검증이 미흡해 발생한다.

#### 1) handleRequestInternal 메서드 검증 과정

web-openapi.jar 에서 확인할 수 있는 Jetbrains.buildServer.controllers.BaseConroller 클래스 내부의 handleRequestInternal 메서드는 HTTP 요청을 처리하는 역할을 한다. 해당 메서드 내부에는 총 두개의 검증 로직이 구현되어 있다.

handleRequestInternal 메서드 내부에 구현된 첫번째 검증 로직은 Model 과 View 를 저장하는 modelAndView[26] 객체가 null 값인지 검사한다. 해당 객체가 null 값일 경우, handleRequestInternal 메서드는 null 값을 반환한다.

두번째 검증 로직은 HTTP 요청에 대한 응답이 리다이렉트 되는지 검사한다. HTTP 302 응답코드와 같은 리다이렉션 응답이 온다면, Model 을 초기화 시킨 후 현재 메서드인 handleRequestInternal 메서드의 결과를 반환한다. 이외의 경우는 updateViewIfRequestHasJspParameter 메서드로 현재의 modelAndView 객체를 전달한다.

handleRequestInternal 메서드의 소스코드는 아래와 같다.

```
public final ModelAndView handleRequestInternal(HttpServletRequest request, HttpServletResponse response)
    try {
        ModelAndView modelAndView = doHandle(request, response);
        if (modelAndView != null) {
            if (modelAndView.getView() instanceof RedirectView) {
                modelAndView.getModel().clear();
            } else {
                updateViewIfRequestHasJspParameter(request, modelAndView);
            }
        }
        return modelAndView;
```

그림 8. handleRequestInternal 메서드

[25] JAR(Java Archive, 자바 아카이브) 파일: 여러 개의 자바 클래스 파일과, 클래스들이 이용하는 관련 리소스(텍스트, 그림 등) 및 메타데이터를 하나의 파일로 모아서 자바 플랫폼에 응용 소프트웨어나 라이브러리를 배포하기 위한 소프트웨어 패키지 파일 포맷.

[26] modelAndView: MVC 는 사용자 인터페이스로부터 비즈니스 로직을 분리하는 소프트웨어 디자인 패턴을 뜻한다. Model, View, Controller 로 구성이 되는데, 이 중 model 과 view 를 합쳐 놓은 클래스가 modelAndView 클래스.

### 2) updateViewIfRequestHasJspParameter 메서드 검증 과정

handleRequestInternal 처리시 사용하는 updateViewIfRequestHasJspParameter 메서드의 소스코드는 다음과 같다.

```
        private void updateViewIfRequestHasJspParameter(@NotNull HttpServletRequest request,
    @NotNull ModelAndView modelAndView) {
            boolean isControllerRequestWithViewName = (modelAndView.getViewName() == null ||
request.getServletPath().endsWith(".jsp")) ? false : true;                                    ①
            String jspFromRequest = getJspFromRequest(request);
            if (isControllerRequestWithViewName && StringUtil.isNotEmpty(jspFromRequest) && !
modelAndView.getViewName().equals(jspFromRequest)) {                                          ②
                modelAndView.setViewName(jspFromRequest);
            }
        }
```

그림 9. updateViewIfRequestHasJspParameter 메서드

① modelAndView 객체의 View가 이름을 가지고 있고 현재 요청의 URL 경로가 .jsp 로 끝나지 않는지 확인한다. 해당 검증결과는 isControllerRequestWithViewName에 저장한다.

② 검증결과를 저장한 isControllerRequestWithViewName이 True고, jspFromRequest가 null 또는 빈 값이 아니며, modelAndView 객체의 View 이름이 jspFromRequest와 같지 않다면 modelAndView 객체의 View 값을 jspFromRequest 값으로 수정한다.

### 3) getJspFromRequest 메서드 검증 과정

getJspFromRequest 메서드의 소스코드는 다음과 같다.

```
protected String getJspFromRequest(@NotNull HttpServletRequest request) {
    String jspFromRequest = request.getParameter("jsp");
    if (jspFromRequest != null && (!jspFromRequest.endsWith(".jsp") || jspFromRequest.contains("admin/"))) {
        return null;
    }                    ①                  ②                          ③
    return jspFromRequest;
}
```

그림 10. getJspFromRequest 메서드

updateViewIfRequestHasJspParameter 메서드에서 호출하는 getJspFromRequest 메서드는 jsp 파라미터의 값을 받아 검증하는 과정이 포함되어 있다. 검증 절차는 다음과 같다.

① 문자열이 null이 아닌지 검증
② 문자열이 “.jsp”로 끝나지 않는지 검증
③ 문자열에 “admin/”을 포함하는지 검사

위의 조건을 통과하지 못하면 null 을 반환한다.

Step 2. 인증 우회

TeamCity 2023.11.3 버전 이전에 존재하는 인증 우회 취약점은 /app/rest/server 경로에 접근하여 확인해볼 수 있다. TeamCity 의 /app/rest/server 경로에 접근하면 인증된 사용자에게는 현재 서버 버전 정보를 반환한다.

