A CASE STUDY

Exfiltrating Remote User Accounts to Inject Ransomware

WHO

Global Manufacturer

7000 Accounts

WHAT

Ransomware

$10 million

WHY

Improperly Trained Personnel

Weak Authentication Controls

Unfiltered Internet Access

Unsophisticated Endpoint Protection

Lack of Data Inventory and Assets Classification

HOW

Phishing Campaign

Compromised VPN Connection

Mimikatz - Password Extractor

MedusaLocker Ransomware

OVERVIEW

HALOCK contained and eradicated a ransomware attack on a Manufacturing company's internal assets and set a wholistic plan to mitigate future risk through enhanced MFA, policies, and training.

ATTACK SUMMARY:

Adversaries performed data theft techniques to exfiltrate vulnerable information and hold ransom internal systems. Incident led to the company negotiating a Bitcoin payment to recover data increasing the financial impact to the organization.

HOW THE ATTACK WAS EXECUTED:

Through a phishing campaign adversaries were able to obtain user credentials and VPN settings to gain internal network access.

Mimikatz was then installed on vulnerable systems to recover Windows Service Accounts. Using the escalated privileges the attackers exfiltrated information through data transfer services and propagated Medusalocker ransomware on internal assets.

Attackers held ransom internal assets and exfiltrated valuable data for financial gain.

VULNERABILITY

HALOCK determined O365 and the corporate VPN solution lacked strong authentication controls. It was discovered that the VPN authentication utilized the same credential as Active Directory. Endpoint detection capabilities of the anti-virus solution lacked anti-exploit monitoring to restrict the execution of Mimikatz and the ransomware Medusalocker.

RECOVERY

The HALOCK team identified the attack vector malicious binary code and shut down all external access which included O365 replication, and all user passwords were reset. Recovered systems that had capable backups. The organization then paid ransom for critical data that was unrecoverable through an insurance-appointed ransom negotiator.

MITIGATING THE VULNERABILITY: Safeguard & Monitor

A comprehensive security plan was developed to continually protect and monitor the manufacturer's network. Safeguards included:

- Implementation of MFA for VPN authentication and O365
- Upgrading endpoint protection
- Launched a robust email filtering system
- Conducting security awareness training on phishing campaigns
- IT training on new protective measures
- Develop critical system back-up plan to ensure they are recoverable from malware attacks
- Scheduling regular vulnerability scans, and threat monitoring to identify risky login attempts

HALOCK SOLUTIONS & SERVICES

Our manufacturing client was able to secure their data, secure vulnerabilities, and implement controls to mitigate their risks through customized solutions. Solutions leveraged:

- Security Awareness Training
- Threat Monitoring Services
- Sophos, Carbon Black, Proofpoint, Duo Security
- Security Architecture Review
- Incident Response (IR) Services including IR planning and training