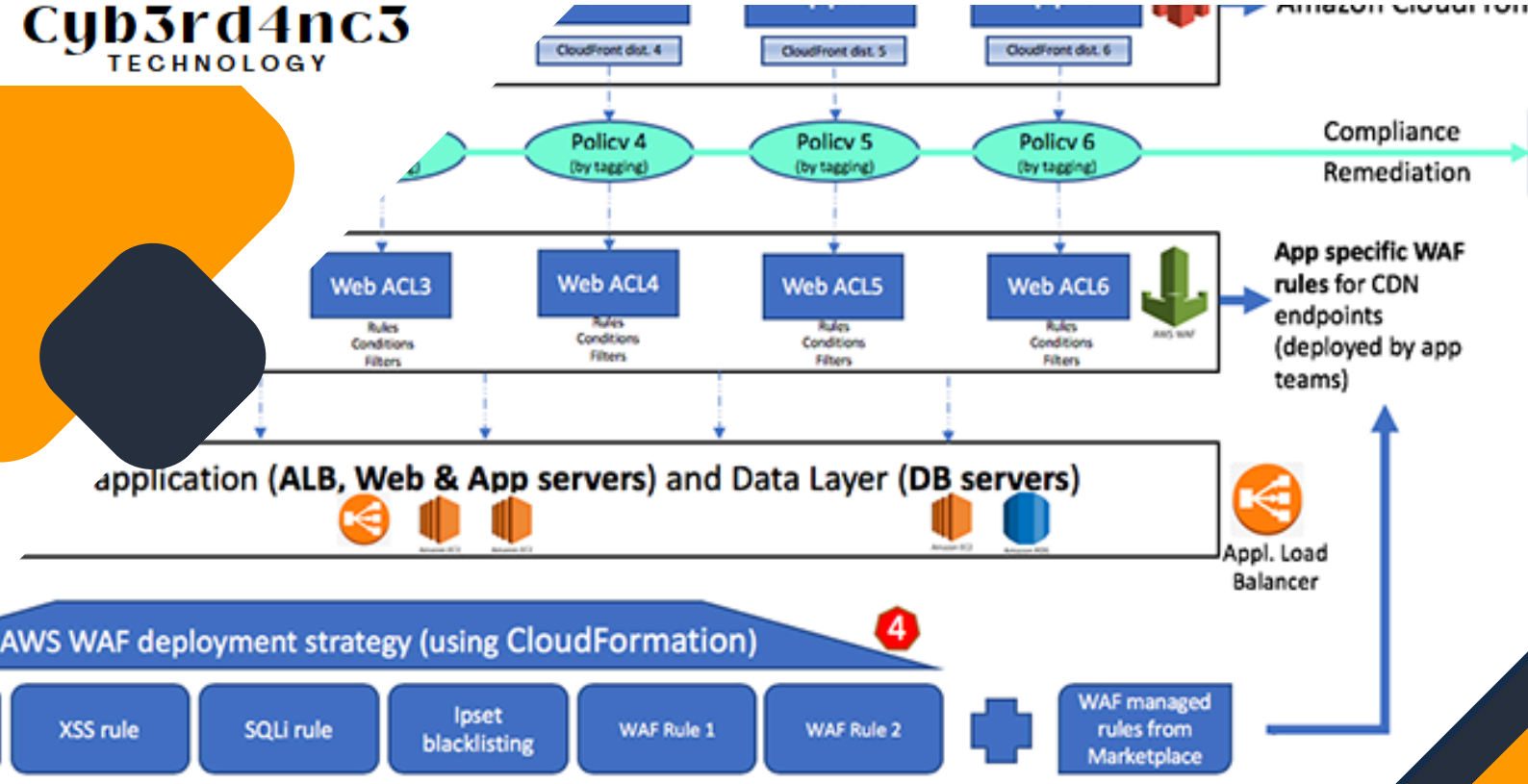
Cyb3rd4nc3
TECHNOLOGY

aws re/start



BLOCKING MALICIOUS DOWNLOADS WITH AWS NETWORK FIREWALL

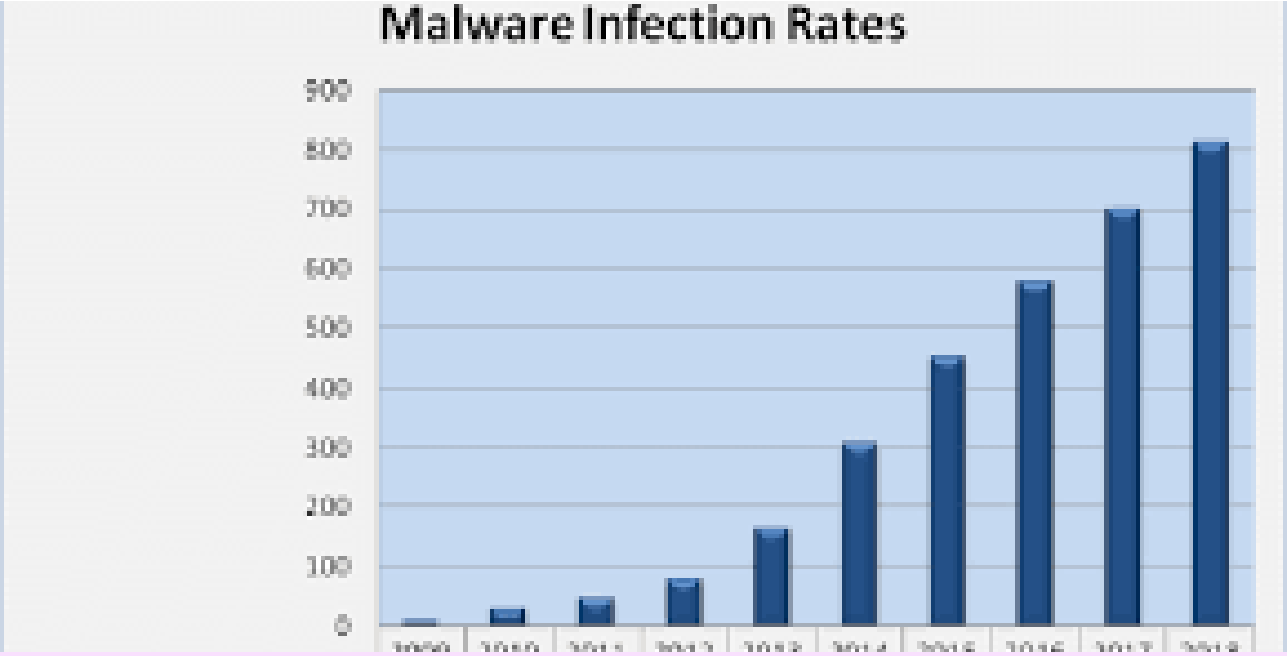
Overview

In today's digital workspace, employees often download software to improve productivity. But what happens when those downloads contain malware? This report explores how organizations can prevent such threats using AWS Network Firewall, ensuring a secure browsing experience while maintaining operational efficiency.

Prepared BY:

Daniel Mwendwa — Cybersecurity Analyst / Cloud security

PROBLEM STATEMENT



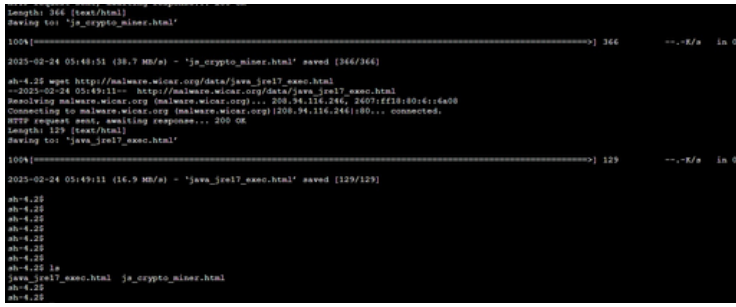
A common cybersecurity concern is employees unknowingly downloading malicious software from unauthorized sites. Attackers often disguise malware as legitimate applications, leading to data breaches, system corruption, and financial losses. To combat this, organizations need a proactive approach to blocking access to these risky sites before any damage occurs.