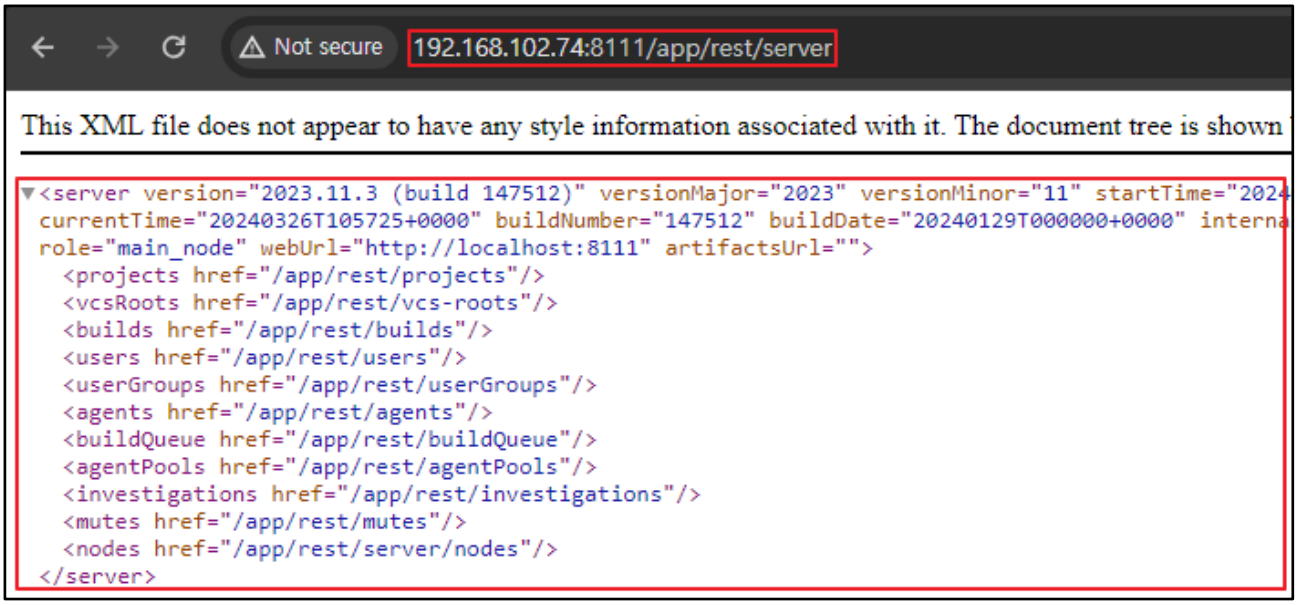



그림 11. /app/rest/server 정상 요청에 대한 응답

하지만 인증된 사용자가 아니라면 서버 버전 정보 대신 401 응답 코드를 반환한다.

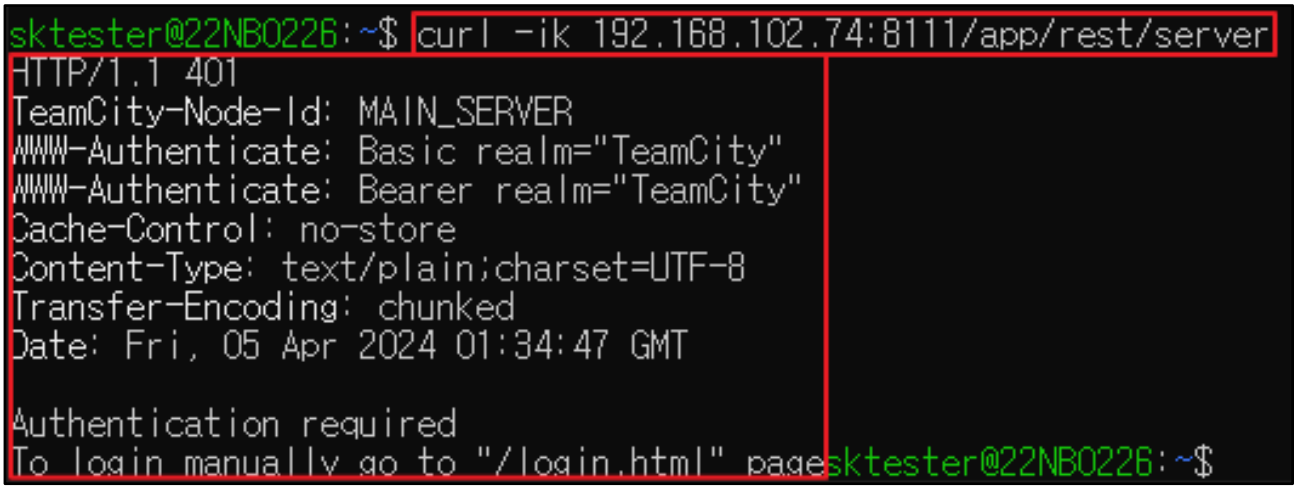



그림 12. /app/rest/server 미인증 요청에 대한 응답

/app/rest/server에 직접 접근 시, 인증이 되지 않아 접근할 수 없으므로 인증없이 view를 교체하는 updateViewIfRequestHasJspParameter 메서드를 활용한다. 우선, 현재 view 를 가지고 있어야 하고 파라미터를 제외한 현재 경로인 servletpath 가 .jsp 로 끝나지 않아야 검증과정을 통과한다. 따라서, 인증 없이도 접근할 수 있는 login.html에 접근하면 해당 과정을 우회할 수 있다.

login.html 뿐 아니라 404 페이지와 같이 인증 없이 접근 가능한 view 가 있는 페이지는 전부 공격에 활용할 수 있다.

다음으로 위 조건을 만족하면 jsp 파라미터를 통해 특정 경로에 접근 가능하다. getJspFromRequest 메서드에서 jsp 파라미터 값이 .jsp 로 끝나는지 검증하기 때문에, 이는 semi-colon(;)을 .jsp 앞에 붙여서 우회할 수 있다.

위 설명에 따라 생성한 공격 payload는 다음과 같다.

```
http://{TeamCity_address}/login.html?jsp=/app/rest/server;.jsp
```

semi-colon 을 .jsp 앞에 붙여 우회할 수 있는 이유는 semi-colon 뒤의 문자열이 jersey-server-1.19.jar 라이브러리의 WebApplicationImpl 클래스 내 stripMatrixParams 메서드에서 HTTP URL path parameter segment[27]가 제거되어 /app/rest/server 경로에 접근이 가능하기 때문이다.

최초 jsp 파라미터 입력을 받았을 때는 아래의 그림과 같이 semi-colon 을 포함한 전체 경로가 저장된다.

