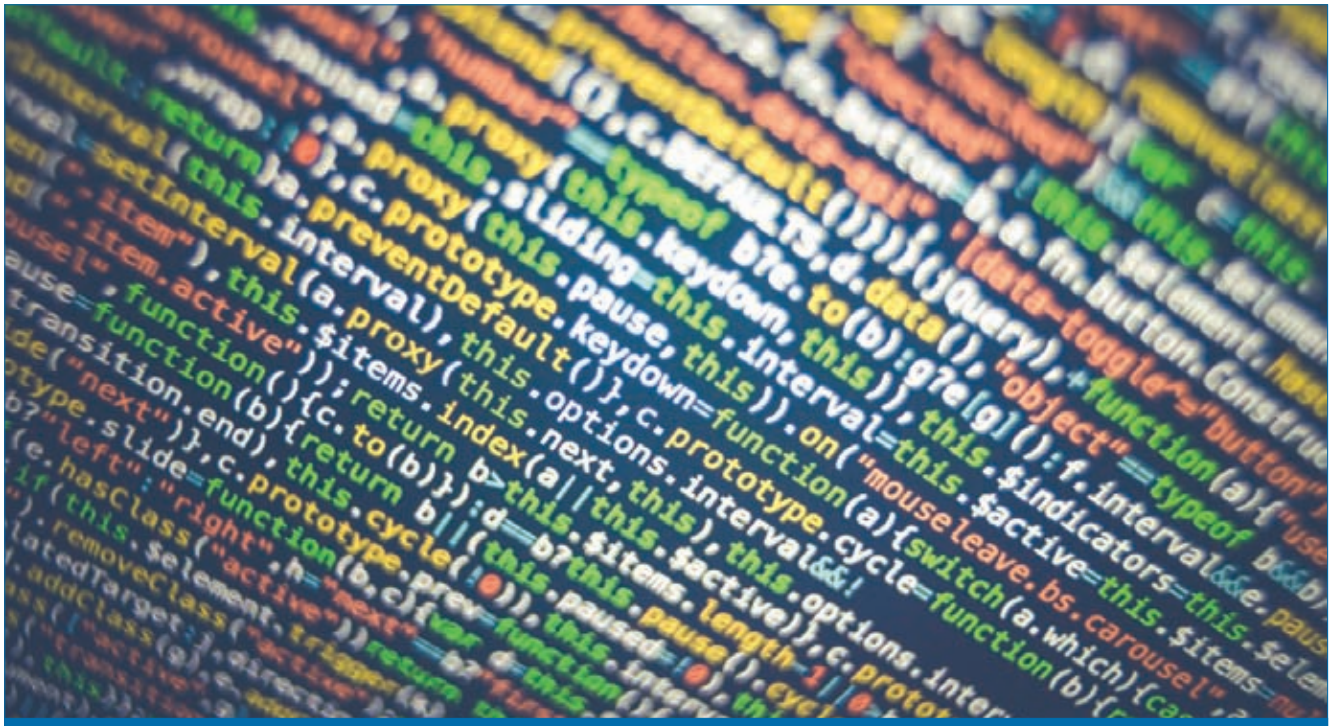

Photo courtesy Markus Spiske

The most common DDoS threats for satellite service providers and how to thwart them

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are a grave concern in today's world as an increasing number of devices, critical to infrastructure, come online. There are several different types that can cripple a network, and as such, it is vital to stay on top of the threats. Maya Canetti, Director of Product at Allot Communications, outlines the threats faced by satellite operators today, and how they might be prevented

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are a grave concern in today's world as an increasing number of devices, critical to infrastructure, come online. There are several different types that can cripple a network, and as such, it is vital to stay on top of the threats. Maya Canetti, Director of Product at Allot Communications, outlines the threats faced by satellite operators today, and how they might be prevented.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks have been a cause for concern for communication service providers (CSPs) since early 1970. In terms of damage to network infrastructure, service continuity and business reputation, DoS/DDoS attacks have racked up some of the most successful cyberattacks to date.

Historically, satellite service providers assigned low risk to being subjected to a DDoS attack. Today, however, technology advances have made it easier to launch flooding attacks and to increase the scope of damage. Service providers can no longer afford to take a passive approach that assume, "If it hasn't happened to my network, it probably won't. And if it does, I'll handle it then."

