A MASSIVE DDOS ATTACK HITS YOUR SERVER.

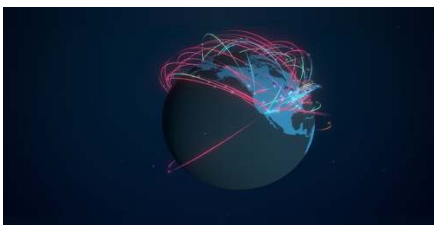
Your basic security systems fail to respond in time. Your webserver can't handle all traffic. Your website is down for hours. You are losing untold amounts of revenue; new customers will click away and maybe won't return to your website. Denial of service attacks are here to stay, and no business can afford to be unprotected.

THE DDOS ATTACK MARKET IS CHANGING.

"New DDoS services appear to have replaced ones shut down by law enforcement agencies. As organizations implement basic countermeasures, attackers target them with long-lasting attacks. It is difficult to say if the number of attacks will continue to grow, but their complexity is showing no signs of slowing down."

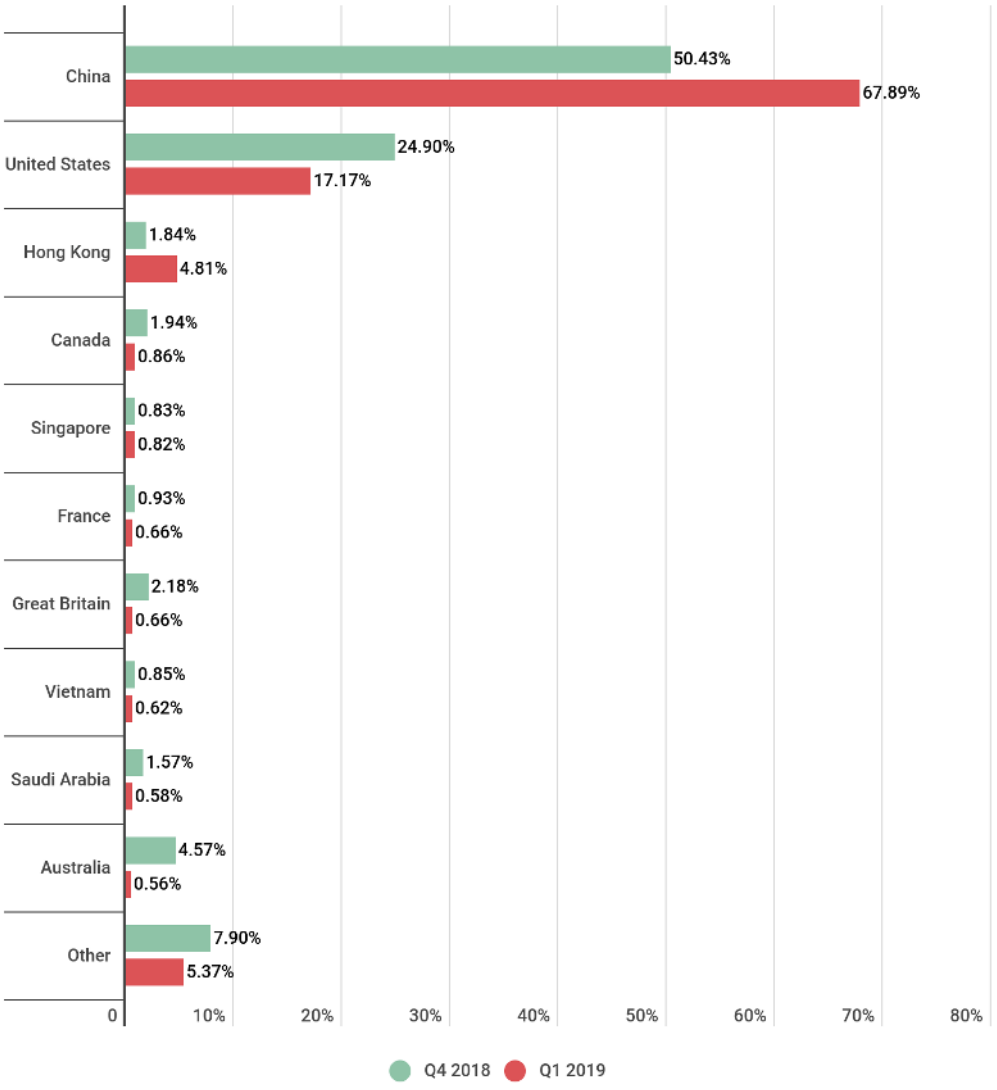
DYNAMICS OF THE NUMBER OF DDOS ATTACKS.

Researcher at Kaspersky reported that "in the last quarter, the most DDoS activity was observed in March, especially the second half". We recommend that organizations prepare themselves effectively, in order to withstand sophisticated DDoS attacks,



ATTACK GEOGRAPHY

Source Kaspersky Lab



What are DDoS Attacks?

