allot
See. Control. Secure.

Success Story

Asian Tier-1 Operator

Assuring Service Availability and QoE by Neutralizing Outbound IoT DDoS Attacks

About the Tier-1 Operator

As one of the leading info-communications companies in the APAC region, this Tier-1 broadband operator offers a full range of information, communications and entertainment services for both consumer and corporate markets. The operator's mobile network provides 4G, 3G and 2G services, while their HFC network delivers high-speed residential broadband services.

Challenge

The fixed network of this APAC Tier-1 operator was hit by a massive zero-day DDoS attack on its Domain Name Services (DNS) infrastructure. The attack overwhelmed the DNS systems and disrupted service to millions of customers. Surprisingly, the Denial of Service attack originated from compromised IoT devices including routers and webcams used by customers connected to the mobile network. The attackers identified vulnerable devices via port scanning techniques and used brute force login to gain access and take control, turning compromised devices into botnets that could launch powerful DDoS attacks.

While the operator already had solutions from Arbor Networks and Radware deployed at the perimeter to defend against incoming DDoS attacks, they were completely blind to anomalous activity and attacks coming from within the network. Following the downtime and damage caused by this massive outbound attack, the Tier-1 operator sought an immediate solution to strengthen existing defenses and to enable fast detection and mitigation of outbound attacks originating inside their network.

Vertical	Service Provider
Industry	Fixed
Region	APAC
Solution	DDoS Protection

Challenge

- Massive zero-day DDoS attack on DNS infrastructure affected millions of customers
- Attack originated in IoT turning vulnerable devices into a Botnet
- Existing defense solutions only cover incoming attacks not outbound attacks

Solution

Fortunately, this Tier-1 already had Allot Service Gateways, so we were able to activate the license for DDoS Secure. DDoS Secure provided protection against bi-directional attacks and utilized Botnet containment software to ensure that the APAC operator did not have to worry about these kinds of attacks in the future.

Benefits

- Resolve urgent security threat rapidly and cost-effectively
- Prevent IoT threats from disrupting network service
- Gain visibility and insight on IoT device traffic and anomalous behavior

Solution

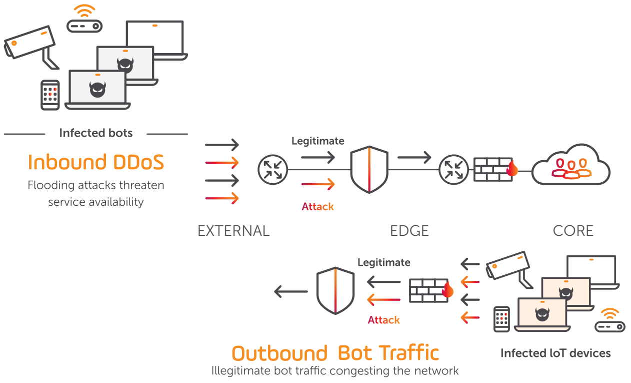
In response to the massive attack, Allot's professional services team were called in to help. Allot Service Gateway platforms are already deployed in the operator's core network, providing a granular data source and real-time record streaming to external systems. These multiservice platforms also host Allot DDoS Protection and Bot Containment services (DDoS Secure). No additional installation is required; all the operator had to do was activate the relevant software license in their platforms.

Once the service was activated, Allot's Host Behavior Anomaly Detection (HBAD) technology started to monitor and learn the normal traffic patterns in the operator's network. A normal traffic profile is achieved in approximately 2 hours and is continuously refined so that traffic anomalies can be instantly spotted. Almost immediately, the operator was able to see anomalous endpoint activity, attempts to port scan connected devices by already-infected IoT devices, and suspicious traffic that acted like outbound spam.

> Allot DDoS Protection and Bot Containment services enabled immediate and effective IoT DDoS defense without installing new equipment or altering existing security systems, so the choice made sense on many levels."
>
> Chief Information Security Officer,
> Tier-1 Service Provider

They continued to evaluate Allot's Bot Containment service for a period of one month. During that time, they were able to

- Detect all suspicious activity
- Identify and block anomalous behavior
- Isolate misbehaving or infected IoT devices from the network



Pleased with Allot's solution in strengthening its network defense, the APAC Tier-1 operator decided to activate DDoS Secure in all of their Allot Service Gateway platforms, managed via a virtualized control console that gives them real-time alerts, event reports, and accurate threat intelligence.

Benefits

By activating Allot DDoS Protection and Bot Containment services in the already-deployed Allot Service Gateway multiservice platforms, this APAC Tier-1 operator can:

- Protect service availability from outbound IoT DDoS attacks complementing the existing inbound DDoS Protection
- Save time and expense by activating IoT DDoS protection immediately in dozens of locations without having to install new equipment or reconfigure network elements
- Gain full visibility of inbound and outbound threats, and valuable threat intelligence that previously was not available

Resources

About DDoS Secure

About Service Aware DDoS Mitigation

Frost & Sullivan IoT Security Whitepaper

Learn more about
Allot's Solutios »