PUBLICATION

The October DDoS Attack – Separating Fact from Fiction

Authors: Samuel Lanier Felker, Zachary B. Busey
November 15, 2016

Baker Donelson's Data Protection, Privacy and Cybersecurity attorneys are pleased to introduce a series of client alerts that will address significant cyber-threats to your business and how you can protect yourself by thoughtful and timely planning before an emergency arises.

Proper planning includes recognition of the threats, assessment of the risk and then examining the tools at your disposal to mitigate the risks. The series will address your options, from adopting appropriate IT policies and procedures to acquiring contractual indemnity and insurance for specific loss risks. When there is a recommended tech solution available, we will consult with leading expert vendors and provide their input. We often hear that in today's tech environment, it's not a matter of whether you will be hacked, but when; therefore, we want to help you be well-prepared for the challenges ahead. Our series will help you get ahead of the game. Now to our first in the series…

Threat One: The October DDoS Attack – *Separating Fact from Fiction*

A few weeks ago the cybersecurity world received its own "October Surprise" when a DDoS attack (short for Distributed Denial of Service) disrupted dozens of major websites, including Paypal, Twitter, Amazon, Spotify, CNN.com and Reddit. A DDoS attack involves using multiple compromised systems, often infected with Trojan malware, to target, overload and shutdown a single system or website. Although various types of DDoS attacks have existed for years, this one generated headlines and extra attention because it exploited security risks specific to the growing "Internet of Things" phenomenon. Some have predicted gloom and doom as a result of the shocking October DDoS attack. It is time to separate fact from fiction and identify how best to protect your company or business.

Did hackers attack the major websites?

No, this claim is fiction. The attack targeted Dyn, a global domain-name-systems (DNS) provider based in New Hampshire. Prior to the attack, a Dyn researcher published and presented a paper on DDoS attacks. Dyn was also investigating a DDoS attack on the paper's co-author. Apparently in retaliation for all of this, a still-unknown group of malicious hackers launched the October 21 DDoS attack.

Like other DNS providers, Dyn translates domain names (e.g., www.twitter.com) to IP addresses. A computer or phone then uses the IP address to find and load the requested website. During the attack, Dyn was so overloaded with Internet traffic that it could not perform these translations. As a result, users were unable to reach Twitter and the other major websites relying on Dyn. These websites were affected by the attack, but the websites themselves were not attacked.

Was this the largest DDoS attack ever?

Yes, this claim is fact, at least as far as we know. It is estimated that the attack used a data rate of 1.2 terabytes per second. A terabyte is roughly 200,000 songs. So, in all, the attack overwhelmed Dyn with Internet traffic equivalent to downloading 240,000 songs per second. By comparison, it takes an iPhone about

one minute to process the download of a single song. To process the Internet traffic directed at Dyn during the attack, an iPhone would have to download 14,400,000 songs per minute.

Did the "Internet of Things" allow the attack to happen?

Not quite; this one is part fact, part fiction. The attack was launched using "Mirai," an automated Internet bot. Mirai seeks out devices that (1) are connected to the Internet and (2) have default administrative passwords (like, 00000, 11111 or "admin"). Mirai uses default administrative passwords to take control of the devices, allowing all devices to be linked together. Once linked, the devices are used to execute a DDoS attack. That is, all of the devices are used to simultaneously direct an overwhelming amount of Internet traffic to a specific system or website.

The "Internet of Things" is the recent phenomenon in which everything – refrigerators, cameras, picture frames, children's toys, etc. – has an independent Internet connection. Hence the phrase: the Internet of Things. Mirai exploits the Internet of Things only to the extent admin passwords on Internet-connected devices had not been changed. Notably, while some Internet-connected devices allow users to create a new admin password, not all allow users to eliminate the default admin password. Internet-connected devices most susceptible to Mirai are those in which the default admin password is permanently coded to the device (i.e., the default admin password cannot be changed). Mirai exploits this, gains control of the device and then allows all devices to be coordinated, for example, in a DDoS attack.

