Name _____ Date/Assignment # _____ Per. ____

Federal Judge: Hacking Someone's Computer Is Definitely a 'Search'

Written by Joshua Kopstein, Contributor.
http://motherboard.vice.com/read/hacking-is-a-search-according-to-federal-judge
September 11, 2016 // 11:00 AM EST

Courts across the country can't seem to agree on whether the FBI's recent hacking activities ran afoul of the law—and the confusion has led to some fairly alarming theories about law enforcement's ability to remotely compromise computers.

In numerous cases spawned from the FBI takeover of a darkweb site that hosted child abuse images, courts have been split on the legality of an FBI campaign that used a single warrant to hack thousands of computers accessing the site from unknown locations, using malware called a Network Investigative Technique, or NIT. Some have gone even further, arguing that hacking a computer doesn't constitute a "search," and therefore doesn't require a warrant at all.

But a federal judge in Texas ruled this week that actually, yes, sending malware to someone's computer to secretly retrieve information from it—as the FBI did with the NIT—is a "search" under the Fourth Amendment.

"[T]he NIT placed code on Mr. Torres' computer without his permission, causing it to transmit his IP address and other identifying data to the government," Judge David Alan Ezra of wrote Friday, in a ruling for one of the NIT cases, in San Antonio, Texas. "That Mr. Torres did not have a reasonable expectation of privacy in his IP address is of no import. This was unquestionably a "search" for Fourth Amendment purposes."

As obvious as that sounds, not everyone agrees. Previously, another judge in Virginia stunningly ruled that a warrant for hacking isn't required at all, because a defendant infected with government malware "has no reasonable expectation of privacy in his computer."

That judgment was a leap from several other rulings, in which judges claimed that users of the Tor anonymity network, where the illegal site was hidden, have no expectation of privacy in their IP address—even though hiding your IP is the entire point of using Tor. The argument—which the Department of Justice apparently agrees with—states this is because Tor users technically "reveal" their true IP address to another computer when they first enter the Tor network, through an entry point called a "guard node." (That computer can not determine what sites the user visits, however)

But while the FBI's use of malware was definitely a search, Judge Ezra of Texas nevertheless denied the defendant's motion to suppress evidence obtained by the NIT.

That's because it can't be proven that the FBI "willfully" violated Rule 41(b), a procedural rule that's meant to stop judges from authorizing searches outside of their districts. The FBI is now controversially seeking to expand that rule, which would grant them the power to hack computers anywhere—not just within the jurisdictions where the hacking was authorized.

Instead, Judge Ezra wrote that the NIT warrant "has brought to light the need for Congressional clarification regarding a magistrate's authority to issue a warrant in the internet age, where the location of criminal activity is obscured through the use of sophisticated systems of servers designed to mask a user's identity."

Name _____ Date/Assignment # _____ Per. ____

Court Rules the FBI Does Not Need a Warrant to Hack a Computer

Written by Joseph Cox, Contributor
https://motherboard.vice.com/read/court-rules-the-fbi-does-not-need-a-warrant-to-hack-a-computer
June 23, 2016 // 05:30 PM EST

In one of the many ongoing legal cases surrounding a dark web child pornography site, a judge has written that the FBI did not require a warrant to hack a suspect's computer. According to activists, the ruling could have serious implications for how law enforcement is able to conduct remote searched: “The Court finds that no Fourth Amendment violation occurred here because the Government did not need a warrant to capture Defendant's IP address,” Henry Coke Morgan, Jr., a senior United States District Judge, wrote in an opinion and order on Tuesday. He adds that the government did not require a warrant to extract other information from the suspect’s computer either.

Morgan, Jr. was ruling on a number of motions pushed by the defense of Edward Matish, who is charged with child pornography crimes. Matish wanted access to the full source code of the malware deployed by the FBI, as well as evidence to be thrown out. The case stems from the FBI's investigation of child pornography site Playpen, which the agency took over in February 2015 and deployed a network investigative technique (NIT)—read: malware—in an attempt to identify the site's visitors.

Morgan, Jr. wrote that the warrant the FBI used to deploy the malware was above board, but he also took the rather extraordinary step of adding that a warrant would not have been necessary at all: “The implications for the decision, if upheld, are staggering: law enforcement would be free to remotely search and seize information from your computer, without a warrant, without probable cause, or without any suspicion at all,” Mark Rumold, senior staff attorney at the Electronic Frontier Foundation wrote in a blog post on Thursday.

Some of the opinion hinges around IP addresses, and whether they are private and subject to the Fourth Amendment, or already public: “Generally, one has no reasonable expectation of privacy in an IP address when using the internet,” Morgan, Jr. writes. This, he posits, is because we all voluntarily give up our IP addresses to third parties everyday, such as internet service providers. And when it comes to Tor, users have to connect to and disclose their IP address to an initial node of the network.

This argument echoes that found in other FBI hacking cases, in which judges have written that suspects have no reasonable expectation of privacy when it comes to their IP address. It came up in another Playpen case, and also a case affected by Carnegie Mellon University's Software Engineering Institute's broad attack on the Tor network in 2014. But those judges didn't go as far to say that a warrant wasn't necessary to hack a computer.

But, the FBI's malware actually grabbed more than just suspects' IP addresses. It also beamed their username and some other system information to the FBI; information that is undoubtedly *within* a user's computer—no two ways about it. This doesn't phase the judge either, who writes that the defendant “has no reasonable expectation of privacy in his computer,” in part because the malware collected a relatively limited amount of details:“The NIT only obtained identifying information; it did not cross the line between collecting addressing information and gathering the contents of any suspect's computer,” he writes.

“It seems unreasonable to think that a computer connected to the Web is immune from invasion,” Morgan, Jr. adds. “Indeed, the opposite holds true: in today's digital world, it appears to be a virtual certainty that computers accessing the Internet can—and eventually will—be hacked,” he writes, and then points to a series of media reports on high profile hacks. He posits that users of Tor cannot expect to be safe from hackers.

Rumold from EFF added that “the decision underscores a broader trend in these cases: courts across the country, faced with unfamiliar technology and unsympathetic defendants, are issuing decisions that threaten everyone's rights.”