

RID Hijacking Technique Utilized by Andariel Attack Group

A asec.ahnlab.com/en/85942/

January 22, 2025



APT

Jan 23 2025



AhnLab SEcurity intelligence Center (ASEC) has identified the Andariel attack group using a malicious file to perform an RID Hijacking attack during the breach process.

RID Hijacking is an attack technique that involves modifying the Relative Identifier (RID) value of an account with restricted privileges, such as a regular user or guest account, to match the RID value of an account with higher privileges, such as an administrator. In the Korea Internet & Security Agency's (KISA) public post, "TTPs #11: Operation An Octopus – Analysis on Attack Strategies Targeting Centralized Management Solutions", it was mentioned that the Andariel threat group uses the RID Hijacking technique when creating a backdoor account within the operating system. RID Hijacking attacks are difficult to detect in behavior-based detection systems because they involve creating a hidden account and modifying the RID value of that account.

This blog will cover the RID Hijacking attack process and the techniques used in breach incidents.

1. Concept of RID Hijacking

RID Hijacking is an attack technique that involves modifying the RID value of an account with low privileges, such as a regular user or a guest account, to match the RID value of an account with higher privileges (Administrator). By modifying the RID value, threat actors can deceive the system into treating the account as having administrator privileges. Threat actors can use various types of accounts to perform RID Hijacking, including:

- Using a regular user account that exists in the system

- Activating the guest account
- Creating a new account

RID Hijacking is typically performed by manipulating the Security Account Manager (SAM) database. Threat actors can create an administrator account or escalate privileges to gain administrator access without knowing the password.

2. RID Hijacking Attack Process

The following are the stages of RID Hijacking attacks identified in breach incident cases.

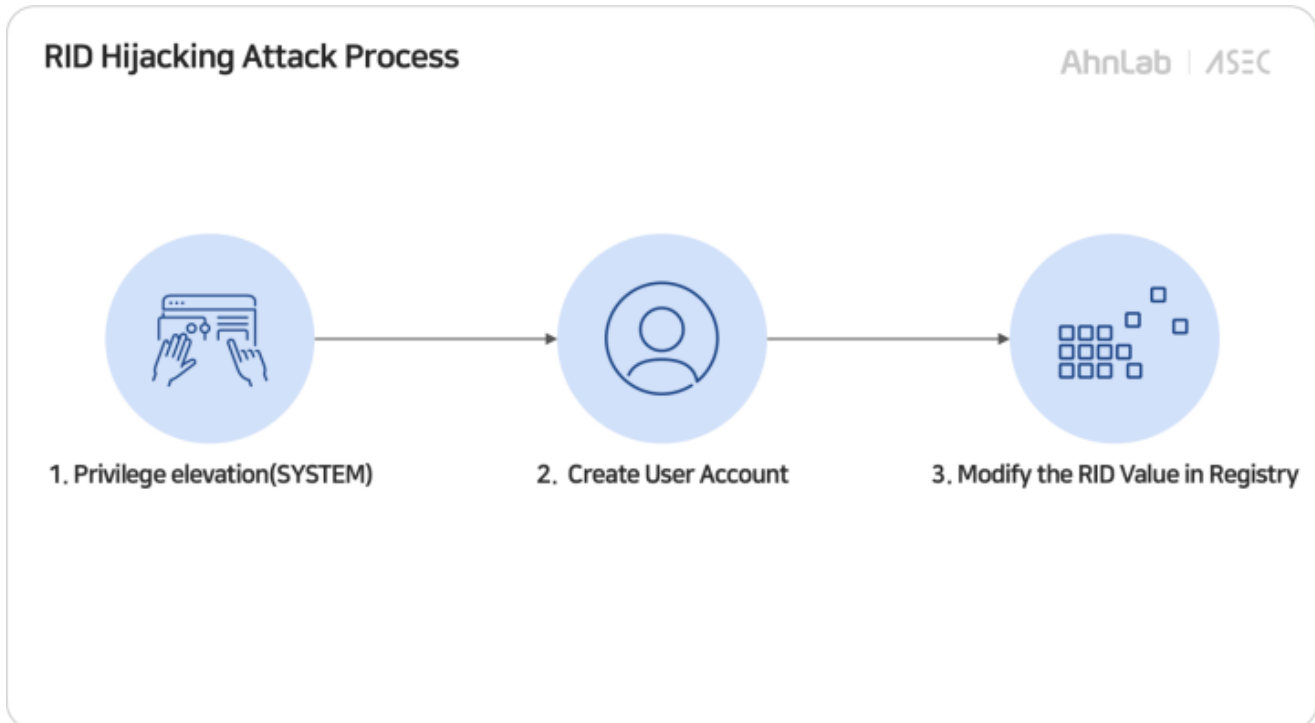


Figure 1. The process of a RID Hijacking attack

2.1 SYSTEM Privilege Escalation

The SAM registry manages authentication and authorization within Windows and stores user account information. It cannot be accessed with regular administrator privileges, requiring SYSTEM privileges for access and modification.

