In confidence

Security Threat Intelligence

GLOBAL SECURITY EVENT

Memcached DDoS

Published: 6 March 2018

BT

Threat	L	M	2c H

1. Risk Assessment

Risk Rating: 2c
Impact: High
Likelihood: Likely

This threat is currently assessed as 2c HIGH. A new DDoS attack vector has been identified as targeting Memcached servers that have UDP port 11211 exposed on the internet. The impact to businesses is considered to be HIGH in most cases, particularly if any services have poorly configured Memcached servers. This new attack vector has been seen in the wild over the past week and is therefore deemed an active threat. The likelihood of this threat should be considered LIKELY, particularly with media-wide news reporting in relation to the type of attack, and the considerable amplification that can be achieved.

2. Technical Analysis

Over the past week, BT has observed a number of DDOS attacks crafted using the latest amplification and reflection method, which is known as 'memcached'. Memcached, which uses UDP port 11211, is an open source distributed memory object caching system that is designed for use with dynamic web applications to speed up retrieval of objects and data and alleviate database load. Much in the same way that web content is cached within an ISP network so that further requests for that same content can be delivered locally via the cache, memcached can cache objects and strings for a web application to reduce dependence on external DB/API calls. However, this application has very poor security out of the box, and by default, will allow connections on UDP as well as TCP. In addition, attackers can 'prime' the server by first inserting their own key/value pairs and then requesting that data as part of the attack, spoofing their source address to be the address of the intended target, and therefore redirecting any responses from open memcached severs to the intended DDOS target.

What makes memcached a highly effective DDOS attack vector is the extremely large amplification factor. All amplification attacks rely on a UDP protocol that on request of a small query, can return a large response. For example, DNS may be used by sending a simple 'dig' for some domain that then returns a large response in the form information from zone files that may include A/MX/NS/PTR/TXT records, or an attacker might locate open NTP servers that allow a simple 'monlist' command to generate a response in the form of a full list of IPs that have interacted with that server. The attacker's aim is to generate as large a response as possible to a given query that is sent with a spoofed source IP address. The amplification factor is the ratio of the size of the request to the size of the response.

As an illustration, the following amplification factors are detailed below:

- SSDP 30x
- DNS 54x
- NTP 500x
- Memcached 10,000 to 51,000x

This shows that a 15 byte request may result in a 750kB response. The maximum size for any object in the cache is 1MB. Because of the large amplification factor, an attacker only needs a relatively small number of open servers to generate a large attack. It is estimated that there are currently around 80,000 to 90,000 open memcached servers currently on the internet.

This attack vector has only been reported as being used by a number of networks over the last few days, and attacks have been reported by Cloudflare and Akamai with the latter reporting an attack against one of their customers that reached 1.3Tbps, and today, a 1.7Tbps attack aimed at an unnamed 'US service provider' has been published.

3. Additional Analysis

There is currently little intelligence that identifies or indicates the origin of these attacks, neither are there any reports of any adversary or collective claiming responsibility specifically for memcached attributed activity. However, BT's Security Threat Intelligence identified a group claiming to be the previously-active and notorious 'Lizard Squad' using the Twitter tag of @LizardCorporate, which tweeted on 1 March that they would "*DDoS every major ISA in america [sic], the uk [sic] and india [sic] if [they did] not get 150k followers within 24 hours*". They then provided a number of company names.

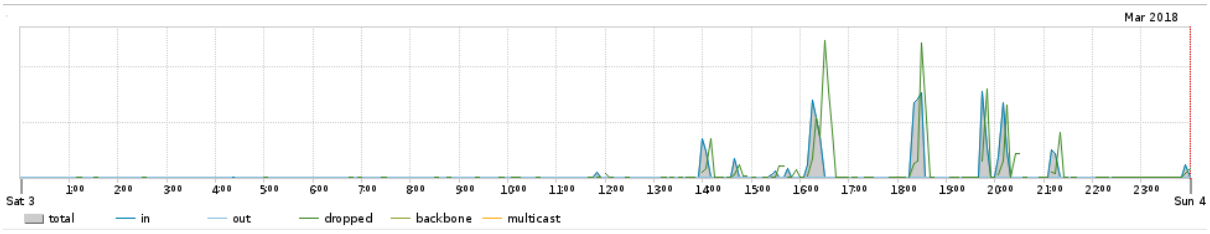
Often social media is used as the preferred medium in which to claim responsibility by those supposedly carrying out the attacks, which is a very common tactic with hacktivists who do so to promote their own motivated activities and ideologies. There is, as yet, no claims of responsibility, for either the 1.3Tbps or the 1.7Tbps attack. This could indicate that the actor(s) behind the attacks may have realised the huge potential and value of their activity, therefore, to prevent any potential disruptions they may be keeping it quiet in order to carry out further attacks.

