DOCUMENTS AND RESOURCES RELATED TO THE DISRUPTION OF THE QAKBOT MALWARE AND BOTNET

justice.gov/usao-cdca/divisions/national-security-division/qakbot-resources

August 28, 2023

Press Releases

Qakbot Malware Disrupted in International Cyber Takedown (US Attorney's Office Press Release)

Qakbot Malware Disrupted in International Cyber Takedown (DOJ National Press Release)

Information for Victims

Beginning on August 25, 2023, law enforcement gained access to the Qakbot botnet, redirected botnet traffic to and through servers controlled by law enforcement, and instructed Qakbot-infected computers to download a Qakbot Uninstall file that uninstalled Qakbot malware from the infected computer. The Qakbot Uninstall file did not remediate other malware that was already installed on infected computers; instead, it was designed to prevent additional Qakbot malware from being installed on the infected computer by untethering the victim computer from the Qakbot botnet.

Hash value for the Qakbot Uninstall file (SHA-256):

7cdee5a583eacf24b1f142413aabb4e556ccf4ef3a4764ad084c1526cc90e117

As a result of this operation, the FBI and the Dutch National Police have identified numerous account credentials that were compromised by the Qakbot actors. The FBI has provided those credentials to the website Have I Been Pwned, which is a free resource for people to quickly assess whether their access credentials have been compromised in a data breach or

other activity. The Dutch National Police have also set up a website that contains information about additional compromised credentials. You can check to see if your credentials were compromised at the following websites:

This webpage will be updated as more resources become available. Victims are encouraged to report the cybercrimes with their local FBI field office or the Internet Crime Complaint Center (IC3) at ic3.gov.

The following documents contain additional information for victims and network defenders:

CISA Cybersecurity Advisory : Identification and Disruption of QakBot Infrastructure (August 30, 2023)

The Shadowserver Foundation: Qakbot Botnet Disruption (August 29, 2023)

Spamhaus: Qakbot Breached Email Accounts (August 29, 2023)

Search Warrant Related to Qakbot Uninstall File

Application, Search Warrant (2:23-MJ-4244), signed August 21, 2023

Search Warrant Related to Qakbot U.S. Server Infrastructure

Application, Search Warrant (2:23-MJ-4248), signed August 23, 2023

Seizure Warrant Related to Virtual Currency Seizure

Application, Seizure Warrant (2:23-MJ-4251), signed August 23, 2023