adlumin™

ADLUMIN'S TOTAL RANSOMWARE DEFENSE STOPS FOG IN ITS TRACKS

A financial firm was targeted by the Fog ransomware variant using compromised VPN credentials.

Attackers aimed to encrypt sensitive data on both Windows and Linux endpoints.

Indicators pointed to Russian-originating IP addresses, but masking techniques were suspected.

ATTACK STARTS

2 MINS

RANSOMWARE PROCESS KILLED

Two Minutes to Kill Process

Adlumin's Total Ransomware Defense quickly detected malicious network activity and took action within 2 minutes to kill the ransomware process, preventing significant damage.

6 MINS

INCIDENT ISOLATED

Stopped the Spread

Within 6 minutes after detection, the customer's affected machines were isolated.

14 MINS

CUSTOMER CONTACTED

Rapid Response

By 14 minutes of detection, the customer was notified, ensuring transparency and coordination for the next steps.

16 MINS

ATTACKERS REMOVED

Complete Removal

In just 16 minutes of detection, the attackers were fully removed, and the network was secured from further infiltration or damage.

8 HOURS FULL RECOVERY

HOW ADLUMIN SECURES SENSITIVE DATA WITH TOTAL RANSOMWARE DEFENSE

Deploys Markers and Files

The system continuously monitors strategically placed markers and files acting as honeypots to attract malicious processes.

Alert and Monitors

Detects processes interacting with preset markers and files, triggering an alert if any attempt is made to move them.

Process Chain Termination

Upon detecting malicious activities, the process chains are terminated, disrupting attacks before ransomware deploys and prevents data exfiltration and extortion.

Contain Threat

The endpoint is automatically isolated to stop the spread of ransomware and decrease the business impact.

Learn more about how Adlumin's Total Ransomware Defense can protect your business in record time.

adlumin.com/platform/total-ransomware-defense/