Severity

High

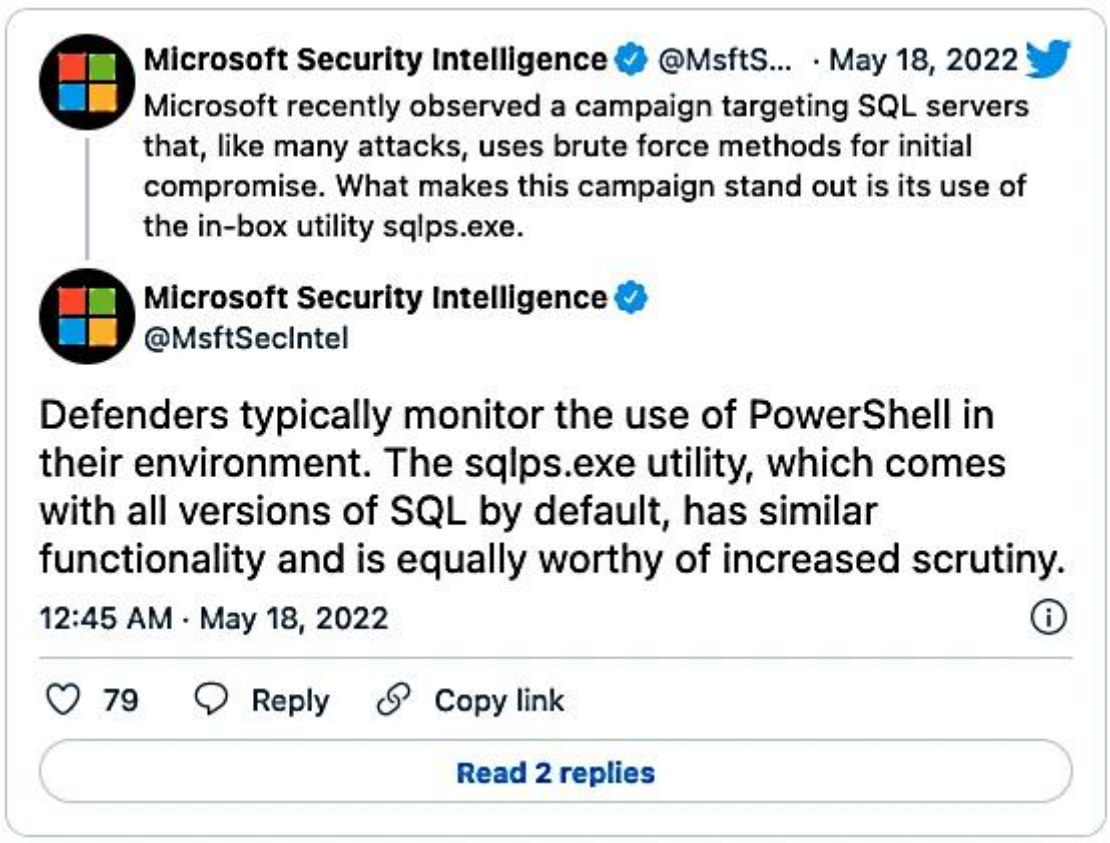
Analysis Summary

Recently, Microsoft has issued a warning on a new hacking campaign targeting MSSQL servers, in which threat actors are initiating brute-force attacks against vulnerable instances. The attacks employ the legitimate tool sqlps.exe, a SQL Server PowerShell program, as a LOLBin (short for living-off-the-land binary).

In a series of tweets, Microsoft warned about the attacks:

The attackers accomplish fileless persistence by using the sqlps.exe tool, which is a PowerShell wrapper for running SQL-built cmdlets, to perform recon commands and change the SQL service's start mode to LocalSystem. The attackers also utilize sqlps.exe to establish a new account and assign it to the sysadmin role, giving them complete access over the SQL server. They then gain the authority to perform other operations, such as deploying payloads like coin miners.

Using sqlps, a utility available with Microsoft SQL Server that allows the loading of SQL Server cmdlets as a LOLBin, allows attackers to run PowerShell commands without fear of defenders detecting their nefarious activity. It also ensures that they leave no traces while analyzing their attacks because sqlps is an excellent approach to bypass Script Block Logging, a PowerShell functionality that would normally report cmdlet activities to the Windows event log.



MSSQL servers have been targeted for years as part of massive campaigns in which threat actors seek to take control of thousands of vulnerable servers every day for various purposes. Therefore, administrators should not expose their MSSQL servers to the Internet, use a strong admin password that cannot be guessed or brute-forced, and put the server behind a firewall to protect it from such attacks.

Impact

- Information Theft
- Exfiltration Of Data

Remediation

- Passwords — Ensure that general security policies are employed including: implementing strong passwords, correct configurations, and proper administration security policies.
- Admin Access — limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- WAF — Web defacement must be stopped at the web application level. Therefore, set up a Web Application Firewall with rules to block suspicious and malicious requests.

- Patch — Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Secure Coding — Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- Apply the latest security updates to decrease the attack surface and block attacks leveraging exploits that target known vulnerabilities