DDoS stands for Distributed Denial of Service.

It is a form of cyber-attack that targets critical systems to disrupt network service or connectivity that causes a denial of service for users of the targeted resource.

A DDoS attack employs the processing power of multiple malware-infected computers (Botnet) to target a single system (ex Webserver).

Understanding the OBJECTIVES OF THE BOTNETS:

Taking a false identity, collect information, Stealing money or property

The bots attack by rotation on many domains, hiding their activity and all bots attack simultaneously the target.

Here is an example of a major DDoS attack taking place:

Botnet / DDoS Attack - Norse Live Footage -

Types of DDoS Attacks & How Each Work

Volumetric Attacks

The most common DDoS attack overwhelms a machine's network bandwidth by flooding it with false data requests on every open port the device has available. Because the bot floods ports with data, the machine continually has to deal with checking the malicious data requests and has no room to accept legitimate traffic. UDP floods and ICMP floods comprise the two primary forms of volumetric attacks.

UDP stands for User Datagram Protocol and refers to the simple transmission of data without checking its integrity. The UDP format lends itself well to fast data transmission, which unfortunately makes it a prime tool for attackers.

ICMP stands for Internet Control Message Protocol, referring to network devices that communicate with one another. An attack focused on ICMP relies on attacking nodes sending false error requests to the target. The target has to deal with these requests and cannot respond to real ones, similar to how a UDP attack works.

Application-Layer Attacks

The application layer is the topmost layer of the OSI network model and the one closest to the user's interaction with the system. Attacks that make use of the application layer focus primarily on direct Web traffic. Potential avenues include HTTP, HTTPS, DNS, or SMTP.

Application-layer attacks are not as easy to catch because they typically make use of a smaller number of machines, sometimes even a single one. Therefore, the server can be tricked into treating the attack as nothing more than a higher volume of legitimate traffic.

Protocol Attacks

A protocol attack focuses on damaging connection tables in network areas that deal directly with verifying connections. By sending successively slow pings, deliberately malformed pings, and partial packets, the attacking computer can cause memory buffers in the target to overload and potentially crash the system. A protocol attack can also target firewalls. This is why a firewall alone will not stop denial of service attacks.

One of the most common protocol attacks is the SYN flood, which makes use of the three-way handshake process for establishing a TCP/IP connection. Typically, the client sends a SYN (synchronize) packet, receives a SYN-ACK (synchronize-acknowledge), and sends an ACK in return before establishing a connection. During an attack, the client only sends SYN packets, causing the server to send a SYN-ACK and wait for the final phase that never occurs. This, in turn, ties up network resources.

Often, would-be hackers combine these three types of approaches to attack a target on multiple fronts, completely overwhelming its defenses until stronger and more thorough countermeasures can be deployed.

7 Best Practices for Preventing DDoS attacks

The evolution of DDoS attacks shows no signs of slowing. They keep growing in volume and frequency, today most commonly involving a "blended" or "hybrid" approach.

Without early threat detection and traffic profiling systems, it's impossible to know they're here. In fact, chances are you know about it only when your website slows to a halt or crashes.

This is especially true for sophisticated attacks, which use a blended approach and target multiple levels simultaneously.

These attacks target data, applications, and infrastructure simultaneously to increase the chances of success. To fight them, you need a battle plan, as well as reliable DDoS prevention and mitigation solutions. You need an integrated security strategy that protects all infrastructure levels.

1. Develop a Denial of Service Response Plan.

Develop a DDoS prevention plan based on a thorough security assessment. Unlike smaller companies, larger businesses may require complex infrastructure and involving multiple teams in DDoS planning.

When DDoS hits, there is no time to think about the best steps to take. They need to be defined in advance to enable prompt reactions and avoid any impacts.

Developing an incident response plan is the critical first step toward comprehensive defense strategy. Depending on the infrastructure, a DDoS response plan can get quite exhaustive. The first step you take when a malicious attack happens can define how it will end. Make sure your data center is prepared, and your team is aware of their responsibilities. That way, you can minimize the impact on your business and save yourself months of recovery.

The key elements remain the same for any company, and they include:

Systems checklist. Develop a full list of assets you should implement to ensure advanced threat identification, assessment, and filtering tools, as well as security-enhanced hardware and software-level protection, is in place.

Form a response team. Define responsibilities for key team members to ensure organized reaction to the attack as it happens.

Define notification and escalation procedures. Make sure your team members know exactly whom to contact in case of the attack.

Include the list of internal and external contacts that should be informed about the attack. You should also develop communication strategies with your customers, cloud service provider, and any security vendors.

2. Secure Your Network Infrastructure.

Mitigating network security threats can only be achieved with multi-level protection strategies in place.

