FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown

FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown

Operation marks one of the largest-ever U.S.-led enforcement actions against a botnet

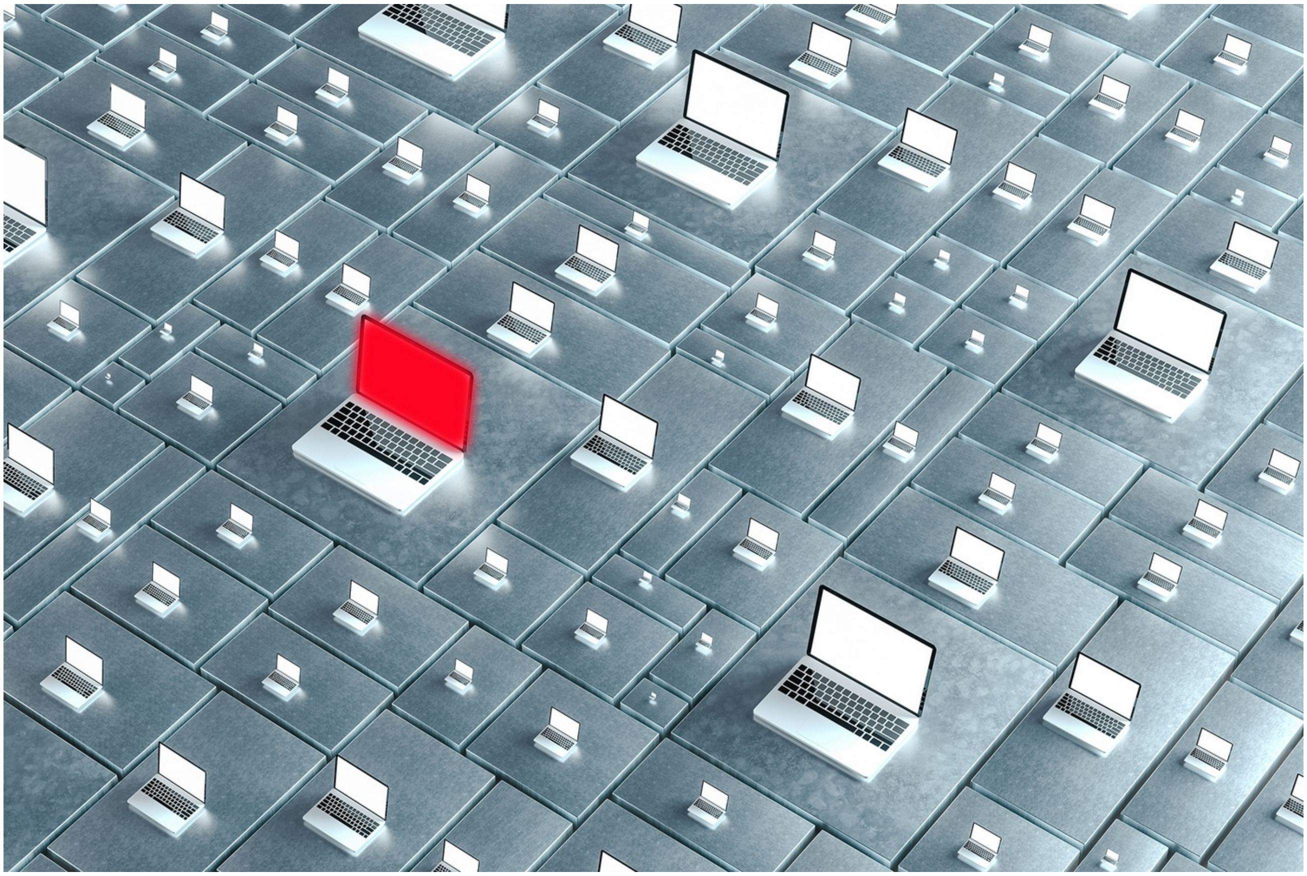
FBI Director Christopher Way announces a major operation targeting the Qakbot botnet.

Transcript / Visit Video Source

On August 29, the FBI and the Justice Department announced a multinational operation to disrupt and dismantle the malware and botnet known as Qakbot.

The action, which took place in the U.S., France, Germany, the Netherlands, Romania, Latvia, and the United Kingdom, represents one of the largest U.S.-led disruptions of a botnet infrastructure used by cybercriminals to commit ransomware, financial fraud, and other cyber-enabled criminal activity.

"The FBI neutralized this far-reaching criminal supply chain, cutting it off at the knees," said FBI Director Christopher Wray. "The victims ranged from financial institutions on the East Coast to a critical infrastructure government contractor in the Midwest to a medical device manufacturer on the West Coast."



> **“The FBI neutralized this far-reaching criminal supply chain, cutting it off at the knees.”**
>
> **FBI Director Christopher Wray**

How the Malware Worked

The Qakbot malware infected victim computers primarily through spam emails that contained malicious attachments or links.

After a user downloaded or clicked the content, Qakbot delivered additional malware—including ransomware—to their computer. The computer also became part of a botnet (a network of compromised computers) and could be controlled remotely by botnet users. All the while, a Qakbot victim was typically unaware that their computer had been infected.

Since its creation in 2008, Qakbot malware has been used in ransomware attacks and other cybercrimes that caused hundreds of millions of dollars in losses to individuals and businesses in the U.S. and abroad.

"This botnet provided cybercriminals like these with a command-and-control infrastructure consisting of hundreds of thousands of computers used to carry out attacks against individuals and businesses all around the globe," Wray said.

Disrupting the Duck

As part of the operation, the FBI gained lawful access to Qakbot's infrastructure and identified over 700,000 infected computers worldwide—including more than 200,000 in the U.S.

To disrupt the botnet, the FBI redirected Qakbot traffic to Bureau-controlled servers that instructed infected computers to download an uninstaller file. This uninstaller—created to remove the Qakbot malware—untethered infected computers from the botnet and prevented the installation of any additional malware.

"All of this was made possible by the dedicated work of FBI Los Angeles, our Cyber Division at FBI Headquarters, and our partners, both here at home and overseas," said Wray. "The cyber threat facing our nation is growing more dangerous and complex every day. But our success proves that our own network and our own capabilities are more powerful."

Resources:

- **Qakbot Malware Disrupted in International Cyber Takedown**

Next

Outreach and Mentorship: Cliff's Crew Visits the FBI

Cliff's Crew—a group of youth mentored by retired NFL Seattle Seahawks player Cliff Avril—visited the FBI Headquarters in Washington, D.C., where they toured the FBI Experience and met with Associate Deputy Director Brian Turner.