Qakbot Botnet Disruption

shadowserver.org/news/qakbot-botnet-disruption/

August 29, 2023

On Tuesday 29th August 2023, the US Department of Justice (DoJ) and US Federal Bureau of Investigations (FBI) – along with law enforcement partners in France, Germany, the Netherlands, and the United Kingdom – announced a disruption action against the very long running **Qakbot** botnet.

Qakbot (also known as QBot, Pinkslipbot, Quakbot and Oakbot) has been active since around 2007, having initially been developed as information stealer and banking trojan malware, before later becoming primarily a distribution network for other malware/ransomware. See Malpedia's timeline for more information about its lengthy evolution.

In recent years, Qakbot has been used as an initial infection vector by many ransomware groups including Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta. This has likely enabled significant financial losses globally.

The outcomes from the coordinated law enforcement action included:

- deleting the Qakbot malware from infected victim computers (to reduce the risk of further harm)
- taking down the Qakbot technical infrastructure
- seizing $8.6M of alleged illicit cryptocurrency profits.

As part of the takedown, the FBI was able to gain access to Qakbot infrastructure and identify over 700,000 computers worldwide that appear to have been infected with Qakbot, including more than 200,000 in the United States. To disrupt the botnet, the FBI was able to redirect Qakbot botnet traffic to and through servers controlled by the FBI, which in turn instructed infected computers in the United States and elsewhere to download a file created by law enforcement that would uninstall the Qakbot malware – thus preventing additional malware from being deployed on victim systems in future.

More detailed information is available in the DoJ court documents, including the hash of the Qakbot Uninstall file (SHA-256 *7cdee5a583eacf24b1f142413aabb4e556ccf4ef3a4764ad084c1526cc90e117*) and associated search warrants. Independent technical analysis of observed deletion activity was reported by Secureworks.

The scope of this law enforcement action was limited to information installed on the victim computers by the Qakbot actors. It did not extend to remediating other malware already installed on the victim computers and did not involve access to or modification of the information of the owners and users of the infected computers. **It is therefore important that anyone who is notified that they might have been infected with Qakbot also looks for and remediates other malware infections that are likely also running on the same computer**. Even after the removal of Qakbot, they **may still be infected with other malware and be a part of other botnets, so at risk from cybercriminals**.

The Shadowserver Foundation is happy to support our law enforcement partners and private sector in this major cybercrime disruption operation. We are currently analyzing the collected data and will soon issue a **Qakbot Special Report** for National CSIRTs and network owners, to help notify and remediate any remaining victims.

If you do not already subscribe to Shadowserver's free daily network reports, which contain many unique cyber threat intelligence data feeds not available elsewhere, please subscribe here now. In the meantime, you can contact us with any questions, follow us on Twitter/X, Mastodon, BlueSky or LinkedIn, and join our public mailing list to receive further updates.

« Back to News & Insights