Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Disrupting Botnets: An Overview of Seizure Warrants and Other Legal Tools

May 16, 2024

In January and February 2024, the Department of Justice (DOJ) announced the disruption of two different foreign-state-sponsored botnets. The term *botnet* is a portmanteau of "robot" and "network." It generally refers to a network of computers and computerized devices infected with malware (i.e., unwanted, malicious software including viruses and spyware) that may be remotely managed to perform various tasks without the knowledge of the underlying owners. Botnets can potentially be used by criminals for espionage, fraud, theft, ransomware-based extortion, and impairment of websites and internet infrastructure through cyberattacks.

Botnets may be of interest to Congress in light of the dangers they pose, and Congress may have several options at its disposal to remediate them. These options include revising the legal authorities relied on by DOJ to disrupt botnets, creating new criminal laws targeting botnet-related conduct, and setting cybersecurity standards for computerized devices to limit the likelihood that those devices become co-opted as part of a botnet. Accordingly, this Legal Sidebar provides an overview of several legal authorities relevant to combatting botnets, focusing primarily on search and seizure warrants under the Federal Rules of Criminal Procedure and also discussing legal authorities governing stored communications, pen-trap devices, and injunctive relief against fraud. It concludes with a discussion of congressional considerations. This Sidebar does not cover the various criminal statutes that may be used to prosecute individuals in connection with botnet-based crime, but an overview of key statutory provisions may be found in CRS Report R47557, *Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes*, by Peter G. Berris (2023).

Botnet Disruption Through Search and Seizure Warrants

Many of DOJ's efforts to remediate botnets have relied on search and seizure warrants. The Supreme Court has said that, with some exceptions, the Fourth Amendment requires law enforcement officers to obtain a warrant when they search or seize property. Rule 41 of the Federal Rules of Criminal Procedure and the Fourth Amendment itself establish a number of requirements for obtaining a search warrant.

Pursuant to the Fourth Amendment, a warrant must be based on probable cause, a standard the Supreme Court has described as "incapable of precise definition or quantification into percentages." Exact formulations vary, but the Supreme Court has characterized the probable-cause standard as "the kind of 'fair probability' on which 'reasonable and prudent'" people act. Probable cause is a higher standard than "reasonable suspicion" but does not require proof that something is "more likely true than false." To satisfy the probable-cause standard to obtain a search warrant, law enforcement must generally show a likelihood that (1) the materials sought are "seizable by virtue of being connected with criminal activity" and (2) the materials "will be found in the place to be searched." Property that may be searched and seized through a warrant generally includes "(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; [and] (3) property designed for use, intended for use, or used in committing a crime." Of particular relevance to botnets, Rule 41(e) expressly authorizes courts to issue warrants for "seizure of electronic storage media or the seizure or copying of electronically stored information" to the extent that the media or information may fall within one of these categories.

Under Rule 41, law enforcement may make the probable-cause showing through a written affidavit or, if "reasonable under the circumstances," by sworn testimony—both of which embody the Fourth Amendment requirement that a warrant must be supported by "oath or affirmation." Once law enforcement provides the affidavit or testimony to a judge in the correct venue (discussed below), that judge "must issue the warrant if there is probable cause to search for and seize" the property. The Fourth Amendment dictates that the resulting warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized."

Venue for Botnet Warrants: Rule 41(b)(6)(B)

Rule 41(b) governs the appropriate venue for seeking a warrant. Among other things, Rule 41(b) authorizes issuance of a warrant by a federal magistrate judge in the district where the property to be searched is located. In 2013, DOJ recommended an amendment to Rule 41 to address, among other things, situations "where the investigation requires law enforcement to coordinate searches of numerous computers in numerous districts." DOJ explained that the preexisting version of Rule 41 posed an obstacle in the botnet context because "a large botnet investigation is likely to require action in all 94 districts, but coordinating 94 simultaneous warrants in the 94 districts would be impossible as a practical matter." The Advisory Committee on Criminal Rules for the Judicial Conference, the "the national policymaking body for the federal courts," echoed these concerns, recognizing the "increasingly common" problem of botnets and the limitations in using Rule 41 warrants to combat them given their cross-jurisdictional nature. In response, the Advisory Committee drafted an amendment to Rule 41, which took effect in 2016 as Rule 41(b)(6)(B):

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Rule 41(b)(6)(B) offers a more geographically flexible alternative to preexisting warrant venue provisions if two requirements are satisfied. First, Rule 41(b)(6)(B) applies only in investigations of 18 U.S.C. § 1030(a)(5) violations. That provision is part of the Computer Fraud and Abuse Act (CFAA)—a civil and criminal law that prohibits a range of computer-based acts. Section 1030(a)(5) bars several acts that result in damage to internet-enabled computers. In practice, § 1030(a)(5) encompasses various types of hacking and can reach a number of activities involving the creation or use of a botnet. Second, Rule 41(b)(6)(B) applies only if the protected computers subject to § 1030(a)(5) are located in at least five judicial districts. As discussed, this threshold is often met in botnet investigations, but if the warrant's subject is a botnet component in a single district, then prosecutors may still employ the other venue provisions of Rule 41.

