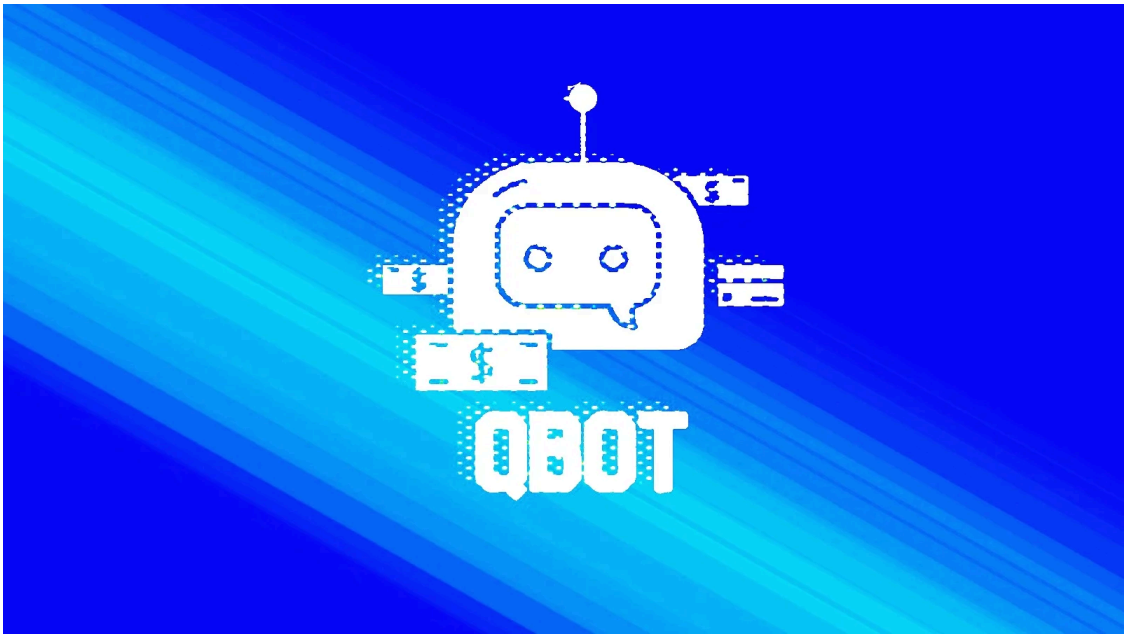
Qbot malware returns in campaign targeting hospitality industry

By Lawrence Abrams

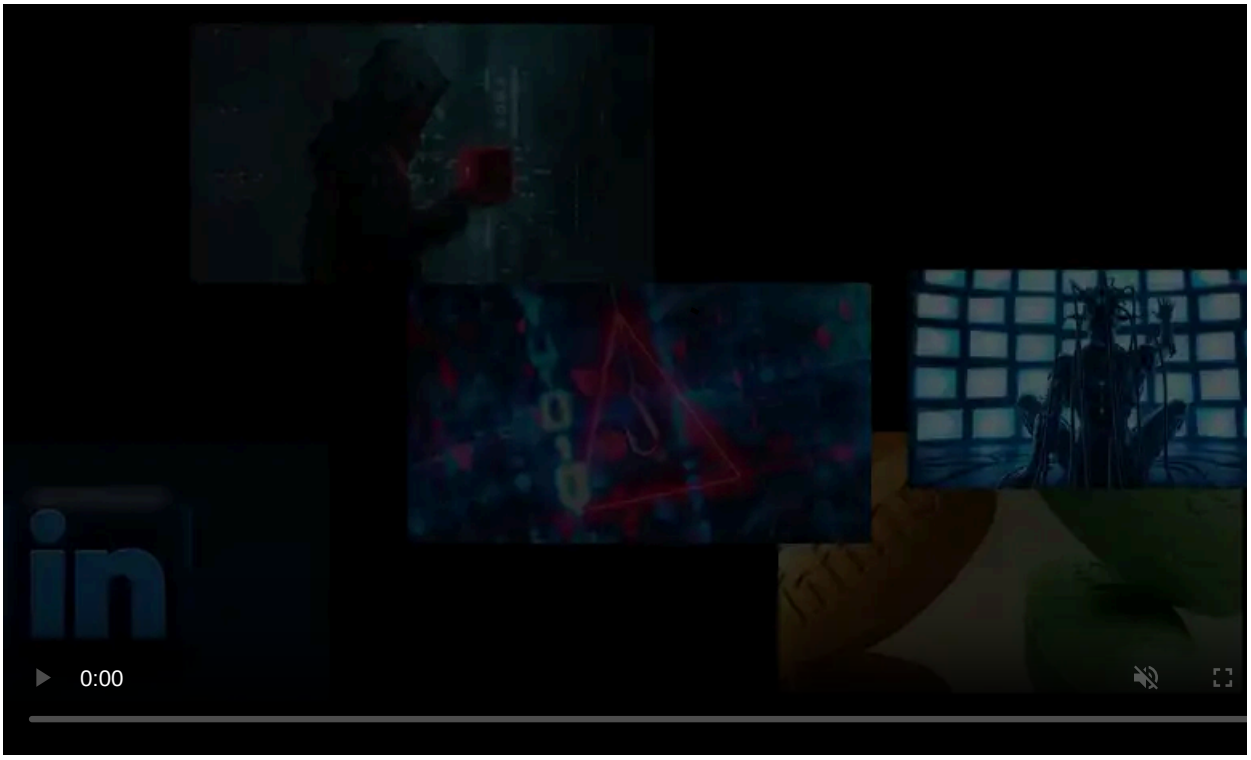
Published: 2023-12-17 · Archived: 2026-04-05 15:43:48 UTC