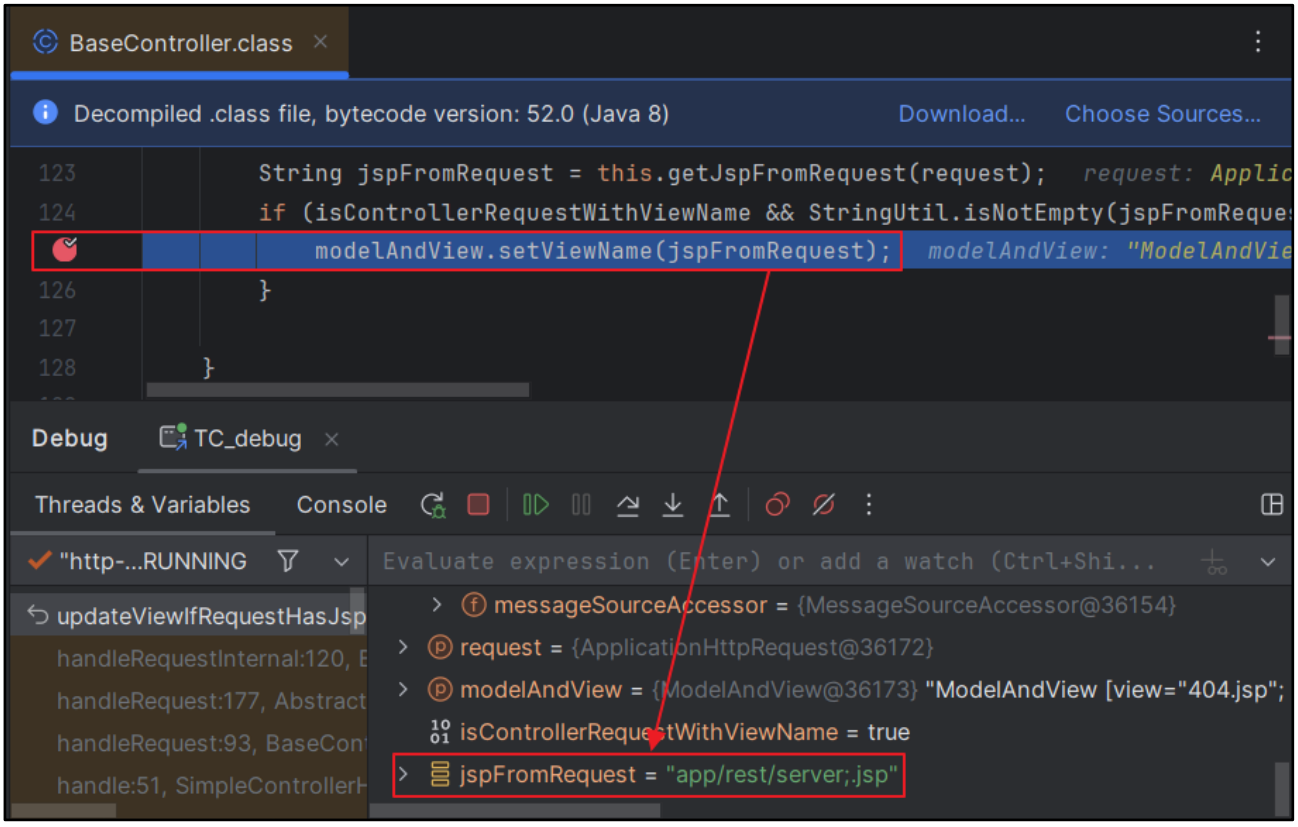



그림 13. jspFromRequest 파라미터 확인

[27] HTTP URL Path Parameter: Matrix Parameter 라고도 하며, 자원의 표현 방식을 제어하기 위해 사용된다. https://eqst.com/main;eqst=test/board;shieldus=test 와 같이 반드시 경로의 마지막이 아닌 원하는 위치에 매개변수를 작성할 수 있다.

이 후 stripMatrixParams 메서드로 인해 path 의 HTTP URL parameter segment 가 제거되어 ;.jsp 가 삭제된 것을 확인할 수 있다.

