Recommendation of ISP Level Port Blocking for DDoS Prevention

Security Advisory AE-Advisory 16-041 **Criticality** High

Advisory Released On 17 November 2016

Description

This recommendation will prevent most of the DDoS attacks that are being distributed currently

Solution

Refer to the “Solution” section below

Summary

aeCERT has noticed that there has been a plethora of DDoS attacks throughout this year, which all have similar malicious behaviour. Most of these attacks use vulnerable protocols that can be used to help amplify and accelerate a DDoS attack. We have noticed that most of these attacks were carried out using the UPnP set of network protocols (UDP port 1900). SSDP is the basis of the discovery protocol of Universal Plug and Play (UPnP) and is intended for use in residential or small office environments. Also, a variation of similar attacks exists which also use different types of vulnerable protocols. From what we have observed, many unused and vulnerable ports can be used to carry out a DDoS attack from an outside intruder. These kind of attacks can be prevented with the cooperation of the ISPs (Internet Service Provider) giving us all the assistance we need to block these unused ports and protocols within the network domain. In this report, we will attempt to explain the types of vulnerable protocols and ports used while conducting a DDoS attack and stress why it is of paramount importance to block them in order to lessen our chances of being hit with another DDoS attack in the near and distant future.

Threat Details

DDoS amplification attacks are based on UDP protocols which are enabled on misconfigured systems on the internet, such as the SSDP protocol on port 1900/UDP. These misconfigured systems are used to launch amplification attacks against various entities within the United Arab Emirates, primarily by spoofing their IP space.

Examples of UDP protocols used for amplification attacks are listed below:

Protocol Name	UDP ports
DNS	53
NTP	123
SNMPv2	161
NetBIOS	137, 138
SSDP	1900
CharGEN	19
QOTD	17
BitTorrent	Any
Kad	Any
Quake Network Protocol	27960
Steam Protocol	27015
RADIUS	1645, 1646, 1812, 1813

Some of these protocols prove to be very difficult from being hard to prevent such as, BitTorrent and Kad (both protocol are used by Peer-2-Peer applications). However, Amplification Attacks can be prevented by blocking or traffic shaping most of the UDP protocols listed above. The blocking and/or shaping should be implemented by the ISP provider (Etisalat and Du) and should be performed on the traffic initiated from the Internet towards the IP space of each entity, based on the source port of the traffic.

We also have noticed that, some of the UDP protocols (blocking or shaping) have created an operational impact for various entities involved. UDP protocols such as NTP and DNS are essential for the functionality of the network operation and blocking or shaping can only be effective if the entities involved are using the DNS and NTP servers of the ISP. DNS requests coming from the entities should be forwarded to the DNS caching resolver servers of the ISP, and the DNS response is returned to the entity via the same DNS caching resolvers of the ISP. This works the same for NTP. Once this change has been made, any DNS response or NTP traffic from Internet towards the entity can be blocked by the ISP based on the source port 53 and 123.

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [1]
NTP	556.9	see: TA14-013A [2]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

Best Practices

- Ensure all IT systems (OSs, applications, websites, etc.) are updated.
- Ensure IT security systems are current, have as wide a view as they can, and can inspect deeply. Can they detect and prevent phases of attack plan.
- Ensure relevant third party vendors are aware and accessible.
- Probe any anomalous network and system behavior and examine it. Reconnaissance phases of the attack are already in play. Opportunities for exploit are being logged and credentials are already being stolen.
- Remind the users to be particularly careful and watch out for phishing and spear-phishing emails.
- Plan or review your incident response procedures with all necessary parties (not only IT groups). Explore how the planned response differs among DDoS, defacement, and disclosure.
- Have IT Security, Attorneys, and External Communications departments prepare or review public statements in the event your organization is affected. Ask the question of "how your statements and response might differ if it wasn't a hacktivist group, but a criminal, nation state, insider, or terrorist?"
- Monitor the many Anonymous sources for any changes in targeting, tools, or motives, lists of accomplishments, or data dumps.

Note that attackers may attack across different time zones, so it can last longer than the 24 hours in UAE time zone. Therefore, please make sure to do the following;

- Continue to monitor the Anonymous' sources for any changes in targeting, tools, motives, lists of accomplishments, or data dumps.
- Exercise a high level of awareness of your IT and IT Security systems and their logs; continue to apply questioning curiosity to anything interesting.
- If you think your organization is affected, assume that you are affected by DDoS, defacement, and disclosure – and not just one of them.

Solution

aeCERT recommends that the UDP protocols, as listed in the above table, are blocked by the ISP with the permission of the entity as per its requirement and needs. aeCERT also recommends the co-operation of the ISP's in the United Arab Emirates to apply any requests the entity would like regarding the ISP level of source port blocking. We also recommend that any entity will use the DNS caching resolver servers and NTP servers of the ISP for the protocols NTP and DNS in order to prevent any DNS or NTP protocols DDoS amplification attacks.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae