



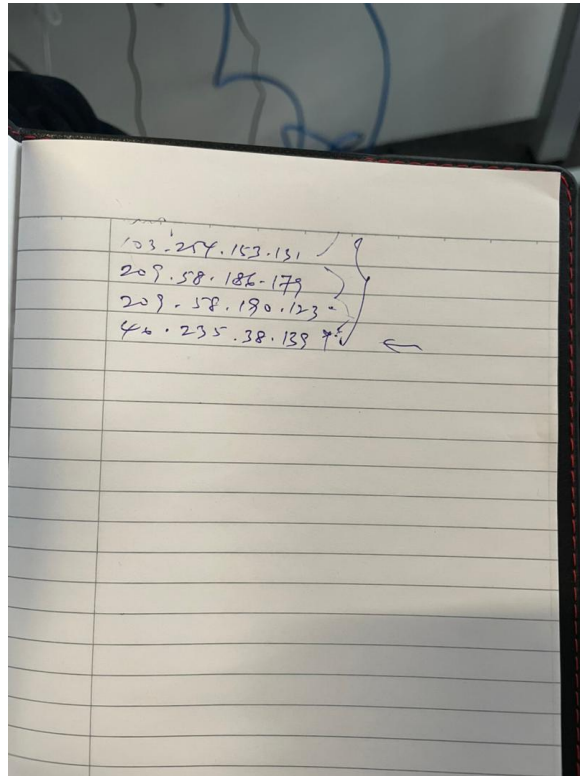
Oroku Edge Trading Server DDOS Issue

Report Period of 16/03/2023 - 17/03/2023

Date	Description
16/03/2023	<p>Arrived from AOR and attended to Oroku Edge's office in Tamarind Square to produce the following findings -</p> <p>Chart servers are hosted in array with different geographical locations:</p> <p>103.254.153.131</p> <ul style="list-style-type: none"> - Up at the time of testing: Yes - Hosting Company: Leaseweb Asia Pacific Pte. Ltd. - Location: Singapore - Address: 18B Keong Saik Road, Singapore 089125 - Reply to ICMP (ping): No - Latency: 14ms (Last Hop) <p>209.58.186.179</p> <ul style="list-style-type: none"> - Up at the time of testing: Yes - Hosting Company: LEASEWEB HONG KONG LIMITED - Location: Hong Kong - Address: Central Plaza 18, Wanchai RD Hong Kong 3806 - Reply to ICMP (ping): Yes - Latency: 221ms <p>209.58.190.123</p> <ul style="list-style-type: none"> - Up at the time of testing: Yes - Hosting Company: LEASEWEB HONG KONG LIMITED - Location: Hong Kong - Address: Central Plaza 18, Wanchai RD Hong Kong 3806 - Reply to ICMP (ping): Yes - Latency: 91ms <p>46.235.38.139</p> <ul style="list-style-type: none"> - Up at the time of testing: No - Hosting Company: Beeks Group (https://beeksgroup.com) - Location: United Kingdom - Address: Suite 1, St James Business Park, Paisley PA3 3AT, United Kingdom - Reply to ICMP (ping): No - Latency: 84ms (Last Hop)

SOUL KATANA

Date **Description**



- 16/03/2023 - Portal server is hosted singularly and no array.
 - There are 2 domains of which both are hosted within a server:

api.orokuedge.com
 my.orokuedge.com

- Both domains resolved to the same IP:

45.77.243.253

- The hosting information/credentials are as follows:

Up at the time of testing: Yes
 Hosting Company: Vultr Holdings, LLC
 Location: Singapore
 Address: 20 Ayer Rajah Crescent, 139964, Singapore
 Reply to ICMP (ping): Yes
 Latency: 14ms

- 17/03/2023 It is found that none of the servers hosted by AWS nor Microsoft Azure in order to reduce DDOS attack probability.
 Speaking to personal by the name 'Boy'; he told that nothing can be done whilst the chart was hung for about 7 hours
 previously and best resort was to log a report to the service provider which was T4B.