INTERNATIONAL INSURANCE FIRMS IN THE MIDDLE EAST FACED AN ISSUE WITH THEIR CORPORATE NETWORK (NETWORK WENT DOWN).

Overview

One of the Major International Insurance firms in the Middle East faced an issue with their corporate network (network went down). The Users were unable to login into the network and even their central authentication methods were also not working.

It was initially suspected to be a targeted attack. Prophaze onboarded the prospect successfully (around 15 minutes) as soon as they reached the team. Traffic logs were gathered from the web servers in real-time and also Windows Server, Router, and firewall configurations were analyzed manually. Finally, based on the investigation, we summarize this instance was not the result of a targeted attack.

On further analysis, Prophaze was able to detect a sophisticated bad bot with command and control software installed. The malicious botnet modified the security policies on the servers stopping legitimate users from logging in. This bad bot was a brand new form of malicious software. The root cause of the vulnerability was identified by the team to be a firewall misconfiguration.

The Results

Our Kubernetes WAF solution has the ability to meet the challenges the company faced:

- Provided an analysis report and recommendation on root cause remediation.
- The Prophaze Team assisted the prospect with the root cause remediation process and restored the network.
- Prophaze WAF helps to distinguish between good and bad bot traffic allows you to block scrapers, scanners, and comment spammers that bring overhead to your server and tries to steal your content.
- Good Visibility and Control over Bot Data
- Updated List of Good Bots and Bad Bots for white and blacklists
- Drill Down for all activity of a particular user (Bot)

Prophaze
The New Phase Of Security

security@prophaze.com or WhatsApp us at +91 7994008420
https://www. prophaze.com