Scattered Spider Threat Actor Profile - Quorum Cyber

Archived: 2026-04-05 13:29:07 UTC

Scattered Spider (also known as UNC3944 and Roasted 0ktapus) is a relatively new, financially motivated threat group that has been active since at least May 2022. The group is yet to receive a Microsoft designation but will fall into the Tempest (financially motivated) category once registered. The group commonly gains initial network access via stolen credentials obtained from SMS phishing operations and have been detected utilising Azure Serial Console to attain administrative console access to virtual machines (VMs) whilst executing a command prompt over the serial port.

Scattered Spider are reported to use a loader named ‘STONESTOP’ to install a malicious signed driver dubbed ‘POORTRY’, which is designed to terminate processes associated with security software and to delete files as part of a Bring Your Own Vulnerable Driver (BYOVD) attack. The group has been attributed to creating the STONESTOP and POORTRY toolkit to terminate security software.

Historically, Scattered Spider has mainly gained initial access to the victim environment via theft of administrative credentials by email and SMS phishing attacks or the use of stealware. Once credentials have been obtained, Scattered Spider use these to impersonate the admin and use sensitive data to gain access to the environment. Furthermore, they have also been observed continuing phishing attacks against other users, by leveraging the employee database. This is likely to maintain persistence and provides them with lateral movement within the network.

Source: https://www.quorumcyber.com/threat-actors/scattered-spider-threat-actor-profile/