WHITEPAPER

Government DDoS Attacks

A Government Guide to Preventing DDoS Attacks

A DDoS attack can bring your government office to its knees. Without a way to detect or mitigate the attack you could be forced to pay to make it stop, or suffer severe consequences with no end in sight. Thankfully, there are ways to fight back against this growing threat, and the first step is knowledge.

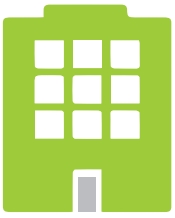
Understanding DDoS Attacks

DDoS Attacks are Common

According to Kaspersky, growth is primarily driven by a rise in attacks against educational websites and administrative domains, including city services. This means that if you haven't yet been attacked, your time may be coming due. Just like ransomware, criminals don't just focus on the largest organizations either. In fact, municipalities are seen as easy targets, as they often have limited resources, are understaffed, and have traditionally considered cyberattacks to be a problem for large corporations.

Cybercriminals Range in Age, Location, and Expertise

Cybercriminals are equal-opportunity hackers, located next door or across the globe, young or old, educated and uneducated. Attackers are targeting work-from-home tools and online learning platforms. DDoS attacks are easy to carry out and don't require specialized training. Attack toolkits are available on the dark web. This may be good news to aspiring criminals, but it is bad news for the rest of us. The ease of launching an attack means we can expect more in the years ahead. The time to prepare is now.

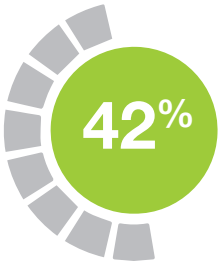


DDoS Attacks Aren't Just Concerning for Large Companies.

As mentioned previously, organizations large and small are vulnerable. In fact, smaller government offices may be perceived as having less rigorous defenses and expertise, fewer resources, and less experience guarding against hackers, so they may actually be a more attractive target.

Just Because You've Been Hit Once Doesn't Mean You Won't be Hit Again.

Like homes that are broken into multiple times, vulnerable organizations are not immune from multiple DDoS attacks. More than 42% of the organizations monitored by one DDoS protection company were hit more than once, and 2.5% were attacked repeatedly more than 10 times.Similar to other cyberattacks, the more effective the attack the more likely the criminal is to keep trying. For companies not ready, they can easily find themselves on their heels for what could be a series of unrelenting DDoS attacks.



I Have a Firewall. Isn't That Enough?

Unfortunately, no. Intrusion prevention systems like firewalls and routers can't prevent DDoS attacks. Because DDoS attacks can involve forging hundreds of thousands of IP sender addresses, the location of attacking machines cannot be easily identified. To ward off attacks, you need a solution that can react within seconds, not minutes. That's why a DDoS solution from a provider like FirstLight is a critical defense.

DDoS Attacks Seriously Impact the Bottom Line

DDoS attacks can cripple your state or municipal budget. Attacks result in lost worker output, potential penalties for non-compliance, revenue loss and damage to your organization's reputation. Sometimes attackers demand a ransom payment from site owners, which only adds to financial losses.

Attacks Often Serve as "Smoke Screens"

Most DDoS attacks do not attempt to breach a company's network, but rather overwhelm with traffic so it comes to a halt. Increasingly though, these attacks are being used as "smokescreens" to distract from the real intent — data breaches. By distracting the organization with a significant DDoS attack, a hacker may stand a better chance of breaking into your systems and gaining sensitive data undetected.

Attacks Damage Your Public Mission

DDoS attacks don't just harm organizations financially — they disrupt basic services provided to local residents and taxpayers. A DDoS attack is more than just a public embarrassment — it adds more distraction to an already challenging administrative environment, and can damage your city's or town's reputation and serve as a beacon conveying your vulnerability to other nefarious actors looking for easy prey.

Attacks are Always Evolving

As organized attacks become more sophisticated and effective, and networks and server capabilities grow, government institutions need to become more savvy about strategies to help defend themselves and their assets. Heating and cooling systems, printers, thermostats, video conferencing, even vending machines are digital gateways. Organizations need to stay one step ahead of these cybercriminals as they continue to get smarter and more strategic.

You Don't Have to be Defenseless

Organizations need to determine the risk of a potential attack and identify what needs protecting. Ideally you need a solution that detects anomalies in network patterns in real time and alerts you to unusually high levels of incoming connections from one or more sources. With FirstLight's DDoS Protection and Mitigation Solution, you can rest easy knowing FirstLight is on alert looking to defend your network and mitigate potential attacks without crippling your critical network traffic.

The Right DDoS Prevention & Mitigation Solution

Your Internet provider should be a partner to help fight back against DDoS attacks as they are in the best position to monitor your traffic and can leverage their network resources to help you mitigate the attack. The right DDoS solution should have the following fundamental components:

24x7 Traffic Monitoring

Suspicious activity filters should be on watch 24×7, updating new threats constantly using algorithms to pinpoint unusual or malicious traffic

Traffic Triage

Mitigation significantly reduces the severity of an attack and allows legitimate traffic to reach the destination network

Traffic Mapping

Normal traffic patterns are identified, and parameters are set for accurate detection

Dashboard

Analytics are provided via a user-friendly portal, along with automated notifications, filters, and alerts

Uniform Pricing

Predictable monthly expense regardless of number of attacks, mitigation, or scale of attack

Why You Should Consider Using FirstLight as Your Internet Provider and for DDoS Prevention & Mitigation

FirstLight's high-speed, low-latency fiber network offers superior performance with an emphasis on redundancy and security. FirstLight has been providing Internet services since 1999 with the philosophy that the greatest quality of service is provided not just by the highest possible connection speed, but also combined with superior peering arrangements and dedicated bandwidth delivered over a stable, fiber-based network.

FirstLight offers a DDoS prevention and mitigation solution coupled with our Internet service and it is available to add on to any Internet connection on our network. FirstLight can help protect your organization from this growing threat while also keeping your applications and staff performing at their best.

Interested to learn more about FirstLight's DDoS solution?
Schedule a demo today or reach out to one of our experts by visiting www.FirstLight.net/DDoS

Some content has been used by permission of FlowTraq ™