## Severity

High

## Analysis Summary

APT-17 group aka BITTER APT group has been recently active and targeting sectors in South Asia for information theft and espionage. This group has a history of targeting Energy, Engineering, Government in South Asia. Spear phishing emails have been the main strike force to target their victims and they've been doing it for years now. Many BITTER victims have been exploited through relatively popular Microsoft Office exploit, in order to download and execute a RAT binary from a website. Although the attack vector of this sample remains unknown of yet, this is an indication of their presence again in the South Asian region.

## Impact

- Information Theft and Espionage

## Indicators of Compromise

### MD5

- c66a35a9c1778ab162e3718afbd8c3ac

### SHA-256

- a979c76afd0e9d2e135ca64a215e1af270222d059d806e7028022060e8cbe72c

### SHA-1

- a32e7a0a0ec97ba0e42d8bb19462a678374731f1

## Remediation

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