Recent Botnet Takedowns Allow U.S. Government to Reach Into Private Devices

Scott R. Anderson ⋮ 21-27 minutes

The U.S. government has recently managed to make life more difficult for state-sponsored hackers. Armed with a new kind of nationwide search warrant, the FBI has taken down malware-infested networks (known as botnets) that Russian and Chinese hackers were using to cover their tracks. Many infected home office routers that were once part of botnets may no longer be put to work on behalf of hackers without the knowledge of their innocent owners.

While these court-authorized operations are a big cybersecurity success story, the breadth of these new nationwide hacking warrants raises troubling questions about the government's ability to reach directly into our personal computers, phones, and other devices. Search warrants do not offer sufficient judicial review of these complex government actions that wipe out code and data on Americans' computers, phones, or other devices—operations that, however beneficial, amount to mass hacking of Americans by their own government.

These new hacking warrants have been embedded within an outdated legal system. A government power to remotely seize, copy, or delete code that it says is criminal is a dangerous one, and the review of a single magistrate judge for probable cause is not enough to prevent abuse. Congress should reject the use of such nationwide hacking warrants in favor of an alternative legal framework that authorizes domestic cybersecurity operations to remediate botnets and other malware in carefully circumscribed situations, with more thorough review and oversight by the courts.

Government Efforts to Remediate Botnets and Other Malware

The Biden administration has enjoyed some significant victories in its recent efforts to combat botnets. Botnets put infected devices under the control of a malicious actor, known as a "bot herder." The hijacked devices can then be used for any number of illicit purposes, such as generating spam, spreading malware, or hiding illicit traffic by making it appear that it originated from the devices that are part of the botnet.

The Justice Department announced on Feb. 15 that the FBI had taken down a botnet being used by GRU Military Unit 26165, better known as Fancy Bear—the Russian hacking group made infamous through its hacking of the Democratic National Committee in 2016. This news comes on the heels of a similar operation

made public at the end of January in which the FBI disrupted a botnet that concealed malicious reconnaissance of U.S. critical infrastructure by Volt Typhoon, a state-sponsored hacking group acting for the People's Republic of China (PRC).

Both botnets consisted of hundreds of small office and home office routers inside the United States that were infected with malware that put them under the control of the hackers. The FBI wrested control from the hackers and ordered the botnet in essence to delete itself. The takedowns required the FBI to take the intrusive step of reaching directly into hundreds of privately owned small office and home office routers belonging to Americans.

Such aggressive actions represent a new phase in the government's fight against botnets and other malware. The earliest U.S. government effort to take down a botnet—Coreflood—took place in 2011. The FBI in that effort succeeded in slashing the number of infected machines in the United States from almost 800,000 to under 100,000 by informing internet service providers (ISPs) of the IP addresses of infected machines. The ISPs then provided notice and remedial tools to their subscribers. While the Coreflood effort significantly reduced the number of infected machines, the fact that 100,000 remained showed the limits of purely voluntary efforts. (For these and other insights, I am indebted to David Aaron, whose research into botnet remediation has been important to my understanding of the problem.)

More recent efforts to remediate botnets and other malware have made use of a new kind of nationwide hacking warrant available under Rule 41 of the Federal Rules of Criminal Procedure. Prior to 2016, judges could normally issue warrants for digital devices only if they were located within their own districts, as provided in Rule 41. Amendments to Rule 41 now allow judges to issue nationwide warrants—permitting the government to copy, seize, and delete data from devices anywhere in the country if they are infected with malware or are using "technological means" to conceal their location.

In 2021, the FBI deleted malware from computers affected by zero day vulnerabilities in Microsoft Exchange Server software. On that occasion, a PRC hacking group known as Hafnium had exploited the vulnerabilities to access email accounts and install web shells—a type of code that allows remote administration—enabling persistent access. Although Microsoft issued a patch, many users did not manage to install it.

The FBI used a nationwide hacking warrant to fill this cybersecurity gap, leveraging the malware by using it to issue a command to delete itself from unpatched machines—much as it would later do with the KV botnet used by Volt Typhoon. At the time, prominent legal scholar James Dempsey noted that the government had "crossed a Rubicon" by "remotely entering privately-owned

computers of entities not suspected of any wrongdoing and deleting malware from those computers, with at most only after-the-fact notice of its actions."