Select Examples

Cyclops Blink

On a number of occasions, federal prosecutors have relied on Rule 41(b)(6)(B) to obtain warrants to disrupt botnets. One example involved DOJ's remediation of Cyclops Blink, "a two-tiered global botnet of thousands of infected network hardware devices" allegedly under the control of Russia's military intelligence branch—the GRU. According to prosecutors, the GRU employed a common system where two layers of devices were compromised. The first layer comprised the end devices constituting the bots in the botnet. The second layer comprised a smaller number of other devices that constituted the command-and-control (C2) infrastructure to communicate and provide instructions to the bots.

To combat Cyclops Blink, prosecutors sought and obtained a warrant in the Western District of Pennsylvania under Rule 41(b)(6)(B) to remotely search computers in at least five judicial districts. In the warrant application, DOJ sought authorization to search Russian-controlled devices and to "retrieve data from the malware," "remove the malware from those devices," and block remote access to the devices. According to DOJ, the malware on the C2 devices qualified as electronically stored information constituting evidence and instrumentalities of § 1030(a)(5)(A) violations. In a press release following the court-authorized disruption, DOJ said it disabled the C2 devices and severed Russia's control of the bots without actually accessing the devices constituting the botnet.

Kelihos

Another example involved the Kelihos botnet. According to DOJ, the Kelihos botnet was "a global network of tens of thousands of infected computers under the control of a cybercriminal that was used to facilitate malicious activities including harvesting login credentials, distributing hundreds of millions of spam e-mails, and installing ransomware and other malicious software." Unlike the C2 model employed by botnets such as Cyclops Blink, the Kelihos botnet relied on a decentralized Peer-To-Peer (P2P) model, which distributed botnet control across the underlying infected devices. To disrupt the Kelihos botnet, the government sought and received authorization for numerous warrants pursuant to Rule 41(b)(6)(B) to search infected computers. Given the P2P nature of the Kelihos botnet, DOJ's warrant applications requested authority to reroute botnet internet traffic to a dead-end server controlled by the FBI. As the warrant applications explained, by permeating the botnet with "new routing information," the "Kelihos infected computers ... cease[d] any current malicious activity and learn[ed] to only communicate with the sinkhole."

Timing, Execution, and Notice of Warrant

With exceptions, Rule 41(e)(2)(A)(i) generally requires execution of a warrant within 14 days of issuance, and many Rule 41(b)(6)(B) applications request the standard 14 days. Rule 41(e)(2)(A)(ii) requires warrant execution during the daytime absent good cause for an exception. In the context of botnets, "the operation and schedule of the botnet may not be within the control of the FBI and there will be a straightforward justification for why execution will need to occur at any time of day or night." Courts have granted numerous Rule 41(b)(6)(B) warrants requesting authorization for execution during the day or night.

Rule 41(f)(1)(C) generally requires that "a copy of the warrant and a receipt for the property taken" be given to the person whose property was searched or seized pursuant to the warrant. In the digital context, however, the Advisory Committee recognized that "when an electronic search is conducted remotely, it is not feasible to provide notice in precisely the same manner as when tangible property has been removed from physical premises." Thus, it proposed an additional amendment to Rule 41, added to Rule

41(f)(1)(C), that requires the officer executing the warrant to make "reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied." This required service "may be accomplished by any means, including electronic means, reasonably calculated to reach that person." In practice, prosecutors have provided notice of botnet-related warrants by, for example, posting public notice on the FBI website and requesting that internet service providers notify clients with infected devices.

Federal prosecutors often request court authorization to delay providing notice of Rule 41(b)(6)(B) warrants. For example, in one application, prosecutors argued that providing "immediate notice to the subscriber or user of the infected computer would seriously jeopardize the ongoing investigation, as such a disclosure would likely become known to the [botnet] administrators and would give them an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution." Rule 41(f)(3) permits courts to delay notice at the request of prosecutors, when authorized by statute. One statute that prosecutors have relied on in this context is 18 U.S.C. § 3103a(b), which authorizes delayed notice if: (1) the court finds "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result"; (2) the "warrant prohibits the seizure of any tangible property" and certain electronic communications, among other things; and (3) the "warrant provides for the giving of such notice within a reasonable period" that is generally "not to exceed 30 days after the date of its execution."