Can companies guard against DDoS and other cyber-attacks?

While it is true that companies can't police the Internet, they can certainly take important steps to protect themselves from DDoS attacks. It starts with employees and the workplace. Like anything employees bring into the workplace, Internet-connected devices can and should be regulated. While the Mirai bot used such devices to coordinate a DDoS attack, they can just as easily be used as a backdoor into a company's private LAN. For this reason, written policies should make clear that only approved Internet-connected devices can be used in the workplace, and even then, the devices should not connect (wirelessly or otherwise) to the company's private LAN. A separate, isolated network should be used. By doing so, the Internet-connected devices can access a network, but they cannot access shared drives, computers or printers on a company's private LAN. This same logic applies to the Internet-connected refrigerator in the break room, the smart TV in the waiting area or the wirelessly connected thermostats throughout the building. None of these devices should be connected (wirelessly or otherwise) to the company's private LAN.

As for devices connected to the private LAN, companies need to proceed with caution. Convenience should not trump security. Internet-connected printers, shared drives, displays and videoconferencing equipment provide tremendous convenience, but they also create yet another access point that must be secured. Think about a brick-and-mortar building – a brick-and-mortar building with five doors is easier to secure than a brick-and-mortar building with 15 doors. A private LAN is no different – fewer access points makes it easier to secure.

Additionally, to the extent your company hosts content or provides online services, one of the best ways to prepare for a DDoS attack is to over-prepare. The point of a DDoS attack is to overwhelm a system or website. By ensuring your website or system can handle traffic beyond what it experiences at times of peak demand, the website or system is better equipped to withstand a DDoS attack. Companies can also turn to hosting services or Internet service providers for assistance. Google, for example, offers Project Shield. In the event of a DDoS attack, Google routes traffic through its servers, which then filters malicious traffic and by design, can withstand large volumes of traffic. While only specific websites and services qualify for Project Shield, there are a variety of similar services. We can pair your company with the service that best fits your needs.

Do cyber-insurance policies cover DDoS attacks?

In last month's alert, available here, we discussed cyber-insurance in detail. A DDoS attack brings with it a few unique considerations. Some policies, for example, may cover outages and lost sales/revenue as a result of a cyber-event. In the event a DDoS takes a website or system offline, these policies may cover some or all of the lost sales/revenue during this time. Other policy provisions may cover damage to software or systems impacted by the DDoS attack. As explained in our last article, the key is to tailor your cyber-insurance to meet the greatest risks faced by your company. If your company is in the market for cyber-insurance, we can assist with obtaining the insurance coverage you desire.

Following a DDoS attack, is there legal recourse?

Likely yes, but identifying the attackers can be very, very difficult. Nonetheless, assuming the attackers can be identified and are within the United States, a company has several legal options. The most powerful option is Section 1030 of the Computer Fraud and Abuse Act, the federal anti-hacking statute. CFAA provides both criminal and civil liability for anyone who intentionally accesses a computer network or system without authorization. Civil actions under CFAA are limited to economic damages (i.e., actual, tangible damages tied directly to the unauthorized access). Traditional common law causes of action may also be available. For example, trespass; conversion (i.e., damaging systems such that they can no longer be used); and interference with business relationships (i.e., taking a website offline so customers can't access it). To the extent individuals assist in but do not directly execute the attack, those individuals could also be held criminally responsible as accomplices, or liable in court as part of a civil conspiracy. The options for taking legal action against an attacker will vary, but the sooner we get involved, the more likely we can hold responsible those who harm your company.

The Firm's Data Protection, Privacy and Cybersecurity Team is here to help your company prepare for cyber-attacks, respond to them and in the event of one, repair your company and go after those responsible. For more information, please contact Samuel L. Felker, Zachary B. Busey or another member of our Data Protection, Privacy and Cybersecurity Team.

Also, stay tuned for our next installment which will discuss the hot topic of ransomware attacks, how they can impact your company and how best to prepare for them.