RESOURCES FOR VICTIMS OF THE QAKBOT MALWARE

Published: 2023-08-28 · Archived: 2026-04-05 16:26:25 UTC

2025 Press Releases

May 22, 2025: Russian National and Leader of Qakbot Malware Conspiracy Indicted in Long-Running Global Ransomware Scheme (U.S. Attorney's Office Press Release)

May 22, 2025: Leader of Qakbot Malware Conspiracy Indicted for Involvement in Global Ransomware Scheme (DOJ National Press Release)

Indictment

May 2, 2025: Indictment, 2:25-CR-00340-SB

2025 Qakbot Asset Forfeiture: Information for Victims

On May 22, 2025, the U.S. Attorney's Office ("USAO") for the Central District of California filed a Complaint for Forfeiture (2:25-CV-04631) against virtual currency and currency ("defendant assets") seized from the operators of the Qakbot botnet. According to the allegations in the Complaint, the defendant assets are traceable proceeds of and were involved in money laundering offenses pertaining to the payment of ransoms for ransomware attacks resulting from computer intrusions by members of the Qakbot conspiracy.

The USAO will be contacting victims who may have an interest in the defendant assets to provide information about your rights. Details on these procedures will be provided in a later communication to you from the USAO.

Are you a Victim?

If you are a victim of the Qakbot malware and associated ransomware, you may have a legal interest in the defendant assets. If you wish to be contacted and provided with information about the legal process involving the defendant assets as it moves forward, please send the following information to Qakbot_Victims@fbi.gov:

- Organization Name (if any)
- Address
- Name of Contact Person
- Contact phone number and/or email address
- Location
- Date of suspected Qakbot infection (if known)
- Whether you were the victim of ransomware
    - If yes, what ransomware variant
    - Was a ransom paid?
    - If yes, provide payment address, amount, and date

- Have you reported to law enforcement?
    - When did you report the incident?
    - To what law enforcement agency?
    - Please provide any report or incident number for your report

2023 Press Releases

August 29, 2023: Qakbot Malware Disrupted in International Cyber Takedown (US Attorney's Office Press Release)

August 29, 2023: Qakbot Malware Disrupted in International Cyber Takedown (DOJ National Press Release)

2023 Botnet Takedown: Information for Victims

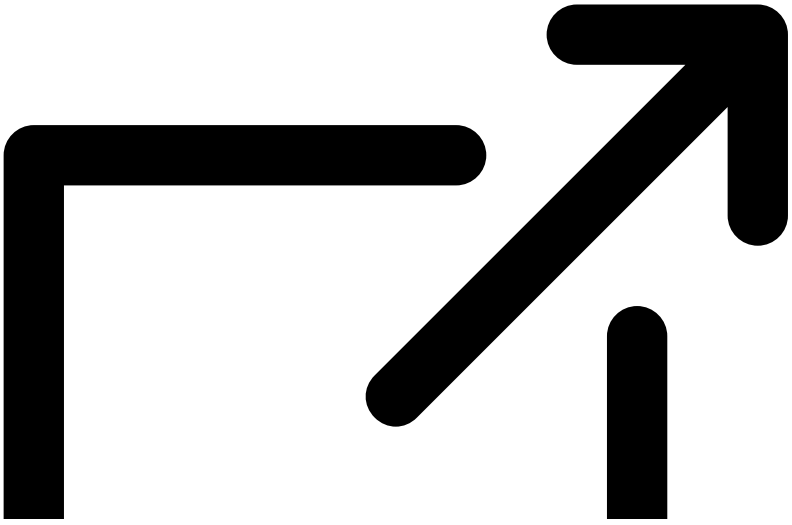
Beginning on August 25, 2023, law enforcement gained access to the Qakbot botnet, redirected botnet traffic to and through servers controlled by law enforcement, and instructed Qakbot-infected computers to download a Qakbot Uninstall file that uninstalled Qakbot malware from the infected computer. The 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):

