COUNCIL *on* FOREIGN RELATIONS

CYBER BRIEF

Cleaning Up U.S. Cyberspace

Robert K. Knake
December 2015

This Cyber Brief is part of the Digital and Cyberspace Policy program.

The U.S. government's effort to persuade other countries to adopt norms of responsibility for cyberspace faces a significant obstacle: computers located in the United States host much of the malicious software used to carry out cyberattacks. Botnets—groups of compromised computers under the control of a malicious actor—are regularly used to distribute spam, spy, break passwords, harvest credentials, and engage in distributed denial-of-service (DDOS) attacks. When botnets located in the United States attack computers in other countries, the victims could view the United States as either being behind the attacks or an accomplice in violation of the norms the United States is pressuring other countries to uphold.

Other countries have nearly eliminated botnets operating under their jurisdiction, but the U.S. government has not aggressively pursued the issue, and U.S. Internet service providers (ISPs) have chosen mostly to ignore this type of malicious traffic when it emanates from their customers. The U.S. government should partner with the private sector to identify infected systems, assist with removal of the malicious software, and align incentives so that owners of infected systems recognize an interest in keeping their systems from being reinfected. To achieve this objective, ISPs should notify their customers of an infection and quarantine systems that remain infected, and work with partners in other industries to establish a center to assist customers with remediation. In addition, Congress should pass legislation that allows victims of DDOS attacks to sue companies whose systems participate in the attacks.

BACKGROUND: STATE RESPONSIBILITY IN CYBERSPACE

In 2013, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications produced a report advocating a series of norms to govern state behavior in cyberspace. Chief among these was that states should be responsible for cyberattacks emanating from their territory. When the group met again in 2015, its report went further, arguing that states must provide assistance to stop attacks emanating from their territory.

The importance of this norm is hard to overstate. The so-called attribution problem, where the culprit behind a cyber incident cannot easily be identified, is in reality, a responsibility problem. When evidence points toward a country's involvement in a cyberattack, the country typically claims that the computers that sent malicious traffic were compromised by a third party in a different country or by criminal groups not under the government's control. When a victim of a cyberattack requests assistance, the government of the country from where the attack emanated either ignores the request or says that its investigation teams are overwhelmed. The trail goes cold. China, in particular, is a master at playing this game, often citing how it is also a victim of cybercrime and, as a developing country, cannot afford to provide assistance. Recognition of a responsibility to provide assistance in stopping cyberattacks puts the onus on the country that hosted the attack to prove through its cooperation that it was not behind the attack. The norm closely adheres to notions of sovereign responsibility that have emerged in the last decade in response to terrorist activity.

While the further development of this norm in the UN report is a positive step, the implications for the United States could be troubling. This year, Symantec ranked the United States as the world's second-largest source of botnet infections. McAfee Labs found that the United States

hosts the most botnet control servers, with 21 percent of the worldwide total. No other country broke out of single digits. (Russia and China are each responsible for 5 percent.) In its most recent reporting, Akamai found that the United States is the third-biggest source of DDOS attacks.

CHALLENGES

That the United States ranks so high on lists of origin countries for malicious cyber activity is not surprising. There are more computers than people in the United States (not even counting smartphones), high bandwidth, and many powerful servers. Moreover, the United States promotes and abides by a vision of an open Internet; the controls that would make it more difficult to use U.S. infrastructure to carry out criminal activity could also be used to control speech and repress dissent. Internet openness not only aligns with U.S. values but also has led to economic growth and efficiency. Securing systems takes time and money and is therefore viewed by some as a hindrance to innovation.

Yet the placement of the United States at the top of the list for botnets and DDOS attacks undermines efforts to promote norms of cyberspace responsibility. Other countries, notably Finland, have been able to nearly eliminate botnets by monitoring for infections and quarantining infected computers from the Internet. U.S. ISPs and hosting providers—such as GoDaddy and Rackspace, two companies whose powerful servers are often used to carry out malicious attacks—have resisted embracing such an approach.

ISPs argue that monitoring their customers' network flows for malicious activity and notifying their customers when they detect it will be viewed as an unreasonable intrusion on customer privacy. They argue that, under current regulations, they are simply responsible for passing on data regardless of its content. Under the Electronic Communications Privacy Act, ISPs can only monitor for malicious activity that interferes with their ability to maintain their systems; under the concept of network neutrality, they cannot choose what traffic they allow on their network or throttle the speed at which traffic is moved. Both consumer ISPs and hosting providers operate on relatively thin margins. Notifying customers of infection creates demands for expensive and time-consuming remediation assistance.

