



Hacker erpressen Besitzer von Qnap-NAS mit Ransomware Qlocker

(Quelle: Qnap)

26. April 2021 - Rund 260'000 US-Dollar sollen Cyberkriminelle bereits von Besitzern eines NAS von Qnap erpresst haben. Dafür setzen sie die Ransomware Qlocker ein und verschlüsseln die Dateien auf dem NAS mit dem Komprimierungstool 7zip.



Bereits im März forderte **Qnap** die Besitzer seiner NAS-Produkte auf, aktuelle Firmware auf ihren Geräten zu installieren, weil zwei Sicherheitslücken Angreifern Zugang zum NAS gewähren könnten ("Swiss IT Magazine" **berichtete**). Nun berichten verschiedene Medien, dass Hacker offenbar die Ransomware Qlocker einsetzen, um die Besitzer eines NAS von Qnap zu erpressen (**via** "Bleeping Computer"). Auf diese Weise sollen sie binnen weniger Tage bereits 260'000 US-Dollar erpresst haben. Betroffen sind vor allem kleine und mittlere Unternehmen, aber auch Privatpersonen.

Das Vorgehen der Hacker ist dabei relativ simpel. Sie schleusen über die Lücken in der Firmware von Qnap eine Ransomware namens Qlocker auf das Gerät, und diese verschlüsselt dann die Dateien der Opfer mit dem frei erhältlichen Komprimierungstool 7zip und einem Passwort. Um rasch an das Geld zu kommen, verlangen sie kleinere Summen in Bitcoin, normalerweise rund 500 US-Dollar. Besitzern eines NAS von Qnap wird deshalb dringend geraten, eine aktuelle Firmware aufzuspielen, in der die Sicherheitslücken nicht mehr vorhanden sind. (luc)

