QakBot Banking Trojan Returned With New Sneaky Tricks to Steal Your Money

By The Hacker News

Published: 2020-08-27 · Archived: 2026-04-05 15:52:23 UTC

A notorious banking trojan aimed at stealing bank account credentials and other financial information has now come back with new tricks up its sleeve to target government, military, and manufacturing sectors in the US and Europe, according to new research.

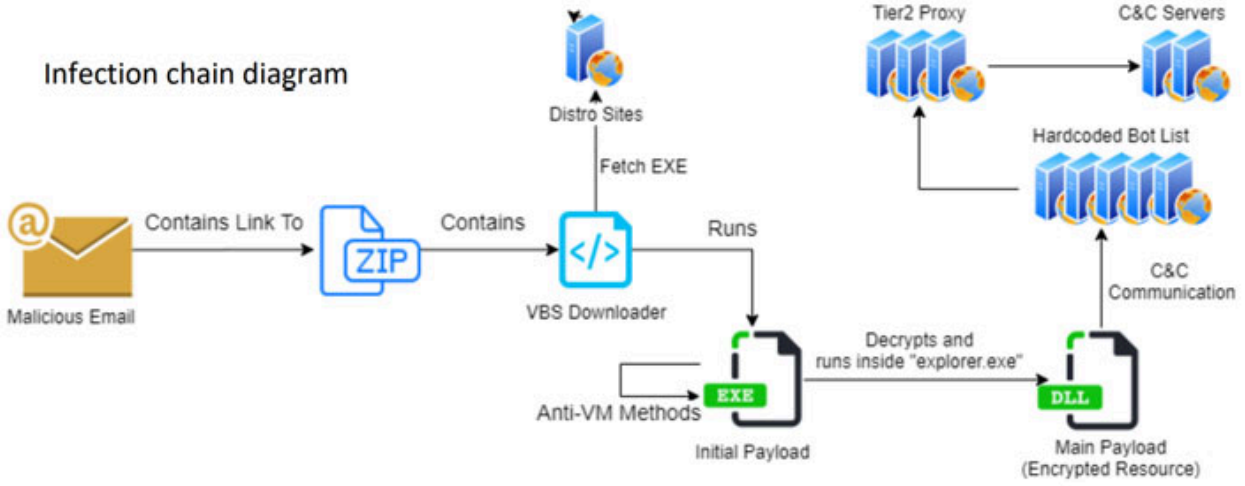
In an analysis released by Check Point Research today, the latest wave of Qbot activity appears to have dovetailed with the return of Emotet — another email-based malware behind several botnet-driven spam campaigns and ransomware attacks — last month, with the new sample capable of covertly gathering all email threads from a victim's Outlook client and using them for later malspam campaigns.

"These days Qbot is much more dangerous than it was previously — it has an active malspam campaign which infects organizations, and it manages to use a 'third-party' infection infrastructure like Emotet's to spread the threat even further," the cybersecurity firm said.

Using Hijacked Email Threads as Lures

First documented in 2008, Qbot (aka QuakBot, QakBot, or Pinkslipbot) has evolved over the years from an information stealer to a "Swiss Army knife" adept in delivering other kinds of malware, including Prolock ransomware, and even remotely connect to a target's Windows system to carry out banking transactions from the victim's IP address.

Attackers usually infect victims using phishing techniques to lure victims to websites that use exploits to inject Qbot via a dropper.