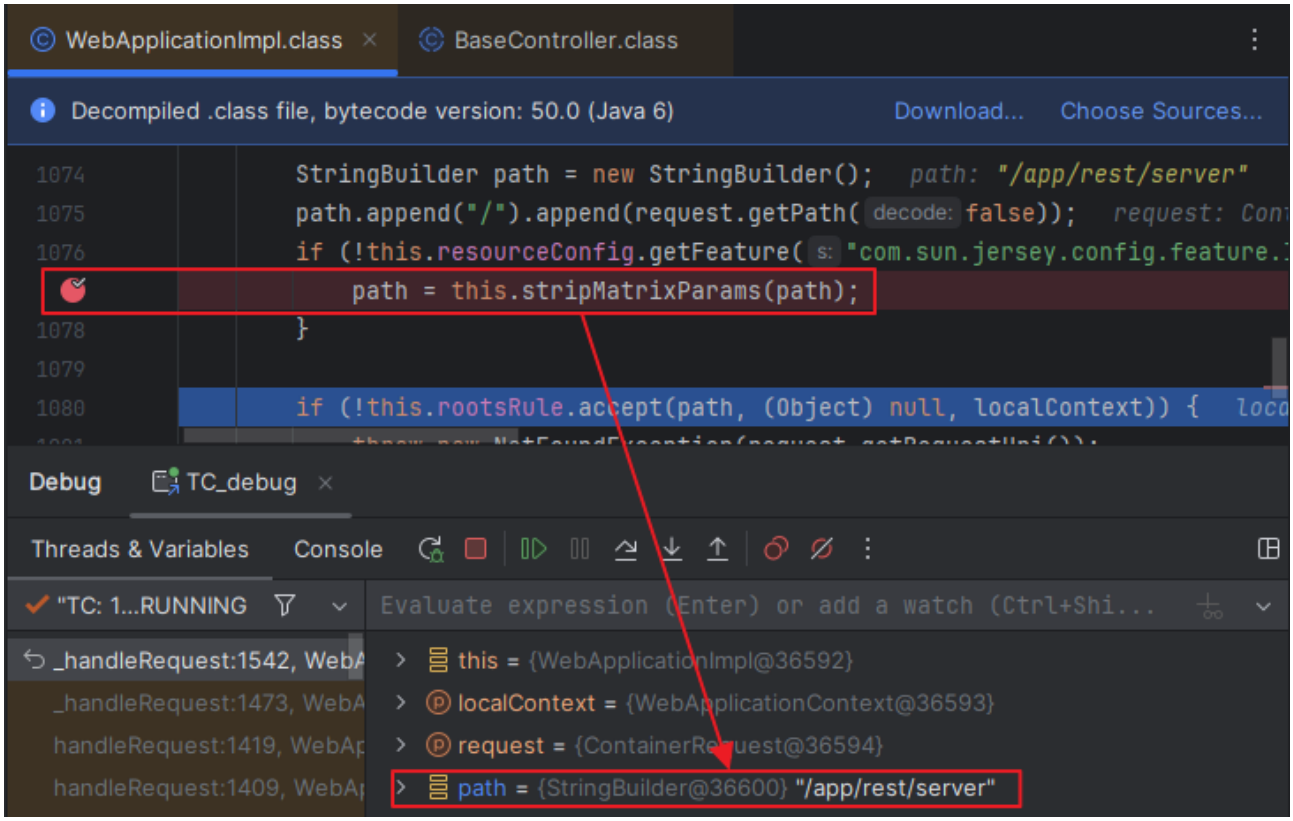


그림 14. stripMatrixParams 메서드 실행 결과

따라서 검증 로직 우회를 하기 위해 /app/rest/server;.jsp를 입력한 결과 /app/rest/server에 접근할 수 있다.

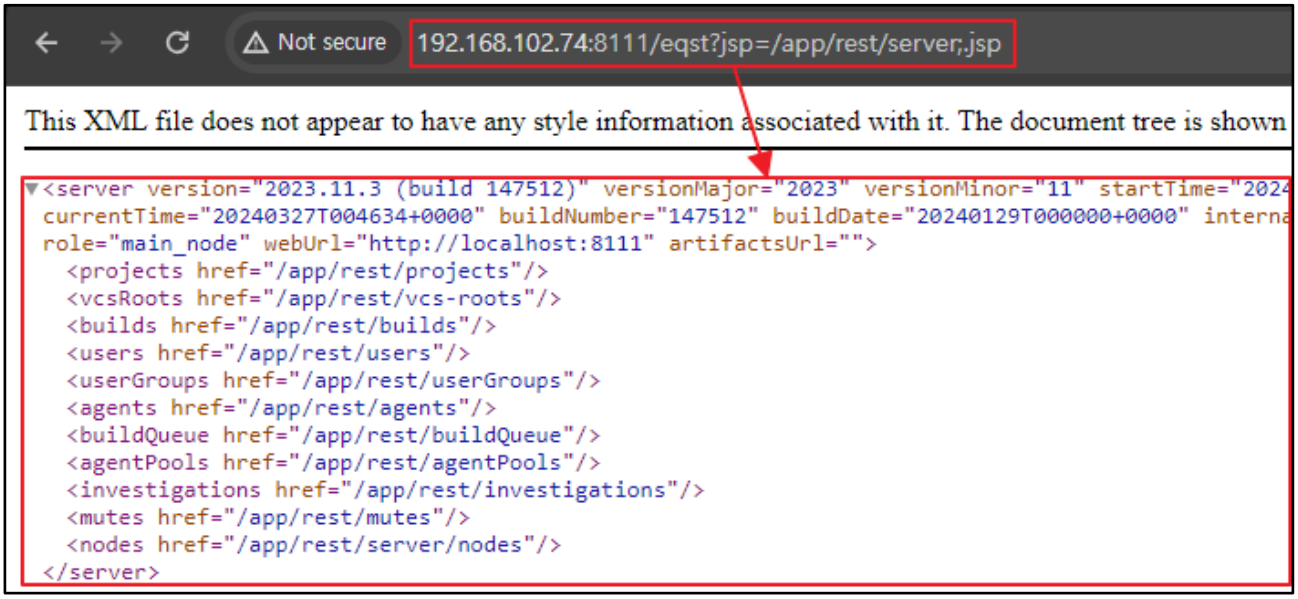


그림 15. payload를 활용한 인증 우회 확인

### Step 3. 관리자 권한 획득

#### 1) admin 등록

앞서 기술한 취약점을 악용하면 TeamCity 내 수많은 endpoint 에 공격이 가능하며, 특히 유저 관리를 수행하는 REST API[28]를 구현한 /app/rest/users 경로를 향한 공격이 치명적이다.

/app/rest/users 는 권한 있는 사용자가 POST 요청을 통한 사용자 등록 기능을 수행한다. 하지만 위의 취약점을 이용하면 인증 없이 임의의 사용자 등록이 가능하다. 아래의 요청을 전송하여 임의의 관리자 계정을 등록할 수 있다.

| Payload | http://192.168.102.74:8111/eqst?jsp=/app/rest/users**;.jsp** |
|---|---|
| JSON Data | {"username":"eqst",<br>"password":"skshieldus",<br>"email":"skshieldus.tester@sk.com",<br>"roles":{"role":[{"roleId":"SYSTEM_ADMIN","scope":"g"}]}} |

