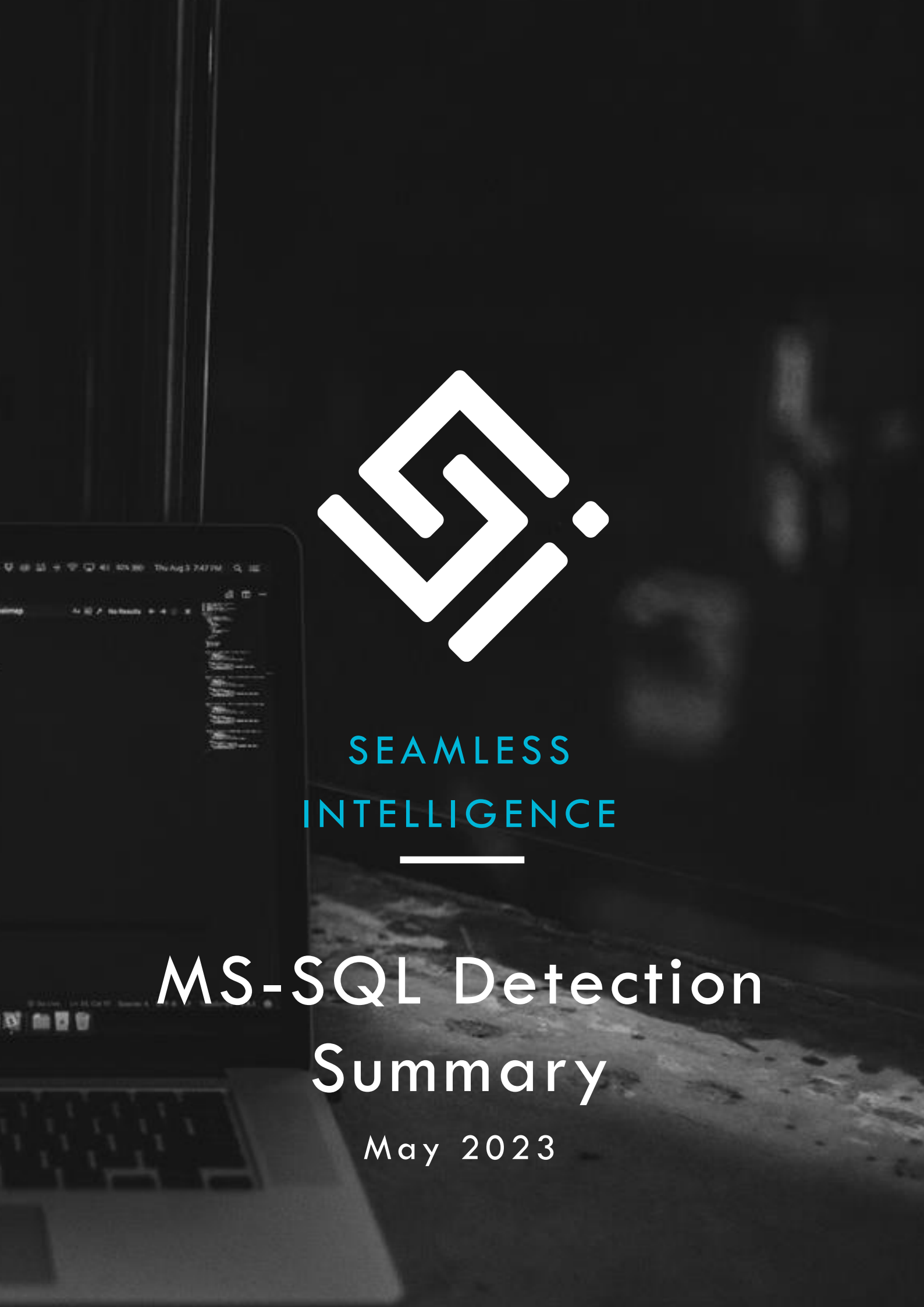

SEAMLESS
INTELLIGENCE

MS-SQL Detection Summary

May 2023

DETECTION SUMMARY

Below is the first phase of malicious activity detections built as part of the Seamless Intelligence MS-SQL logging research.

Detection name	Description	ATT&CK Tactic	Reference
Database - Config Changed - sp_configure - ole automation	Detects when a stored procedure is used to change the configuration of OLE Automation which can allow an attacker to execute commands from the database.	Server Software Component	https://github.com/NetSPI/PowerUpSQL
Database - Config Changed - sp_configure - show advanced options	Detects when a stored procedure is used to show or change some of the advanced configuration of a database. This can be used to see if xp_cmdshell is enabled and then enable it if needed.	Server Software Component	https://github.com/NetSPI/PowerUpSQL
Database - Config Changed - sp_configure - xp_cmdshell	Detects when a stored procedure is used to change the configuration of xp_cmdshell. This can allow an attacker to execute commands from the database into the OS	Server Software Component	https://github.com/NetSPI/PowerUpSQL
Database - Local Account Creation	Detects when an account is created within the database itself.	Valid Accounts	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Multiple Suspicious Activities - User	Detects when many related events occur that are related to database monitoring and linked to the same user.	Valid Accounts	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Priv Esc - Execute As Login	Detects when another login is impersonated. This allows an attacker to execute commands as another user for the rest of the session.	Valid Accounts	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Priv Esc - Grant Impersonate On	Detects when a login is granted the permission to impersonate another user. This could allow for an attacker to impersonate and execute commands as the 'sa' account for the duration of the session.	Valid Accounts	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Query - information_schema.tables	Detects when a SQL query is executed to return information related to all the tables in the database. A query such as this can allow an attacker to understand the structure of the database further.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql

