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

- 28a7893757c09322c01043d505ecfc11

SHA-256

- 92364e7c1bb87d1a954ffe89c6b6b1dba163626c11607a69f970337d49597f67

SHA-1

- ca713137c995aac0dd91046bb5a1a498d5c64055

Remediation

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