Rewterz Threat Alert - Evilnum APT Group Targeting Financial Sector - Rewterz

Published: 2020-12-23 · Archived: 2026-04-05 17:45:12 UTC

Severity

High

Analysis Summary

APT group Evilnum aka Jointworm has been seen targeting financial sector with malicious emails. The group first seen in 2018 with the motivation of information theft and espionage has been active recently in attempt to rob users off their credentials and gaining sensitive information for their gain. The group has primarily targeted fintech organizations based in Israel. These attacks have possible relationship between Cardinal RAT and another malware family named EVILNUM. EVILNUM is a JavaScript-based malware family that is used in attacks against similar organizations.

Impact

- Information theft
- Exposure of sensitive data

Indicators of Compromise

Filename

- Account compliance[.] zip

MD5

- 178c15b02451a29f3bed0a068adc2049

SHA-256

- 3c7def980dfdebc0e03d8a3d3e2ee8367268ea676050e767e3c6ad77b8f9219e

SHA1

- 93f5b77065216f6d1eebed5ee3fe1b56937d9835

URL

- http[:]//community-approch[.]com/

Remediation

- Block all threat indicators at your respective controls.
- Always be suspicious about emails sent by unknown senders.
- Never click on links/attachments sent by unknown senders.