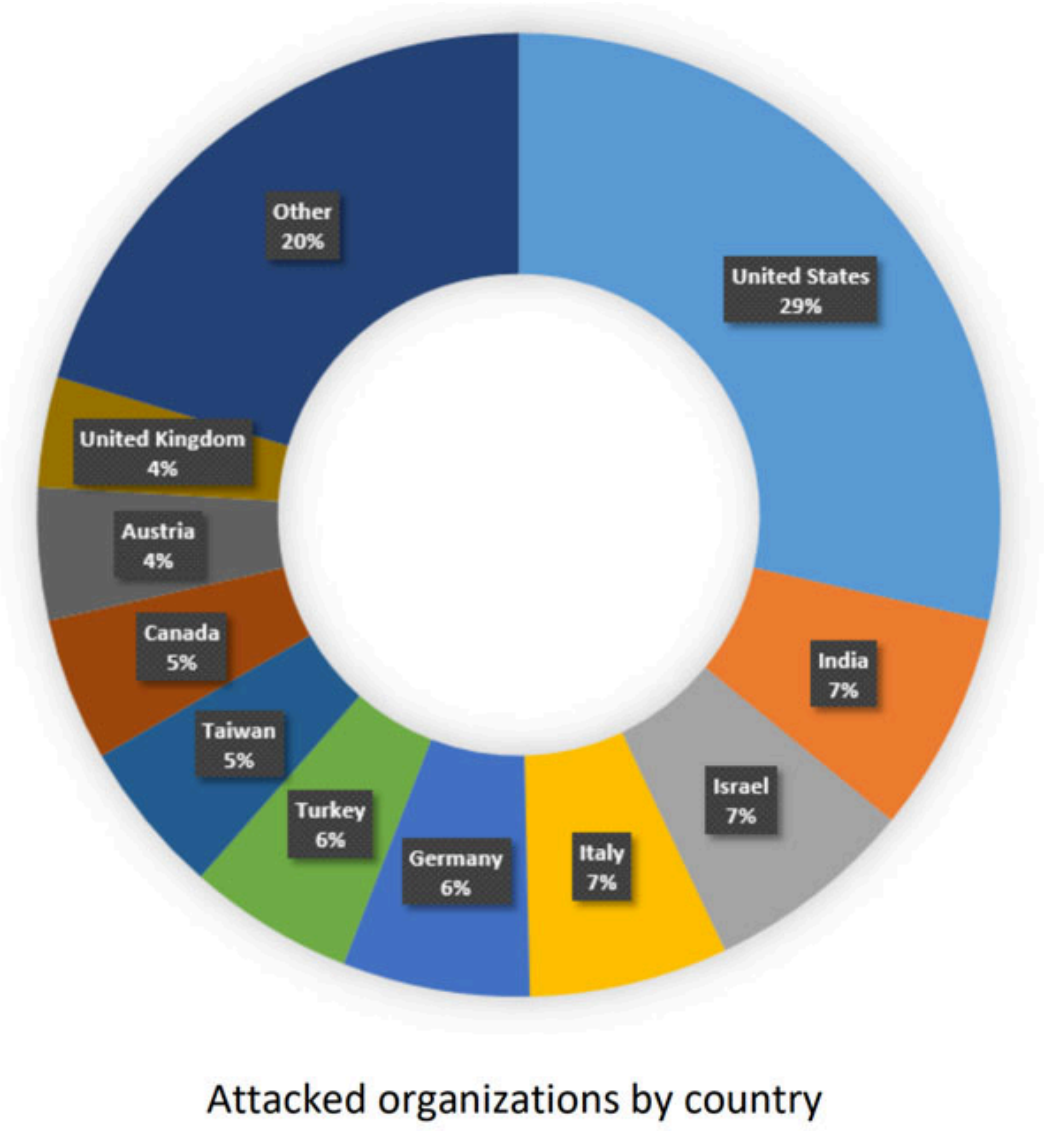


A malspam offensive observed by F5 Labs in June found the malware to be equipped with detection and research-evasion techniques with the goal of evading forensic examination. Then last week, Morphisec unpacked a Qbot sample that came with two new methods designed to bypass Content Disarm and Reconstruction (CDR) and Endpoint Detection and Response (EDR) systems.

The infection chain detailed by Check Point follows a similar pattern.

The first step begins with a specially crafted phishing email containing an attached ZIP file or a link to a ZIP file that includes a malicious Visual Basic Script (VBS), which then proceeds to download additional payloads responsible for maintaining a proper communication channel with an attacker-controlled server and executing the commands received.

Notably, the phishing emails sent to the targeted organizations, which take the form of COVID-19 lures, tax payment reminders, and job recruitments, not only includes the malicious content but is also inserted with archived email threads between the two parties to lend an air of credibility.



Attacked organizations by country

To achieve this, the conversations are gathered beforehand using an email collector module that extracts all email threads from the victim's Outlook client and uploads them to a hardcoded remote server.

Aside from packing components for grabbing passwords, browser cookies, and injecting JavaScript code on banking websites, the Qbot operators released as many as 15 versions of the malware since the start of the year, with the last known version released on August 7.

What's more, Qbot comes with an hVNC Plugin that makes it possible to control the victim machine through a remote VNC connection.

"An external operator can perform bank transactions without the user's knowledge, even while he is logged into his computer," Check Point noted. "The module shares a high percentage of code with similar modules like TrickBot's hVNC."

From an Infected Machine to a Control Server

That's not all. Qbot is also equipped with a separate mechanism to recruit the compromised machines into a botnet by making use of a proxy module that allows the infected machine to be used as a control server.

With Qbot hijacking legitimate email threads to spread the malware, it's essential that users monitor their emails for phishing attacks, even in cases they appear to come from a trusted source.

"Our research shows how even older forms of malware can be updated with new features to make them a dangerous and persistent threat," Check Point Research's Yaniv Balmas said. "The threat actors behind Qbot are investing heavily in its development to enable data theft on a massive scale from organizations and individuals."

"We have seen active malspam campaigns distributing Qbot directly, as well as the use of third-party infection infrastructures like Emotet's to spread the threat even further," Balmas added.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