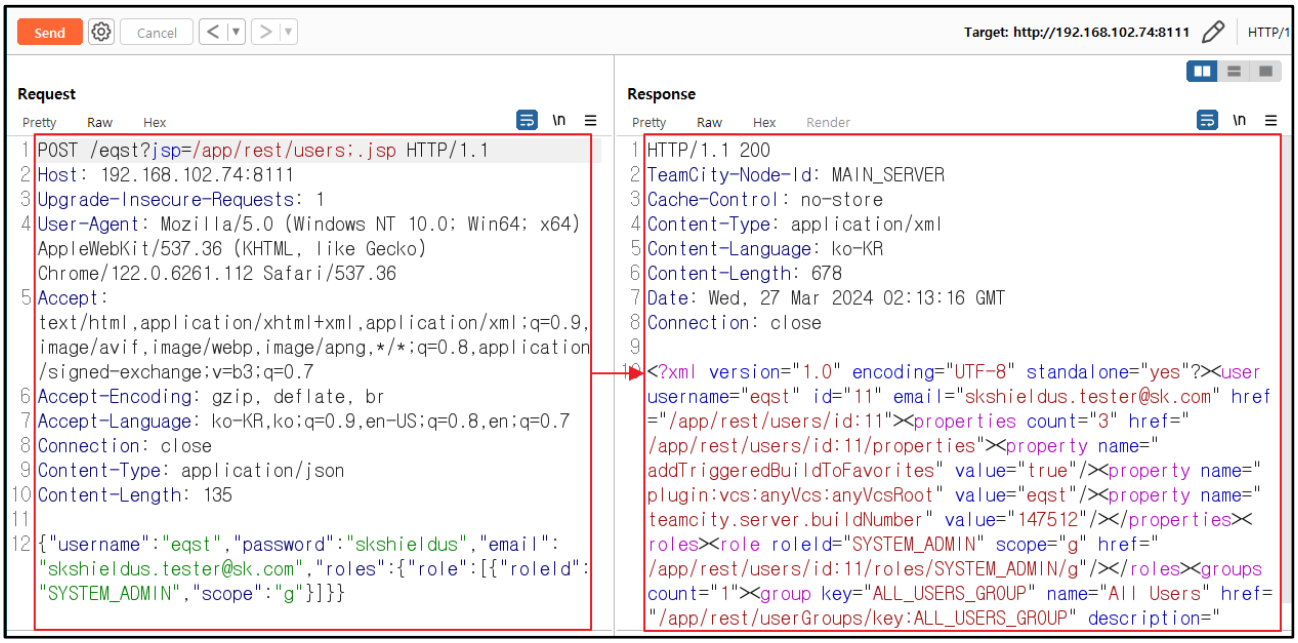



그림 16. 임의의 관리자 계정 등록

[28] REST API: HTTP 요청을 통해 통신함으로써 리소스 내에서 레코드의 작성, 읽기, 업데이트 및 삭제 등의 표준 데이터베이스 기능을 수행하는 API. 예를 들어 GET 요청으로 레코드 검색, POST 요청으로 레코드 작성, PUT 요청으로 레코드 업데이트, DELETE 요청으로 레코드 삭제를 수행함.

요청 Payload 와 JSON Data 전송 결과, Teamcity 관리 메뉴에서 임의로 등록한 관리자 계정을 확인할 수 있다.

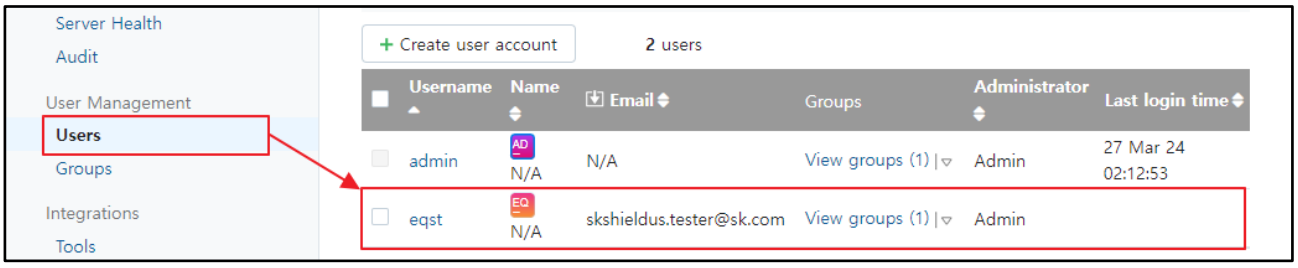



그림 17. 공격 결과

2) access token 발급

/app/rest/users/id:{id 값}/tokens/{Token_name}은 새로운 access token 을 발급하는 API 다. id 값 1 번이 초기 설정에서 등록한 관리자이기 때문에 다음 Payload 를 전송하여 관리자 access token 을 인증 없이 발급할 수 있다.

