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.

Emotet spreads by email phishing attacks, which transmit malicious emails from infected PCs. The emails can take a variety of forms, including plain text emails with no context or responses to stolen email threads. In most cases, the emails include an Excel/Word attachment, a password-protected zip file, or a link to download the document. But on April 22, researchers discovered Emotet employing LNK files instead of the normal Excel files, indicating that the threat actors are attempting to enhance their techniques in order to maximize the success rate of their infections.

Impact

- Credential Theft
- Information Theft
- Financial Loss

Indicators of Compromise

IP

- 1[.]234[.]21[.]73
- 1[.]234[.]65[.]61
- 101[.]50[.]0[.]91
- 103[.]132[.]242[.]26
- 103[.]133[.]214[.]242
- 103[.]134[.]85[.]85
- 103[.]221[.]221[.]164
- 103[.]221[.]221[.]247
- 103[.]253[.]145[.]28
- 103[.]30[.]145[.]119
- 103[.]41[.]204[.]169
- 103[.]42[.]57[.]17
- 103[.]42[.]58[.]120
- 103[.]43[.]46[.]182
- 103[.]44[.]138[.]22
- 103[.]56[.]149[.]105
- 103[.]70[.]28[.]102
- 103[.]75[.]201[.]2
- 103[.]75[.]201[.]4
- 103[.]8[.]26[.]102
- 103[.]8[.]26[.]103
- 103[.]82[.]248[.]59
- 103[.]85[.]160[.]5
- 104[.]131[.]11[.]205
- 104[.]131[.]62[.]48

- 104[.]168[.]154[.]79
- 104[.]168[.]155[.]129
- 104[.]245[.]52[.]73
- 104[.]251[.]214[.]46
- 104[.]251[.]215[.]148

Remediation

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