The Volt Typhoon Botnet Takedown

At the end of January 2024, the Justice Department made public its innovative use of a new form of search warrant to counter a substantial national security threat from the PRC, perhaps the United States's most significant cyber adversary. A PRC hacking team—given the name Volt Typhoon by Microsoft security researchers when they initially identified the threat in May of last year—had been breaking into private-sector computer networks since the middle of 2021. The hackers had been collecting intelligence and seeking to maintain covert access inside a variety of organizations, including those in the "communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors."

One of Volt Typhoon's goals has been to develop cyberwarfare capabilities in the event of a future conflict between the United States and China. Volt Typhoon was probing weaknesses in international communications infrastructure, with the goal of giving the PRC the power to disrupt communications between the United States and Asia with an offensive cyber operation, if ordered by Beijing.

Volt Typhoon was able to redirect its malicious traffic by taking advantage of a botnet. The botnet used by Volt Typhoon—the KV botnet—consisted of older Cisco and Netgear home office routers that were vulnerable to infection because their manufacturers no longer supported them with software security updates.

According to a special agent in the cyber squad of the FBI's Houston division, the government proposed to wrest control of the botnet from the hackers by "us[ing] the botnet's own functionality" to identify infected nodes. The FBI would then employ "the malware's communications protocols" to issue a command to delete itself from infected devices. The FBI essentially replaced the hackers as the bot herder, turning the botnet against itself. The FBI took additional steps to disrupt communications with the command-and-control (C2) nodes under the control of the bot herder.

According to the government, the operation worked. "The Justice Department has disrupted a PRC-backed hacking group," said Attorney General Merrick Garland in a Justice Department statement. The court-authorized FBI operation succeeded in "wiping out the KV Botnet from hundreds of routers nationwide," according to Deputy Attorney General Lisa Monaco.

The extent to which the operation has actually frustrated Volt Typhoon's larger goals is unknown. The FBI deleted malware only from U.S.-based routers; the KV botnet is worldwide. Even if a botnet remediation effort cleans up the vast majority of infected nodes—previous efforts have deleted malware from

hundreds of thousands of computers—a remnant of infected machines may allow a botnet to reform. In any event, even a successful takedown of the KV botnet will be only a temporary setback for China's hackers. Volt Typhoon or another group is likely to find or create a new botnet or use other tactics, techniques, and procedures to accomplish its objectives.

It was not the job of the magistrate judge who reviewed the Volt Typhoon operation to ask wide-ranging questions about its effectiveness or potential dangers if it went awry. Instead, the court was asked to sign off on a warrant that would make the government's seizure of private devices legal.

The Government's Theory: Warrants Make Government Mass Hacking Legal

To authorize the government's efforts to remediate botnets and other malware, the Justice Department and the FBI have developed a new playbook, employing a nationwide hacking warrant. In the Volt Typhoon case, Justice Department prosecutors obtained four virtually identical such warrants from federal magistrate judges in Houston, Texas.

Warrants that allow the government to search or seize private property in criminal investigations are a centuries-old tool with origins in British common law, refined and given teeth in the United States through the experience of the American Revolution, which inspired the Fourth Amendment's prohibition against unreasonable searches and seizures. While the warrants the FBI used to delete malware from hundreds of small office and home office routers have the same form as traditional warrants, a closer look shows just how little they have in common with them.

First, the purpose of these nationwide hacking warrants is not criminal investigation, but cybersecurity. The targets are not criminals, but devices belonging to the innocent victims of foreign hackers who will almost certainly never see the inside of a courtroom. The government's actions are best characterized as technical mitigation of a cybersecurity threat, which the warrant serves to make legal.

In the Volt Typhoon case, the warrant did not authorize one or a few searches or seizures within the geographic reach of the court's jurisdiction, the Southern District of Texas. Instead, it applied to any router anywhere in the United States infected with KV botnet malware. The warrant was also secret, at least temporarily. To ensure that the Volt Typhoon hackers did not interfere with the operation, the prosecutors sought and obtained an order allowing them to delay notice of the warrant to affected owners for up to 60 days.

Because Congress has not provided specific authority for such operations to disrupt botnets, delete malware, or otherwise counter malicious cyber activity on

privately owned devices, it is these warrants that allowed the FBI to secretly use a criminal botnet to reach into hundreds of devices in American homes and offices without consent or even prior notice to their owners. In other words, malicious code used in cybercrime is fair game for such hacking because it is either evidence of a crime or what is known as a fruit or instrumentality of crime. According to prosecutors, the malicious code on the devices was "property designed for," "intended for," or "used in" criminal activity, making it subject to seizure (and deletion) by the government.

