A good portion of our activity came from two web crawlers, Nimbostratus and NetSystemsResearch.

Nimbostratus-bot

Docs: <https://andresriancho.github.io/nimbostratus/>

Cloud system networks: <http://cloudsystemnetworks.com>

User-agent: “Mozilla/5.0 (compatible; Nimbostratus-Bot/v1.3.2; <http://cloudsystemnetworks.com>)”

This web crawler seems to be just scanning for open ports on the internet. It revisits every couple of days. Note that each revisit seems to be coming from a different IP. Assuming that these are not simply different instances of the crawler, this could be some feature of the crawler itself to avoid blacklisting. I’m not clear on the details.

According to the docs page, it was initially developed for a demo in exploiting and pivoting around Amazon cloud infrastructure instances. Thus it makes sense we are seeing activity as we are running on EC2. I hypothesize that if we were using a different cloud service like Azure, we would not see activity from this specific web crawler. There is no clear link between the assumed operator of the web crawler (<http://cloudsystemnetworks.com>) and the assumed author of the software (<https://andresriancho.github.io/nimbostratus/>).

Additionally in the user agent field, it refers to a website, <http://cloudsystemnetworks.com>. They claim to be a network monitoring company (with an http only website). The only mention of the bot I can find on their website is at this link: <http://cloudsystemnetworks.com/services/>, where they claim to provide a service called “Stratus.” There is some contact information listed on the site, but I did not investigate further.

NetSystemsResearch

User-agent: “NetSystemsResearch studies the availability of various serices across the internet. Our website is netsystemsresearch.com”

Website: <http://www.netsystemsresearch.com/>

This web crawler also seems to be scanning open ports. Revisits consistently. Again, each connection comes from different IPs, with some variance (92.181.161.\* or 92.181.160.\*).

Another internet security organization with an http only website. From their site, this group seems to be purely research oriented which aligns with the use of a web crawler for information gathering. There is little else information and nothing about the web crawler itself on the website. There is contact information but I did not investigate further.

I did find a single source that claimed NetSystemsResearch sells data (<https://hakdefnet.org/2019/01/05/docker-bug-firewall-workaround/>) but there is no citation for the claim.