Malware Trend

Statistical Report on Malware Targeting MS-SQL Servers in Q1 2024

Apr 05 2024

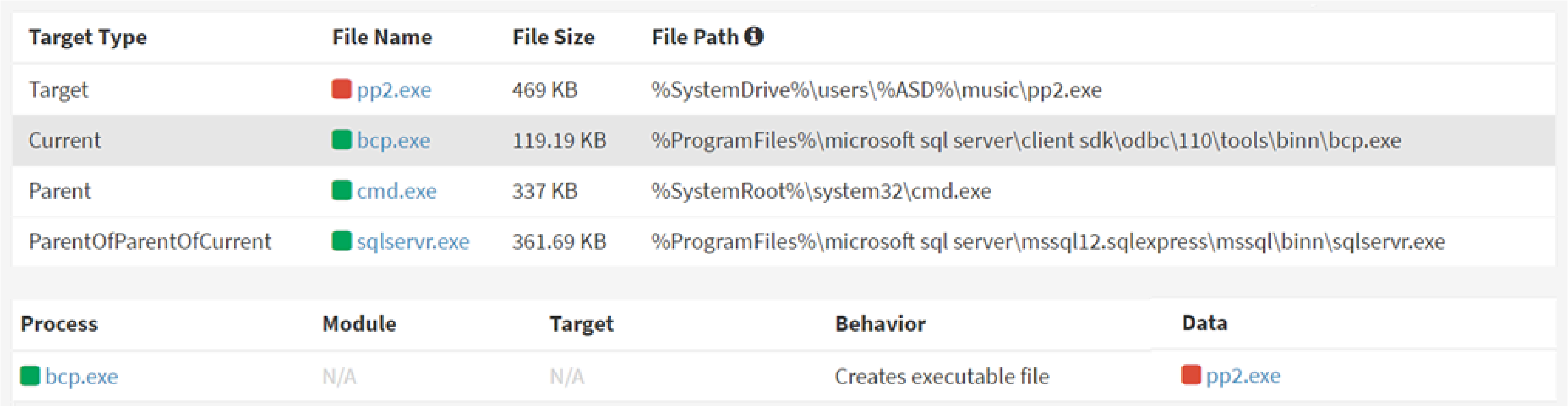
Overview

The ASEC analysis team uses the AhnLab Smart Defense (ASD) infrastructure to categorize and respond to attacks on vulnerable MS-SQL servers. This report will cover the current state of damage to MS-SQL servers which have become the target of attacks based on the logs discovered in Q1 2024, and also discuss statistics on the attacks launched against said servers. Furthermore, the malware used in each attack will be categorized with a summary of the statistical details. Malware strains are categorized by type, such as CoinMiner, backdoor, Trojan, ransomware, and HackTool, and detailed statistics are also given for known malware in each category.

Trigona ransomware attacks were newly identified in Q1 2024. The Trigona ransomware operator has been launching attacks against poorly managed MS-SQL servers since around 2022. However, the recently identified attacks were notable in that they also used Mimic ransomware and abused the bulk copy program (BCP) utility of MS-SQL servers.

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 files. Recently, some have been abusing SQLPS, a PowerShell tool included in SQL servers. However, in this attack case, the threat actor employed the method of saving their malware strain 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 1. Creating malware using BCP

Statistics

1. Attacks Against MS-SQL Servers

The following statistics are based on the ASD logs for MS-SQL server-targeted attacks confirmed during the first quarter of 2024.

AhnLab TIP
Stay Ahead of Rapidly Evolving Threats
Make the Best-Informed Decisions
Get Started with AhnLab's State-of-the-Art Threat Intelligence
atip.ahnlab.com

Tags: 통계 MS-SQL

Previous Post

"Totally Unexpected" Package Malware Using Modified Notepad++ Plug-in (WikiLoader)

Next Post

Threat Trend Report on APT Attacks (South Korea) – March 2024 Major Issues on APT Attacks