Severity

High

Analysis Summary

Emotet was initially discovered in 2014 when it infected clients of German and Austrian institutions. Emotet serves as a downloader for other malware variants like TrickBot, QakBot, and IcedID. Phishing attempts are the most common way to propagate emotet trojan, which employs an email with malicious links or Macro-embedded Microsoft Word files. It has mostly been used to attack the banking industry. Emotet can launch several malware payloads depending on the target system after deployment. Emotet is frequently used as a downloader for other malware and is a particularly common delivery method for banking Trojans such as Qakbot and TrickBot. Emotet can steal data such as saved user passwords on the browser by eavesdropping on network traffic. Its modules focus on credential theft, email theft, and spamming.

Impact

- Credential Theft
- Information Theft
- Financial Loss

Indicators of Compromise

IP

- 138[.]201[.]142[.]73

MD5

- 3952caf999263773be599357388159e0

SHA-256

- 09f44c33ba0a5f1e22cd5b8b0d40c9808e2668ee9050ac855a6ae0744bc9e924

SHA-1

- 76c39a3a4823beab79e497bfcdbc2367188d95c4

URL

- http[:]//focusmedica[.]in/fmlib/IxBABMh0I2cLM3qq1GVv/

Remediation

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