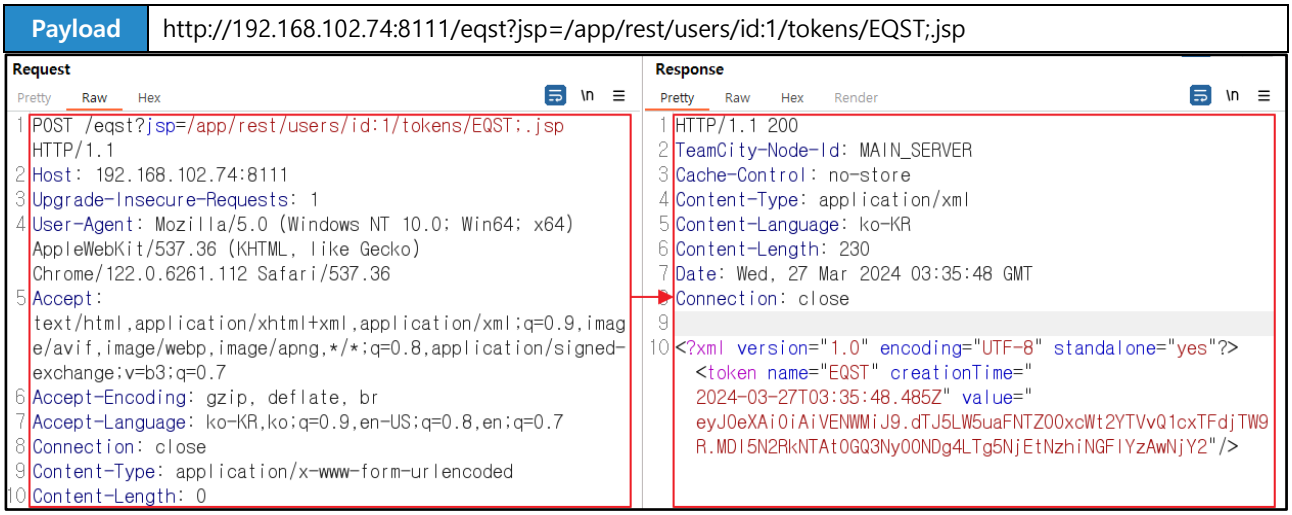



그림 18. 관리자 access token 발급 공격

공격 결과는 토큰 발급 현황에서 확인할 수 있다. 해당 access token 을 Authorization: Bearer 헤더 값으로 입력해 패스워드 대신 사용하여 관리자 권한 탈취가 가능하다.

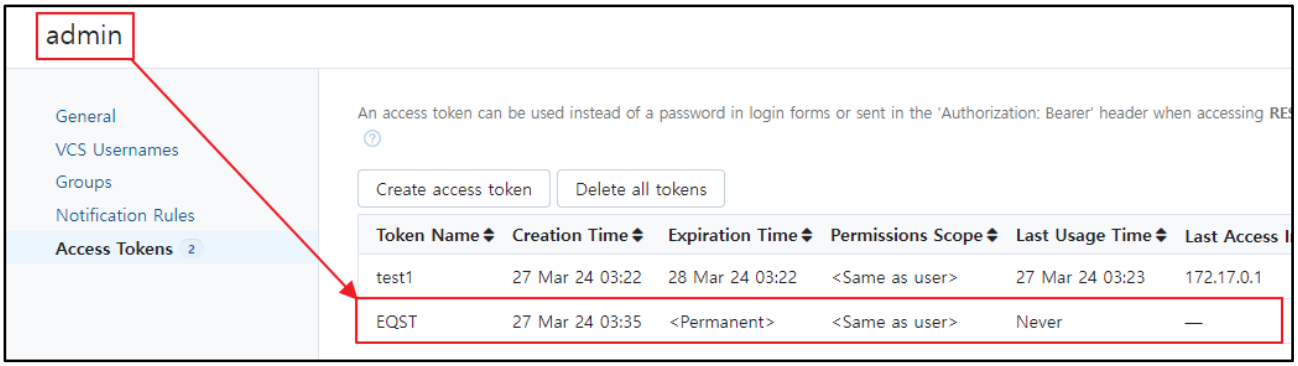



그림 19. 관리자 access token 발급 결과

## Step 4. 원격 코드 실행

### 1) TeamCity 악성 Plugin 구조

TeamCity 악성 Plugin 을 업로드하기 위해서는 최소한 아래와 같은 구조로 이뤄져 있어야 한다.

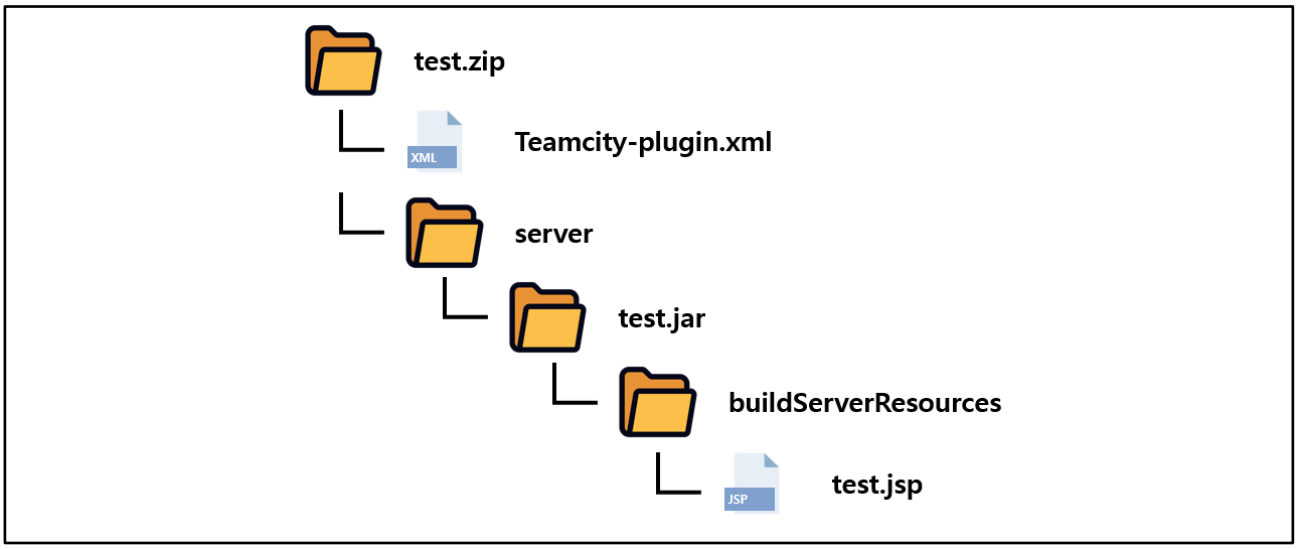



그림 20. TeamCity 악성 Plugin 구조

TeamCity 에 업로드할 Plugin 은 zip 파일의 루트 경로에 Plugin 에 대한 정보가 기입된 Teamcity-plugin.xml 이 반드시 필요하다. 악성코드가 포함된 jsp 파일은 buildServerResources 디렉토리에 넣고 jar 파일로 만들어야 한다.

