

FBI, Air Force investigators mapped North Korean botnet to aid shutdown

Enlarge / Computer Hacker

reader comments

4 with 4 posters participating

Share this story

On January 30, the US Department of Justice announced that it, the Federal Bureau of Investigation, and the Air Force Office of Special Investigations were engaged in a campaign to “map and further disrupt” a botnet tied to North Korean intelligence activities detailed in an indictment unsealed last September. Search warrants obtained by the FBI and AFOSI allowed the agencies to essentially join the botnet, creating servers that mimicked the beacons of the malware.

“While the Joanap botnet was identified years ago and can be defeated with antivirus software,” said United States Attorney Nick Hanna, “we identified numerous unprotected computers that hosted the malware underlying the botnet. The search warrants and court orders announced today as part of our efforts to eradicate this botnet are just one of the many tools we will use to prevent cybercriminals from using botnets to stage damaging computer intrusions.”

Joanap is a remote access tool (RAT) identified as part of “Hidden Cobra”, the Department of Homeland Security designator for the North Korean hacking operation also known as the

Lazarus Group. The same group has been tied to the WannaCry worm and the hacking of Sony Motion Pictures. Joanap's spread dates back to 2009, when it was distributed by Brambul, a Server Message Block (SMB) file-sharing protocol worm. Joanap and Brambul were recovered from computers of the victims of the campaigns listed in the indictment of Park Jin Hyok in September.

Even though Joanap is caught by many malware protection systems (including Windows Defender), there are still large numbers of computers infected with the malware connected to the Internet. And unlike centrally controlled botnets, Joanap's commands are spread via peer-to-peer connections, so every infected computer essentially becomes part of the command and control system for the malware.

With servers mimicking Joanap, the FBI and AFOSI collected identifying metadata about computers infected with the malware, including IP addresses, port numbers, and connection timestamps. This allowed the agencies to build a map of the current Joanap botnet.

"Using the information obtained from the warrants, the government is notifying victims in the United States of the presence of Joanap on an infected computer," a DOJ spokesperson said. "The FBI is both notifying victims through their Internet Service Providers and providing personal notification to victims whose computers are not behind a router or a firewall."

The DOJ and FBI will also assist in the notification of overseas victims of the malware by passing the data to other governments.

<https://arstechnica.com/?p=1448911>