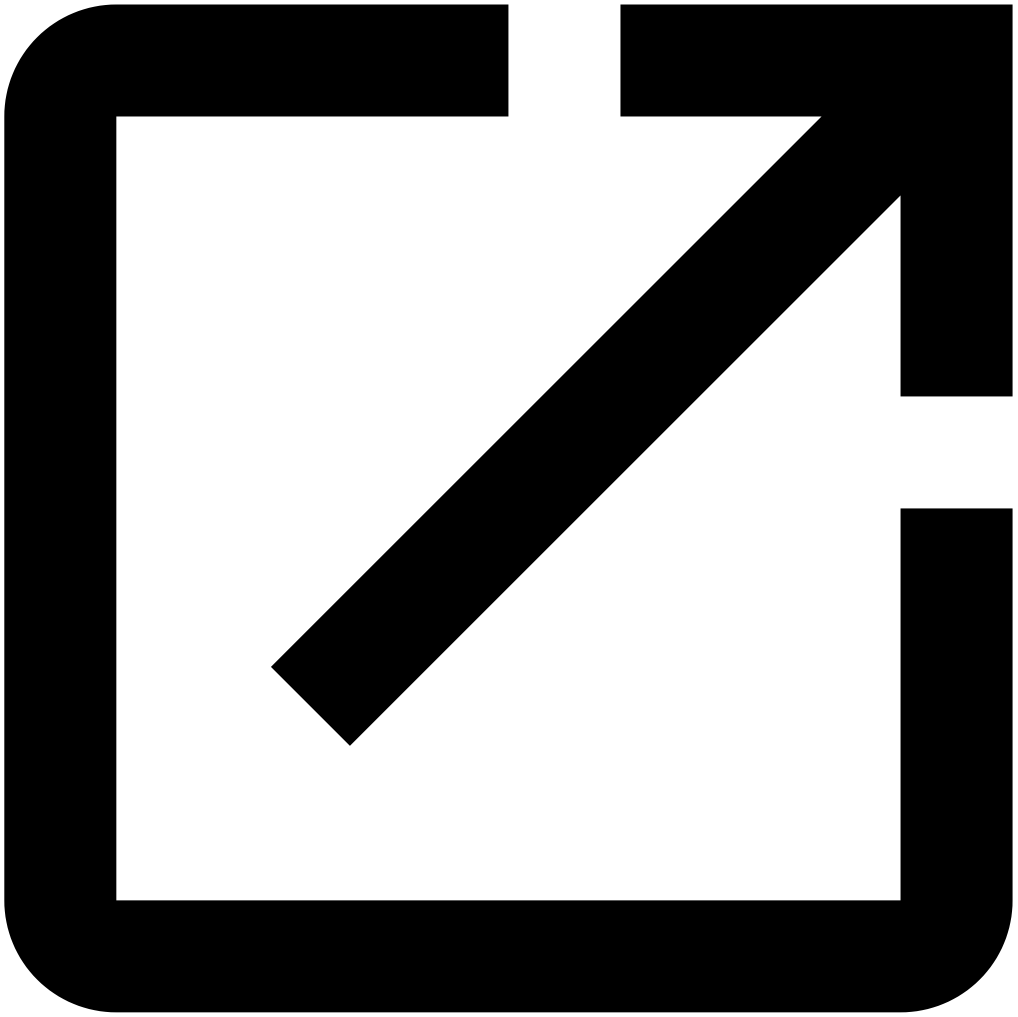


The QakBot malware is once again being distributed in phishing campaigns after the botnet was disrupted by law enforcement over the summer.

In August, a multinational law enforcement operation called Operation Duck Hunt accessed the QakBot admin's servers and mapped out the botnet's infrastructure.

After gaining access to the botnet's encryption keys used for malware communication, the FBI was able to hijack the botnet to push a custom Windows DLL module to infected devices. This DLL executed a command that terminated the QakBot malware, effectively disrupting the botnet.


0:00



While a phishing service that was used to distribute the Qbot malware has seen activity since the disruption, there was no distribution of the QakBot malware until this past Monday, when the new phishing campaign started.

QakBot returns

Microsoft is now warning that QakBot is being distributed again in a phishing campaign pretending to be an email from an IRS employee.

Microsoft says it first observed the phishing attack on December 11th in a small campaign targeting the hospitality industry.

Attached to the email is a PDF file pretending to be a guest list that says "Document preview is not available," and then prompts the user to download the PDF to view it properly.

However, when clicking on the download button, recipients will download an MSI that, when installed, launches the Qakbot malware DLL into memory.

Microsoft says the DLL was generated on December 11th, the same day the phishing campaign started, and uses a campaign code of 'tchk06' and command and control servers at 45.138.74.191:443 and 65.108.218.24:443.

"Most notably, the delivered Qakbot payload was configured with the previously unseen version 0x500," Microsoft tweeted, indicating the continued development of the malware.

Security researchers Pim Trouerbach and Tommy Madjar have also confirmed that the Qakbot payload being distributed is new, with some minor changes.

Trouerbach told BleepingComputer that there are minor changes to the new QakBot DLL, including using AES to decrypt strings rather than XOR in the previous version.