### 2) 악성 Plugin 업로드 및 실행

탈취한 관리자 계정으로 Administration>Plugins>Upload plugin zip 메뉴에서 공격에 사용할 악성 Plugin 을 업로드할 수 있다.

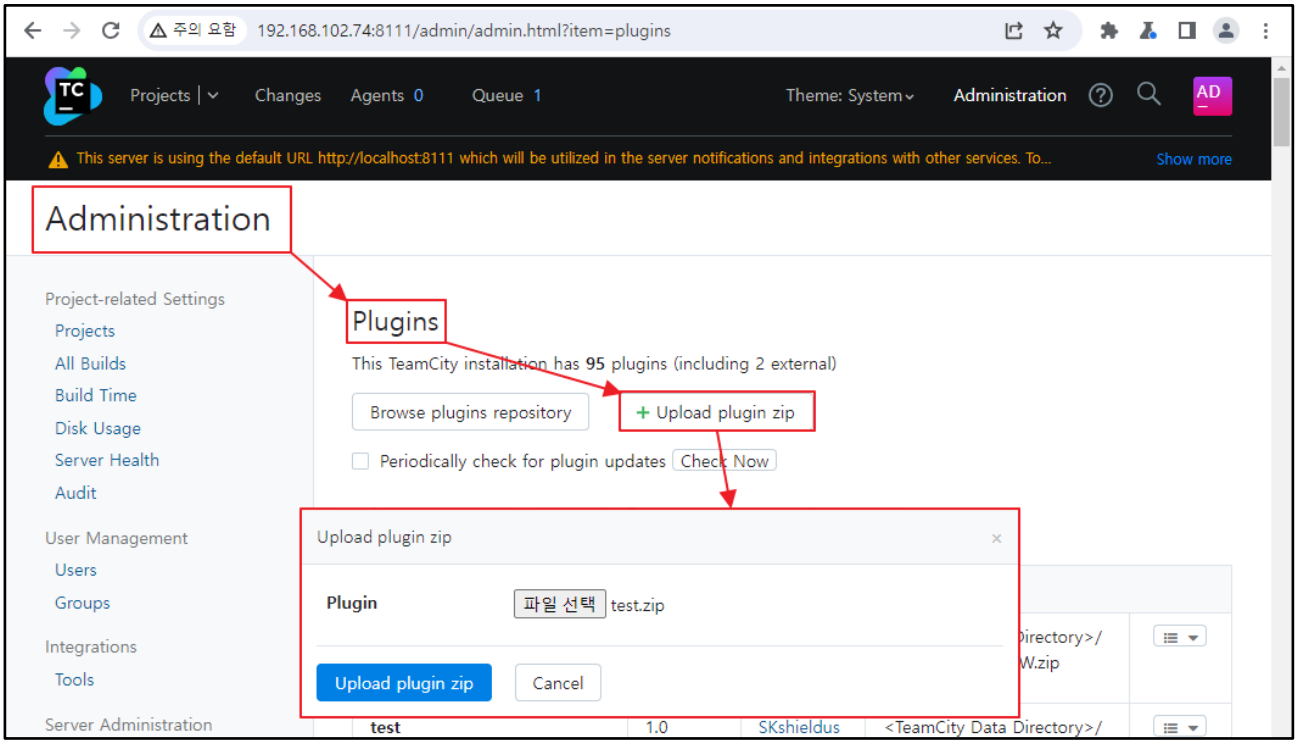



그림 21. 악성 Plugin 업로드

악성 Plugin 을 업로드한 후 /plugins/{Plugin 이름}/{jsp 파일명} 경로로 접근하여 실행할 수 있다. 공격에 사용한 악성 Plugin 은 JSP WebShell 이며, 다음과 같은 공격 payload 로 원격 명령 실행이 가능하다.

**http://{TeamCity_address}/plugins/{Plugin_name}/{jsp_file}?cmd={command}**

ls 명령 실행 결과는 다음과 같다.

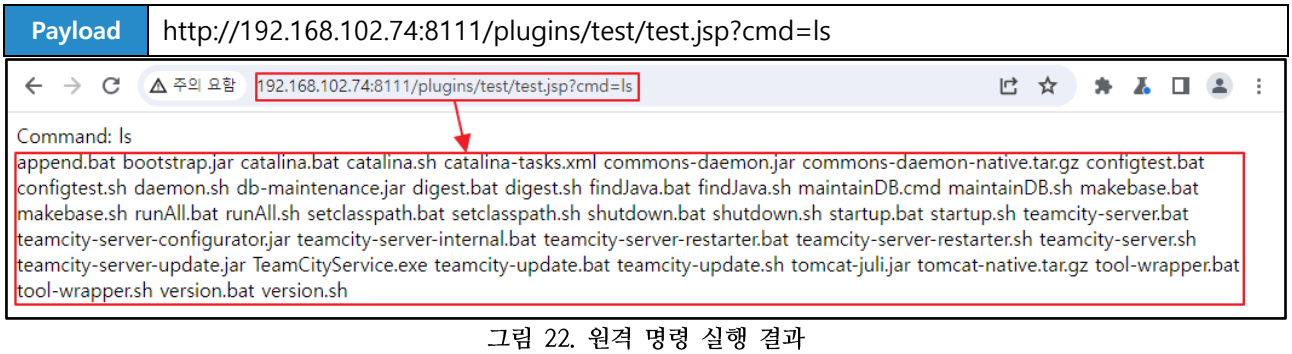



그림 22. 원격 명령 실행 결과

## ■ 대응 방안

CVE-2024-27198 발표 후 JetBrains 는 취약점 패치가 적용된 2023.11.4 버전으로 업데이트하거나, 불가할 경우 보안 패치 Plugin 을 적용하는 대응 방안을 공지했다. 하지만 두 가지 방법 모두 대응이 미흡한 것을 확인했다.

