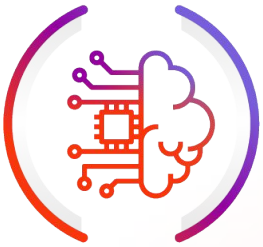
CASE STUDY

Protecting Critical Infrastructure

This case study examines the challenges and solutions involved in securing critical infrastructure from cyber threats. It highlights the importance of a multi-layered security approach and proactive threat intelligence that is provided by CloudJacket.



BACKGROUND

Our SOC team recently alerted on an Attempted Hosts File Exfil in Linux which is an unauthorized attempt to access and extract (exfiltrate) the contents of the /etc/hosts file from a system. While the /etc/hosts file itself may not seem sensitive at first glance, the implications of such an exploit can be serious, especially when viewed in the broader context of system and network security.

The /etc/hosts file often contains custom mappings to internal servers, services, or development environments.

IF EXFILTRATED

An attacker now has visibility into parts of the internal network not exposed to the public. It helps them plan targeted attacks on internal assets.

WITH KNOWLEDGE OF INTERNAL HOSTNAMES AND IPS

The attacker can attempt to pivot within the network using lateral movement techniques (e.g., SSH, RCE on internal web apps). These are low-hanging fruit for attackers.

THE SOLUTION

The Cloudjacket system notified and alerted on this malicious signature. A Palo Alto firewall deployed at the edge of the customer network did not catch this malicious request. The Palo Alto threat vault had no evidence or any signature related to this exploit attempt

Our SOC team went ahead and blocked the external request and blocked the malicious IP address attached to it.