Furthermore, Trouerbach believes the new version is still being developed as it contains some unusual bugs.

As Trouerbach tweeted, after Emotet was disrupted by law enforcement in 2021, the threat actors attempted to revive their botnet with little success.

While it is too soon to tell if Qbot will have trouble regaining its former size, admins and users need to be on the lookout for reply-chain phishing emails that are commonly used to distribute the malware.

What is the Qbot malware

QakBot, aka Qbot, started out as a banking trojan in 2008, with malware developers using it to steal banking credentials, website cookies, and credit cards to commit financial fraud.

Over time, the malware evolved into a malware delivery service, partnering with other threat actors to provide initial access to networks for conducting ransomware attacks, espionage, or data theft.

Qakbot is distributed through phishing campaigns that utilize a variety of lures, including reply-chain email attacks, which is when threat actors use a stolen email thread and then reply to it with their own message and an attached malicious document.

These emails typically include malicious documents as attachments or links to download malicious files that install the Qakbot malware on a user's device.

These documents change between phishing campaigns and range from Word or Excel documents with malicious macros, OneNote files with embedded files, to ISO attachments with executables and Windows shortcuts. Some of them are also designed to exploit zero-day vulnerabilities in Windows.

Once installed, the malware will inject a DLL into a legitimate Windows process, such as wermgr.exe or AtBroker.exe, and quietly run in the background while deploying additional payloads.

In the past, Qakbot has partnered with multiple ransomware operations, including Conti, ProLock, Egregor, REvil, RansomExx, MegaCortex, and, most recently, Black Basta and BlackCat/ALPHV.

Source: https://www.bleepingcomputer.com/news/security/qbot-malware-returns-in-campaign-targeting-hospitality-industry/