# FBI makes a massive botnet infecting more than 700,000 computers uninstall itself

The US government just helped dismantle a massive network of computers infected with one of the world's most notorious pieces of malware. According to the FBI, a multinational effort led by the US took down Qakbot, a malware that made its way into over 700,000 computers around the globe.

Hackers typically target victims with Qakbot by sending them spam emails containing malicious attachments or links. As soon as a victim downloads the attachment or clicks the link, Qakbot infects their computer, which then becomes part of a botnet — or a network of infected computers controlled remotely by hackers. From there, bad actors can install additional malware on their victims' devices, such as ransomware.

To take down the network, the FBI routed Qakbot through FBI-controlled servers, where it instructed infected computers in the US and elsewhere to download software that uninstalled the Qakbot malware. The installer also separated infected computers from the botnet, "preventing further installation of malware through Qakbot." As noted by the DOJ, the action was only limited to the malware installed by Qakbot actors and "did not extend to remediating other malware already installed on the victim computers."

In addition to the US, Operation "Duck Hunt" also involved Europol, France, Germany, the Netherlands, the UK, Romania, and Latvia. The US says the botnet was responsible for hundreds of millions of dollars in damages and infected more

than 200,000 computers in the US. Qakbot has been around since 2008 and was leveraged by several prolific ransomware groups in the past, including Conti, REvil, MegaCortex, and more. As part of the operation, the DOJ seized $8.6 million worth of extorted funds in crypto.

“An international partnership led by the Justice Department and the FBI has resulted in the dismantling of Qakbot, one of the most notorious botnets ever, responsible for massive losses to victims around the world,” US Attorney Martin Estrada says in a statement. “Qakbot was the botnet of choice for some of the most infamous ransomware gangs, but we have now taken it out.”

The FBI has since provided Have I Been Pwned with the compromised credentials it found during the operation, allowing you to enter your email on the site to check if you were affected. The Dutch National Police has also added affected credentials to its Check Your Hack site.

https://www.theverge.com/2023/8/29/23851227/fbi-doj-qakbot-botnet-malware