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

- 3193bcc62484eb3a2896fd31088ff220
- 35d6a3b193d8de78a4e7843ca17c2cc1
- 3afb9b66d3be7744862ae569e0b97a58
- 53854751a580f6791c7cb4344d46c0d8
- 597083912f39f1831b62d9e5b9762d4a
- c43fd2dc05b3ff2d5bd49c1e7f3eca64
- cf7bdabc4bae60831fe8691ae1521f7e
- ea6f6914f5014945b4069a80057da78b

SHA-256

- f4020e0173456d06a84a5c904293c8a2d4abf6a92929bc69eefd85e8527fe0d0
- b3eec596547bbed4af412d7671a339606e0459791d4c04939360f422a62665a5
- 25346c40d4e9b875ce5489a73325eee13c658c6fc9c39d64f09c0abd246d18ee
- d43490594399133ade4938d033261d0b4cdd12900a27c8e3c9bfbb8bfa17ce0e
- 7f807ad12de97f05be91de2a517bb64e368b20d6e1fc95ca505b13bc12a88046
- 954d66a8fb0d8c25b9ae2a6a851b2a0b33bae3687c3c5a3ed44c8bb485d9955a
- a853f326d1b2dda5f082450dee003549f33bddbf4c5c9c81bb2acf50d8864cab
- e81645c9b65130210f894441c47eaa173af8e8efe1eae12ffd49e6297fb7bf12

SHA-1

- 0b1c39c6385fc5be95dc29dc6980f78a47b5109f
- 8a8dc89ba0e9fa89a1b4398787a0bbc9e970adf2
- 7797ca442624d7bef8c472d75006f2cce1027a40
- c7161d8604f08ececebcc520a9db0ac807b9d943
- 15cd99890296ea5b5efdb6593adaa68a19f0df47
- a6ad7b53e527b4bd9616bcd66622d5fbdee7fb6b
- 007d9443e716974c3b005a036b5ac03cb1a9e2b4
- 3a55e317088b62ff8f4dbe0ce392b2e94d501dd7

Remediation

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