Threat actors use privilege escalation tools such as PsExec and JuicyPotato to obtain SYSTEM privileges on the compromised system. In this case, the threat actor used PsExec to execute a malicious file through a remote command, and the malicious file operated with SYSTEM privileges.

Processes Performance App history Startup Users Details Services						
Name	PID	Status	User name	CPU	Memory (a...	UAC virtualizat...
powershell.exe	1804	Running	SYSTEM	00	32,280 K	Not allowed
OneDrive.exe	2348	Running	office02	00	24,444 K	Disabled
NisSrv.exe	6792	Running	LOCAL SE...	00	2,764 K	Not allowed

Figure 2. Example of file permission when using the PsExec command (SYSTEM)

2.2 Creating a Local User Account

Threat actors either use existing user accounts in the system or create new accounts. In this case, the threat actor created an account to perform the RID Hijacking attack.

The threat actor created an account using the 'net user' command. When a \$ is added to the end of the account name during account creation, the account is created with a hidden attribute. In this case, the account cannot be identified using the 'net user' command, and can only be identified in the SAM registry.

```

C:\Windows\system32>net user admin$ /add
The command completed successfully.

C:\Windows\system32>net user

User accounts for \\OFFICEPC02

-----
Administrator          DefaultAccount          Guest
office02                WDAGUtilityAccount
The command completed successfully.

```

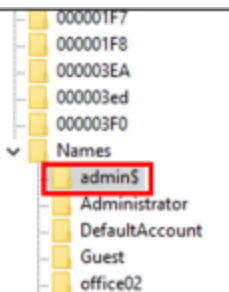


Figure 3. Checking the account creation result (net user, registry)

The threat actor then added the created account to the Remote Desktop Users group and Administrators group using the "net localgroup" command. When an account is added to the Remote Desktop Users group, the account can be accessed by using RDP.

2.3 Changing RID via Registry Value Modification

In a RID Hijacking attack, threat actors modify the RID value of an account in the SAM registry so that the Windows operating system recognizes it as a changed RID. As such, threat actors modify the values in the SAM registry to change the RID value.

In the Windows operating system, the registry key related to user accounts are stored in the path 'HKEY_LOCAL_MACHINE\ SAM\SAM\Domains\Account\Users'. The RID of a user account is written in the little-endian format as 4 bytes in the 0x30 – 0x33 area of the 'F' value under each account key. Threat actors change the value at this offset to the RID of the hijacking target.

Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003EA			
Computer	Name	Type	Data
> HKEY_CLASSES_ROOT	ab (Default)	REG_SZ	(value not set)
> HKEY_CURRENT_USER	F	REG_BINARY	03 00 01 00 00 00 00 00 6c 2b 69 9c 51 3a d
> HKEY_LOCAL_MACHINE			

Figure 4. Account-related key in the SAM registry

```
memset(SubKey, 0, 0x104uLL);
sprintf2(SubKey, "SAM\\SAM\\Domains\\Account\\Users\\000000%x", a1);
if ( RegOpenKeyExA(HKEY_LOCAL_MACHINE, SubKey, 0, 0x20006u, &hKey) )
{
    printf_1("[ - ] %x type key open failed\r\n", a1);
    return 0;
}
else if ( RegSetValueExW(hKey, "F", 0, 'x03', a2, a3) )
{
```

Figure 5. Feature for changing the RID inside the malware

Once the RID value has been changed, the Windows OS recognizes the account created by the threat actor as having the same privileges as the target account, enabling privilege escalation.

3. Malicious File Used by Threat Actor

The Andariel threat group utilized a malicious file and an open-source tool that they created themselves to perform the RID Hijacking attack. Both malicious files contain the attack process described in the RID Hijacking attack process, but there are differences in some of the features.

