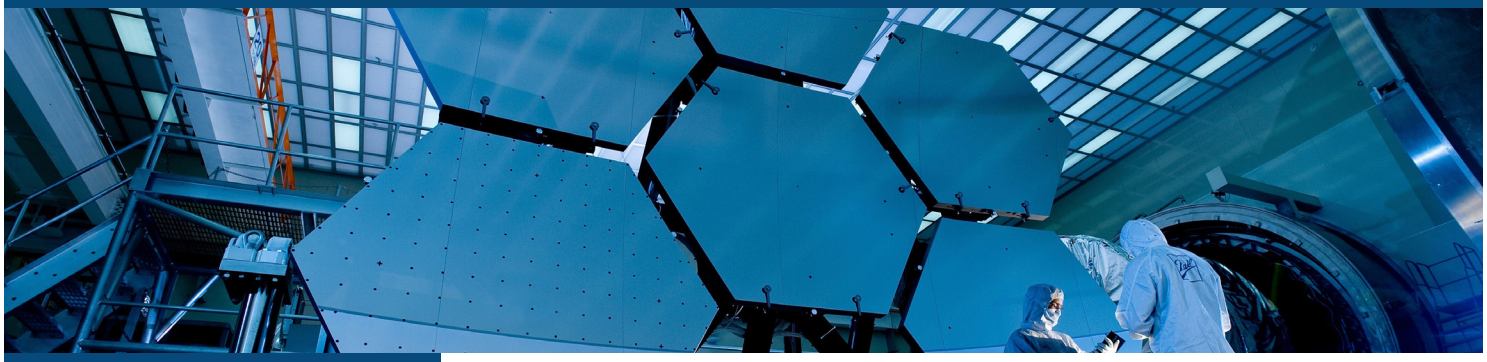
A CASE STUDY

When Ransomware Attacks, and You Don't Have Documented Data Inventory.

What am I missing?



WHO

Global Manufacturer

WHAT

Data reconnaissance and exfiltration techniques

Implementing audit plans and controls to manage data

WHY

Lack of Data Inventory and Assets Classification

HOW

Data was taken with:

Mega Sync or Sync.com
Box.com
Dropbox.com

OVERVIEW

HALOCK partnered with a Manufacturing company to recover data exfiltrated from a ransomware attack and implemented controls to help inventory, backup, and protect assets from future security incidents.

SUMMARY

Multiple attacked organizations lacked formal controls to identify what systems attackers accessed and the type of data files were encrypted and stolen. Moreover, back-up volumes were also encrypted, limiting the ability to determine what files would have been encrypted by the attacker and whether they posed a risk to themselves or others if lost or stolen.

APPROACH

With the combination of no system backups, and an incomplete data inventory and asset classification, HALOCK worked to save any recoverable data. HALOCK then proposed reasonable and appropriate safeguards to secure their data against future attacks.

SAFEGUARDS

Perform Data Inventory - Conduct ongoing data retention and classification audits to verify inventories are comprehensive, current, and can be reliably used to locate all sensitive data in the environment.

Restrict Internet Traffic - Implement NextGen firewalls to restrict and monitor outbound traffic. Each server or segment is blocked to restrict traffic to the Internet if there is no business justification.

Formalize Backup Plan - Ensure all critical systems are recoverable from malware attacks.

Deploy Data Monitoring Tools - Preform constant vulnerability scans both internal and external on a regularly scheduled basis.

- Implement Data Loss Protection (DLP) solution
- Tripwire File Integrity Monitoring (FIM)
- Security Information and Event Management (SIEM)
- AD Audit Plus - Windows Active Directory change reporting software
- NextGen Firewalls

Backup Designation - Validate that all backups have at least one backup destination that is not continuously addressable through operating system calls.

REASONABLE SECURITY

The impact of the incident would have been reduced implementing reasonable controls through these solutions.

- Privacy – Data Inventory
- Risk Assessment
- Compromise Assessment
- Incident Response (IR) Services including IR Planning and training

HALOCK Threat Monitoring Partner Solutions

- Sophos Endpoint Protection
- Carbon Black Cloud-Native Endpoint Protection
- Sensitive Data Scanning