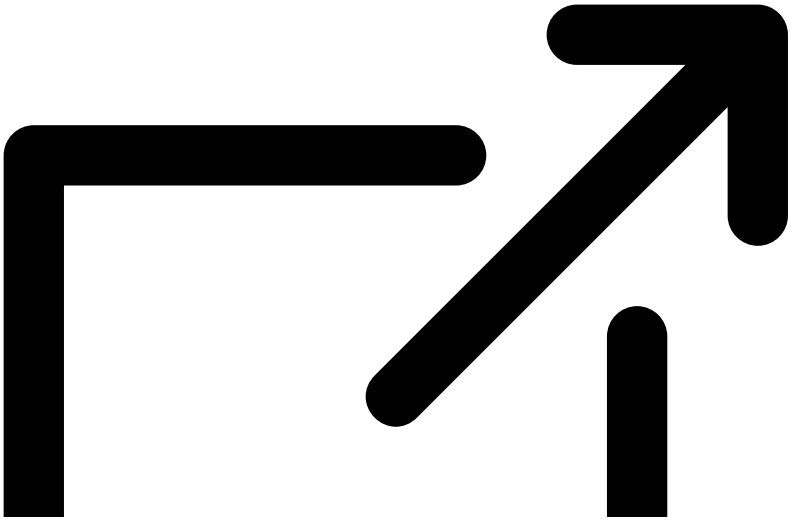
- 7cdee5a583eacf24b1f142413aabb4e556ccf4ef3a4764ad084c1526cc90e117

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:

- Have I Been Pwned (https://haveibeenpwned.com/)



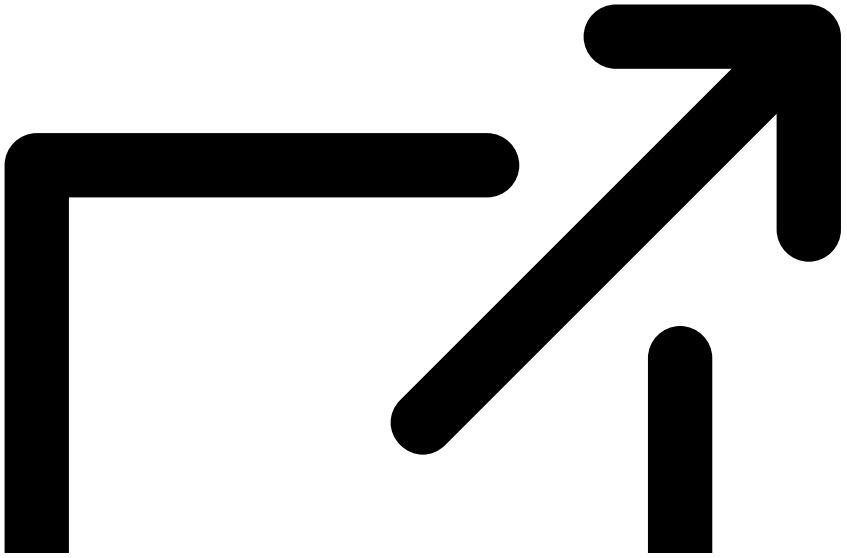
- Dutch National Police (https://politie.nl/checkyourhack)



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.

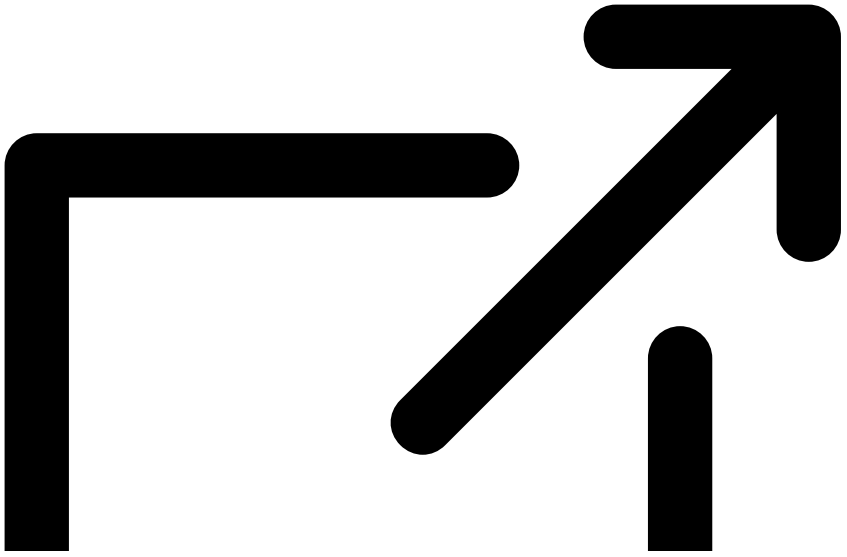
Shadowserver has disseminated data about historical Qakbot infections to 201 National Computer Security Incident Response Teams and to affected network owners around the world.

