IDS Findings

Produced by: Marvin the Martian SOC

Commissioned by: WIley E. Coyote

Date: 11/05/2022

IDS Findings

IDS logs show that at 10AM on 12/17/2017 we were the target of brute force DNS attacks. Hosts (10.0.0.102, 10.0.0.100, 31993) appear to have been successfully exploited. Multiple DNS servers were exploited and outbound traffic was detected. Host 201.116.53.92 in charge of Microsoft directory services was registered with outbound traffic to malicious IPs.

Understanding our findings

A sustained attack beginning 12/17/2017 at 10AM and ending 12/18/2017 at 10AM, exactly 24hrs was launched on ACME. Brute force attacks to enumerate our domain names on the DNS servers were launched, and Brute force attacks were launched on determined valid DNS, Web, and Mail servers. The attack was successful, and we were breached, the attacker then navigated our network, and managed to produce reverse shells on a few of our servers, exfiltrating data from the network. Multiple unused UDP ports show spyware activity, and we can safely say spyware was installed on multiple unused and unsecured ports, allowing for fast data transmission. IMAP servers were breached, allowing attackers to intercept incoming email to ACME.