Abstract

Cloud platforms are now being used by hackers in an attempt to launch largescale distributed denial-of-service (DDoS) attacks. In addition to DDoS attacks, hackers leverage these services to conduct phishing attacks along with other malicious activity such as API abuse. In just a few hours, hackers can use a cloud platform to load attack scripts and launch their assaults (See Figure 1). Organizations leveraging cloud infrastructure for mission-critical business operations face immense security challenges since they cannot block communication with these public cloud platforms.

Figure 1: Google Cloud used to launch a Denial of Service attack

Background

A cloud computing platform is a network of servers hosted offsite by a third party which provides shared computer processing resources and data on-demand. With progressive pay-per-use cost structures, from local service providers to technology giants such as Amazon, Apple, Google and Microsoft offer a variety of services, many of which provide capabilities that hackers find attractive:

- Bandwidth and computing power – hackers can easily scale their operations/ attacks far beyond their home lab capacity
- Cost – conduct a large attack volume using similar competence to that of a stresser service, but without paying for it
- A private virtual environment where they can upload, store and test their scripts
- A camouflaged platform for management of attack operations

Hackers are even discovering new ways to use Twitter, Facebook and Gmail as command and control servers. It was recently discovered that a hacker was using Twitter as a C2 for their botnet. Some operators of stresser services such as DownThem.xyz are using cloud environments and VPS to control and launch their denial of service attacks for profit. The more servers they have, the more bandwidth and power they can provide to their customers (See Figure 2).

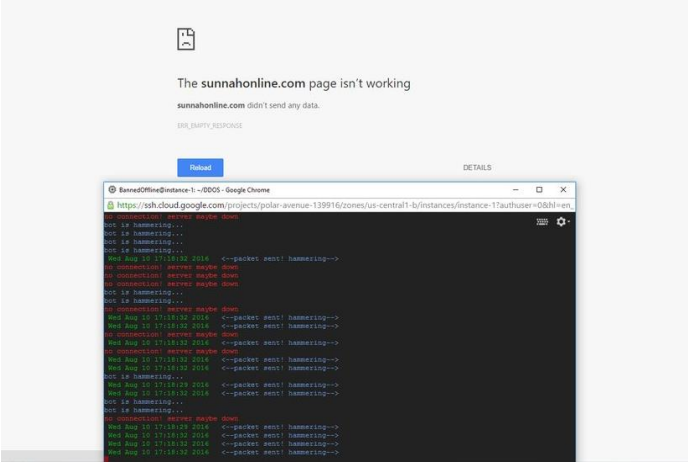

Figure 2: @BannedOffline using Google Cloud to launch a Layer 7 (HTTP/S) DDoS attack

Reasons for Concern

Hackers are continually looking for new methods to conduct their malicious activity. Radware's cyber analysts have identified an increased trend of attackers leveraging trusted sources to conduct their malicious activity. It poses a challenge to organizations as the attack traffic appear legitimate because other business processes leverage the very same cloud platform.

Here are three steps attackers take to launch an attack from the public cloud:

1. Create a free anonymized email to sign up for the service (Often times the attacker is not paying for the service and is abusing free offers).
2. Adding an additional layer of anonymization by using a third-party infrastructure
3. Load attack scripts on multiple instances and launch a massive DDoS attack

Common Attack Methods and Techniques

- Most cloud environments will not allow spoofing, thus limiting the attacker to non-UDP spoofed attacks
- Once an attacker finds a cloud service that allows spoofing, they will be able to utilize more attack vectors like reflection and amplification floods
- Dynamic IP attacks that use real IP addresses to generate a three-way handshake can be used in cloud environments to bypass mitigation techniques and make it nearly impossible to distinguish between legitimate and attack traffic
- In addition, perpetrators are able to distribute the attack via multiple cloud instances, thus allowing them to conduct low rate denial-of-service attacks that evade rate-based detection mechanisms