Qakbot Historical Bot Infections Special Report (September 8, 2023), https://www.shadowserver.org/news/qakbot-historical-bot-infections-special-report/



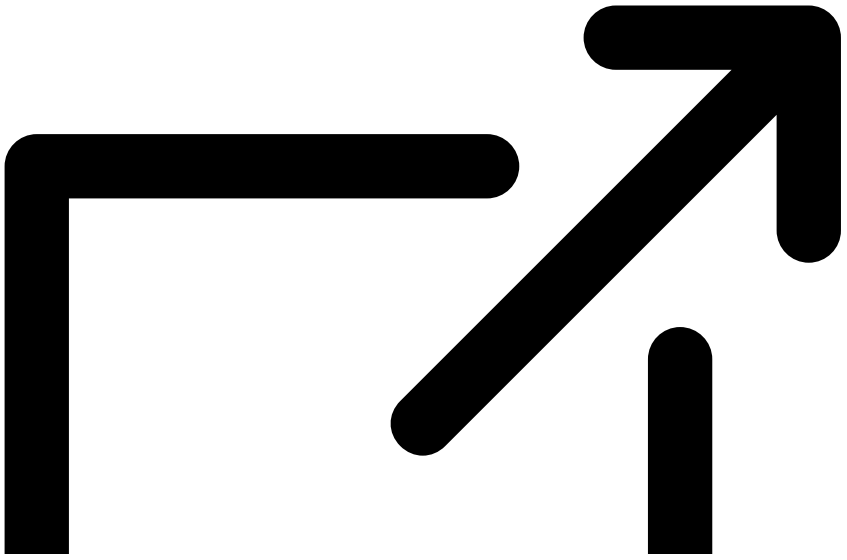
The following documents contain additional information for victims and network defenders:

CISA Cybersecurity Advisory: Identification and Disruption of QakBot Infrastructure



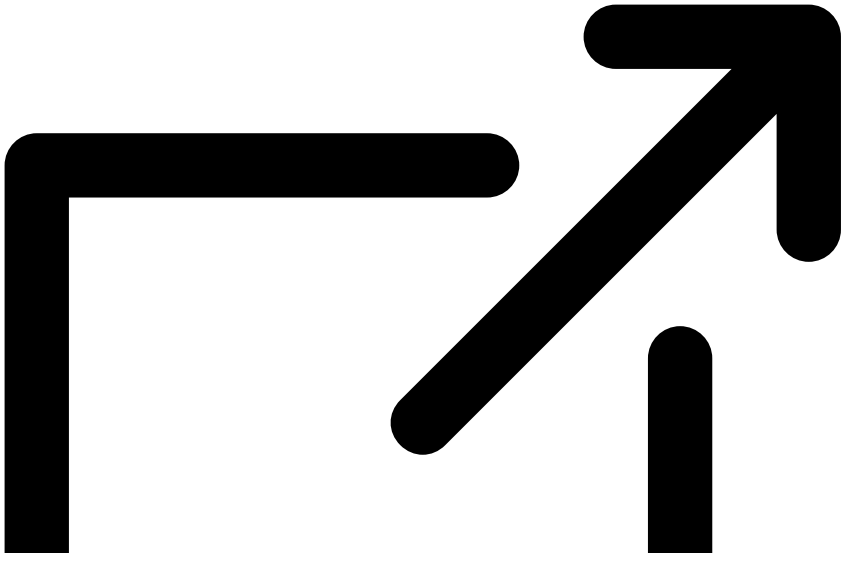
(August 30, 2023)

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
