Severity

Medium

Analysis Summary

Quasar virus is a Remote Access Trojan (RAT) that is often abused by cybercriminals to take remote control over users' computers for malicious purposes. Exploiting a path traversal vulnerability of WinRAR, a Molerats spear-phishing campaign is discovered. It is suspected that a Gaza Cyber gang group is behind the campaign. In the first step, the victim installs a downloader in their operating system which then gets infected with a RAT (Quasar). The downloader typically first tries to connect to a geolocation domain and then the RAT is downloaded.

Impact

- Data Theft
- Exposure of Sensitive DatA

Indicators of Compromise

MD5

b4864ef86be2c148c18b1a960f3ca3fc d602ab124b403aa3898d171dc6daae8e

SHA-256

c1e3245d0374cf5d3970377d8252ce9b707991a220759f153c4dba34de2e49bd
02a687dd88c2f28be215280db64000d830708f51ac9c7d215216813bf159e2be

SHA-1

5bfd398f7e64f39ebbcda4f25dd213ccd0199587 919b1c2b70eb059ad1b0278fc7bf40ef5e12e326

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.