Severity

High

Analysis Summary

QBot, often known as QakBot, is modular information malware. It has been operational since 2007. This banking Trojan, QakBot steals financial data from infected systems, and a loader using C2 servers for payload targeting and download. Qakbot has worm capabilities, which let it propagate to other computers on the same network, as well as rootkit capabilities, which allow it to mask its existence and build persistence on infected computers.

A malware attachment to a phishing email is commonly used in QakBot attacks. This particular campaign includes an xls file that contains macros. These macros run a script that fetches the Qakbot payload from a list of URLs. To get the victim to activate macros, the attackers employ a common trick, like when the target downloads the file, it is asked to allow changes and then content before viewing the document.

Impact

- Unauthorized Access
- Financial Theft
- Information Theft

Indicators of Compromise

IP

- 192[.]254[.]236[.]149
- 192[.]254[.]234[.]63
- 66[.]29[.]136[.]162

MD5

- f22ba4294963318d789b32900ab4e151

SHA-256

- 6e90fd1e2d004819c5b3052ae3bdc56f014e2dc37e2cba9665502f339b351c2e

SHA-1

- f6a42b001101d541abe3090cd8f8c38b212763fd

Remediation

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