However, ISPs' legal concerns over monitoring and notification are overstated. Customers sign end-user licensing agreements that allow ISPs to monitor for malicious activity. The Cybersecurity Information Sharing Act, recently passed by Congress, would remove this concern entirely. Cost concerns are justifiable but can be addressed by spreading the burden to the other sectors of the economy, all of which benefit from a clean and vibrant Internet.

RECOMMENDATIONS

As the U.S. government pushes other countries to accept responsibility for malicious cyber activity emanating from their territories, it should also pressure private companies and individuals in the United States to take responsibility for malicious activity on their networks and systems. Congress, the White House, ISPs, and sectors with an interest in reducing malicious activity

online (such as the financial industry) should all work together to improve cyber hygiene, monitor for infections, and take action when notified of infections.

While ISPs should not be made wholly responsible for remediating botnet infections, only ISPs are positioned to accurately attribute malicious traffic to specific customer accounts. With an Internet protocol address and timestamp, they can identify down to the individual customer the computers participating in a DDOS attack or showing other signs of infection. Under a voluntary agreement with the Federal Communications Commission, the major ISPs have agreed to a notification protocol. However, under the agreement, ISPs only need to respond to customers who want to know if they are infected; they do not have to actively inform the customer in advance. Some ISPs, notably Centurylink, Comcast, and Verizon, have established programs to notify customers if their accounts are associated with infected systems. These programs can serve as a model for other ISPs.

In addition to notifying customers, ISPs should work with industry partners to develop a national protocol for quarantining infected computers. After multiple notifications of the presence of an infection, or when a device is participating in a DDOS attack, ISPs and hosting providers should block or limit access to the Internet for all traffic from the infected device.

ISPs should also work with partners in other industries to jointly establish a National Remediation Center, modeled on Japan's Cyber Clean Center, as a publicly available resource for individuals and small businesses to get help with cleaning up infected machines. The center should be privately funded as an Information Sharing and Analysis Organization under Executive Order 13691. The financial industry, which suffers many of the ill effects of infected consumer computers through DDOS attacks and account takeovers, should actively support the center, as should the makers of hardware and software whose products often contain vulnerabilities that are exploited by malware. Companies in these sectors have a clear financial interest in cleaning up U.S. cyberspace. The center should also produce real-time public reporting on botnet infection rates within ISPs, hosting companies, and large enterprises to name and shame them.

Finally, Congress should create a private right of action for companies suffering from a DDOS attack to sue companies that hosted machines participating in the attack. In the early 1990s, when fax machines used a type of thermal paper that was very expensive, "fax spamming" was a significant problem for businesses. In response, Congress created a national "do not fax" list and a private right of action that allowed businesses that had registered on the list the right to sue fax spammers for $500 per violation in small-claims court. The problem of fax spamming disappeared almost overnight. Congress should create a similar private right of action for DDOS attacks, allowing the victim to sue the owners of any machine that participates in the attack for failing to stop it upon notification.

Together, these steps would provide the incentives for the private sector to clean up U.S. cyberspace through a system that places responsibility on the owners and operators of infected systems, establishes processes for monitoring and notification, and provides assistance with remediation. Such a system would demonstrate that the United States is serious about its commitment to complying with international norms and preventing cyberattacks.

About the Author

Robert K. Knake is the Whitney Shepardson senior fellow at the Council on Foreign Relations. He served from 2011 to 2015 as director for cybersecurity policy at the National Security Council. In this role, he was responsible for the development of presidential policy on cybersecurity, and built and managed federal processes for cyber incident response and vulnerability management. A frequent writer and speaker on cybersecurity, he has been quoted by the *New York Times*, *Wall Street Journal*, and *Washington Post* and has appeared on CNN, MSNBC, and National Public Radio. He holds undergraduate degrees in history and government from Connecticut College and a master's degree in public policy from Harvard's Kennedy School of Government.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

The Digital and Cyberspace Policy program addresses one of the twenty-first century's most pressing challenges: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program's fellows produce timely analysis on the most important issues in cyberspace. Cyber Briefs are short memos that offer concrete recommendations on cybersecurity, Internet governance, online privacy, and the trade of digital goods and services.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.