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

- 2e349a1aecdb29b80e60b609a78f0373
- 781fe6f211a064529646aa862fddf627
- 91b2ee2ffa2661cf9905520d55988f54
- 239063e0fdfd1c3620724330a7b0ecda
- 7a3c40282328433e08e52f4436b55fac
- 09f71e7d509184ef6babe6a2463f7bfd

SHA-256

- 791b070589eb4484261f3a79ae0a88d7123222cee014cb36d93e323fade9cc00
- d374174ffdc62d52993c64fa29145a9868a25f2d7db5fe631feb9cedf8235167
- c802b9ab9914602a57b3e4e8ce02abc297067bb95c1db14eb9a5a998dba281ed
- 0fd024bc7f0ee27219014d30b74c0c602e60a946b8e962e37366d424bc6e9cd1
- eae8729b153d2802f2c8d788ee1224baee8b25ead50d76253ae5730f91fa169f
- b44ff94810d92c518d61ed33f4cf4161968802a0c4f599c6eb938d76b77df5fb

SHA-1

- f9e8e07542a1e6dcdaae9f1a62c401069d832d77
- d442b9bf87586667b71698535f3856ae55805f5f
- a39187b307655be681ca3779c6e26d2bd7144de0
- 1b5015c03553ff4fe6e016a8e35f2c1f2c48c1e8
- f463b433ef60b82477654664e62b7f8363c8ace5
- 258ed123eab99bf2cc60011f96c33e4efd8b2ef1

URL

- http[:]//162[.]19[.]135[.]167/599785764[.]dat
- http[:]//138[.]124[.]184[.]233/599785764[.]dat
- http[:]//188[.]165[.]62[.]1/599785764[.]dat

- http[:]//162[.]19[.]135[.]167/718523242[.]dat
- http[:]//138[.]124[.]184[.]233/718523242[.]dat
- http[:]//188[.]165[.]62[.]1/718523242[.]dat

Remediation

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