



Josue Bustos <josueabrahannieto@gmail.com>

[DigitalOcean] Ticket #11334514: [Notification Only] Droplet Detected Sending Potentially Malicious Traffic: ref:!00Df2018t5m.!500QP018wpl1:ref

1 mensaje

DigitalOcean Abuse <abuse-replies@digitalocean.com>
Para: "josueabrahannieto@gmail.com" <josueabrahannieto@gmail.com>

8 de diciembre de 2025 a las 9:37 a.m.

Hi,

We are writing to let you know that one of your droplets is contributing to unusually high outbound traffic. We have high confidence that it may be actively being used as part of Distributed Denial of Service attacks against specific victims.

While investigating this recent DDoS attack, we discovered strong indicators that your Droplet trawi-stats at 142.93.65.119 was used to contribute 70.3 Mbps to this 46.8 Gbps outbound denial of service and may be running an instance potentially vulnerable to "React CVE-2025-55182". If this traffic wasn't intentional, it's very likely your droplet has been compromised and is being used in Distributed Denial of Service attacks. Future reports for additional DDoS activity may require us to temporarily disconnect your droplet from the network to prevent additional abuse.

To mitigate this, it is critical for you to follow one of our recovery paths to reduce any potential harm.

Your path to resolution will be influenced by how you use the trawi-stats, your technical expertise, and/or your time available for investigation.

Path 1 - If trawi-stats does not collect or contain any data you need to preserve, we suggest destroying this Droplet and starting over. This is the most straightforward way to get back up and running.

Path 2 - If trawi-stats stores data you need to recover, please follow our recovery checklist on <https://www.digitalocean.com/docs/droplets/resources/recovery-iso/> before destroying this Droplet and starting over.

Path 3 - If you are confident in your technical ability and want to troubleshoot, identify, and secure the problem on your own, we do have a resource available at <https://www.digitalocean.com/docs/droplets/resources/ddos/> that includes some suggestions.

Regardless of the path you chose to take, if you continue running similar instances, we strongly encourage you to:

- * Stay up to date with the latest releases from your software vendor to ensure security vulnerabilities are patched.
- * Follow your software vendor's best practices for securing your environment.
- * If possible, ensure you are signed up to receive notifications from your software vendor about important security release updates.

We understand this may be added work on your part; however, to protect our customers and the broader internet community, we need your help in resolving this issue.

Let us know once you have completed your resolution path, and we will provide any applicable follow-up.

Best,
Security Operations Center
DigitalOcean

ref:!00Df2018t5m.!500QP018wpl1:ref