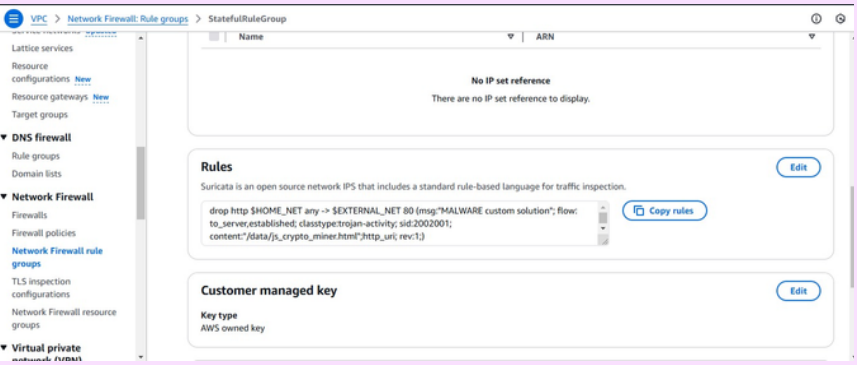
THE APPROACH

To mitigate this risk, I used **Suricata**, an open-source network threat detection engine, within **AWS Network Firewall** to block access to malicious domains. The goal was to test whether employees could access a known malware-hosting website and then enforce a rule preventing such access.

IMPLEMENTATION OVERVIEW

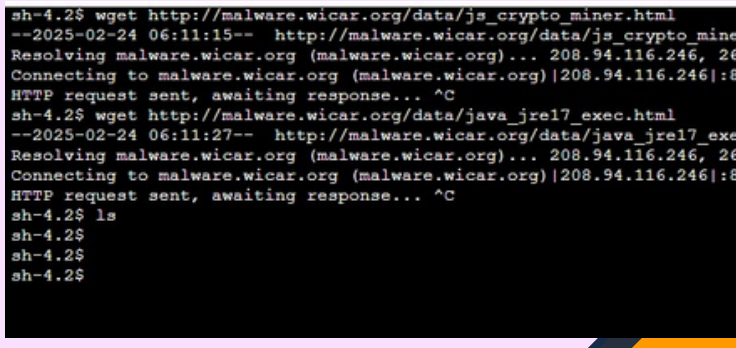
Initial Testing – First, I tried to access a test malicious site. As expected, it was reachable, indicating a security gap.
To understand how this works, I used a controlled environment to download the malware, interact with it and understand what are some of the impacts it could have caused to our system





