Malware | Qakbot - the takedown and the remediation | Spamhaus

Archived: 2026-04-05 23:13:49 UTC

Introduction

Writing "Qakbot" and "takedown" in the same sentence is quite something. Usually, Spamhaus is bemoaning the ever-growing numbers of compromised IPs associated with this malware. But, on Tuesday, August 29th, 2023, the Federal Bureau of Investigation (FBI) announced that it coordinated an international group of law enforcement authorities in Operation 'Duck Hunt' to take control of the Qakbot infrastructure. Working together with the relevant authorities, the Spamhaus Project is assisting with remediation efforts.

We've previously reported on takedowns, for example, Emotet, when its infrastructure was disrupted in January 2021. Similar to the takedown of Qakbot, it resulted from a highly coordinated effort between multiple countries. This time, the United States, France, Germany, The Netherlands, The United Kingdom, Romania, and Latvia all worked together, led by the FBI, to disrupt the Qakbot botnet infrastructure used by cybercriminals.

However, one notable difference between the Emotet and Qakbot takedown is the novel method employed to "disrupt the duck". Through Bureau-controlled servers, the FBI instructed infected computers to download an uninstaller file. This uninstaller, specifically created to remove Qakbot malware, untethered infected computers from the botnet and prevented the installation of any additional malware. We won't lie - we think this is genius.

To be honest, we think the entire operation is to be hugely applauded, and it once again illustrates that in the World Wide Web era, a World Wide Community is required to keep its users safe.

Want to know more about Qakbot?

Anyone who has read the Botnet Updates or Malware Digests will have heard about this malware. Qakbot, around since 2008, has been one of the most significant malware threats for corporate networks. To understand the size of this malware, here's a data point: In 2022, every fourth malware site shared by abuse.ch's URLHaus was related to Qakbot.

Often acting as Initial Access, Qakbot has been used by many prolific ransomware groups in recent years, including Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta. Subsequently, these ransomware actors extort their victims, seeking ransom payments in bitcoin before returning access to the victim's computer networks.

These ransomware groups have caused significant harm to businesses, healthcare providers, and government agencies worldwide. Investigators have found evidence that, between October 2021 and April 2023, Qakbot administrators received fees corresponding to approximately $58 million in ransoms paid by victims.

Over the past year, our researchers have observed increased activity; in Q4 2022, Qakbot botnet command and controllers (C&Cs) were associated with 379% more IP addresses than in the previous quarter. Meanwhile, in

February 2023, the largest number of Indicators of Compromise (IOCs) reported via abuse.ch's ThreatFox platform were associated with Qakbot.

The disruption of this malware cannot have come soon enough. We are deeply grateful to all those concerned, and look forward to contributing to the remediation efforts.

Help and recommended content

See below for helpful articles and recommended content

Operation Endgame | Botnets disrupted after international action

On Thursday, May 30th, 2024, a coalition of international law enforcement agencies announced "Operation Endgame". This effort targeted multiple botnets, such as IcedID, Smokeloader, SystemBC, Pikabot, and Bumblebee, as well as their operators, and Spamhaus is assisting with the remediation efforts.

News • May 30, 2024 • The Spamhaus Team

Source: https://www.spamhaus.org/news/article/819/qakbot-the-takedown-and-the-remediation