The Rise of the Mass Hacking Warrant

General warrants—called writs of assistance in colonial times—were one of the abuses the framers intended to prohibit when they adopted the Bill of Rights. Under the Fourth Amendment, which prohibits "unreasonable searches and seizures," warrants may not be issued without "particularly describing the place to be searched, and the persons or things to be seized."

Rule 41 of the Federal Rules of Criminal Procedure fleshes out the details of how warrants that satisfy these constitutional safeguards are issued by federal judges and magistrates, including where property may be searched or seized. Prior to 2016, Rule 41 generally limited searches and seizures—whether physical or digital—to places, objects, or devices within the court's jurisdiction. An amendment to Rule 41 adopted in 2016 eliminated this geographic limit for digital searches and seizures in two circumstances—(a) where the location of computers or devices "has been concealed through technological means," such as through a Tor browser or virtual private network that obscures the user's IP address, or (b) when devices "have been damaged without authorization" by (for example) being infected with malware. In either case, a magistrate judge may "issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside th[e] district"—authorizing federal law enforcement to launch a hacking operation to copy, delete, or modify data or code within any computer anywhere in the United States.

These changes to Rule 41 have their origins in the FBI's fight against online distribution of child sexual abuse material (CSAM). Even before the 2016 amendments, the government was using mass hacking techniques to circumvent software used by consumers of such abusive and illegal content to hide their tracks. A CSAM distribution site on the dark web—chillingly named Playpen—was accessible to visitors only if they used a Tor browser, which provides enhanced security by scrambling the routing of user requests so that specific users cannot be identified through their IP addresses. The FBI took over the website and used it to investigate the perpetrators.

The FBI's mass hacking operation was authorized in two steps. First, a single search warrant was issued to authorize the delivery of government malware—

which the FBI calls a Network Investigative Technique (NIT)—to defeat the Tor browsers used to visit the (then government-controlled) Playpen site. Second, after these machines were unmasked, the government obtained individual search warrants to probe the visitors' computers for the illegal CSAM itself.

In the Playpen case, the FBI's investigation resulted in well over 100 arrests. Defense attorneys challenged the NIT warrant, arguing that because it did not—and could not—apply only to computers within the jurisdiction of the federal magistrate who issued it, it was illegal under both Rule 41 and the Fourth Amendment. Multiple federal courts agreed with this argument, although generally without excluding the damning CSAM evidence that was the ultimate fruit of the illegal NIT warrant because they found the government had acted with good faith. See, for example, *United States v. Taylor*.

Hoping to forestall future challenges, the Justice Department successfully lobbied the Judicial Conference to change Rule 41—not only to legalize NIT warrants but also to authorize hacking operations to delete malware from victim computers. At the time, opponents of the change raised concerns about how broadly the government's powers might extend.

It is time to revisit those concerns. As the government's recent botnet takedowns show, the nationwide hacking warrants that Rule 41 now allows make legal what amounts to domestic cyber operations to delete illicit code. In the Volt Typhoon and Fancy Bear cases, the FBI used its power for a very good purpose: to clean up infected small office and home office routers and disrupt foreign hacking operations that were using those devices to collect intelligence on U.S. critical infrastructure. Yet such a sweeping power could easily be abused.

A general digital warrant that allows a single judge to authorize a mass hacking operation that deletes "illegal" code directly from devices across the nation offers the potential for all sorts of mischief. The government argues that its operations satisfy the particularity requirements of the Fourth Amendment's warrant clause because they specify the code they are seeking to delete and the devices they are seeking to access, even if there are a large number of them and neither the government nor the authorizing judge knows where they are, who possesses them, or other details normally described in a traditional search warrant.

The Fourth Amendment's more than two-centuries-old language was drafted with physical searches in mind, generally of contraband. How these words apply in the context of complex hacking operations targeting illegal code is not obvious and is beyond the scope of this piece. Whether constitutional or not, to give the government a creeping power to launch nationwide cyber operations in circumstances where a single judge agrees that the code or data residing on hundreds of thousands—if not millions—of computers, phones, or other devices may be illegal at the very least raises the specter of abuses the framers intended to prevent.

