More Signs of a Qakbot Resurgence

By Akshaya Asokan

Cybercrime , Endpoint Detection & Response (EDR) , Fraud Management & Cybercrime

Qakbot Wouldn't Be the First Trojan to Come Back After a Takedown (asokan_akshaya) • February 13, 2024

Security researchers are seeing new examples of Qakbot malware. (Image: Shutterstock)

Takedowns aren't always forever in cyberspace. Months after a U.S. law enforcement operation dismantled the notorious Qakbot botnet, security researchers say signs point to a resurgence.

See Also: 5 Keys to Building an Adversary-Ready SOC

Someone with access to the Qakbot - also known as Qbot - source code is experimenting with new builds and making incremental changes, said researchers from Sophos on social media.

Malware analysts said they had first spotted new Qakbot samples in mid-December - around the time that Microsoft Threat Intelligence tweeted that it had found a low-volume campaign targeting the hospitality industry through a PDF purportedly from the U.S. Internal Revenue Service that contained a downloader that calls the Trojan.

At the time of the August takedown, Qakbot was one of the world's longest-running botnets and accounted for hundreds of millions of dollars of losses. As part of an operation dubbed "Duck Hunt," authorities pushed a removal tool to more than 700,000 Qakbot-infected endpoints to excise malware from system memory.

Although the malware took shape in 2008 as a banking Trojan, its operators evolved over the years to become an initial access broker for other cybercriminals. They sold access to criminal gangs, including Russian-speaking ransomware operations (see: *Operation 'Duck Hunt' Dismantles Qakbot*).

"It's likely the evolution of Qakbot will continue, until and unless its creators face criminal prosecution," said Andrew Brandt, principal researcher at Sophos. Many cybercrime service providers operate from Russia, which doesn't extradite its citizens. "The good news is: For now, these new Qakbot variants are easy to detect and block with previously created signatures in endpoint detection software."

Researchers from Cisco Talos identified phishing messages from Qakbot as early as October, which suggests that Duck Hunt may have not affected Qakbot operators' spam delivery infrastructure.

Among the malware's new capabilities are improved encryption to conceal strings and to communicate with the command-and-control server. It also now checks to see whether it's running inside a virtual machine and enters an infinite loop if it detects one. Previous generations of the malware had that capability, but the operators had removed it.

The new variant seems to be in the development stage, and malware authors are adding more capabilities on the go.

Qakbot would hardly be the first major Trojan to come back from the dead. Operators of TrickBot and Emotet rebounded from infrastructure takedowns, although their later iterations were less fearsome (see: *Cybercrime Tremors: Experts Forecast Qakbot Resurgence*).
