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

- c881b5ffdc8a66792a004afbf64e4791
- 0364b9434b216fa03785a4b60beca637
- 982145ff1392a8ea4dcabb5ea2f66e89

SHA-256

- f9272801e9f70757819b7d49ebd1b09ec846c1119026aacf5e1ea7f7a77e9125
- 31aff7c4ab72817fc99d95cdde8fb48ff743a92b717a13835ce6410d126a7e0e
- 8a383f890745370e6f256396858a94062600f1efd2d1df36ef8a291e41494277

SHA-1

- de131619139e5a13fdd1e00b453bfb7d61656dc1
- 9ad994ad01a5a66e04b723a47e81981149f14894
- 336b1763a1c6bc0091a2abb4eb1d9ef3adfb9547

URL

- http[:]//meumundocatolico[.]com[.]br/pla/xmmuite
- http[:]//meumundocatolico[.]com[.]br/pla/U1810259023[.]zip
- https[:]//smartleasesonora[.]com/yVuL6RYk/EW[.]png

Remediation

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