Defending Against Carpet Bombing Attacks

DDoS attacks usually come from many sources, targeting a single (or very small number) of destinations (the victim).

'Carpet Bombing' is a term used to describe DDoS attacks that target a range of addresses or subnets, which can contain hundreds or even thousands of destination IP addresses. Carpet bombing can impact a service provider's ability to deliver service (either generally or to a specific customer). It can also be used to obfuscate the individual target, thus increasing the difficulty of mitigation.

Challenge

Carpet bombing is not new, it has been around for 4-5 years and has been used sporadically by attackers. A recent, late 2019, storm of these attacks targeted networks in Turkey, France, Italy and South Africa.

The addresses targeted during a Carpet Bombing attack are not always static and may change during the lifetime of an attack. These attacks are often combined with reflection-amplification techniques. Reflection amplification uses poorly secured or configured Internet infrastructure to amplify and obfuscate the true source of a DDoS attack.

Reflection amplification has been behind most of the largest DDoS attacks seen on the Internet over the past decade. Many protocols can be used for reflection amplification, including DNS, NTP, SSDP, SNMP etc. Recently attackers have also used TCP based (SYN-ACK) reflection amplification which adds a stateful element to the attack impact (where firewalls, NAT, load-balancers are being targeted).

Combined with advanced reconnaissance of the online business relationships between targeted organizations, combining Carpet Bombing and Reflection Amplification tactics allows attackers to raise the bar for defenders in terms of accurately detecting, classifying, tracing back, and mitigating DDoS attacks.

Risk

Carpet bombing attacks are harder to manage because:

1. By targeting a range of addresses there is often a smaller amount of traffic per target host. This can mean that some detection mechanisms do not fire.
2. Systems that initiate a mitigation per target address can run out of resources if thousands of addresses are targeted.
3. Diverting traffic for large numbers of hosts can mean that very large volumes of attack / clean traffic are delivered to mitigation Arbor Threat Mitigation System (TMS) infrastructure.
4. Often specific Internet infrastructure, from one or more businesses or networks, is used to reflect traffic towards the target of the carpet-bombing attack.

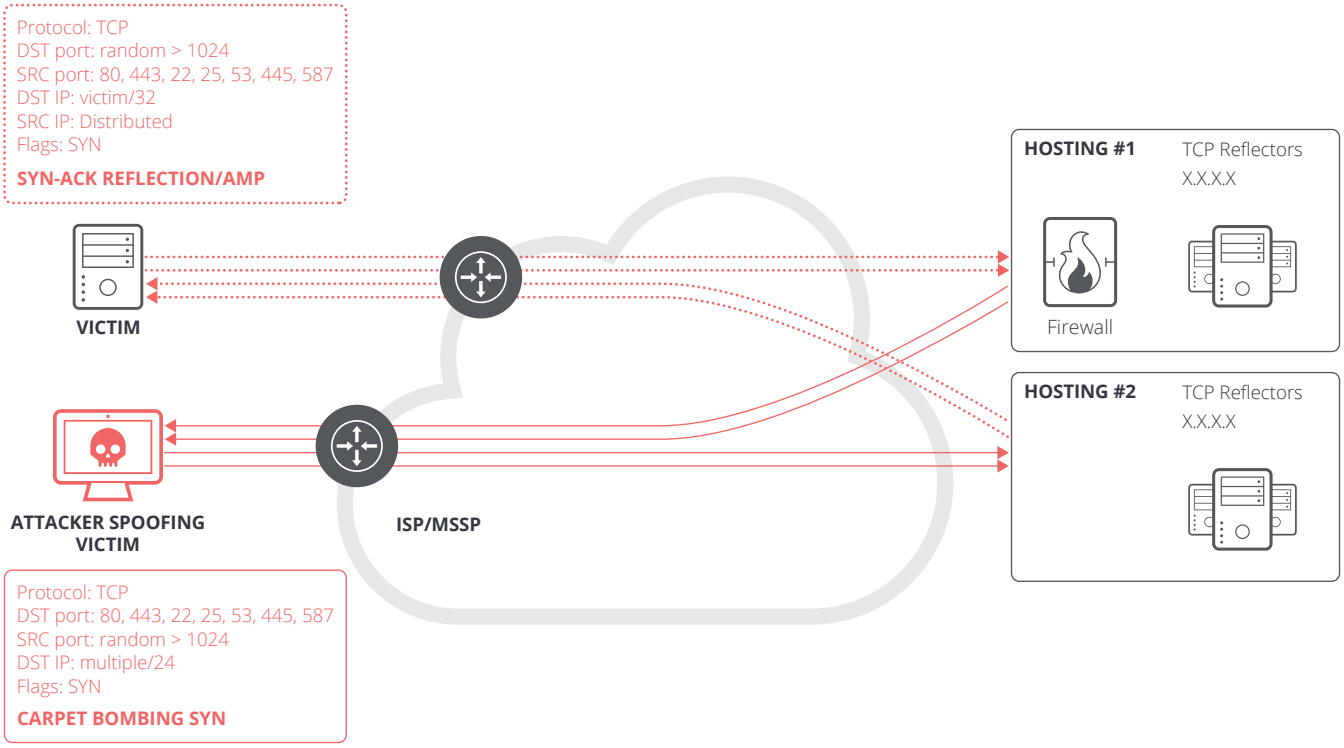

Figure 1: End-to-End Attack Topology.

Solution

Scrutinizing large traffic volumes over time, contextualizing and refining this data, and quickly acting on anomalies that threaten network availability has never been more necessary. But resource constraints continue to impact network operators, increasing the value of scalable, end-to-end, automated analytics workflows and protections. Arbor Sightline has multiple detection mechanisms that can identify carpet-bombing attacks ensuring customers are protected. Arbor Sightline has features to track the prefixes involved in an attack so that only the relevant traffic is diverted to mitigation infrastructure, and can use Flowspec to help manage the attack, leveraging infrastructure capabilities.

Arbor Sightline can identify carpet-bombing DDoS attacks in as little as one second using fast-flood detection, and can automatically mitigate these attacks by identifying the IP ranges under attack and diverting only that traffic to the Arbor TMS mitigation infrastructure. Flowspec rules can also be used.

Arbor Sightline can add new targets automatically to existing mitigations, managing resources effectively. Arbor Sightline can automatically manage available Arbor TMS mitigation capacity by dynamically moving attacks among available Arbor TMS mitigation infrastructure, as attack traffic volumes change. These features make sure network infrastructure isn't overloaded and cuts down the time operations staff spend managing DDoS attack response.

Carpet-bombing defense capabilities include:

- Automated mitigation that scales to hundreds of millions of packets per second
- Tracking of attack targets so that (only) needed traffic is inspected
- Analytics to identify attack sources for Flowspec filtering

Summary

Although carpet-bombing and reflection-amplification attacks are complex and difficult to manage, with Arbor Sightline's multitude of detection mechanisms and Sentinel's Orchestration you can identify these attacks and manage them to mitigate the impact on your network and your customers.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECUC_005_EN-2002 05/2020