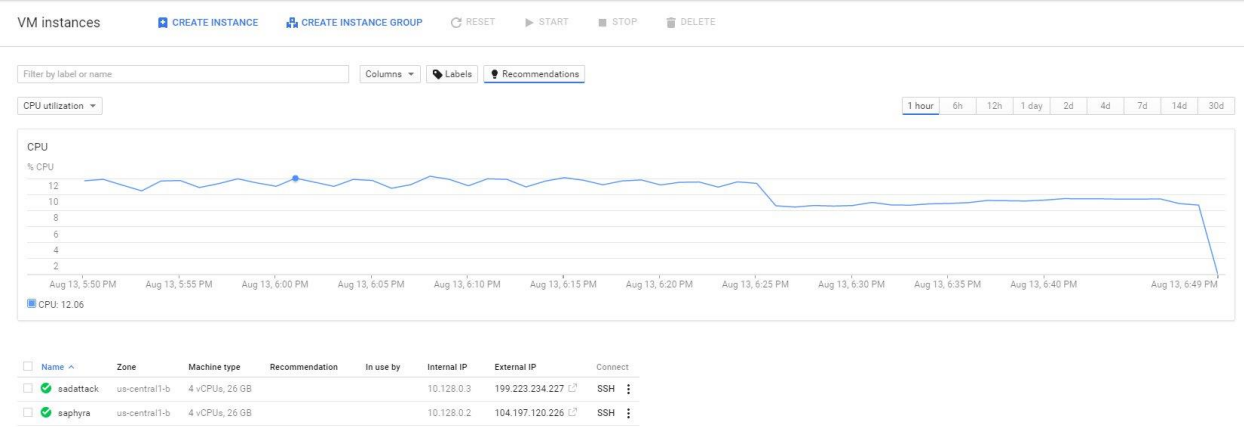

Figure 3: VM instance on Google Cloud by @BannedOffline

Attack vectors

Distributed Denial of Service – a DoS variant where perpetrators employ multiple machines (computers, servers, and mobile devices) to carry out a DoS attack simultaneously, thus increasing its effectiveness. The attack leverages a net of infected zombie computers (bots) controlled by a Command and Control Server. Botnets are well-coordinated and could count millions of machines. Perpetrators use botnets to insure their anonymity, since the attack traffic originates from the bots' IPs rather than theirs.

Reflection Denial of Service - taking advantage of a legitimate third-party component to send the attack traffic to a victim, ultimately hiding the attackers' identity. The packets are sent to the reflector servers with a source IP address set to their victim's IP therefore indirectly overwhelming the victim with the response packets. The disguise behind a legitimate server makes this kind of attack particularly difficult to mitigate. A common example for this type of attack is a Reflective DNS Response attack.

DNS amplification attack - a two-step sophisticated DoS attack: First, the attacker spoofs the IP address of the DNS resolver and replaces it with the victim's IP address, so all DNS replies will be sent to the victim's servers. Second, the attacker finds an Internet domain that is registered with many DNS records. During the attack, the attacker sends DNS queries that request the entire list of DNS records for that domain. The DNS server's replies are usually so big that they need to be split over several packets.

Layer 7 (HTTP) Flood - An HTTP flood is an attack method used by hackers to attack web servers and applications. It consists of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a target web server. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service condition (without necessarily requiring a high rate of network traffic). Such requests are often sent en masse by means of a botnet, increasing the attack's overall power.

SQL Injection – This technique takes advantage of poor application coding. When the application inputs are not sanitized it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database and more.

Organizations under Threat Should Consider

- Maintaining service availability under attack by choosing a solution that monitors traffic behavior and distinguishes between legitimate users and attack traffic, thereby blocking malicious packets while allowing appropriate traffic to pass.
- A hybrid solution combining on-premise detection and mitigation with cloud-based protection for volumetric attacks. It facilitates quick detection, immediate mitigation and prevents Internet pipe saturation.
- An integrated, synchronized solution that can protect from multi-vector attacks such as network floods, and application layer attacks such as low-and-slow service disruptions or HTTP/S floods.
- A cyber-security emergency response plan that includes a dedicated emergency team of experts and clear actions in the event of attack.

Radware recommends IT staff to monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats when they occur.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.