One of the main factors driving service providers to adopt a DDoS Protection strategy is the Quality of Experience (QoE) that consumers expect. Sluggish response time is not appreciated, and downtime is not tolerated. To assure service availability and performance, CSPs must take measures to protect against DDoS

Maya Canetti, Director of Product at Allot Communications

attacks that are designed to overwhelm network resources and deny service to legitimate users.

But how much do satellite service providers know about the threat as it currently stands? Below we outline the most common attacks and their implications for CSP network assets and the business.

Three common types of DDoS attacks

There is unfortunately more than one type of DDoS attack which satellite service providers need to be aware of. TOS Floods, SYN Floods and PING floods all vary in their approach, and it's important to know the difference:

TOS (Type of Service) Flood

In a TOS (Type of Service) Flood, attackers forge the 'TOS' field of the IP packet header, which is used for Explicit Congestion Notification (ECN) and Differentiated Services (DiffServ) flags. There are two known types of TOS attack scenarios. In the first, the attacker spoofs the ECN flag, which reduces the throughput of individual connections thereby causing a server to appear out of service or non-responsive. In the second, the attacker utilises the DiffServ class flags in the TOS field to increase the priority of attack traffic over legitimate traffic in order to intensify the impact of the DDoS attack.

CSPs will see their services slow down or become non-responsive due to reduced connection throughput caused by the TOS forging. Applications like VoIP, that require fast response time, will suffer dropped calls and bad QoE due to attack traffic receiving higher DiffServ priority than legitimate VoIP traffic.

IoT botnet attack

IoT botnets are created as hackers infect numerous Internet-connected (IoT) devices and recruit them to launch large-scale DDoS attacks that have been measured in Terabits per sec. These attacks are difficult to detect and mitigate because they use hit-and-run tactics that originate from numerous IoT vectors distributed across many locations – often worldwide.

IoT botnets utilise malware source code that was leaked in early 2015 and has been parlayed into many variants. The most infamous of these is called 'Mirai.' In a Mirai botnet attack, the attacker scans for vulnerable IoT devices such as digital surveillance cameras, modems and DVR players (with open L4 ports), and employs a sequence of known passwords to gain access. Once inside, the attacker downloads the malicious code, which enables remote control of the device and the ability to recruit it for attacks.

Ping Flood

In a Ping Flood, the attacker sends spoofed ICMP echo requests (pings) packets at a high rate from random source IP ranges or using the victim's IP address. Most devices on a network will, by default, respond to the ping by sending a reply to the source IP address. If numerous endpoints on the network receive and respond to these pings, the victim IP addresses will be flooded with traffic and their devices/computers/servers will become unusable. Once the pinging succeeds in flooding its target, customer response time will become sluggish or worse, customers will experience a blackout.

There's a common misconception that the DDoS threat only originates from outside the network. However, once a third party gains access, there's no stopping them using your network to launch an attack. It's important that any protection deployed offers this visibility and can mitigate an attack from both inbound and outbound threats.

When a DDoS attack strikes, the clock starts ticking on your credibility

Massive DDoS attacks can cause immediate service interruption. Effective protection must be able to detect the attack and act fast enough to thwart it, so there is little or no impact on the network and/or its hosted targets. Fast detection and mitigation is even more important when dealing with hit-and-run DDoS attacks that are designed to do maximum damage in just a few minutes and then disappear. Real-time threat detection can detect and mitigates DDoS attacks inline, on the spot, and within seconds, leaving the CSP network and hosted targets unharmed.

It's not uncommon for attacks to exceed 100Gbps and to strike with no advanced warning, to inflict maximum damage. To protect service networks against today's and tomorrow's attacks, service providers need a solution that can scale to match the ever- increasing volume and innovation of these attacks – which often come in even at Terabits per second. Ideally, satellite service providers should look for a solution which also offers granular policy management to allow them to accurately block attack traffic and avoid false positives, and to trigger traffic shaping to assure user Quality of Experience (QoE).

Finally, visibility is critical to effective DDoS Protection. Service providers need essential threat intelligence stats that facilitate root cause investigation to find out how big the attack is; what type of attack it is; who is the attacker and what are the intended targets. These questions can only be answered with analysis of network usage statistics together with threat intelligence to obtain a clear assessment of DDoS attack impact on the service provider's business.

Photo courtesy Markus Spiske