Additional Legal Tools for Disrupting Botnets

Prosecutors have relied on a number of other statutory authorities in disrupting botnets, sometimes in conjunction with Rule 41(b)(6)(B). Select examples include:

- **Asset forfeiture:** Criminal asset forfeiture is a statutorily created consequence of conviction through which the federal government may confiscate tangible and intangible property connected with certain federal crimes. Depending on the particular offense, property subject to criminal forfeiture may include, among other things, property "involved in [the] offense," "constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of [the] violation," or "traceable to the gross proceeds obtained, directly or indirectly, as a result of such violation." Another form of asset forfeiture is civil asset forfeiture—a statutory regime enabling DOJ to file lawsuits against certain property that is derived from, or used in, various crimes. In 2018, DOJ used criminal asset forfeiture authorities to obtain a warrant to seize a domain that was part of a botnet's C2 infrastructure. A further examination of asset forfeiture may be found in CRS Report 97-139, *Crime and Forfeiture*, by Charles Doyle (2023).
- **Injunctive relief:** 18 U.S.C. § 1345 permits federal prosecutors to bring civil actions to enjoin certain types of fraud. Under the statute, a district court may enter pre-trial restraining orders or prohibitions or take other actions as "warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought." Another source of injunctive relief is 18 U.S.C § 2521, which authorizes federal prosecutors to seek restraining orders and other relief to enjoin conduct such as unlawful interception of certain electronic communications. In 2014, DOJ relied on these dual authorities to obtain court authorization to combat the Gameover Zeus ("GOZ") botnet. DOJ obtained an order directing several internet domain registries to, among other things, "block access to the domain names used to control GOZ and to redirect connection" to a substitute server.
- **Stored Communications Act:** 18 U.S.C. § 2703 authorizes law enforcement to compel service providers to disclose certain customer communications or records through

warrants, court orders, and subpoenas. In 2023, federal prosecutors obtained a § 2703 warrant to obtain customer information pertaining to Qakbot botnet infrastructure. For more information on § 2703, see generally CRS Legal Sidebar LSB10801, *Overview of Governmental Action Under the Stored Communications Act (SCA)*, by Jimmy Balser (2022).

- **Pen-trap devices:** A pen register is a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." A trap and trace device is a "device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." Both are defined to exclude the contents of communications. Federal prosecutors have sought court authorization for pen-trap devices in the botnet context. Generally speaking, pen-trap devices enable law enforcement to identify the victims of a botnet by collecting the internet protocol addresses that connect to botnet infrastructure.

Private entities have also taken legal actions to remediate botnets. For example, in 2020 Microsoft obtained a preliminary injunctive order to disrupt the Trickbot botnet. In its complaint, Microsoft relied on the CFAA, intellectual property law, and various tort claims.

Congressional Considerations

Congress potentially has numerous avenues for legislating with respect to botnets. It could, for example, modify or supplant one or more of the legal authorities currently employed by federal law enforcement to disrupt botnets. For example, one bill introduced in the 117th Congress—the International Cybercrime Prevention Act—contained a provision intended to enhance "prosecutors' ability to shut down botnets." It would have, among other things, amended § 1345 (the provision permitting injunctive relief for certain types of fraud) to permit relief for actual or imminent violations of § 1030(a)(5)—assuming the conduct damaged (or *would* damage) at least 100 protected computers in a one-year period. It described one type of qualifying damage as "installing or maintaining control over malicious software on the protected computers that, without authorization, has caused or would cause damage to the protected computers," a description seemingly encompassing botnets. The other type of qualifying damage in the bill was "impairing the availability or integrity of the protected computers without authorization," which could potentially describe the impact on a protected computer by co-opting it to serve as part of a botnet. Another bill introduced in the 117th Congress, the CCP Trade Secrets Act, contained largely similar provisions.

Congress could also consider seeking to combat botnets in other ways, including by criminalizing additional botnet-related conduct or by imposing minimum cybersecurity standards on new internet-connected devices like routers and Internet of Things devices to limit their vulnerability. (The Federal Communications Commission issued a Notice of Proposed Rulemaking on this subject in March.) At least one of the botnets disrupted by DOJ relied on devices "that were vulnerable because they had reached 'end of life' status" and "were no longer supported through their manufacturer's security patches or other software updates."

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.