Mitigating Amplified DDoS and HTTP IOT Attacks

Due to the current spate of amplified reflection DDoS and HTTP-IOT-SATORI-BOTNET attacks experienced over the past few days, we are hereby issuing this advisory notice to all customers on how to reinforce security on their infrastructure to guard against these types of attacks.

Amplified reflection attacks are a type of DDoS attack that exploits the connectionless nature of UDPs with spoofed requests to misconfigured open servers on the internet. The attack sends a volume of small requests with the spoofed victim's IP address to accessible servers. The servers reply with large amplified responses to the unwitting victim. The servers can do this because they are configured with services that the attackers sought out for their ability to aid in this attack. The most common types of these attacks can use millions of exposed DNS, NTP, SSDP, SNMP and other UDP-based services.

The devices likely to be exploited are "misconfigured open servers or servers with no access controls in place, or may have been forgotten and left unmanaged, or may have been unintentionally exposed to the internet for no apparent reason. Applying aggressive port blocking and blacklisting IPs based on is an effective, proactive way to mitigate attacks. This strategy uses reputation as a determining factor for blocking traffic, enabling more precise mitigation.

The table below details the protocols and ports used for known amplification attacks. It is highly recommended to block these ports **OUTBOUND** on the internet edge.

REFLECTED AMPLIFIED ATTACK TYPE	***ATTACK SOURCE PORT***	***RECOMMENDED MITIGATION STRATEGY***
BitTorrent	UDP 6881	Block source port
CharGEN	UDP 19	Block source port

CLDAP	UDP 389	Block source port
DNS	UDP 53	Threat Intel. Do not block if required for legitimate business services
Kad (P2P)	UDP 751	Block source port
Memcached	UDP 11211	Block source port or Threat Intelligence
MSSQL	UDP 1434	Block source port
Multicast DNS	UDP 5353	Block source port
NetBIOS	UDP 137	Block source port
NTP	UDP 123	Threat Intel. Do not block if required for legitimate business services
Portmap (RPCbind)	UDP 111	Block source port
QOTD	UDP 17	Block source port
Quake Network Protocol	UDP 27960	Block source port
RIPv1	UDP 520	Block source port
SNMP	UDP 161	Threat Intel. Do not block if required for legitimate business services
SSDP	UDP 1900	Block source port
Steam Protocol	UDP 27015	Block source port
TFTP	Ephemeral	Threat Intelligence

To mitigate the IoT Botnet attacks, make sure the following are implemented on all IoT devices such as CCTV, Cameras, Smart Doors, Lights etc.

1. Change the default/generic passwords.
2. Disable all remote (WAN/Internet) access to your devices by blocking ports SSH (22), Telnet (23) and HTTP/HTTPS (80/443) **INBOUND** on your internet edge (create filters or access lists specific to the devices, so that legitimate traffic is not affected).