Working Together Against **Malicious** Cyber Attacks

A study recalling the malicious attack and mitigation of an International Bank's web based network head-quartered in Bahrain

Client Overview

The client is an international banking group head-quartered in the Kingdom of Bahrain. Operating through 19 subsidiaries, branches and representative offices, the Bank's global network spans 17 countries across the Middle East, North Africa, Europe, the Americas and Asia.

They offer a wide range of international wholesale banking services. These include trade finance, treasury, project and structured finance, syndications, corporate and institutional banking, and Islamic banking. They also have a growing retail banking network in the MENA region.

The Bank's Business Challenge

- Need for highly-available, reliable and stable network connectivity globally.
- Protection against compromising integrity and taking the Bank's internet services off line.

$50,000

Is the amount DDoS attacks can cost victim organizations per hour

$150

Can buy a week-long DDoS attack from the black market

1/3

Of all downtime incidents are attributed to DDoS attacks.

Operating through 19 subsidiaries, the Bank's global network spans 17 countries across the Middle East and North Africa, Europe, the Americas and Asia.

The Bank's Business Challenge

Global connectivity

As an international banking group, operating across 17 countries, the bank had a critical need for highly available, reliable and stable network connectivity between its subsidiaries, branches and representative offices around the world. It was important for this network to be professionally managed, and for service levels to be committed and monitored for delivery.

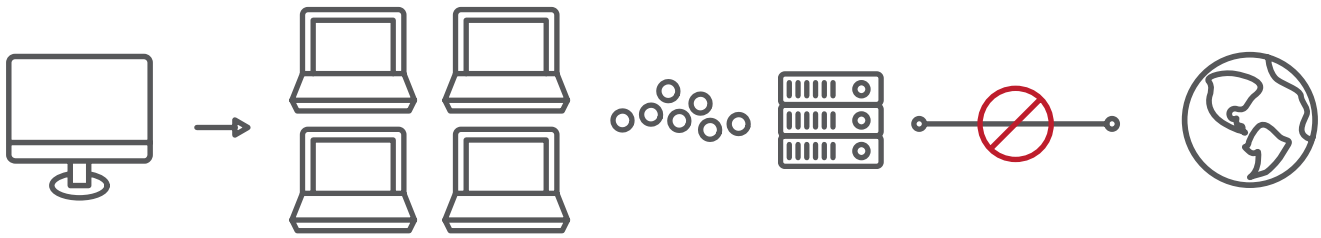
Malicious cyber attacks

The bank had been targeted by advanced threats seeking to steal data,compromise integrity or disrupt the banks online presence. Such malicious attacks, known as Distributed Denial of Service (DDoS), are capable of overloading an organisation's complete internet bandwidth and paralysing its entire internet network. DDoS had the potential of placing the Bank's online services at risk and affecting revenues through service downtime, as well as irrevocably harming its global reputation.

Batelco's Strategic Solution

- Connectivity and protection One-Stop solution for complete global and regional high-speed WAN connectivity.
- Reliable cloud-based protection services to monitor, detect and mitigate (DDoS) attacks.

How DDoS attacks work



Step 1

Attacker infects unsecured computers with malware which are known as 'botnets' or 'zombies'.

Step 2

The attacker then sends a command to each of the compromised hosts and commands them to flood the target with seemingly legitimate web requests.

Step 3

This significantly slows and cripples the target company's web servers causing them to crash and lose connection to the rest of the world.

Attacks can last as long as the attacker wants.

Batelco's Strategic Solution

Robust Global network

Batelco provided a global multi-protocol label switching (GMPLS) one-stop solution, with 19 circuits for complete wide area network (WAN) connectivity across the globe, linking the bank's locations in the Middle East and North Africa, Europe, the Americas and Asia.

The global WAN connectivity offered complete resiliency in core and access links, with automatic fail-over on the last-mile access and international uplinks. Last mile access resiliency provided redundant local access links connecting different points of presences.

