Do they **DDoS** via Memcached?

What

To what extent is the Memcached protocol still abused for DDoS amplification in the post-patch era, and which tactics, techniques, and procedures characterise the adversaries that engage with it?

Why

Memcached is widely considered patched. Used to have ≈51,000× amplification in 2018. This patch applies only to newly deployed services set to default config

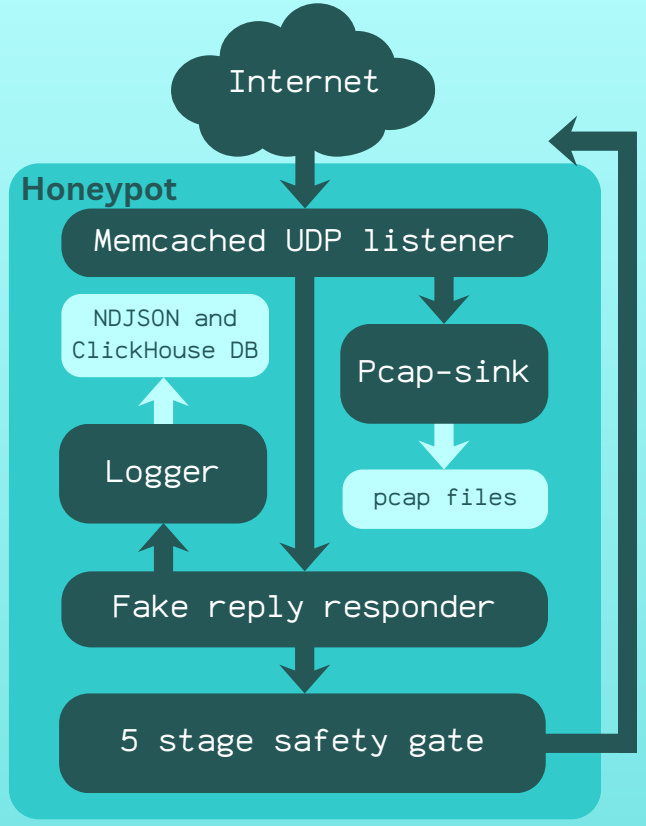
Could the legacy and manually configured systems be vulnerable? Let's find out!

How

Create a series of honeypot IP addresses hosted on a virtual machine (VM) that will offer misconfigured Memcached services for attackers to attempt exploiting

Rate-limit outgoing traffic to prevent contributing to actual DDoS attacks

Collect data on interactions with attackers



Traffic overview

2026-05-29 → 06-19

Traffic	
Total events	4,261
Distinct sources	465
Honeypot IPs	16
Replies sent	1,570
Bytes egressed	277 KiB
Peak rate	26 pps

Protocol	
Text	3,224 (76%)
Non-protocol	1,037 (24%)
Binary	0 (0%)
Dropped	
Same-port	1,646
No-reply	1,027
Silent mode	18
Rate cap	0

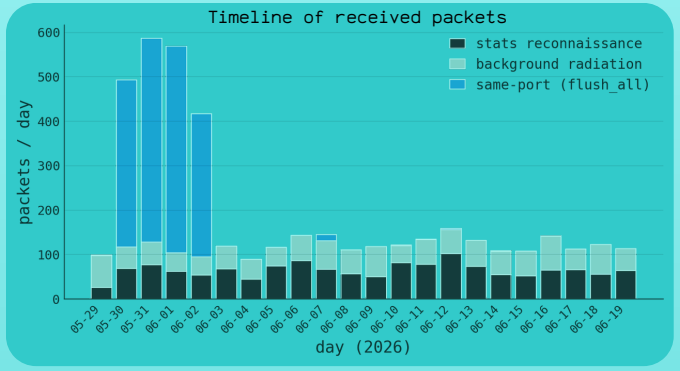
Observations

Traffic is dominated by stats command

Small sub-population using id 1 in 8-byte UDP header (2018 Memcrashed PoC)

No set/store commands → precondition for high amplification never met

Only abuse-related traffic: 4-day same port flush_all burst



Takeaways

Attacker behaviour stops at scan + test

Execute phase never materialised against our fresh, unpopulated amplifier

Limitations: short window, single vantage point, and a small stats bait (≈13× compared to ≈51,000× in 2018)

Absence of execute ≠ proof it has stopped

Memcached today is a catalogued but dormant amplifier

TU Delft

Maxim Hájek
M.Hajek-1@student.tudelft.nl
Supervisor: Harm Griffioen