Qakbot Takedown Aftermath: Mitigations and Protecting Against Future Threats

By The Hacker News

Published: 2023-12-01 · Archived: 2026-04-05 15:04:03 UTC

The U.S. Department of Justice (DOJ) and the FBI recently collaborated in a multinational operation to dismantle the notorious Qakbot malware and botnet. While the operation was successful in disrupting this long-running threat, concerns have arisen as it appears that Qakbot may still pose a danger in a reduced form. This article discusses the aftermath of the takedown, provides mitigation strategies, and offers guidance on determining past infections.

The Takedown and Its Limitations

During the takedown operation, law enforcement secured court orders to remove Qakbot malware from infected devices remotely. It was discovered that the malware had infected a substantial number of devices, with 700,000 machines globally, including 200,000 computers in the U.S., being compromised at the time of the takedown. However, recent reports suggest that Qakbot is still active but in a diminished state.

The absence of arrests during the takedown operation indicates that only the command-and-control (C2) servers were affected, leaving the spam delivery infrastructure untouched. Therefore, the threat actors behind Qakbot continue to operate, presenting an ongoing threat.

Mitigations for Future Protection

To safeguard against potential Qakbot resurgence or similar threats, the FBI, and the Cybersecurity & Infrastructure Security Agency (CISA) recommend several key mitigations:

1. **Require Multi-Factor Authentication (MFA):** Implement MFA for remote access to internal networks, particularly in critical infrastructure sectors like healthcare. MFA is highly effective in preventing automated cyberattacks.
2. **Regularly Conduct Employee Security Training:** Educate employees about security best practices, including avoiding clicking on suspicious links. Encourage practices like verifying the source of links and typing website names directly into browsers.
3. **Update Corporate Software:** Keep operating systems, applications, and firmware up to date. Use centralized patch management systems to ensure timely updates and assess the risk for each network asset.
4. **Eliminate Weak Passwords:** Comply with NIST guidelines for employee password policies and prioritize MFA over password reliance wherever possible.
5. **Filter Network Traffic:** Block ingoing and outgoing communications with known malicious IP addresses by implementing block/allow lists.
6. **Develop a Recovery Plan:** Prepare and maintain a recovery plan to guide security teams in the event of a breach.
7. **Follow the "3-2-1" Backup Rule:** Maintain at least three copies of critical data, with two stored in separate locations and one stored off-site.

Checking for Past Infections

For individuals concerned about past Qakbot infections, there is some good news. The DOJ has recovered over 6.5 million stolen passwords and credentials from Qakbot's operators. To check if your login information has been exposed, you can use the following resources:

1. **Have I Been Pwned:** This widely known site allows you to check if your email address has been compromised in data breaches. It now includes the Qakbot dataset in its database.
2. **Check Your Hack:** Created by the Dutch National Police using Qakbot's seized data, this site lets you enter your email address and provides an automatic email notification if your address is found in the dataset.
3. **World's Worst Passwords List:** Since Qakbot utilizes a list of common passwords for brute-force attacks, you can check this list to ensure your password is not among the worst.

Conclusion

While the takedown of Qakbot was a significant achievement, the threat landscape remains complex. There is a possibility of Qakbot's resurgence, given its operators' adaptability and resources. Staying vigilant and implementing security measures is crucial to prevent future infections. BlackBerry's CylanceENDPOINT solution is recommended to protect against Qakbot's execution, and specific rules within CylanceOPTICS can enhance protection against threats like Qakbot.

For additional information and resources on mitigations, visit the DOJ's Qakbot resources page.

Found this article interesting? This article is a contributed piece from one of our valued partners. Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
