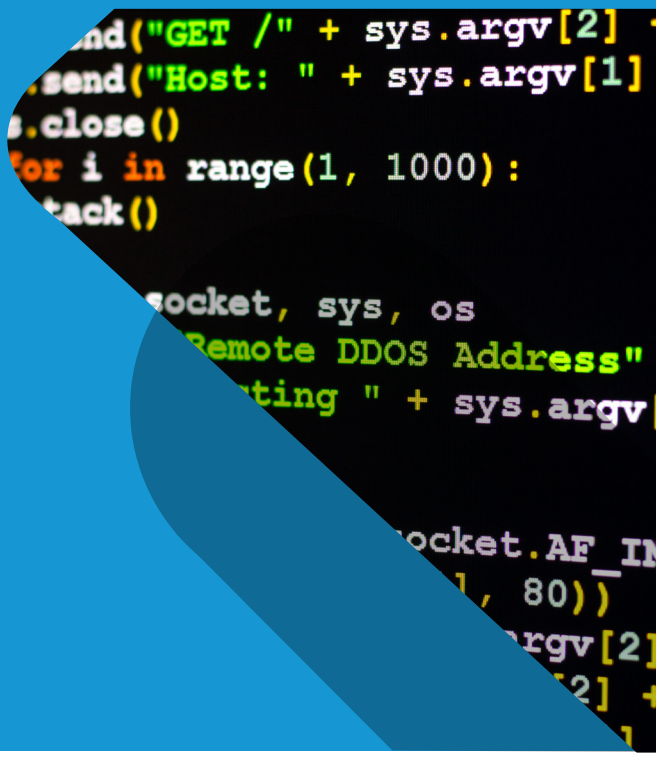
Government Technology Insider

LUMEN

DDOS MITIGATION PROTECTS GOVERNMENT AGENCIES AND CONSTITUENTS AGAINST CYBER THREATS

Nina Jacobs



Distributed Denial of Service (DDoS) attacks are increasing in frequency, duration, and impact. At the same time, they are becoming more discreet and sophisticated as staging multi-vector attacks becomes easier. In the face of the return of DDoS attacks, all public sector agencies need to take measures to limit the amount of damage DDoS attacks can cause.

Why are DDoS attacks a threat to the public sector?

DDoS attacks are used for different purposes than other types of cyberattacks and can often manifest differently as well. Unlike other malware attacks, the effects of which might not be discovered for some time, the impact of a DDoS attack is immediate and widespread. Frequent perpetrators of these attacks include hacktivists who want to use the disruption of services to promote a message or cause. These messages are often political in nature, making government agencies a common target for ideologically motivated attacks.

Additionally, as government agencies integrate Internet of Things (IoT) devices into their workflows they become more vulnerable to DDoS attacks. While these devices can provide support for mission objectives, they can also pose security risks that agencies must plan for. Without proper risk management, IoT devices can become vulnerabilities that attackers can exploit.

Who is affected by DDoS attacks?

At first glance, DDoS attacks may seem like a minor inconvenience. However, these attacks can cause much more damage than just a temporary website outage. Federal, state, local, and education agencies can all be harmed by DDoS attacks in a multitude of ways, ranging from reputational damage to inability to deliver services, and even life-threatening service outages.

Federal: Attacks on federal agencies are often highly visible and impact large populations of employees and customers. These attacks are often highly publicized, making them an appealing way to promote a political message.

State & Local: DDoS attacks at the state level can impact day-to-day resources such as city or county services. For example, an attack targeting local 911 services, even for a short time, can prevent emergency responders from delivering life-saving care. State and local government agencies often have limited cybersecurity resources, making them attractive targets for easy entry.

Higher Education: Interruptions to college and university websites and apps can prevent students from attending classes, submitting tests and assignments, and accessing essential school resources.

Solutions

The goal of any DDoS mitigation strategy is to minimize the damage an attack is able to do. DDoS attacks differ from other kinds of breaches in that they cannot be predicted or preempted—the attack must happen before a response can be enacted. For this reason, one of the most valuable tools for government DDoS mitigation is relationships with industry partners that can detect and mitigate attacks. Two primary relationships are key to protecting agencies from DDoS attacks:

1. **Internet Service Providers (ISPs)** have visibility over their networks, making it easy for them to detect an attack. When an ISP detects an attack, it can redirect the attack traffic to a scrubbing center to separate DDoS traffic from legitimate traffic, which is then sent back to the customer.

   Lumen's Black Lotus Labs® global threat intelligence powers its Rapid Threat Defense service, an automated threat detection and response capability, which automatically blocks DDoS botnet traffic before it impacts an organization's network. This multi-layered security approach, which pairs scrubbing center solutions with enhanced network routing, rate limiting, and filtering, enables agencies to defend against a variety of sophisticated attack types. Lumen DDoS Mitigation service is backed by

Lumen's multi-tiered scrubbing architecture, enacted at 500+ global scrubbing locations, which enables Lumen to act as a solid partner to help agencies protect their digital ecosystems.

2. **Cloud Service Providers (CSPs)** also offer DDoS protections for the web domains they host. They can implement resources to withstand and mitigate attacks without impacting application availability or performance.

Conclusion

As cyber attackers develop new attack vectors and governments shift more toward the digital realm strategies, DDoS attacks will likely continue to increase in frequency, size, and complexity. Protecting government and constituent data and ensuring access to services remains critical under this evolving threat environment, making DDoS mitigation an essential part of any agency's cybersecurity strategy.

Talk to a Lumen security expert today:
888-597-2544