As Justice Louis Brandeis wrote a century ago of government wiretapping —"'That places the liberty of every man in the hands of every petty officer' was said by James Otis of much lesser intrusions than these."

Why Easy Cases Make Bad Law

It is tempting to regard the amendments to Rule 41 of the Federal Rules of Criminal Procedure simply as a success. They have authorized valuable cybersecurity operations by the government, apparently without negative consequences. The Justice Department and the FBI deserve praise for rooting out a complex cyber operation targeting the devices of innocent Americans, and for obtaining court permission to do so. Russian, Chinese, and other state-sponsored hackers are a serious threat to U.S. national security, and most Americans would be happy to learn that the government has deleted malware from their old home routers.

But some dangerous implications flow from the legal theory the government used. While Rule 41 currently limits the government's nationwide hacking to the circumstances discussed above (malware cleanup and use of technology to conceal a device's location), nothing prevents the rule from being expanded further. If nationwide hacking can be authorized by a criminal search warrant, it could be used to delete virtually any code or data the government says is being used illegally or is evidence of crime.

Criminal warrants are largely concerned with whether the government has satisfied the legal standard of probable cause before searching or seizing a device. The Supreme Court has emphasized that probable cause deals merely in "probabilities" and requires "nontechnical" and "common sense judgments" that are "less demanding" than the standards "used in more formal legal proceedings."

What prevents the government from using the same theory to hack into devices using peer-to-peer file sharing, visiting cryptocurrency exchanges, or even facilitating access to reproductive health care? In all these cases, private devices might be harboring code or data that a prosecutor believes is facilitating crimes like copyright infringement, tax evasion, or obtaining an abortion. Would Americans trust the government to engage in nationwide hacking operations in such cases, based only on a one-sided presentation of government prosecutors —an ex parte showing—of probable cause before a single federal judge?

The government has so far limited its use of mass hacking warrants to seemingly easy cases—in which it has engaged in carefully crafted cyber operations to disrupt very serious criminal and national security threats. "Hard cases make bad law" captures the idea that judges must sometimes tolerate injustice rather than mangling broad legal principles to accommodate idiosyncratic situations. Yet easy cases may also make bad law.

Criminal law is expansive—and expanding. If Congress were to approve legislation that effectively criminalizes end-to-end encryption—and such legislation has been proposed year after year—the very software on which we rely to protect our personal communications and data might become illegal. A rule that permits the government to reach into our devices and remotely delete code or data it says is illegal on the low standard of a criminal search warrant—probable cause—is a recipe for abuse.

A Legislative Alternative for Court Review of Government Cybersecurity Mitigation

Congress should craft specific legislation to authorize such operations for the remote deletion of malware, with appropriate technical and legal safeguards, where voluntary approaches have proved ineffective. While a complete legislative proposal is beyond the scope of this piece, any bill should include the following:

- *Carefully delimited authorization for cybersecurity remediation operations.* The government has had success with taking control of botnets and other malware, ordering malicious code to delete itself. A law should authorize such operations, where (a) the targets are devices that have been hijacked from their innocent owners, (b) the operation will not interfere with the legitimate functions of the devices, and (c) the operation does not seek and will not copy or acquire any other code or data on the targeted devices.
- *Further study of government-authorized malware for investigative purposes (so-called Network Investigative Techniques).* The mass delivery of government malware to interfere with user efforts to keep their location private raises serious (and possibly insurmountable) civil liberties, privacy, and cybersecurity concerns. Such operations should be authorized, if at all, only after careful study and should not be combined with a bill that addresses the very different issue of cybersecurity mitigation.
- *Technical review of cybersecurity mitigation operations for unintended consequences.* Courts should be authorized (and perhaps required) to seek independent technical advice on the potential downsides of any operation the government seeks to authorize under the new law. They should not have to rely on the government's say-so.
- *Protections for civil liberties and privacy.* Courts should be able to impose minimization or other detailed protections, as appropriate, for any data that might be obtained—on purpose or by accident—in the course of an authorized operation.
- *Reporting and oversight.* The government should be required to conduct a technical audit of its operation and report back to the court on the outcome of any authorized operations, including whether it was effective in achieving its intended goals, and any mistakes or problems encountered.

The takedown of a botnet used by the PRC Volt Typhoon group shows that government-sponsored remote operations to delete malware from affected devices has a place in countering cybersecurity threats. Legalizing such hacking by stretching the concept of criminal warrants beyond recognition is not the right answer.