This includes advanced intrusion prevention and threat management systems, which combine firewalls, VPN, anti-spam, content filtering, load balancing, and other layers of DDoS defense techniques. Together they enable constant and consistent network protection to prevent a DDoS attack from happening. This includes everything from identifying possible traffic inconsistencies with the highest level of precision in blocking the attack.

Most of the standard network equipment comes with limited DDoS mitigation options, so you may want to outsource some of the additional services. With cloud-based solutions, you can access advanced mitigation and protection resources on a pay-per-use basis. This is an excellent option for small and medium-sized businesses that may want to keep their security budgets within projected limits.

In addition to this, you should also make sure your systems are up-to-date. Outdated systems are usually the ones with most loopholes. Dental of Service attackers find holes. By regularly patching your infrastructure and installing new software versions, you can close more doors to the attackers.

Given the complexity of DDoS attacks, there's hardly a way to defend against them without appropriate systems to identify anomalies in traffic and provide instant response. Backed by secure infrastructure and a battle-plan, such systems can minimize the threat. More than that, they can bring the needed peace of mind and confidence to everyone from a system admin to CEO.

3. Practice Basic Network Security

The most basic countermeasure to preventing DDoS attacks is to allow as little user error as possible.

Engaging in strong security practices can keep business networks from being compromised. Secure practices include complex passwords that change on a regular basis, anti-phishing methods, and secure firewalls that allow little outside traffic. These measures alone will not stop DDoS, but they serve as a critical security foundation.

4. Maintain Strong Network Architecture

Focusing on a secure network architecture is vital to security. Business should create redundant network resources; if one server is attacked, the others can handle the extra network traffic. When possible, servers should be located in different places geographically. Spread-out resources are more difficult for attackers to target.

5. Leverage the Cloud

Outsourcing DDoS prevention to cloud-based service providers offers several advantages. First, the cloud has far more bandwidth, and resources than a private network likely does. With the increased magnitude of DDoS attacks, relying solely on on-premises hardware is likely to fail.

Second, the nature of the cloud means it is a diffuse resource. Cloud-based apps can absorb harmful or malicious traffic before it ever reaches its intended destination. Third, cloud-based services are operated by software engineers whose job consists of monitoring the Web for the latest DDoS tactics.

Deciding on the right environment for data and applications will differ between companies and industries. Hybrid environments can be convenient for achieving the right balance between security and flexibility, especially with vendors providing tailor-made solutions.

6. Understand the Warning Signs

Some symptoms of a DDoS attack include network slowdown, spotty connectivity on a company intranet, or intermittent website shutdowns. No network is perfect, but if a lack of performance seems to be prolonged or more severe than usual, the network likely is experiencing a DDoS and the company should take action.
Monitoring is the key to understand possible DDoS Attacks.

7. Consider DDoS-as-a-Service.

DDoS-as-a-Service provides improved flexibility for environments that combine in-house and third-party resources, or cloud and dedicated server hosting.

At the same time, it ensures that all the security infrastructure components meet the highest security standards and compliance requirements. The key benefit of this model is the ability of tailor-made security architecture for the needs of a particular company, making the high-level DDoS protection available to businesses of any size.

How to Stop a DDoS attack?

Monitor for Unusual Activity

Early threat detection is one of the most efficient ways to prevent the attack.

Denial of service can come in multiple forms, and it is critical to recognize its most common telltale. Any dramatic slowdown in network performance or an increase in the number of spam emails can be a sign of an intrusion. These should be addressed as soon as they are noticed, even if deviations do not look that important at first.

Businesses also need to understand their equipment's capabilities to identify both network-layer and application-layer attacks. If you do not have these resources in-house, you may want to work with your ISP, data center, or security vendor to get advanced protection resources.

With proper systems to detect and react to all types of attacks, you already set your business for a successful defense.

What to Look For In a DDoS Mitigation Service

When possible, it is beneficial to choose a DDoS mitigation service that keeps engineers and network administrators on site continuously monitoring traffic. By doing so, it enables a faster response time than having to do work remotely.

Another factor is whether the service deals with SSL attacks. Sites that provide commercial transactions run on SSL, and a successful attack against this protocol can cost thousands of dollars in lost revenue.

The more comprehensive the mitigation plan, the better off networks are when it comes to protection against DDoS attack. Many different services exist on the market. For example: Cloudflare, Akamai, Sucuri and many others.

Be Prepared For Denial of Service Attacks

DDoS attacks are painfully real and are no longer massive corporation's problem only. Small and medium-sized companies are increasingly the targets. This trend has sparked even greater demand for multi-layered security solutions that can provide full protection of sensitive workloads.

While the threat landscape continues to develop, so do security technologies. Following that trend, we recently released the fourth phase of DDoS enhancements for all our services. We will be increasing our focus on **educated businesses** on the most common cyber threats and best security strategies to defend.

Ask our professional advice, we can help you putting in place the best cost-effective solution tailor made for the systems you which to protect!

Contact: info@security-taskforce.be or just call: +32 496619154