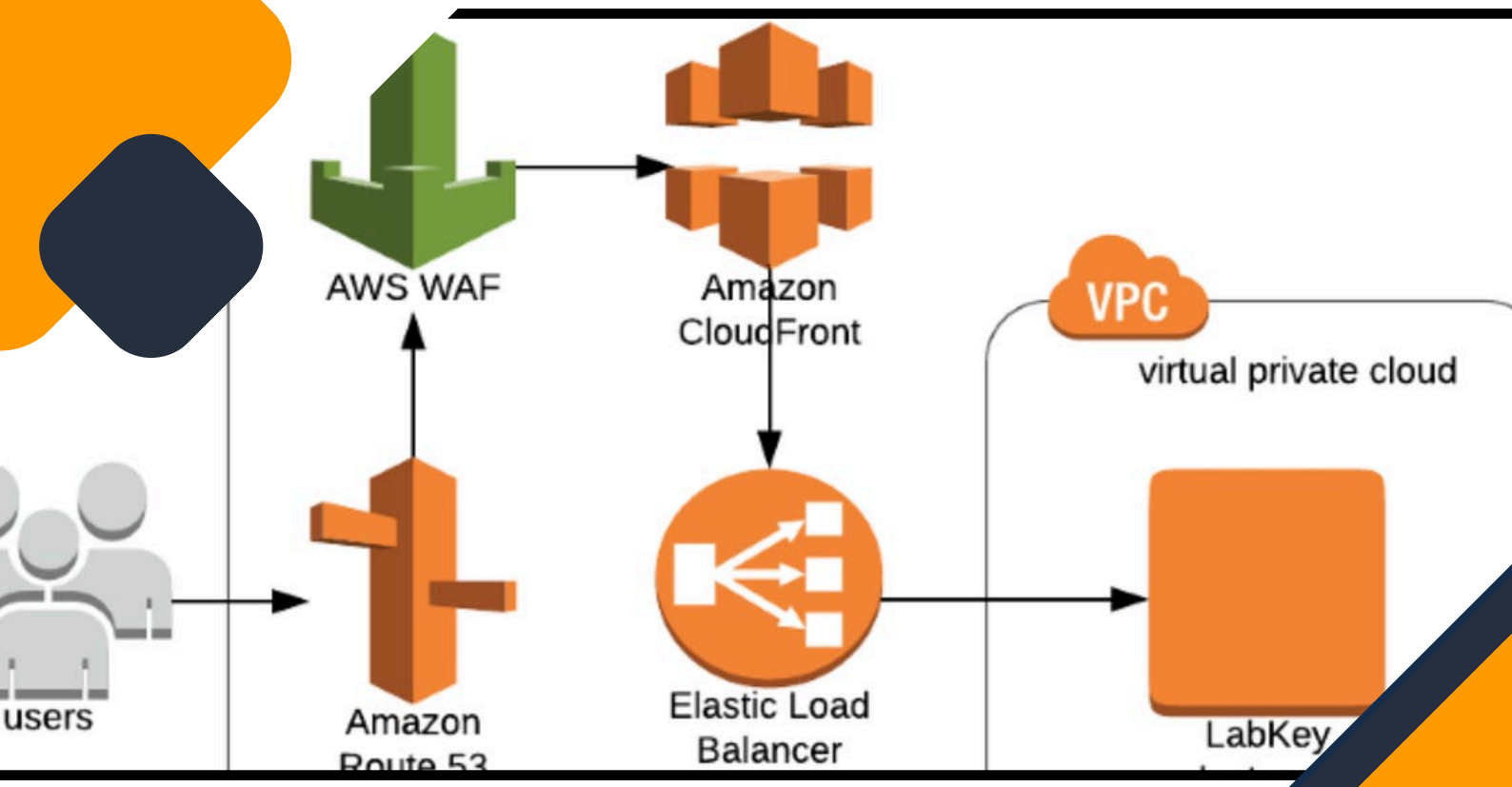
Deploying AWS Network Firewall – I configured Suricata rules to identify and block traffic to the malicious domain.
I used AWS VPC and suricata to add a firewall security group that blocks the sites that our employees download the malware from. This is just to make sure that the employees now cannot access the site and thus our system is secured.

Verification – Finally, I tested access again. This time, the request was denied, confirming that the firewall was successfully filtering out harmful traffic. Now our employees cannot access the site anymore, We do not have to worry about.



Cyb3rd4nc3
TECHNOLOGY

aws re/start



CONCLUSION

By using AWS Network Firewall with Suricata rules, we successfully blocked access to a malicious website, reinforcing cybersecurity measures. This simple yet effective solution showcases the importance of proactive network security strategies. The next step? Expanding these rules to cover a broader range of threats, keeping our network one step ahead of attackers!