**Anchor Hospital Security In**cid**ent Report**

**Incident Report #:** IT4070-A.

**Incident Reported Date:** November 25, 2022

**Incident Reported Time:** 12:00 AM EST

**Technician Assigned:** Chris Misch

## Incident Details

**Incident Location:** Remote Desktop Services. Port 3389

**Attack Type:** Denial of service

**Internal Systems Likely Affected:** Remote Desktop Server, Load Balancer, Stateful Firewall.

**Containment Steps Taken:** Steps to contain the incident

1. Authorized devices with known IP addresses connecting to RDS will be rerouted to a secondary port TCP 5985 to ensure continued access
2. Close RDP access via UDP on port 3389
3. Set up a filter via Snort IDS to block repeated connection attempts through port 3389 based on the ingress to egress traffic (Kottler, 2018). DOS attacks can have signatures like time-based or PGA (packet generation algorithms).
4. Block ICMP traffic.
5. Reroute all other traffic through Akamai which will help to filter out traffic into smaller groups of packages.
6. Coordinate with the ISP by informing them of the ongoing attack.
7. Increase the allowed bandwidth – allows more room for the packets to enter which will help to prevent bandwidth overload.

**Countermeasures Deployed:**

1. Allow RDP only through TCP connection. By allowing RDP to connect via TCP you can mitigate the use of it for a future DDoS attack. The UDP port 3389 is frequently used in DDoS reflection/amplification attacks. “The amplified attack traffic consists of non-fragmented UDP packets sourced from UDP/3389 and directed towards the destination IP addresses(es) and UDP port(s) of the attacker’s choice.” Kovacs, 2021. Ebun-Amu (2021) has also said that removing RDP authentication on port 3389 will stop attackers from using this port to enhance a reflected/amplification attack.
2. I will also filter IP sources by creating a whitelist for approved IP connections. By creating a whitelist, I can quickly block all other connections or reroute thoes connections to a third-party packet filter like Akamai. This 3rd party can scrub the packets and filter out legitimate traffic to be rerouted back to Anchor Hospital’s RDS.
3. To ensure vendors and employees can still access RDS I will change the listing port to a private for employees only. This will help to ensure business continuity.
4. Add two factor authentication to all remote access. Then add a filter that prevents continued access if the user is not able to successfully connect after 3 tries. After 3 tries the connecting IP address will not be blocked from sending SYN packets for 30 minutes.

**Recommended Non countermeasure Control to Mitigate Future Attacks:**

1. Update security policies specifically Business continuity plan (BCP) to include a DDoS response plan to include a second ISP to allow for more bandwidth. This will help to absorb the large number of packets being sent. When there is an occurrence where Anchor Hospital is receiving more traffic than it should we can increase the bandwidth while we take proactive steps to reroute the traffic to a 3rd party scraper for further cleaning and analyzing if it is a potential DOS attack.
2. Add a load balancer to the network. This will provide high availability to the network via remote desktop application. We can set the load balancer to filter at layer 4 on TCP/UDP port 3389 and any other custom port we end up using for remote desktop access. The load balancer can redirect traffic to an online packet scrapper like Akamai which will forward cleaned packets back to the network. It can also forward traffic to a static website that can help to handle the increased traffic if the service goes down.

Resources:

Kottler, S. (2018, March 1) *February 28th DDOS Incident Report*. <https://github.blog/2018-03-01-ddos-incident-report/>

Ebun-Amu, Calvin (2021, February 24) *6 New DDoS Attack Types and How They Affect Your Security.* <https://www.makeuseof.com/new-ddos-attacks-how-they-affect-security/>

IANS Faculty (2021, October 14) *DDoS Attack Prevention and Response Tactics.* <https://www.iansresearch.com/resources/all-blogs/post/security-blog/2021/10/14/ddos-attack-prevention-and-response-tactics>

Kovacs, E. (2021, January 22) *Thousands of Unprotected RDP Serers Can Be Abused for DDoS Attacks.* <https://www.securityweek.com/thousands-unprotected-rdp-servers-can-be-abused-ddos-attacks>