CYBERSAFE CASE STUDY **MANUFACTURING INDUSTRY**

Ransomware Hits a Multimillion-Dollar Manufacturing Company

A major manufacturing company with multiple offices across the country was hit by ransomware. The company reached out to Cybersafe, which helped it resume business operations.

THE BREACH

On a late Wednesday night, a multimillion-dollar manufacturing company came to a complete halt due to a criminal cyber-attack. Threat actors had infiltrated workstations and servers across their 15 facilities and global offices leaving the company's infrastructure frozen and encrypted by ransomware. Their day-to-day operations and were paralyzed as the ransomware locked critical inventory and order taking systems . While the company's network was frozen, employees sat idle in the warehouse with no way to do their work.

On a late Wednesday night, a **multimillion-dollar** manufacturing company came to a complete halt due to a criminal cyber-attack.

OUR SOLUTION

Cybersafe's Incident Response team was brought in to help the company recover from the attack. The Security Operations team moved quickly to create visibility by deploying endpoint detection and response agents as well as a SIEM to remove the threat actors from the environment.

Upon inspection of the encrypted endpoints, It was obvious that the company was dealing with a RYUK ransomware infection deployed via malware known as TrickBot. Ransomware is often the last stage in an attack, coming after other malware and tools have been used to infiltrate and establish persistence in an environment. Cybersafe was able to identify and clean hosts across their network so that restoration could proceed without interruption. Ultimately, clean-up and restoration required 14 days before operations could resume.

FACTS OF THE CASE

TYPE OF ATTACK
Ransomware

TARGET
Multimillion-dollar manufacturing company

ASSESMENTS & RESULTS

Upon completion of the incident response investigation, the Cybersafe IR team was able to identify numerous opportunities to have detected the threat actors before the encryption occurred. Cybersafe's forensic investigation revealed that access was achieved via a targeted phishing email campaign using a malicious document hosted at docs.google.com. Since legitimate files are hosted at docs.google.com such access was permitted and trusted by their spam filters. Once opened, the document disabled local Anti-Virus protection mechanisms and beaconed home to a Russian based command and control (C&C) server. Through the C&C, the attackers used local vulnerabilities to deploy malware, escalate privileges and move laterally within the environment using the Windows administrative utility PowerShell. We also determined that the attackers exfiltrated approximately 500 Gigabytes of sensitive data. Cybersafe determined that the attackers spent approximately 72 hours in their environment before moving to encrypt systems.

The company suffered millions of dollars in lost revenue by being unable to manufacture for two weeks and the full restoration of workstations and servers will take months and cost millions more in lost productivity and labor costs.

The manufacturing company has now engaged with Cybersafe Solutions SOC-as-a-Service offering. With 24/7/365 Security Operations Center which provides real time detection, response, and containment capabilities, the company is now confident they will have best in class detection capabilities to quickly identify and eradicate future cyber threats.

CYBERSAFE SOLUTIONS®