Qakbot - the takedown and the remediation

spamhaus.org/news/article/819/qakbot-the-takedown-and-the-remediation

2023-08-29 20:28:17 UTC | by Spamhaus Team | Category: qakbot, botnet, takedown, compromise, email

Recent News Articles

Want to submit data? Be our guest!

The return of the ASN-DROP

Qakbot - the takedown and the remediation

Poor sending practices trigger a tidal wave of informational listings

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.

Qakbot email accounts victim remediation

Before diving into the nitty gritty of Qakbot and the takedown tale, we want to outline what assistance we will provide to owners and operators of Qakbot compromised email accounts.

- Qakbot relied on compromised accounts to spread its malicious emails. If a receiver interacted with one of these emails, it is highly likely that their device became infected. As a result, they would have become part of the Qakbot botnet.
- The authorities have provided Spamhaus with data pertaining to these compromised accounts to assist with the remediation effort.
- Over the coming days, Spamhaus will notify email service providers, hosting companies, and other parties responsible for these accounts.
- We request that all those organizations contacted secure the accounts in question via a simple password reset.

For more information see our dedicated Qakbot remediation page.

The takedown tale

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.

Spamhaus Botnet Threat Update: Q4-2021

SERVICE UPDATE | Spamhaus DNSBL users who query via Cloudflare DNS need to make changes to email set-up

Spamhaus Botnet Threat Update: Q3-2021

Spammer Abuse of Free Google Services

Older News Articles:

Spamhaus News INDEX

RSS

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.

Press releases & announcements

FBI: FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown
US Attorney's Office: Qakbot Malware Disrupted in International Cyber Takedown
Netherlands Public Prosecution Service: Grootste wereldwijde botnet

Qakbot onschadelijk gemaakt
UK National Crime Agency: Qakbot: cyber crime service taken out in international operation