ILDER

@保存到为知笔记

@网路冷眼

【DDoS Attacks: Best Practices for Prevention and Response】 http://t.cn/RfalTv9 卡内基梅隆大学软件工程研究所（SET）的文章--分布式拒绝服务（DDoS）攻击：预防和应对的4个最佳实践。

Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response

POSTED ON NOVEMBER 21, 2016 BY RACHEL KARTCH IN DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

Late last month, Internet users across the eastern seaboard of the United States had trouble accessing popular websites, such as Reddit, Netflix, and the New York Times. As reported in Wired Magazine, the disruption was the result of multiple distributed denial of service (DDoS) attacks against a single organization: Dyn, a New Hampshire-based Internet infrastructure company.

DDoS attacks can be extremely disruptive, and they are on the rise. The Verisign Distributed Denial of Service Trends Report states that DDoS attack activity increased 85 percent in each of the last two years with 32 percent of those attacks in the fourth quarter of 2015 targeting IT services, cloud computing, and software-as-a-service companies. In this blog post, I provide an overview of DDoS attacks and best practices for mitigating and responding to them based on cumulative experience in this field.

More Sophisticated DDoS Attacks

Before I came to the SEI CERT Division, I worked as a network engineer in various environments, including for Internet service providers, where I assisted organizations that were on the receiving end of DDoS attacks and and also had to handle clients who were either unknowingly or deliberately sourcing attacks themselves. I also worked as a network engineer for enterprises that had to be ready to defend themselves against DDoS attacks. At CERT, I lead a team that performs network data analysis to understand traffic on our sponsors' networks, often working to identify abnormal conditions and anomalous behavior that might indicate attacks or other threats to the environment.

We have recently seen more sophisticated attacks, such as the recent Dyn attack. As IEEE Spectrum recently reported, "Attacking a DNS or a content delivery provider such as Dyn or Akamai in this manner gives hackers the ability to interrupt many more companies than they could by directly attacking corporate servers, because several companies shared Dyn's network."

Before we examine prevention and mitigation to DDoS attacks, it is important to reach a common definition of a DDoS attack, which is based on my own experience in the field:

A DDoS attack is an attack intended to take an organization or a service offline, or otherwise render resources unusable, which originates from (or **appears** *to originate from) multiple hosts. The "multiple hosts" part of the attack is what makes it "distributed," and is what makes the attack more difficult to defend against. An attack that originates from a single host or IP address can be easily blocked with a simple router access list or firewall rule.*

While there is no standard way to classify DDoS attacks, one of the systems in use divides them into volumetric, protocol, and application attacks.

Volumetric attacks, which are believed to comprise more than 50 percent of attacks launched,

are focused on filling up a victim's network bandwidth. Among the most common volumetric attacks are User Datagram Protocol (UDP) flood attacks, where an attacker sends a large number of UDP packets to random ports on a remote host. UDP floods accounted for approximately 75 percent of DDoS attacks in the last quarter of 2015, according to the Versign DDoS Trends Report.

A common form of UDP flood attack relies on reflection and amplification. UDP is a connectionless protocol (that is, it doesn't require that the two ends of a conversation establish a connection before exchanging data). An attacker can therefore forge UDP packets with fake source addresses, and use those packets to generate reply traffic. By setting the source of the UDP packets to be the IP address of the intended victim, and then sending those packets to various servers for UDP-based applications, the attacker will cause the servers to send reply traffic to the forged source IP address--the victim. This reply traffic is the "reflection" part of the attack. It's a lot like calling every pizza place in your county, and ordering a lot of pizzas to be delivered to someone you really don't like.

The "amplification" part comes in when you understand that many UDP services generate replies that are much larger than the initial request size. For instance, the Domain Name Service (DNS) has a bandwidth amplification factor of 28 to 54 (the reply to a DNS request can be between 28 and 54 times larger than the request). The Network Time Protocol (NTP) has a bandwidth amplification factor of 556. By combining reflection (the server sends reply traffic to a spoofed source address) with amplification (the reply traffic is a lot larger than the initial request), attackers can do a lot of damage to a victim with very little effort on their part. A number of UDP-based applications and services can be used to generate amplification and reflection attacks, including DNS, NTP, Simple Service Discovery Protocol (SSDP), and Simple Network Management Protocol (SNMP).

Protocol attacks (sometimes also called state-exhaustion attacks) target a weakness in how a protocol operates. A well-known protocol attack is the SYN flood, which targets the three-way handshake mechanism in TCP. When a server receives a SYN packet, this is a signal to the server that another machine wants to open a TCP connection. The server will allocate some of its resources to this half-open connection, and send a SYN ACK packet back to the initiating machine. Under normal circumstances, the initiator will then send an ACK packet to the server, the three-way handshake is complete, and the machines will then exchange data.

