Severity

High

Analysis Summary

APT36, just like many other threat actors, is capitalizing on fear, compromising victims with scams or malware campaigns. APT36 is using a decoy health advisory document to spread a Remote Administration Tool (RAT). The group is also called Transparent Tribe, ProjectM, Mythic Leopard, and TEMP.Lapis. APT36 mainly relies on both spear phishing and watering hole attacks to gain its foothold on victims. The phishing email is either a malicious macro document or an rtf file exploiting vulnerabilities, such as CVE-2017-0199. In the coronavirus-themed attack, APT36 used a spear phishing email with a link to a malicious document masquerading as the government of India.

The malicious document has two hidden macros that drop a RAT variant called Crimson RAT. The malicious macro first creates two directories with the names “Edlacar” and “Uahaiws” and then checks the OS type.

Crimson RAT’s capabilities include:

- Stealing credentials from the victim’s browser
- Listing running processes, drives, and directories on the victim’s machine
- Retrieving files from its C&C server
- Using custom TCP protocol for its C&C communications
- Collecting information about antivirus software
- Capturing screenshots
-

Impact

- Credential Theft
- Unauthorized Remote Access
- Code Execution
- Possible Security Bypass
- Information Theft

Indicators of Compromise

MD5

- eda714cb2dd474bb4607710a6e9bac61
- 7a195036865fdbfd31c555fd78ee60c9
- bfb3b66718d6b8ece139481325710321
- e7d7bd8a20f6b5f9e62de008cbfcdfc0

SHA-256

- 1e0fe0c057163e5cc1a2598b7de1adf06db8bfe814e172557383eea3acbf9a2b
- 5091ca8bcfee8d3980700de91d3b1f6286420f85be9069bde944ffceac2b02fd
- b53e73189ad4db83a5891d0dd73fd86d290fb7de8ab9378a1b9f29cddfc14d8c
- b9e1c9e0e8a169b7055d39720b862782922090f0a08cf73de730e2e6ce73eac8

SHA-1

- 1772280afd0b49bdc07a2d09095e9b19995e3494
- c5063ff9d9a0aba85769d80ca306c4843efd5b30
- ef3791dc929cda94489d27155a253ec14b9513b4

- e3d5be717b98b6e532c7390abe9ea3c0b0f5c008

Remediation

- Block the threat indicators at their respective controls.
- Do not respond to unexpected emails from untrusted email addresses.