Cloud-based Distribution Denial of Service (DDoS) mitigation

Batelco provided a cloud-based DDoS mitigation solution to the bank over an internet link to mitigate DDoS attacks. The service recognises when a DDoS attack happens, identifies and blocks the flow of malicious traffic while accepting legitimate traffic. Through this solution, all traffic to the bank's internet protocol (IP) addresses flows through multiple scrubbing nodes, detecting and filtering malicious traffic targeted at disrupting the bank's enterprise web based network.

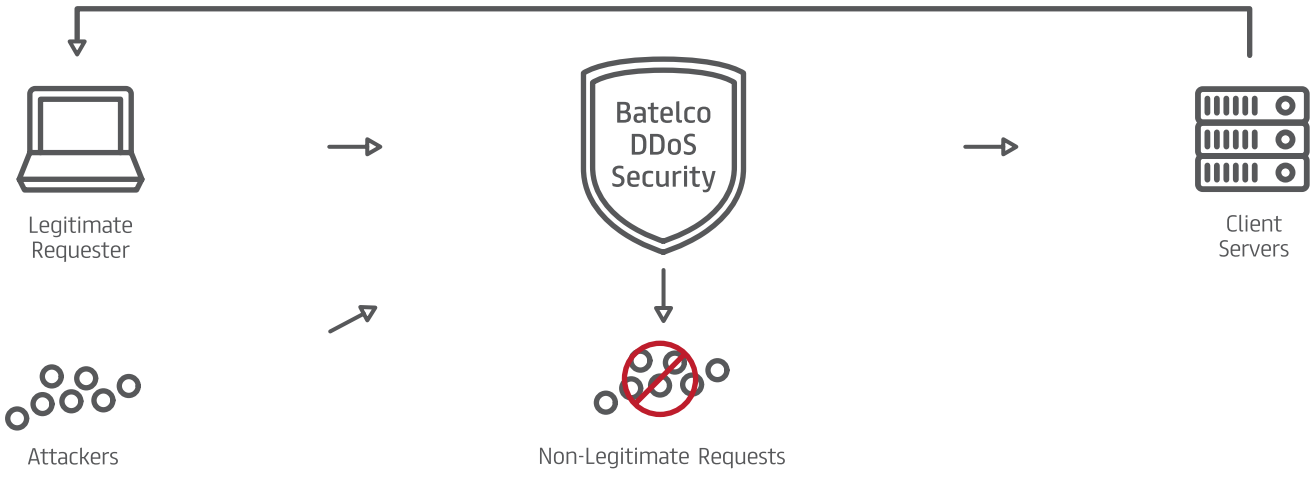
DDoS filters the traffic while it is still on the cloud, before it can reach or harm the bank. The layered protection strategy evaluates complex attacks on a request-by-request basis, so there is never a false positive. The DDoS solution from Batelco features 24x7 management and support through an on-site network operations centre (NOC) and service operations centre (SOC) providing 99.9% service availability. In addition to a range of on-line management tools includes real-time reporting of attack statistics.

2,355

number of threats detected and stopped on the bank's network

98%

network availability has been insured by Batelco's DDoS protection



Customer Benefits

Seamless, reliable global WAN

The bank now enjoys a professionally-managed, reliable and stable wide area network linking its 19 subsidiaries, branches and representative offices in the Middle East and North Africa, Europe, the Americas and Asia, managed professionally through a committed and monitored service level agreement (SLA) with 99.9% service availability.

Safeguarded the Banks reputation and protected revenue

The proprietary mitigation methods and techniques of Batelco's cloud-based DDoS mitigation solution has proved successful in stopping over 1,000 real-world DDoS attacks on the bank's network. This has dramatically reduced the risk to their online services, revenues, and global reputation.

Batelco's cloud-based DDoS mitigation solution has proved successful in stopping over 1,000 real-world DDoS attacks on the banks network