The Armada Collective
DDos Amplification and Mitigation Recommendations

US-CERT
Cyber Threat Information Sharing Branch (CTIS)

07 December 2015

Overall Classification: UNCLASSIFIED//TLP AMBER

Homeland
Security

The Armada Collective Overview

-The Armada Collective is a Distributed Denial of Service Extortion Group that is currently unattributed

-This group of malicious actors utilize tactics similar to those used by the group DD4BC (Ddos for Bit Coin)

-Actors email potential targets and threaten a DDoS unless a ransom is paid.

-Initially suspected to be DD4BC resuming attacks under a new name; but now appears more likely that this is a copycat group

-This group claims to have the abilityt o unleash a DDoS attack of more than 1 Tbps per second. (Note: the biggest Armada Collective attack mitigated to date has only peaked at 772 Mbs)

The Armada Collective Targets

-To date, the Armada Collective is known to have targeted:

-Australian Organizations

-Other International Organizations

-Japanese, Swiss and Thai financial institutions

-ProtonMail

-Hushmail

-Runbox

The Armada Collective Tactics, Techniques and Procedures

-Armada Collective Tactics, Techniques and Procedures (TTPs) include:

-Conduct limited DDos attacks against organizations

-Send Ransom emails following the initial attack(s)

-Threaten another, longer, DDos attack will occur if an extortion payment is not made by the victim

-Initial extortion email has different senders and subjects:

-"A little taste"

-"Ransom request: DDoS Attack"

-"Last Warning"

-Maximum observed traffic throughput reported to be approximately 50 Gbps

-Traffic predominately originated from source ports 1900/UDP and NTP

-DDoS attacks have used UDP reflection and amplification

US-CERT Alert (TA14-017A) UDP-Based Amplification Attacks

-Original release date: January 17, 2014 | Last revised: August 19, 2015

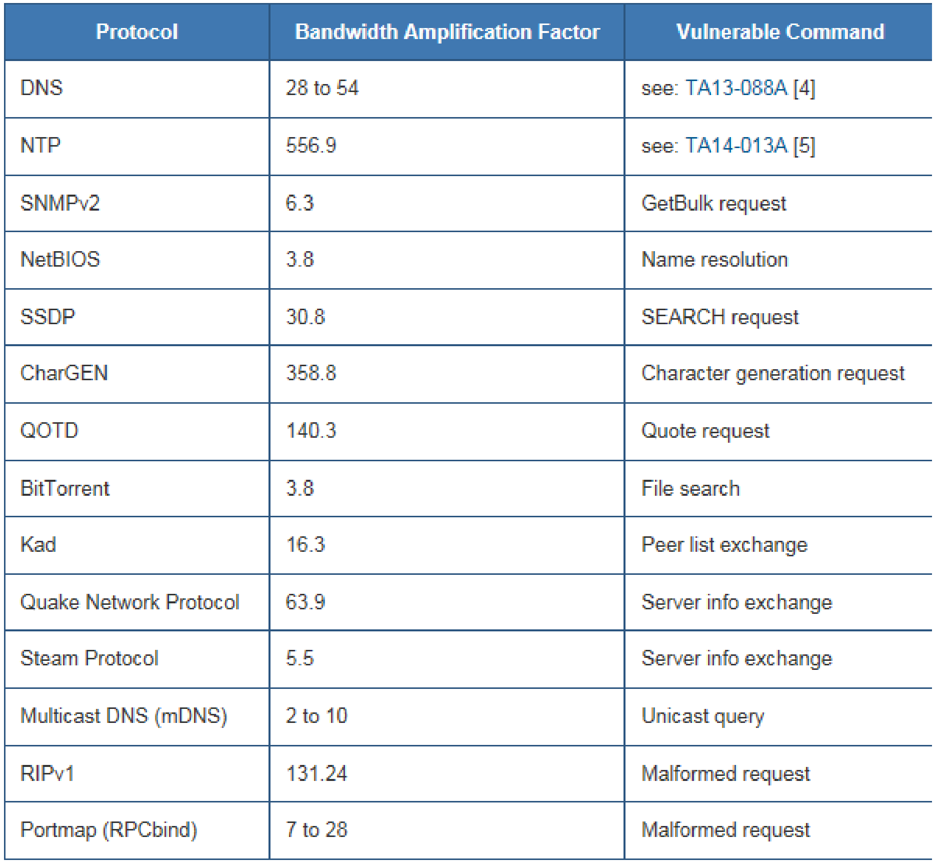
Systems Affected

Certain UDP protocols have been identified as potential attack vectors:

DNS
NTP
SNMPv2
NetBIOS
SSDP
CharGEN
QOTD
BitTorrent
Kad
Quake Network Protocol
Steam Protocol
RIPv1
Multicast DNS (mDNS)
Portmap

US-CERT Alert (TA14-017A) Known Protocols/Amplification Factors

-The list of known protocols—and their associated bandwidth amplification factors—are listed below. US-CERT offers thanks to Christian Rossow for providing this information. For more information on bandwith amplificatication factors, please see Christian's blog and associated research paper.



Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
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
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request

Homeland Security

US-CERT Alert (TA14-017A) DDoS Impact, Detection, Mitigation

Impact: Attackers can utilize the bandwidth and relative trust of large servers that provide the above UDP protocols to flood victims with unwanted traffic, a DDoS attack.

Solution

Detection: Detection of DRDoS attacks is not easy because of their use of large, trusted servers that provide UDP services. Network operators of these exploitable services may apply traditional DoS mitigation techniques. In addition, watch out for abnormally large responses to a particular IP address, which may indicate that an attacker is using the service to conduct a DRDoS attack.

Mitigation: Source IP Verification. Because the UDP requests being sent by the attacker-controlled clients must have a source IP address spoofed to appear as the victim's IP, the first step to reducing the effectiveness of UDP amplification is for Internet service providers (ISPs) to reject any UDP traffic with spoofed addresses. The Network Working Group of the Internet Engineering Task Force (IETF) released Best Current Practice 38 in May 2000 and Best Current Practice 84 in March 2004. These documents describe how an ISP can filter network traffic on their network to reject packets with source addresses not reachable via the actual packet's path. Recommended changes would cause a routing device to evaluate whether it is possible to reach the source IP address of the packet via the interface that transmitted the packet. If it is not possible, then the packet most likely has a spoofed source IP address. This configuration change would substantially reduce the potential for many popular types of DDoS attacks. As such, US-CERT highly recommends all network operators perform network ingress filtering if possible. Note that such filtering will not explicitly protect a UDP service provider from being exploited in a DRDoS because all network providers must use ingress filtering to eliminate the threat completely.

References

References

[1] SIP: Session Initiation Protocol

[2] Amplification Hell: Abusing Network Protocols for DDoS (link is external)

[3] Amplification Hell: Revisiting Network Protocols for DDoS Abuse (link is external)

[4] DNS Amplification Attacks

[5] NTP Amplification Attacks Using CVE-2013-5211

[6] VU#550620: Multicast DNS (mDNS) implementations may respond to unicast queries originating outside the local link

[7] RIPv1 Reflection DDoS [Medium Risk] (link is external)

[8] A New New DDoS Reflection Attack: Portmapper; An Early Warning to the Industry (link is external)

[9] Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing

[10] Ingress Filtering for Multihomed Networks

[11] The Spoofer Project

[12] An Architecture for Differentiated Services

[13] New Terminology and Clarifications for Diffserv