• URL: https://blog.jetbrains.com/teamcity/2024/03/teamcity-2023-11-4-is-out/

2023.11.3 버전에서 취약점을 권한 검증으로 대응했기에 jsp 파라미터는 그대로 사용할 수 있다. 따라서 접근 제어가 누락된 경로들에 대해 여전히 접근이 가능하다. 2023.11.4 버전에서 수행한 공격 예시는 다음과 같다.


그림 23. 공격 결과

이 후 3 월경 2024.03 버전의 TeamCity 가 출시됐다.

해당 버전의 TeamCity 는 updateViewIfRequestHasJspParameter 메서드를 삭제 조치했다.

```
    public final ModelAndView handleRequestInternal(HttpServletRequest request,
HttpServletResponse response) throws Exception {
        try {
            ModelAndView modelAndView = doHandle(request, response);
            if (modelAndView != null && (modelAndView.getView() instanceof RedirectView)) {
                modelAndView.getModel().clear();
            }
            return modelAndView;
```

그림 24. updateViewIfRequestHasJspParameter 메서드 삭제

그림 23 과 동일한 공격 payload 전송 시 더 이상 요청에 대한 jsp 파라미터를 처리하지 않아 공격이 불가능하다.

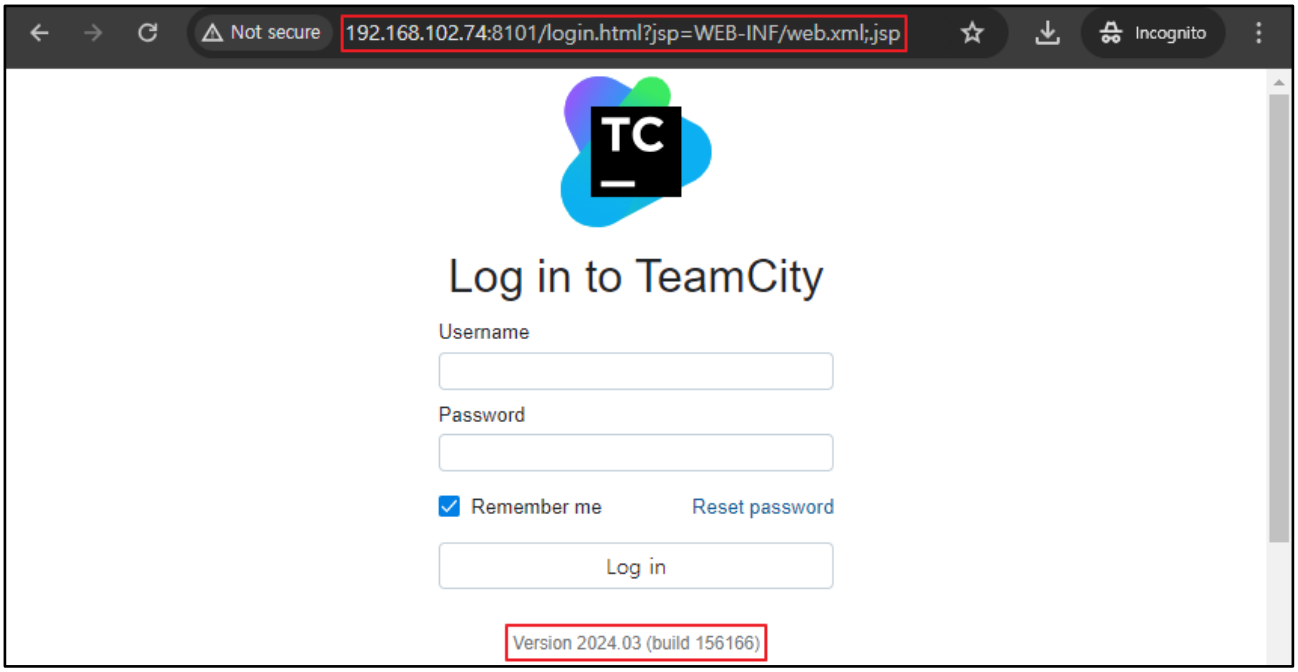



그림 25. jsp 파라미터를 처리하지 않는 모습

따라서, 2023.11.4 버전의 TeamCity는 불완전한 패치로 인한 추가적인 공격 가능성을 가지고 있어, 가장 최신 버전인 2024.03 TeamCity 로 패치할 것을 권장한다.

| 제품 | 권장 버전 |
|---|---|
| **JetBrains TeamCity** | 2024.03 |

## ■ 참고 사이트


• RFC2396 (https://datatracker.ietf.org/doc/html/rfc2396)
• IBM-What is a REST API? (https://www.ibm.com/topics/rest-apis)
• TeamCity Plugin Development Help (https://plugins.jetbrains.com/docs/teamcity/plugins-packaging.html#Server-Side+Plugins)
• The TeamCity Blog: TeamCity 2023.11.4 IsOut (https://blog.jetbrains.com/teamcity/2024/03/teamcity-2023-11-4-is-out/)
• The TeamCity Blog: Additional Critical Security Issues Affecting TeamCity On-Premises - Update to 2023.11.4 Now (https://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now/)
• Rapid7: CVE-2024-27198 and CVE-2024-27199: JetBrains TeamCity Multiple Authentication Bypass Vulnerabilities (FIXED) (https://www.rapid7.com/blog/post/2024/03/04/etr-cve-2024-27198-and-cve-2024-27199-jetbrains-teamcity-multiple-authentication-bypass-vulnerabilities-fixed/)
• TeamCity Vulnerability Exploits Lead to Jasmin Ransomeware, Other Malware Types (https://www.trendmicro.com/en_us/research/24/c/teamcity-vulnerability-exploits-lead-to-jasmin-ransomware.html?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=032024_TeamCity)
• HTTP URL Path Pa

# EQST INSIGHT

2024.04

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

발행인 : SK쉴더스 EQST사업그룹
제　작 : SK쉴더스 마케팅그룹