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

MD5

- 7d1c096cba6d86a3d75727af5fa28c62
- fe61080715e97b623082d86305828bd2

SHA-256

- 936762ac61ecd3ed975e97c2f8f328f62ecbc4ee2ef79c82943226a911751cc1
- f0fc0e1700296e299a34707361b859d20a07b147da4b0c1c0401696d655fd605

SHA-1

- 3faf5cd7a3e3e9787dda9517992aa3227b02cae8
- e50bfb7820c52202c65c0e65139310dd374f0bb8

Remediation

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