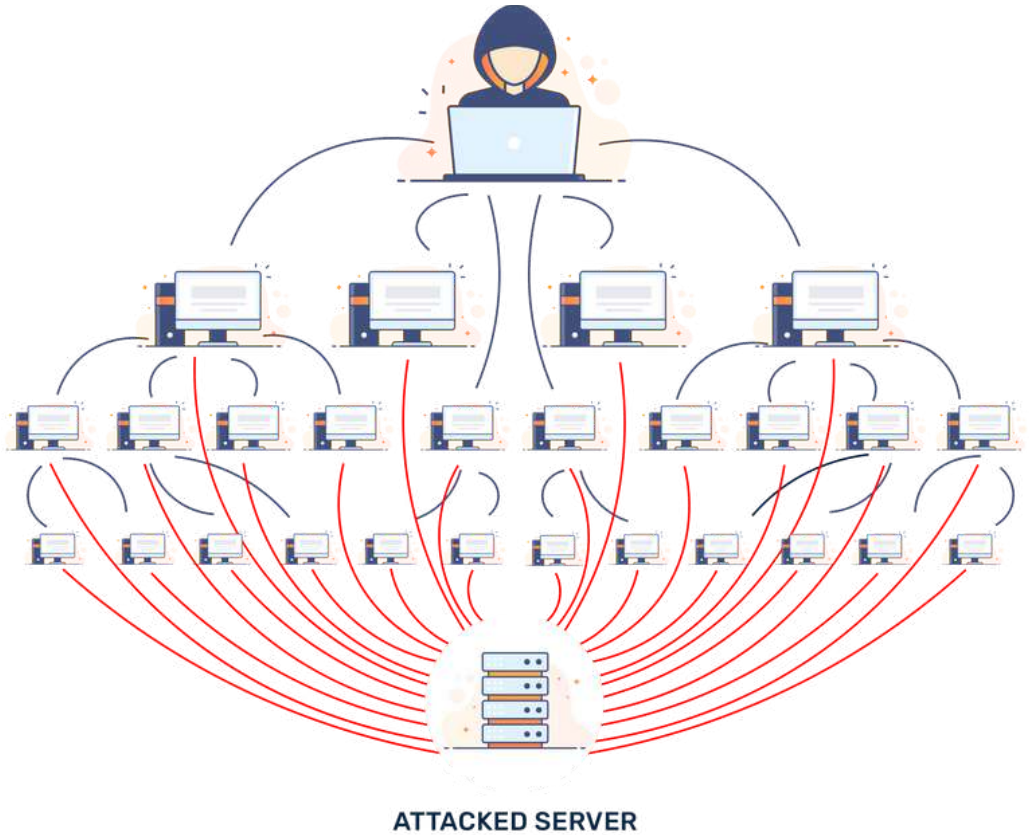
DISTRIBUTED DENIAL OF SERVICE (DDOS)

A COMPLETE GUIDE

What is a DDoS attack, and how does it work?

The IT industry has recently seen a steady increase in distributed denial of service (DDoS) attacks. A few years ago, DDoS attacks were considered a minor nuisance perpetrated by inexperienced attackers for fun, and it was relatively easy to mitigate them. Unfortunately, that is no longer the case. DDoS attacks are now a sophisticated activity and, in many cases, big business.



InfoSecurity Magazine reported 2.9 million DDoS attacks in the first quarter of 2021, a 31% increase from the same period in 2020. The number of DDoS attacks increased 31% to 2.9 million attacks in the first quarter of 2021 compared to the same period in 2020.

Tactical Warfare:
How DDoS Attackers Avoid Detection

SPOOFING

By default, IPv4 and IPv6 cannot authenticate and trace traffic. With IPv4 networks especially, it is pretty simple to spoof source and destination addresses. DDoS attackers take advantage of this issue by forging packets that have bogus source addresses. As a result, an attacker can trick legitimate devices into responding to these packets by sending millions of replies to a victim host that never actually requested in the first place.

REFLECTION

Attackers usually want to hide any trace of their involvement in a DDoS attack. To do this, they manipulate the default behaviour of internet services to hide the actual attacker effectively. Services often used in these types of attacks include:

- The thousands of Domain Name System (DNS).
- Network Time Protocol (NTP).
- Simple Network Management (SNMP) servers.

This is one of the primary reasons that attackers are attracted to a DDoS strategy. Internet services provide the traffic, but they also tend to make it more difficult for defenders to trace the origin of the attack because most servers don't keep detailed logs of the services used.

AMPLIFICATION

Amplification is a tactic that lets a DDoS attacker generate a large amount of traffic using a source multiplier which can then be aimed at a victim host. Amplification attacks don't use a botnet; it is simply a tactic that allows an attacker to send a single forged packet which then tricks a legitimate service into sending hundreds, if not thousands, of replies to a victim network or server.

Responding to a threat: 5 steps for responding to a DDoS attack

DETECTION

Early detection is critical to defending against a DDoS attack. Look for the warning signs above that indicate you may be a target. DDoS detection can examine the contents of packets to detect Layer 7 and protocol-based attacks, or it can use rate-based measures to detect volumetric attacks. Rate-based detection is usually discussed first for DDoS attacks, but most effective DDoS attacks are not blocked by rate-based detection.

FILTERING

A transparent filtering process helps in rejecting unwanted traffic. This is done by installing effective rules on network devices to eliminate DDoS traffic.

REROUTING AND REDIRECTION

In this step, the traffic is redirected so that it does not affect your critical resources. You can redirect the DDoS traffic by sending it to a scrubbing centre or another resource that acts as a sinkhole. It is usually recommended that you transparently communicate what is going on so that employees and customers do not have to change their behaviour to accommodate the slowdown.

REFERRAL AND ANALYSIS

It's important to understand where the DDoS attack is coming from. This knowledge can help you develop protocols to protect against future attacks proactively. While it may be tempting to take down the botnet, this can lead to logistical issues and legal ramifications. In general, this is not recommended.

ALTERNATIVE DELIVERY

It is possible to use alternative resources that can offer new content or open new network connections almost immediately in an attack.

About ISmile Technologies

ISmile Technologies is a proud automation-enabled intelligent cloud solution and managed IT services provider, and it is your multi-cloud technology advisor & key implementation partner.

We operate globally and leverage disruptive technologies alongside deep expertise to deliver business-specific cloud solutions. We maximize impact at an unparalleled value and securely accelerate business agility while infusing competitive excellence.

https://www.ismiletechnologies.com

sales@ISmileTechnologies.com

501 S Weber Rd Unit 108, Bolingbrook, IL 60490