In a SYN flood attack, an attacker sends a rapid succession of TCP SYN requests--typically from spoofed source IP addresses--to open a connection to a network server. The server sends SYN ACK packets back to the source addresses, which never reply with an ACK. The server keeps the half-open TCP connections around, using up resources, until the server is no longer able to accept any new connections.

Application attacks target weaknesses in how an application works. One well-known application attack is Slowloris, which targets web servers. In a Slowloris attack, the attacker sends HTTP requests to a web server without ever completing the requests. Periodically (and slowly--hence the name), the attacker will send additional headers, thus keeping the request "alive" but not finished. Similar to a SYN flood, this forces the web server to maintain open connections for these partially completed HTTP requests, eventually preventing it from accepting any new connections.

The remainder of this post details strategies for preparing networks to defend against DDoS attacks.

Defending Against DDoS Attacks

Generally speaking, organizations should start planning for DDoS attacks in advance. It is much harder to respond after an attack is already under way. While DDoS attacks can't be prevented, steps can be taken to make it harder for an attacker to render a network unresponsive.

Architecture. To fortify resources against a DDoS attack, it is important to make the architecture as resilient as possible. Fortifying network architecture is an important step not just in DDoS network defense, but in ensuring business continuity and protection from any kind of outage or disaster situation.

The following steps will help disperse organizational assets as to avoid presenting a single rich target to an attacker:

- Locate servers in different data centers.
- Ensure that data centers are located on different networks.
- Ensure that data centers have diverse paths.
- Ensure that the data centers, or the networks that the data centers are connected to, have no notable bottlenecks or single points of failure.

For an organization that depends on servers and Internet presence, it is important to make sure that resources are geographically dispersed and not located in a single data center.

If resources are already geographically dispersed, it is important to view each data center as having more than one pipe to Internet, and ensure that not all data centers are connected to the same Internet provider.

Overall, priorities for architecture should be geographic diversity, provider diversity, and elimination of bottlenecks. While these are best practices for general business continuity and disaster recovery, they will help ensure organizational resiliency in response to a DDoS attack.

Hardware. Deploy appropriate hardware that can handle known attack types and use the options that are in the hardware that would protect network resources. Again, while bolstering resources will not prevent a DDoS attack from happening, doing so will lessen the impact of an attack.

In particular, certain types of DDoS attacks have been in existence for quite some time, and a lot of network and security hardware is capable of mitigating them. For example, many commercially available network firewalls, web application firewalls, and load balancers can defend against layer 4 attacks (also known as protocol attacks) and application-layer attacks (such as Slowloris). Specialty DDoS mitigation appliances also can protect against these attacks.

Hardware upgrades are also effective against SYN flood attacks. Most modern hardware, network firewalls, web application firewalls, and load balancers, will generally have a setting that allows a network operator to start closing out TCP connections once they reach a certain threshold.

Bandwidth. If affordable, scale up network bandwidth. For volumetric attacks, the solution some organizations have adopted is simply to scale bandwidth up to be able to absorb a large volume of traffic if necessary. That said, volumetric attacks are something of an arms race, and many organizations won't be able or willing to pay for the network bandwidth needed to handle some of the very large attacks we have recently seen. This is primarily an option for very large organizations and service providers.

In late September, the Krebs on Security blog was hit by an unusually large DDoS attack--double the size that had been previously seen by its hosting provider, --according to a post on the site. A large part of the reason that the provider was able to hold off the attack for so long was because of the significant bandwidth available, which allowed the provider to absorb the attack while trying to mitigate it.

Outsourcing. There are several large providers that specialize in scaling infrastructure to respond to attacks. These providers can implement cloud scrubbing services for attack traffic to remove the majority of the problematic traffic before it ever hits a victim's network. As with many of these remedies, the best time to fortify your defenses is not in the wake of an attack, but rather beforehand to ensure a quick and effective response.

An ISP can offer DDoS mitigation services that will help organizations respond in the wake of an attack. Even ISPs that don't have a formal DDoS mitigation product should be able to specify the type assistance they would provide to their customers in the event of a DDoS attack.

On a separate front, there are providers who specifically work in DDoS mitigation. During an attack, these services reroute traffic destined for the victim's network to the mitigation center where it is scrubbed, and legitimate traffic is then forwarded to the organization. These DDoS mitigation providers have the type of scalable and dynamic load balancing available to respond to the unprecedented levels of traffic that often result from a DDoS attack.

Wrapping Up and Looking Ahead

While DDoS attack prevention is partly a technical issue, it is also largely a business issue. Many

While DDoS attack prevention is partly a technical issue, it is also largely a business issue. Many of these recommendations are simply best practices for establishing organizational resilience, including planning for a resilient architecture and dispersing resources.

We welcome your feedback in the comments section below.

Additional Resources

View this DDoS Security Guide from U.S. CERT .

Learn more about CERT's incident handling courses for computer security incident response team (CSIRT) technical personnel.

View CERT's CSIRT handbook.

2016年11月23日 02:13 来自 荣耀畅玩4X·快科技