Cyber Command has sought to disrupt the world’s largest botnet, hoping to reduce its potential impact on the election

Gen. Paul Nakasone, head of U.S. Cyber Command, testifies to the Senate Intelligence Committee on worldwide threats in January 2019. (Salwan Georges/The Washington Post)

By **Ellen Nakashima**
Oct. 10, 2020 at 2:16 a.m. GMT+2

In recent weeks, the U.S. military has mounted an operation to temporarily disrupt what is described as the world’s largest botnet — one used also to drop ransomware, which officials say is one of the top threats to the 2020 election.

U.S. Cyber Command’s campaign against the Trickbot botnet, an army of at least 1 million hijacked computers run by Russian-speaking criminals, is not expected to permanently dismantle the network, said four U.S. officials, who spoke on the condition of anonymity because of the matter’s sensitivity. But it is one way to distract them at least for a while as they seek to restore operations.

The effort is part of what Gen. Paul Nakasone, the head of Cyber Command, calls “persistent engagement,” or the imposition of cumulative costs on an adversary by keeping them constantly engaged. And that is a key feature of CyberCom’s activities to help protect the election against foreign threats, officials said.

“Right now, my top priority is for a safe, secure, and legitimate 2020 election,” Nakasone said in August in a set of written responses to Washington Post questions. “The Department of Defense, and Cyber Command specifically, are supporting a broader ‘whole-of-government’ approach to secure our elections.”

U.S. Cyber Command disrupted Internet access of Russian trolls during 2018 midterms

Trickbot is malware that can steal financial data and drop other malicious software onto infected systems. Cyber criminals have used it to install ransomware, a particularly nasty form of malware that encrypts users' data and for which the criminals then demand payment — usually in cryptocurrency — to unlock.

Brian Krebs, who writes the blog KrebsonSecurity, first reported on the existence of the operation. Cyber Command's role was previously unreported. The command declined to comment.

Department of Homeland Security Officials fear that a ransomware attack on state or local voter registration offices and related systems could disrupt preparations for Nov. 3 or cause confusion or long lines on Election Day. They also note that ransomware is a major threat beyond elections.

Trickbot was used last month in a damaging attack against a major health-care provider, Universal Health Services, whose systems were locked up by the ransomware known as Ryuk. The attack forced personnel to resort to manual systems and paper records, according to reports. UHS runs more than 400 facilities across the United States and Britain. Some patients reportedly were rerouted to other emergency rooms and experienced delays in getting test results.

A woman in Germany died last month when the hospital she went to for emergency care turned her away because it had suffered a ransomware attack; she died en route to another facility. It is unclear whether Trickbot was involved in that case — said to represent the first death linked to ransomware.

Over the last year or so the botnet has been used to deliver ransomware to municipalities in the United States as well as software vendors that service these cities, researchers say.

On Sept. 22, cyber threat researchers who monitor the Trickbot network noticed the disruption of command and control servers. They did not know who was behind the disruption, but saw that someone had hacked the servers and sent out updates to all infected computers — including in the United States — that effectively severed the communication between the victimized computers and the servers.

But the next day, the criminals showed signs of restoring operations, according to Mark Arena, CEO of Intel 471, a U.S.-based threat intelligence company.

On Oct. 1, another similar disruption took place, Arena said. The operators were annoyed — some of them typed messages to each other all in capital letters, expressing frustration, said Alex Holden, chief information security officer and president of Milwaukee-based Hold Security, who also monitored the activity.

But again, the criminals recovered.

"This was a punch in the gut for the bad guys, but not a knockout blow,'" Holden said. "It was perceived as inconvenient, but most activity resumed within two to three days."

The only way "you're going to be completely successful against cyber criminals is to lock them up in jail," said Arena.

Still, CyberCom's action is worthy, U.S. officials said.

"At a time when ransomware is eating the world, this is an operation against one of the biggest and most active threat streams," said one official. "Is this permanent? Of course not." But any effort to degrade the botnet should be applauded, the official said.