Another reason that may result in no claims of responsibility may be that the DDoS attacks could be leveraged against gaming servers, which could result in significant collateral impact. DDoS attacks used by gamers against gamers are a common tactic, and with the existence of DDoS-for-hire-Services, it is very easy for gamers to get a hold of the tools necessary to carry out such activity.

With the large media reports on this new attack vector, focusing on the considerable 1.3Tbps and 1.7Tbps attacks, this is likely to raise interest, with many actors and groups involved in DDoS-related activity and hacktivism. This could potentially lead, if not already, to DDoS-for-hire-Services incorporating the attack vector in to their services, which then increases the reach of the capability to more low-level actors. The more actors or groups that gain access to such DDoS services, the higher the risk that this attack vector will be leveraged against numerous businesses, crossing multiple industries worldwide. Akamai have already seen a noticeable increase in active scanning for open memcached servers since the media broke news of the new attack vector several days ago.

Imperva also reported on 1 March 2018, that they had observed two massive DDoS amplification attacks on 28 February, which was the same day as the 1.3Tbps attack. These two attacks were targeted against a cryptocurrency exchange, as well as e-commerce websites.

In the last week, since BT first saw this attack vector, we have seen over 30 attempted attacks across the BT estate and additional attacks on the EE network. Below is a typical 24-hour period, showing the attack data:



4. Recommendations

General recommendations for overall DDoS protection:

An organisation can help to protect themselves in the event of a DDoS incident by considering the following recommendations:

- The use of a third party DDoS mitigation tool or service.
- Have a well-established DDoS playbook to call upon when an incident occurs. Appropriately skilled personnel should be called upon to ensure the best level of protection and mitigation.
- Conducting a review of current DDoS mitigation tools with a view to assessing whether they are currently fit for purpose.
- Ensure your network has been target hardened.

Specific technical recommendations for this attack vector are as follows:

- To reduce the impact of UDP/11211 implement one of the following at your network edge (or ask your service provider):
    - Rate limiting
    - Access Control Lists
- Other approaches such as deploying Flowspec at the edge to block this traffic to the target address may be considered, but there is a significant delay in deploying this option as it is a manual process.

Appendix: Risk Matrix

There are 4 categories of risk:

- CRITICAL
- HIGH
- MODERATE
- LOW

Risk ratings are assessed based on the IMPACT that the threat poses against the LIKELIHOOD of the threat occurring.

		LIKELIHOOD			
		UNLIKELY (0-24%)	POSSIBLE (25-59%)	LIKELY (60-89%)	ALMOST CERTAIN (90-100%)
		Downward trend Low number of actors Low number of victims Low opportunity Fluid / disorganised membership Unknown motivation Lack of skill / resource No known exploit Vulnerability risk inside the network - risk of exposure / local availability	Emerging / continuing trend Low number of prolific individuals Low number of victims Little opportunity Display structure and competence Potentially motivated actor / group Some use of skill / resource Exploit skill required - difficult Vulnerability risk inside the network - local access / local priviledged	Continuing trend High number of individuals High number of victims Medium Opportunity Display structure and competence Well motivated actor / group Use of skill and resource availability - some use of specialists Exploit skill required - moderate to easy Vulnerability risk outside the network - remote availability / remote access	Increasing trend / seasonal High number of prolific individuals High number of victims High opportunity Highly organised, disciplined Highly motivated actor / group Expert skill and resource availability inc corruption / coercion Exploit skill required - automated Vulnerability risk outside the network - remote priviledged
IMPACT					
LOW	Low impact on brand / reputation / share price affecting Low threat of public disorder impact Low financial risk Mitigation / patches available Low impact on service delivery	4e LOW Minor concern	4d LOW Minor concern	4b LOW Minor concern	3g MODERATE Intermediate concern
MODERATE	Moderate impact on brand / reputation / share price affecting Moderate threat of public disorder impact Moderate financial risk Moderate impact on service delivery Mitigation / patches available and / or difficult to implement	4c LOW Minor concern	3e MODERATE Intermediate concern	3d MODERATE Intermediate concern	3b MODERATE Intermediate concern
HIGH	High impact on brand / reputation / share price affecting High threat of public disorder impact High financial risk Mitigation / patches not yet available High impact on service delivery	4a LOW Minor concern	3c MODERATE Intermediate concern	2c HIGH Significant concern	2b HIGH Significant concern
VERY HIGH	Critical impact on brand / reputation / share price affecting Critical threat of public disorder impact Critical financial risk Mitigation / patches not yet available, inc 0-day Critical impact on service delivery Threat to life	3f MODERATE Intermediate concern	3a MODERATE Intermediate concern	2a HIGH Significant concern	1a CRITICAL
