Threat Intelligence Report

Summary

1. On the 25th of October 2019 an unknown sample was observed
2. Initial investigation reveals that the inital attack vector was phishing
3. Analysis has been conducted, artifacts of the analysis can be found in the following section of this document

Analysis artifacts

- Date: 25.10.2019
- SHA256 of the sample: `6de788187b9a790f0a378b94f02582e1453d4f77f5ac4c742c7ffc4bef0ea157`
- During dynamic analysis of the sample following distribution urls were found
  - `https://mokhoafacebookvn.com/wp-content/themes/lalita/Kj6VMJsiof/`
  - `http://newgensolutions.net/joomla_30/n0k0/`
  - `https://sodadino.com/wp-admin/gczk/`
- Initial reverse engineering of the sample revealed that it's a known malware that belongs in the `emotet` family
- Another artifacts you were able to extract are the ips that the sample is connecting to during execution
  - `47.100.43.55`
  - `66.228.39.137`
  - `108.58.41.242`
  - `104.199.245.51`
  - `104.18.60.46`