DDoS Extortion Battle Checklist

With distributed denial-of-service (DDoS) attacks on the rise, are you prepared to fight back? Organizations without a DDoS mitigation strategy in place will be left with two choices – pay the ransom or risk unexpected downtime. Follow these steps to minimize the risk of an extortion-driven DDoS attack on your organization.

1. Do not feed the bears (fancy or otherwise)

Akamai recommends not making ransom or extortion payments; there is no guarantee the attacker will follow through on their threats or that payment would prevent a DDoS attack. Threat actors are attempting to capitalize on the "fear of the unknown" to make money quickly before moving on to the next target.

2. Bring in the mitigation experts

Determine whether business-critical assets and back-end infrastructure are protected. If you don't have DDoS mitigation controls in place, engage cloud-based providers that can quickly turn-up emergency services (contact Akamai's DDoS Hotline) to reduce risk. Our global SOCC specialists have been successfully fighting DDoS attacks for more than 20 years.

3. Let the DDoS games begin

With the right mitigation partner and security controls in place, attackers don't stand a chance. For Akamai, nearly all of the DDoS attacks associated with this campaign have been proactively mitigated with our zero-second SLA; only a small percentage required active mitigation by our global SOCC. In fact, approximately 70% of all attacks we mitigated in 2020 have been fully blocked with Prolexic's zero-second SLA.

4. Switch up your security posture

It only takes one attack to know DDoS defenses are a must in today's threatscape. Evaluate your risk tolerance to determine if an on-demand or always-on cloud-based mitigation posture is best designed to keep your internet-facing presence protected.

5. Revisit your DDoS playbook

If you haven't already, pull together your IT, operations, security, and customer communication staff to ensure you are prepared and know what to do in the event of an attack. At Akamai, we create custom defense runbooks with each customer and execute a variety of tabletop attack drills to ensure the right people, processes, and procedures are in place to optimize incident response.

To keep today's business-critical assets up and running, enterprises – both large and small alike – need access to high-quality mitigation controls, platform scale, and the expertise to stop DDoS attack campaigns in their tracks. Visit akamai.com/ddos-briefing to request your own custom DDoS threat briefing and get the insights to help keep your business protected.