rent it out to other potential attackers in an "attack-for-hire" scheme, which enables unskilled users to launch DDoS attacks.

The more traffic a DDoS attack produces, the more difficulty an organization will have responding and recovering from the attack. The increase in traffic also increases the difficulty of attribution because it makes the true source of the attack harder to identify. Although the impact of DDoS attacks may often be negligible—depending on the scale of the attack—it could be severe and include loss or degradation of critical services, loss of productivity, extensive remediation costs, and acute reputational damage. Organizations should include steps to address these potential effects in their incident response and continuity of operations playbooks.

Although a DDoS attack is unlikely to impact the confidentiality or integrity of a system and associated data, it does affect availability by interfering with the legitimate use of that system. Because a cyber threat actor may use a DDoS attack to divert attention away from more malicious acts they are carrying out—e.g., malware insertion or data exfiltration—victims should stay on guard to other possible compromises throughout a DDoS response. Victims should not become so focused on defending against a DDoS attack that they ignore other security monitoring.

In a progressively interconnected world with additional post-pandemic remote connectivity requirements, maintaining the availability of business-essential external-facing resources can be challenging for even the most mature IT and incident response teams. It is impossible to completely avoid becoming a target of a DDoS attack. However, there are proactive steps organizations can take to reduce the effects of an attack on the availability of their resources.

What Steps Should You Take Before a DDoS Attack?

- **Understand your critical assets and services.** Identify the services you have exposed to the public internet and the vulnerabilities of those services. Prioritize assets based on mission criticality and need for availability. Implement ways to lower the risk of an attack by committing to good cyber hygiene (e.g., server hardening, patching). Determine whether your web application firewall (WAF) covers your critical assets and is configured in a Deny state.
- **Understand how your users connect to your network.** Identify the disparate ways your user base connects to your organization's network, whether onsite or remotely via virtual private networks (VPNs). Identify potential network chokepoints and any mitigations that may minimize disruptions to key personnel.
- **Enroll in a DDoS protection service.** Many internet service providers (ISPs) have DDoS protections, but a dedicated DDoS protection service may have more robust protections against larger or more advanced DDoS attacks. Protect systems and

Executive Summary

The Internet is the world's largest computing network, with hundreds of million of users. From the perspective of a user, each node or resource on this network is identified by a unique name—the domain name—such as www.nist.gov. However, from the perspective of network equipment that routes communications across the Internet, the unique identifier for a resource is an Internet Protocol (IP) address, such as 172.30.128.27. To access Internet resources by user-friendly domain names rather than IP addresses, users need a system that translates domain names to IP addresses and back. This translation is the primary task of an engine called the Domain Name System (DNS).

The DNS infrastructure is made up of computing and communication entities that are geographically distributed throughout the world. There are more than 250 top-level domains, such as .gov and .com, and several million second-level domains, such as nist.gov and ietf.org. Accordingly, there are many name servers in the DNS infrastructure, which each contain information about a small portion of the domain name space. The DNS infrastructure functions through collaboration among the various entities involved. The domain name data provided by DNS is intended to be available to any computer located anywhere in the Internet.

This document provides deployment guidelines for securing DNS within an enterprise. Because DNS data is meant to be public, preserving the confidentiality of DNS data pertaining to publicly accessible IT resources is not a concern. The primary security goals for DNS are data integrity and source authentication, which are needed to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit. This document provides extensive guidance on maintaining data integrity and performing source authentication. Availability of DNS services and data is also very important; DNS components are often subjected to denial-of-service attacks intended to disrupt access to the resources whose domain names are handled by the attacked DNS components. This document presents guidelines for configuring DNS deployments to prevent many denial-of-service attacks that exploit vulnerabilities in various DNS components.

DNS is susceptible to the same types of vulnerabilities (platform, software, and network-level) as any other distributed computing system. However, because it is an infrastructure system for the global Internet, it has the following special characteristics not found in many distributed computing systems:

- No well-defined system boundaries—participating entities are not subject to geographic or topologic confinement rules
- No need for data confidentiality—the data should be accessible to any entity regardless of the entity's location or affiliation.

Because of these characteristics, conventional network-level attacks such as masquerading and message tampering, as well as violations of the integrity of the hosted and disseminated data, have a completely different set of functional impacts, as follows:

- A masquerader that spoofs the identity of a DNS node can deny access to services for the set of Internet resources for which the node provides information (i.e., domains served by the node). This denial is not only for a limited set of clients but for the entire universe of all clients needing access to those resources
- Bogus DNS information provided by a masquerader or intruder can poison the information cache of the DNS node providing that subset of DNS information (i.e., the name server providing