FBI and European partners seize major malware network in blow to global cybercrime

August 30 2023, by FRANK BAJAK and STEFANIE DAZIO

U.S. Attorney Martin Estrada, left, and FBI Asst. Director in Charge Don Alway announce in Los Angeles on Tuesday, Aug. 29, 2023 the multinational take down operation of Qakbot malware which infected more than 700,000 computers including LAUSD and San Bernardino County Sheriff Department computer systems. Credit: Sarah Reingewirtz/The Orange County Register via AP

U.S. officials said Tuesday that the FBI and its European partners infiltrated and seized control of a major global malware network used for more than 15 years to commit a gamut of online crimes including crippling ransomware attacks.

They then remotely removed the malicious software agent—known as Qakbot—from thousands of infected computers.

Cybersecurity experts said they were impressed by the deft dismantling of the network but cautioned that any setback to cybercrime would likely be temporary.

"Nearly ever sector of the economy has been victimized by Qakbot," Martin Estrada, the U.S. attorney in Los Angeles, said Tuesday in announcing the takedown. He said the criminal network had facilitated about 40 ransomware attacks alone over 18 months that investigators said netted Qakbot administrators about $58 million.

Qakbot's ransomware victims included an Illinois-based engineering firm, financial services organizations in Alabama and Kansas, along with a Maryland defense manufacturer and a Southern California food distribution company, Estrada said.

Officials said $8.6 million in cybercurrency was seized or frozen but no arrests were announced.

Estrada said the investigation is ongoing. He would not say where administrators of the malware, which marshaled infected machines into a botnet of zombie computers, were located. Cybersecurity researchers say they are believed to be in Russia and/or other former Soviet states.

U.S. Attorney Martin Estrada announces in Los Angeles on Tuesday, Aug. 29, 2023 the multinational take down operation of Qakbot malware. In their latest disruption of global cybercrime, the FBI and partners in Europe infiltrated and seized control of a major malware network that was used for more than 15 years to commit a gamut of online crimes including crippling ransomware attacks. Credit: Sarah Reingewirtz/The Orange County Register via AP

Officials estimated the so-called malware loader, a digital Swiss knife for cybercrooks also known as Pinkslipbot and Qbot, was leveraged to cause hundreds of millions of dollars in damage since first appearing in 2008 as an information-stealing bank trojan. They said millions of people in nearly every country in the world have been affected.

Typically delivered via phishing email infections, Qakbot gave criminal

hackers initial access to violated computers. They could then deploy additional payloads including ransomware, steal sensitive information or gather intelligence on victims to facilitate financial fraud and crimes such as tech support and romance scams.

The Qakbot network was "literally feeding the global cybercrime supply chain," said Donald Alway, assistant director in charge of the FBI's Los Angeles office, calling it "one of the most devastating cybercriminal tools in history." The most commonly detected malware in the first half of 2023, Qakbot impacted one in 10 corporate networks and accounted for about 30% of attacks globally, a pair of cybersecurity firms found. Such "initial access" tools allow extortionist ransomware gangs to skip the initial step of penetrating computer networks, making them major facilitators for the far-flung, mostly Russian-speaking criminals who have wreaked havoc by stealing data and disrupting schools, hospitals, local governments and businesses worldwide.

Beginning Friday in an operation officials dubbed "Duck Hunt," the FBI along with Europol and law enforcement and justice partners in France, the United Kingdom, Germany, the Netherlands, Romania and Latvia seized more than 50 Qakbot servers and identified more than 700,000 infected computers, more than 200,000 of them in the U.S.—effectively cutting off criminals from their quarry.

FBI Asst. Director in Charge Don Alway announces in Los Angeles on Tuesday, Aug. 29, 2023 the multinational take down operation of Qakbot malware which infected more than 700,000 computers including LAUSD and San Bernardino County Sheriff Department computer systems. Credit: Sarah Reingewirtz/The Orange County Register via AP

U.S. Attorney Martin Estrada announces in Los Angeles on Tuesday, Aug. 29, 2023 the multinational take down operation of Qakbot malware which infected more than 700,000 computers including LAUSD and San Bernardino County Sheriff Department computer systems. Credit: Sarah Reingewirtz/The Orange County Register via AP

The FBI then used the seized Qakbot infrastructure to remotely dispatch updates that deleted the malware from thousands of infected computers. A senior FBI official, briefing reporters on condition he not be further identified, called that number "fluid" and cautioned that other malware may have remained on machines liberated from Qakbot.

It was the FBI's biggest success against cybercrooks since it "hacked the hackers" with the January takedown of the prolific Hive ransomware

gang.

"It is an impressive takedown. Qakbot was the largest botnet" in number of victims, said Alex Holden, founder of Milwaukee-based Hold Security. But he said it may have been a casualty of its own success in its staggering growth over the past few years. "Large botnets today tend to implode as too many threat actors are mining this data for various types of abuse."

Cybersecurity expert Chester Wisniewski at Sophos agreed that while there could be a temporary drop in ransomware attacks, the criminals can be expected to either revive infrastructure elsewhere or move to other botnets.

"This will cause a lot of disruption to some gangs in the short term, but it will do nothing from it being rebooted," he said. "Albeit it takes a long time to recruit 700,000 PCs."

Citation: FBI and European partners seize major malware network in blow to global cybercrime (2023, August 30) retrieved 2 May 2024 from https://techxplore.com/news/2023-08-fbi-european-partners-seize-major.html