A CONVERGE COMPANY

CASE STUDY

Industrial Manufacturer Mitigates Ransomware Without Paying Attackers

Challenge

A supplier of industrial robotics was hit by Mount Locker ransomware. As it began to propagate, their on-premises Microsoft Exchange server went down. Staff attempted to contain the incident by disabling network and VPN access, resetting domain-level passwords, and powering affected computers off. A failed password reset left them locked out of virtual servers, effectively cutting them off from their environment. Making matters worse, offline backups were not in use, and the backup server was compromised.

The organization had no intention of paying the attackers. The situation was chaotic as the understaffed security team sought ways to regain access and stop the malware from spreading further.

Solution

The client reached out to CBI, A Converge Company and our Incident Response and Advanced Testing Services (ATS) teams were engaged. A CBI ATS team member joined the client on-site and successfully broke into their locked VMware ESXi environment after the password was forgotten amidst the ransomware attack. They effectively reset it, enabling them to avoid server reinstallation and regain desperately needed access.

With that accomplished, a virtual Microsoft Exchange server was spun up. The CrowdStrike Falcon endpoint protection platform—which uses AI-powered machine learning and behavioral indicators of attack (IOAs) to identify and block ransomware—was then deployed to salvage remaining systems and assist with containment and eradication.

Results

CBI worked quickly to overcome the password issue that threatened the organization's ability to address and recover from the incident. In two days, the attack was remediated, state-of-the-art endpoint security was deployed, and the Mount Locker ransomware gang left empty-handed.

Critical business functions continued safely, and the client was provided with detailed recommendations designed to advance their overall security posture. These included initiatives focused on security awareness training, incident response testing, penetration testing, and establishing an effective backup solution. The company was left with an actionable cybersecurity roadmap for defending against threats now and in the future.

Contact **CBI** to enhance your cybersecurity program.

800-747-8585 • help@cbisecure.com