DDoS Protection for Governments

DDoS Challenges

Governments worldwide offer online services to increase accessibility and reduce expenditures. In the process, they need to ensure regulatory, and compliance adherence such as data sovereignty, privacy, and sensitive data protection. Often, they are expected to be role models in implementing network security best practices.

Most democratic nations have decentralized organizational structures and these models come with their challenges, such as limiting agencies' abilities to develop tailored, agile solutions for their cybersecurity challenges.

FBI Reportedly Says DDoS Attack Targeted Voter Registration
– Published in BankInfoSecurity.

Over a month, the FBI reported that a series of DDoS attacks targeted a state-level voter registration and information site. The attacks bombarded the site with malicious traffic in intervals to overwhelm the DNS server and shut down the website.

Strike to Hurt

Hackers factor in all and more of the above-mentioned obligations as vulnerabilities and they strike. Attacks often coincide with large scale public happenings such as elections. Before and during the US elections, political campaigns experienced an average of 4,949 cyber-threats per day, and larger campaigns even more. This is problematic given that nowadays, campaigns rely heavily on online platforms like video conferencing, online fundraising, and social media to reach voters.

As a result, mitigating DDoS attacks has become one of the biggest challenges for government agencies today as they face attacks with limited cybersecurity resources.

Why Governments?

Hackers factor in all and more of the above-mentioned obligations as vulnerabilities and they strike. Attacks often coincide with large scale public happenings such as elections. Before and during the US elections, political campaigns experienced an average of 4,949 cyber-threats per day, and larger campaigns even more. Government election-related sites were seeing over 122,000 threats every day. This is problematic given that nowadays, campaigns rely heavily on online platforms like video conferencing, online fundraising, and social media to reach voters.

Political Upheavals: DDoS attacks are among the most visible and disruptive of cyber-attacks to cause political disruptions. Politically motivated attacks are aimed to cause the victim damage or register their displeasure with some actions. These types of attacks can often be witnessed during elections.

Ideological Belief: Hackers become motivated to attack political targets because of their ideological beliefs against nation-state or government policies. This motivation has become an influential reason behind many DDoS attacks. In January 2019, Zimbabwean government-related websites were hit with a DDoS attack by the hacktivist group Anonymous protesting internet censorship in the country.

Cyber Warfare: There are also incidents of "state-sponsored" attacks. The 2020 Australia government attacks, targeted Australian businesses and governments. The attacks were described as "state-sponsored", which means a foreign government was believed to be behind it.

Intellectual Challenge: Some hackers launch attacks to demonstrate their technical capabilities skills. DDoS tools and even services are available via the Dark Web making it easy for attackers to deploy and experiment with the latest technologies such as automation and botnets against numerous targets.

Ulterior Motives: Historical data indicates that for hackers, any large-scale event is an invitation to launch a DDoS attack. In March 2020, the US Department of Health and Human Services was hit by a DDoS attack just as the agency was scrambling to provide information and critical services in response to the COVID-19 coronavirus pandemic. While the attack was unsuccessful, the potential impact of a successful attack would have been enormous. With the HHS system down, it would have been easy for cyber attackers to spread disinformation, set up fake government websites, and potentially steal data from network systems left exposed.

Extortion: Along with political motives, hackers indulge in attacks for cyber extortion demanding ransom in the form of Bitcoin. The hackers demand ransom threatening data exposure or long periods of downtime.

What Governments Do to Mitigate Attacks - After They are Launched

- Install Web service applications on many independent servers based in different parts of the world. However, they could still be hacked, though all of them going down at the same time may not happen.

- Use the services of independent DDoS proxy service providers but this could involve some latency and even some points of failure.

- Protect systems with the best IP filtering appliances available but that would need weekly testing using tools designed for this for effective management.

- Use specialized DDoS mitigation services from leading vendors but even with regular testing and the best mitigation systems installed, DDoS traffic still manages to bypass DDoS mitigation defenses and cause damage. The resulting DDoS vulnerability gap is a staggering 48%, causing system disruption and downtime.

The main problem

DDoS attacks are increasingly more complex and quick. They leave much less time for current DDoS mitigation systems to react. Many DDoS attacks manage to penetrate the best mitigation solutions. To address these challenges, there is a need to detect and close all DDoS vulnerabilities on going, before an attack is launched. Allowing mitigation solutions to respond in the fastest possible way with minimal manual intervention.

Introducing RADAR™ - detecting open vulnerabilities in real time

RADAR™ analyzes the target network attack surface exactly like a hacker would. By simulating known attacks against all web facing IP's targets without any downtime, RADAR™ detects open vulnerabilities in the target network. RADAR™ clearly identifies the attack surface risks (DDoS vulnerabilities) automatically as they are generated across live production web facing IP's. Then it prioritizes the vulnerabilities by the number of targets found prone to, and details the nature of those vulnerabilities through unprecedented information. This information enables proper mitigation and remediation setup. Once the remediation is completed RADAR™ validates the remediated vulnerabilities ensuring the remediation process was successful.

Benefits of RADAR™ for Governments

- **Operational continuity –** DDoS tests are designed to identify basic vulnerabilities in DDoS mitigation posture and are run without disruption to government websites. This ensures that government sites will continue to always function normally, irrespective of whether there are elections or political upheavals.
- **Data-driven protection –** Reports are generated representing the number of connections per second sent by MazeBolt's simulation cloud, with the corresponding number of connections per second that bypassed the current DDoS defenses. These reports empower the IT personnel to remediate the vulnerability gaps in real-time and reduce risk of DDoS attacks at all times.
- **Security at all times –** RADAR™ highlights the most important DDoS vulnerabilities in the mitigation apparatus and/or architecture, allowing security personnel to make the least amount of changes. At the same time making the biggest impact in strengthening the IT infrastructure against DDoS attacks. Since it works continuously and non-disruptively, government sites are always available irrespective of the political changes or upheavals that could be taking place.
- **Reduce the workload of in-house IT staff –** As a result of the inherent weakness in existing mitigation solutions, the IT staff are pulled into action after an attack has occurred. This results in the staff being taken away from their regular activities to identify and mitigate DDoS attacks. Since RADAR™ prevents attacks, the workload of mitigating attacks is non-existent. IT teams are spared from sudden, stressful mitigation activities and can continue to focus on their day-to-day activities.

About MazeBolt

MazeBolt is an innovation leader in cybersecurity and part of the DDoS mitigation space. Offering full DDoS risk detection and elimination and working with any mitigation system to provide end to end full coverage. Supporting organizations in avoiding downtime and closing DDoS vulnerabilities before an attack happens.

For more information,
please visit: www.mazebolt.com
or e-mail: info@mazebolt.com