Cybersecurity Threat Advisory: New QBot malware delivering campaigns discovered

By Barracuda Networks

Published: 2023-04-25 · Archived: 2026-04-05 17:18:24 UTC

Note: This article was originally published on SmarterMSP

A new QBot malware campaign has been discovered. Using hijacked business emails, bad actors are distributing PDF and WSF file formats in reply-chain phishing emails to distribute malware. The campaign is designed to steal sensitive data from the target system, including login credentials and financial information.

Associated Indicators of Compromise (IOCs) have been added to Barracuda XDR threat intelligence and our SOC is actively monitoring this threat.

What is the threat?

The QBot (aka Qakbot), a former banking Trojan turned malware, has been active since 2008. It has evolved to include sophisticated capabilities that enable it to bypass security measures and remain undetected. This malware is typically distributed through phishing emails that contain malicious attachments or links to infected websites. Once the malware is installed, it can capture keystrokes, steal sensitive data, and even manipulate online banking sessions to steal funds.

Why is it noteworthy?

The QBot malware is a persistent threat that has been linked to multiple high-profile data breaches and financial losses over the years. The latest campaign is noteworthy because it uses a combination of file formats in email attachments to evade detection by security software. Similar to the QBot campaign that utilized OneNote Packages, the current campaign uses PDF and WSF (Windows Script) files to deliver the malware. This technique makes it more difficult for organizations to detect and block the malware.

Additionally, the malware is currently being distributed through reply-chain phishing emails. Threat actors use stolen email exchanges and reply to them with malicious links/attachments. This is very dangerous, as the email threads are legitimate, and users may not realize the threat until it is too late.

What is the exposure or risk?

Organizations that fall victim to the campaign are at risk of losing sensitive data and funds, which can have significant financial and reputational consequences. The malware can also spread to other systems within the organization, causing further damage and disruption. Additionally, the use of sophisticated techniques to distribute the malware means that it may be more difficult for organizations to detect and respond to the threat in a timely manner.

What are the recommendations?

Barracuda SOC highly recommends implementing a multi-layered security approach to prevent and protect against these malware and phishing campaigns.

- Protect user mailboxes by using an email security solution, such as Barracuda's Email Gateway Defense.
- Utilize Barracuda XDR network security to monitor for malicious traffic.
- Use a next-gen endpoint protection solution, such as Sentinel One. Next-gen protection includes behavioral analysis and does not rely solely on signature-based detection. Recent malware campaigns are highly effective at evading detection by traditional anti-virus/security solutions.
- Employees should be trained on how to recognize and report suspicious emails and attachments. Time and time again, humans are the weakest link in security.
- Make sure your entire organization is protected with multi-factor authentication (MFA).
- Keep all systems up to date. Unpatched or outdated systems offer an easy entry point for hackers.
- Implement a response plan that includes regular backups, incident response procedures, and communication plans to minimize the impact of a successful attack.
- Leverage the protection of the Barracuda XDR platform. Our 24x7x365 Security Operations Center monitors your environment around the clock to ensure your protection.

Note: This article was originally published on SmarterMSP

Walker is a Cybersecurity Analyst at Barracuda MSP. He's a security expert working on our Blue Team within our Security Operations Center. Walker supports our XDR service delivery and is highly skilled at analyzing security events to detect cyber threats, helping keep our partners and their customers protected.
