Qakbot Malware Disrupted in International Cyber Takedown

justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown

August 29, 2023

Press Release

Qakbot Malware Infected More Than 700,000 Victim Computers, Facilitated Ransomware Deployments, and Caused Hundreds of Millions of Dollars in Damage

LOS ANGELES – The Justice Department today announced a multinational operation involving actions in the United States, France, Germany, the Netherlands, the United Kingdom, Romania, and Latvia to disrupt the botnet and malware known as Qakbot and take down its infrastructure.

The Qakbot malicious code is being deleted from victim computers, preventing it from doing any more harm. The Department also announced the seizure of more than $8.6 million in cryptocurrency in illicit profits.

The action represents the largest U.S.-led financial and technical disruption of a botnet infrastructure leveraged by cybercriminals to commit ransomware, financial fraud, and other cyber-enabled criminal activity.

“Cybercriminals who rely on malware like Qakbot to steal private data from innocent victims have been reminded today that they do not operate outside the bounds of the law,” said Attorney General Merrick B. Garland. “Together with our international partners, the Justice Department has hacked Qakbot’s infrastructure, launched an aggressive campaign to uninstall the malware from victim computers in the United States and around the world, and seized $8.6 million in extorted funds.”

“An international partnership led by the Justice Department and the FBI has resulted in the dismantling of Qakbot, one of the most notorious botnets ever, responsible for massive losses to victims around the world,” said United States Attorney Martin Estrada. “Qakbot was the botnet of choice for some of the most infamous ransomware gangs, but we have now taken it out. This operation also has led to the seizure of almost 9 million dollars in cryptocurrency from the Qakbot cybercriminal organization, which will now be made available to victims. My Office’s focus is on protecting and vindicating the rights of victims, and this multifaceted attack on computer-enabled crime demonstrates our commitment to safeguarding our nation from harm.”

“The Operation ‘Duck Hunt’ Team utilized their expertise in science and technology, but also relied on their ingenuity and passion to identify and cripple Qakbot, a highly structured and multi-layered bot network that was literally feeding the global cybercrime supply chain,” said Donald Alway, the Assistant Director in Charge of the FBI’s Los Angeles Field Office. “These actions will prevent an untold number of cyberattacks at all levels, from the compromised personal computer to a catastrophic attack on our critical infrastructure."

According to court documents, Qakbot, also known by various other names, including “Qbot” and “Pinkslipbot,” is controlled by a cybercriminal organization and used to target critical industries worldwide. The Qakbot malware primarily infects victim computers through spam email messages containing malicious attachments or hyperlinks. Once it has infected a victim computer, Qakbot can deliver additional malware, including ransomware, to the infected computer. Qakbot has been used as an initial means of infection by many prolific ransomware groups in recent years, including Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta. The ransomware actors then extort their victims, seeking ransom payments in bitcoin before returning access to the victim computer networks.

These ransomware groups caused significant harm to businesses, healthcare providers, and government agencies all over the world, including to a power engineering firm based in Illinois; financial services organizations based in Alabama, Kansas, and Maryland; a defense manufacturer based in Maryland; and a food distribution company in Southern California. Investigators have found evidence that, between October 2021 and April 2023, Qakbot administrators received fees corresponding to approximately $58 million in ransoms paid by victims.

The victim computers infected with Qakbot malware are part of a botnet (a network of compromised computers), meaning the perpetrators can remotely control all the infected computers in a coordinated manner. The owners and operators of the victim computers are typically unaware of the infection.

As part of the takedown, the FBI was able to gain access to Qakbot infrastructure and identify over 700,000 computers worldwide, including more than 200,000 in the United States, that appear to have been infected with Qakbot. To disrupt the botnet, the FBI was

able to redirect Qakbot botnet traffic to and through servers controlled by the FBI, which in turn instructed infected computers in the United States and elsewhere to download a file created by law enforcement that would uninstall the Qakbot malware. This uninstaller was designed to untether the victim computer from the Qakbot botnet, preventing further installation of malware through Qakbot.

The scope of this law enforcement action was limited to information installed on the victim computers by the Qakbot actors. It did not extend to remediating other malware already installed on the victim computers and did not involve access to or modification of the information of the owners and users of the infected computers.

Valuable technical assistance was provided by Zscaler. The FBI has partnered with the Cybersecurity and Infrastructure Security Agency, Shadowserver, Microsoft Digital Crimes Unit, the National Cyber Forensics and Training Alliance, and Have I Been Pwned to aid in victim notification and remediation.

The FBI Los Angeles Field Office, the U.S. Attorney's Office for the Central District of California, and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) conducted the operation in close cooperation with Eurojust. Investigators and prosecutors from several jurisdictions provided crucial assistance, including Europol, French Police Cybercrime Central Bureau and the Cybercrime Section of the Paris Prosecution Office, Germany's Federal Criminal Police and General Public Prosecutor's Office Frankfurt/Main, Netherlands National Police and National Public Prosecution Office, the United Kingdom's National Crime Agency, Romania's National Police, and Latvia's State Police. The Justice Department's Office of International Affairs and the FBI Milwaukee Field Office provided significant assistance.

Assistant United States Attorneys Khaldoun Shobaki and Lauren Restrepo of the Cyber and Intellectual Property Crimes Section, along with CCIPS Trial Attorneys Jessica Peck, Ryan K.J. Dickey and Benjamin Proctor.

Additional information and resources, including for victims, can be found on the following website, which will be updated as additional information and resources become available: https://www.justice.gov/usao-cdca/divisions/national-security-division/qakbot-resources

Contact

Thom Mrozek
Director of Media Relations
thom.mrozek@usdoj.gov
(213) 894-6947

Updated August 29, 2023

Topic

Cybercrime

Component

USAO - California, Central
Press Release Number: 23-187