Malicious file of the Andariel threat group		Open Source Tool CreateHiddenAccount
File Type	Created by Threat Actor	Open Source
Permission	Execute as system privilege	Run as administrator
Behavior	<ol style="list-style-type: none"> 1. Create Account and Add to Group (remote desktop users) 2. Retrieve the RID of the created account and the target account 3. Access the F key in the registry of the created account and modify it with the RID value of the target account 4. Extract the registry 5. Delete the created account 6. Add to the registry 	<ol style="list-style-type: none"> 1. Create account and add to group (administrator) 2. Access the SAM registry using regini 3. Get the RID of the created account and the target account 4. Delete the created account 5. Create a .reg file and copy the registry value of the existing user 6. Add to registry 7. Activate account
Target Account	Hardcoded to befit the environment of the affected company	Designated as a parameter value

Table 1. Comparison of malicious files performing RID Hijacking attacks

3.1 Modify SAM Registry Access Permission

RID Hijacking requires SYSTEM privileges because it needs to access the SAM registry key. Samples developed by the Andariel threat group cannot perform their functions properly without system privileges. The open-source tool CreateHiddenAccount can perform all of its functions even with administrator privileges. Analyzing the operation process of this tool revealed that it uses the Windows default program, regini, to grant permissions.

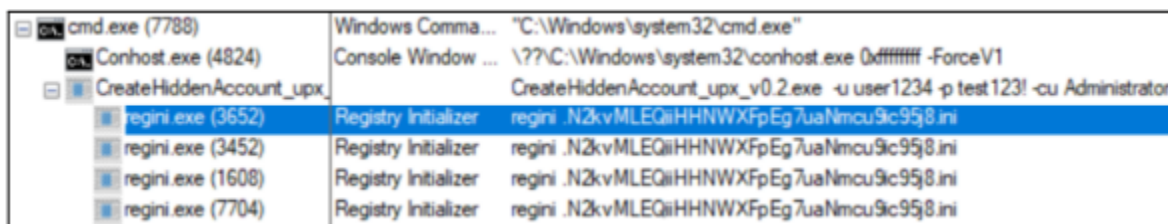


Figure 6. Using regini.exe to access the registry with Administrators permission

regini is a CLI tool provided by Microsoft that can edit the Windows registry through a text file. By specifying the registry key path and permissions in a text file, behaviors such as creating, modifying, deleting, and changing permissions for registry keys can be performed. The ini file identified in CreateHiddenAccount modified the access permissions to the SAM registry required for the RID Hijacking attack. In this case, the default permission (System) 17 was added to the SAM registry path along with option 1 (Administrator), allowing the modification of the SAM registry key with administrator privileges.

```
HKEY_LOCAL_MACHINE\SAM\SAM [1 17]
```

Figure 7. Example of the contents of the ini file

3.2 Behavior of Adding to Registry

In addition to creating a hidden account with a '\$' in the account name, the malicious file used by the Andariel attack group performs additional behaviors to minimize exposure. After completing RID Hijacking, the 'reg export' command is used to extract the registry key related to the account.

Behavior	Command
Key that performs the role of mapping user names to RIDs	reg export hklm\sam\sam\domains\account\users\names\<AccountName> names.reg
Extracted registry key that contains all details and settings for the user account	reg export hklm\sam\sam\domains\account\users\<Account RID Hex Value> users.reg

Table 2. Behavior and commands of extracting registry keys related to accounts

Afterwards, the threat actor deletes their account and adds the registry key again using the previously extracted REG file. By going through this process, the account will not appear in commands and tools that check the account list in the system. However, unlike other methods, if the system is rebooted, the 'Local Users and Groups' in Computer Management will be able to search the account again, allowing the account status to be checked.

The account created using the above method cannot be completely hidden. However, the threat actor's behavior can be interpreted as intending to minimize account exposure and maintain persistence.

Category	Subcategory	Account verification status	
		Registry before re-registration	Registry after re-registering
Control Panel	User Account	O	X
Computer Management	Local Users and Groups	O	X
Command prompt (cmd)	net user command	X	X
PowerShell	Get-LocalUser command	O	O
WMIC	useraccount command	O	O
Registry editor	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	X	X
	HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users	O	O

Table 3. Comparison of the methods to check the account list and whether the account can be checked before and after reboot

MD5

b500a8ffd4907a1dfda985683f1de1df