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

- 4eb0d5dc174a8d3643d60ad2047a20a7
- 22a8ff8eb7aa7e68c634bd7937e3b915
- ef94d698e4995fed1873f60d3c986ba9

SHA-256

- 3d698b828bad59f2697ab4a8ce2163da14ab6a81a45544212476f48e03c7ae4a
- 2d3d04833b15cb8fd319a112021526bee32d91124c5c2963bc575819ca8ab3e0
- c344b69876c07fe5d9e96a556ab7fb636a92521a8471c526010ab7d49aee7573

SHA-1

- ba069d89d6f02afc5f2c51164766be2171820183
- 49755b332d89176e468c8b85745b5349e1d9eaad
- c136c194e6b1708d0c01327a172a1c8efde18c99

Remediation

- Block the threat indicators at their respective controls.

- Do not respond to unexpected emails from untrusted email addresses