Database - Query - master..sysdatabases	Detects when a SQL query is executed to all the database names in the database. A query such as this can allow an attacker to understand the structure of the database further.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - password_hash	Detects when a SQL query is executed to return information that contains reference to a password hash. A query such as this can allow an attacker to gather local account password hashes for cracking.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - sys.configurations	Detects when a SQL query is executed to return information related to configuration. A query such as this can allow an attacker to understand if xp_cmdshell is enabled without needing to use a stored procedure.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - sys.database_principals	Detects when a SQL query is executed to return information related to database principles which have a high privilege within the database. A query such as this can allow an attacker to understand which accounts to target for further abuse.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - sys.servers	Detects when a SQL query is executed to return information to find other linked servers. A query such as this can allow an attacker to understand which servers to target for further abuse.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - sys.server_principals	Detects when a SQL query is executed to return information related to server principles which have a high privilege within the database. A query such as this can allow an attacker to understand which accounts to target for further abuse.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - sys.syslogins	Detects when a SQL query is executed to return information to find the database login accounts and can extract the local password hashes. A query such as this can allow an attacker to understand which users to target for further abuse.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - sysjobs - Job Enumeration	Detects when a SQL query is executed to return information to find the database job details. A query such as this can allow an attacker to understand what the jobs are doing and the commands can sometimes contain sensitive information.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - sysobjects - mail	Detects when a SQL query is executed to return information to find if the email related stored procedures are enabled. If the email stored procedure is enabled the attacker can abuse it to exfiltrate data.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql

Database - Query - sysobjects - sp_OA	Detects when a SQL query is executed to return information to find if the Ole Automation Object stored procedures are enabled. If these stored procedures are enabled the attacker can abuse them to execute commands on the system.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - sysprocesses - SQL Agent	Detects when a SQL query is executed to return information to find SQL agent is running. If the agent is running then the attacker is able to abuse built in SQL jobs to execute commands on the system.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Query - sysusers	Detects when a SQL query is executed to return information related to the users in the database. A query such as this allows an attacker to understand which accounts they can target for abuse.	System Information Discovery	https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/admin/mssql
Database - Stored Procedure - add_job	Detects the usage of a stored procedure to add a job for SQL to execute. By abusing this mechanism the attacker can run commands as the context of the user running the SQL service.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - helprotect	Detects the usage of a stored procedure to query the user permissions for an object. Using this stored procedure an attacker can understand which users have rights to execute which stored procedures.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - sp_addsrvrolemember	Detects the usage of a stored procedure to add a role to a user account. By abusing this mechanism the attacker with the correct permissions will be able to assign privileges to other accounts.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - sp_add_trusted_assembly	Detects the usage of a stored procedure to add the file hash for an assembly that can then be executed by the SQL server. Using this stored procedure an attacker get the SQL server to trust a malicious DLL and then use a custom job to execute it.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - sp_add_trusted_assembly - HTTP	Detects the usage of a stored procedure to add the file hash for an assembly from a website that can then be executed by the SQL server. Using this stored procedure an attacker get the SQL server to trust a malicious DLL and then use a custom job to execute it.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - sp_execute_external_script	Detects the usage of a stored procedure to execute an external script such a R or Python. Using this stored procedure an attacker get the SQL server to execute a script they control in the context of the user account running the SQL service.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server

Database - Stored Procedure - sp_linkedservers	Detects the usage of a stored procedure to list out all of the linked servers. Using this stored procedure allows an attacker to understand which servers to target for further abuse.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - sp_oacreate wscript	Detects the usage of a stored procedure to create an automation using a VB script. Using this stored procedure an attacker can get commands executed in the context of the user account running the SQL service.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - xp_cmdshell	Detects the usage of a stored procedure to execute commands via the Command Prompt locally. Using this stored procedure an attacker can get commands executed in the context of the user account running the SQL service.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - xp_dirtree	Detects the usage of a stored procedure to list the directories of a share. Using this stored procedure an attacker can abuse SMB to leak the NTLM hash of the account running the SQL service using a tool such as Responder to capture it.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - xp_regread	Detects the usage of a stored procedure to read keys from the local Windows Registry. Using this stored procedure an attacker can gain an understanding of possible abuse paths on the server.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - Stored Procedure - xp_regwrite	Detects the usage of a stored procedure to write keys to the local Windows Registry. Using this stored procedure an attacker can change registry keys that may allow for further abuse such as the WDigest setting for abusing LSASS.	Server Software Component	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - User Bruteforce	Detects the same account unsuccessfully attempting to authenticate to the database within a short period of time.	Valid Accounts	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
Database - User Enumeration	Detects failed authentication from an excessive amount of unique usernames to a single database.	Valid Accounts	https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server