CANSOL CONSULTING

TECHNICAL ANALYSIS OF THE QAKBOT BANKING TROJAN

Threat Advisory

https://t.me/learningnets

Summary

QakBot, also known as QBot, QuackBot and Pinkslipbot, is a banking Trojan that has existed for over a decade. It was found in the wild in 2007 and since then it has been continually maintained and developed. In recent years, QakBot has become one of the leading banking Trojans around the globe. Its main purpose is to steal banking credentials (e.g., logins, passwords, etc.), though it has also acquired functionality allowing it to spy on financial operations, spread itself, and install ransomware in order to maximize revenue from compromised organizations.

To this day, QakBot continues to grow in terms of functionality, with even more capabilities and new techniques such as logging keystrokes, a backdoor functionality, and techniques to evade detection. It's worth mentioning that the latter includes virtual environment detection, regular self-updates and cryptor/packer changes. In addition, QakBot tries to protect itself from being analyzed and debugged by experts and automated tools. Another interesting piece of functionality is the ability to steal emails. These are later used by the attackers to send targeted emails to the victims, with the obtained information being used to lure victims into opening those emails.

The infection chain of recent QakBot releases (2020-2021 variants) is as follows:

- The user receives a phishing email with a ZIP attachment containing an Office document with embedded macros, the document itself or a link to download malicious document.
- The user opens the malicious attachment/link and is tricked into clicking "Enable content".
- A malicious macro is executed. Some variants perform a 'GET' request to a URL requesting a 'PNG' However, the file is in fact a binary.
- The loaded payload (stager) includes another binary containing encrypted resource modules. One of the encrypted resources has the DLL binary (loader) which is decrypted later during runtime.
- The 'Stager' loads the 'Loader' into the memory, which decrypts and runs the payload during runtime. The configuration settings are retrieved from another resource.
- The payload communicates with the C2 server.
- Additional threats such as ProLock ransomware can now be pushed to the infected machine.

https://t.me/learninghets

Detection Date	Category	Severity
2021-09-02	Trojan	**High**

Impact

- Information Theft and Espionage
- Data exfiltration
- Data Obfuscation
- Unauthorize Access
- Exfiltration Over C2 Channel
- OS Credential Dumping
- Email Collection

IP

- 98.252.118.134
- 98.192.185.86
- 97.69.160.4
- 96.61.23.88
- 96.37.113.36
- 96.253.46.210
- 96.21.251.127
- 95.77.223.148
- 92.96.3.180
- 92.59.35.196
- 90.65.234.26
- 89.137.211.239
- 86.236.77.68
- 86.220.60.247
- 84.72.35.226
- 83.196.56.65
- 83.110.9.71
- 83.110.109.155
- 83.110.103.152
- 82.12.157.95
- 81.214.126.173
- 80.227.5.69

https://t.me/learninghets

- 78.97.207.104
- 78.63.226.32
- 77.27.207.217
- 76.94.200.148
- 76.25.142.196
- 76.168.147.166
- 75.67.192.125
- 75.188.35.168
- 75.137.47.174
- 74.68.144.202
- 74.222.204.82
- 73.25.124.140
- 73.151.236.31
- 72.252.201.69
- 72.240.200.181
- 71.74.12.34
- 71.63.120.101
- 71.41.184.10
- 71.199.192.62
- 71.187.170.235
- 71.163.222.223
- 70.168.130.172
- 70.163.161.79
- 69.58.147.82
- 68.204.7.158
- 68.186.192.69
- 67.165.206.193
- 64.121.114.87
- 59.90.246.200
- 50.29.166.232
- 50.244.112.106
- 47.22.148.6
- 47.196.213.73
- 46.149.81.250
- 45.77.117.108
- 45.77.115.208
- 45.67.231.247
- 45.63.107.192
- 45.46.53.140
- 45.32.211.207
- 31.4.242.233
- 27.223.92.142
- 24.95.61.62
- 24.55.112.61

https://t.me/learninghets

- 24.229.150.54
- 24.179.77.236
- 24.152.219.253
- 24.139.72.117
- 24.122.166.173
- 222.153.122.173
- 217.133.54.140
- 216.201.162.158
- 213.60.147.140
- 213.122.113.120
- 209.210.187.52
- 207.246.77.75
- 207.246.116.237
- 202.188.138.162
- 202.185.166.181
- 2.7.116.188
- 197.45.110.165
- 197.161.154.132
- 196.221.207.137
- 196.151.252.84
- 195.43.173.70
- 195.12.154.8
- 193.248.221.184
- 189.222.59.177
- 189.210.115.207
- 189.146.183.105
- 188.27.179.172
- 187.250.238.164
- 186.154.175.13
- 186.144.33.73
- 184.185.103.157
- 175.143.92.16
- 174.104.22.30
- 173.21.10.71
- 172.78.59.180
- 156.223.110.23
- 151.205.102.42
- 149.28.99.97
- 149.28.98.196
- 149.28.101.90
- 144.202.38.185
- 144.139.47.206
- 144.139.166.18
- 142.117.191.18

https://t.me/learninghets

- 140.82.49.12
- 136.232.34.70
- 125.63.101.62
- 125.62.192.220
- 122.148.156.131
- 109.12.111.14
- 109.106.69.138
- 108.46.145.30
- 106.250.150.98
- 105.198.236.99
- 105.198.236.101

Reference

- https://securelist.com/qakbot-technical-analysis/103931/

Remediation

- Sweep the above-mentioned IOCs in your environment.
- Block all indicators on their respective control environment.

https://t.me/learninghets