The Washington Times

'Inherently invasive': FBI counter-hacking operations raise red flags over privacy

Jeff Mordock

Thursday, January 31, 2019

To catch a hacker, sometimes you have to be a hacker. But when it's the FBI doing the hacking, civil liberties groups get worried.

The agency's revelation this week that it joined a computer botnet attack piggybacking on the malware's signal to track its activities has raised new questions about what is acceptable in cybersecurity.

The problem, the civil liberties advocates say, is that the FBI collected IP addresses and "ancillary" information from computers it traversed as it tried to map the Joanap malware.

"The powers that the FBI is using here are inherently invasive," said Andrew Crocker, a senior staff attorney at the Electronic Frontier Foundation. "Directing someone's computer to things like this gives the FBI pretty broad rein, and that is concerning."

The FBI and Air Force investigators obtained court orders approving the moves. They said the actions were critical to disrupting the botnet, which spawned a global network of computers infected with the Joanap malware. The malware gives hackers control of the computer, which they can use to commit wire fraud and other crimes.

Nicola T. Hanna, U.S. attorney for the Central District of California, defended the federal investigators' tactics. He said they allowed investigators to identify computers that were being infected and spreading the botnet.

"The warrants and court orders announced 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," he said in a statement.

An FBI spokeswoman declined to comment.

Cybersecurity analysts say the FBI's hacking of infected computers is a double-edged sword, giving authorities a new tool to fight crime in an increasingly digital world, but also exposing sensitive and unrelated files to law enforcement.

“Even if you need to get this information, hacking is an awfully intrusive method to do that,” said Julian Sanchez, a senior fellow at the Cato Institute. “It is not ideal to revictimize the crime victim by hacking the victim again.”

Federal investigators claimed authority to piggyback on the botnet from a 2016 change to an obscure federal criminal procedure statute, known as Rule 41. The change allows the government to use hacking software on computers to gain evidence.

Rule 41 has largely been used in financial crime and child pornography cases in which criminals are using devices to mask their computers’ IP addresses. Federal investigators need only permission from a judge to obtain the search warrant.
At the time, the Obama administration promised that the changes would be employed only in “narrow circumstances.”

Since then, some lawmakers on Capitol Hill have questioned the expansion. They worry about federal investigators judge-shopping to find friendly courts willing to sign warrants and question what steps the government would take to alert people that it had hacked their computers.

In a 2016 reply to the lawmakers, the Justice Department said that while taking control of computers to have them send back a unique signal — to calculate the size of a botnet — might be legal, searching “related private files” would not.

The department said it would take “reasonable” steps to alert innocent computer owners affected by a Rule 41 warrant, but it didn’t lay out a specific path for doing so.

The Justice Department said this week that it will notify affected users of its Joanap actions through their internet service providers and through personal notifications to computers not behind a router or firewall.

Authorities blame North Korean hackers for the botnet. Last year, the Justice Department filed charges against Park Jin-hyok, a North Korean national who is accused of leading the 2014 state-sponsored hack of Sony Pictures Entertainment.

Although accessing citizens’ computers without their consent or knowledge is murky, it doesn’t violate the Constitution, Mr. Sanchez said.

“There is nothing in the privacy laws that says a search warrant can only be executed on a criminal,” he said. “A search warrant has to be looking for evidence of a crime, but it doesn’t say anything about the place being searched has to be owned by a criminal.”

Even before Rule 41 was modified, the government was hacking private computers. In a child porn investigation, authorities used a search warrant to hack more than 8,000 computers and build cases against more than 200 defendants. But in some cases, the evidence was tossed when judges declared the warrants invalid.

Allen Butler, senior counsel at the Electronic Privacy Information Center, said the Justice Department would be on firmer legal ground if it sought approval from Congress for the powers in Rule 41.

“If the Justice Department had gone to Congress and asked for explicit statutory authority, what would have come out of that is a nuanced, detailed set of rules, but they pushed this through the rules committee, a more favorable venue,” he said.

For now, analysts say, courts will have to serve as protection against overintrusive hacking by the government.

Mr. Crocker said that was done in the North Korean botnet case.

“I think it’s reassuring and heartening to see the court putting narrow limits on the FBI and the type of information they are collecting,” he said.

Others say it is uncharted territory and raises too many questions for the courts to handle on their own.

“Congress has to assert its oversight,” Mr. Butler said. “The courts have little control because these are not questions that the traditional warrant application process was designed to answer.”