Operation ‘Duck Hunt’ brings down Quackbot

Daniel Iwugo
3 min read · 1 day ago

Ducks ¦ Credit: Pixabay

Yeah, you read the title correctly. On the 29th of August, 2023, the Federal Bureau of Investigation announced that they and other International law enforcement agencies had brought down the infamous Quackbot botnet.

The Malware

Quackbot (more commonly known as Qakbot) is a malware operated by the threat group GOLD CABIN and has been active since at least 2008. The botnet initially started off as a banking trojan delivered via phishing, but has evolved since to create a very functional diverse botnet.

The malware works by being first delivered as an attachment or link in a phishing mail. Once the victim opened the attachment, the malware was installed, making the infected system part of a large network of zombie computers.

Some of the botnet's features include the following:

- Credential theft
- Spam delivery
- Web traffic manipulation
- Remote access
- Network enumeration
- Payload delivery

The botnet has been notably used in incidents related to Conti, REvil, and Black Basta. It has infected over 700,000 systems, with 200,000 of those in the United States alone. The infected systems include those used in financial, emergency, and commercial services, as well as election infrastructure.

The Operation

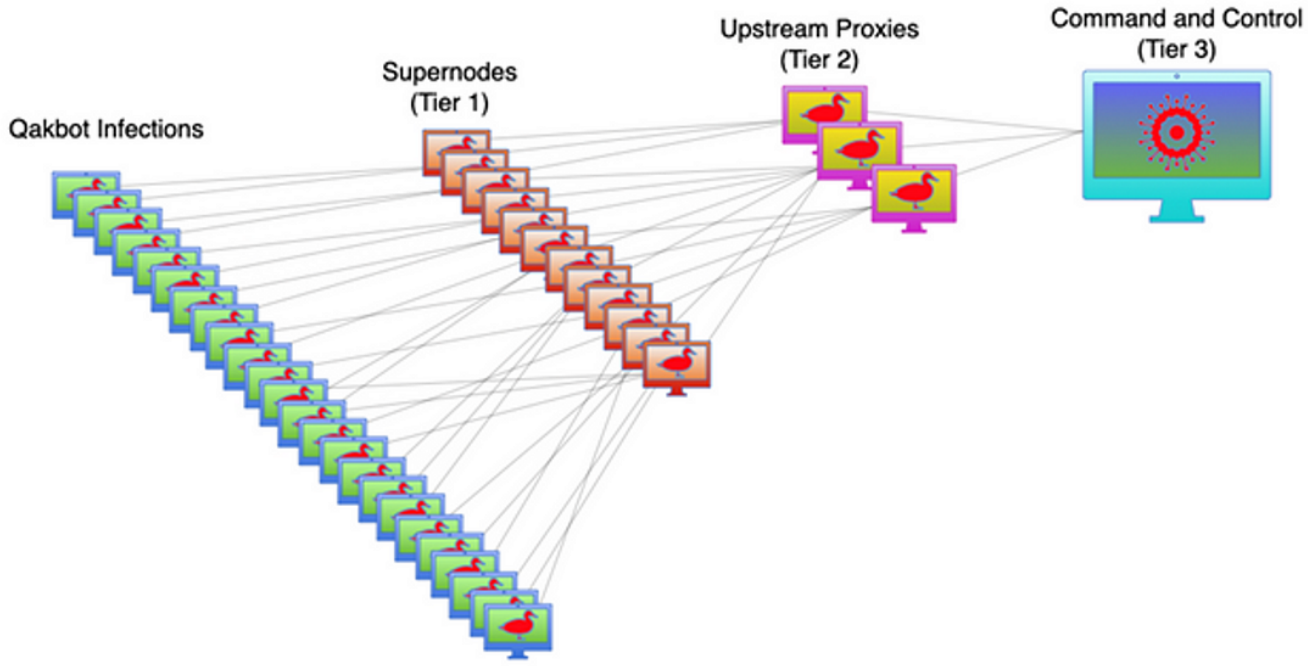
At 11:37 pm UTC on August 25, researchers at Secureworks CTU observed the takedown. The botnet suddenly turned on it's initial instructions and sent code to terminate the running Qakbot process. The researchers also noticed that the initial Command and Control Servers (C2) had stopped responding and were replaced.

Four days later, the FBI announced that an international operation had been carried out to dismantle the botnet. Countries involved were the United States, France, Germany, the Netherlands, Latvia, Romania and the United Kingdom.

According to documents related to the operation, the FBI first accessed servers hosting the botnet, which were owned by an unnamed company. Next the servers were duplicated to avoid any suspicions on the side of the botnet administrators.

While investigating they discovered virtual machines for testing malware, servers for phishing campaigns, and even crypto wallets containing stolen funds.

Before we continue, you need to understand the botnet a bit better. Below it a graphical representation of it.



The Qakbot Structure ¦ Credit: CISA

Infected computers communicate with Tier 1 Supernodes, located in the US. Supernodes are frequently changed systems used to directly control the zombie computers, which in turn direct their traffic to Tier 2 Proxies. These proxies serve as a protection layer, that directly communicate to the main Tier 3 C2 server.

According to the analysis by Secureworks, the takedown occurred by taking over the Supernodes, then directing their traffic to the FBI owned servers, away from the proxy servers. Next, the FBI servers instructed the infected devices to download an uninstaller to remove the initial Qakbot infection. While this did not remove other dropped malware, it did avoid further Qakbot infections.

What now?

While you may not be a part of a botnet right now, it is important to know how to prevent that situation in the first place. Here are some suggestion:

- Regularly update software

- Use strong passwords and enable 2FA where possible
- Install Antivirus software
- Be careful handling emails with red flags
- Stay cyber aware with Mercurysnotes 🙃

Qakbot Botnet FBI International Mercurysnotes

Edit profile

Written by Daniel Iwugo

120 Followers

Just another guy fascinated by the world of Hacking, Cybersecurity and the Internet.

More from Daniel Iwugo