

CASE STUDY:**RANSOMWARE ATTACK**

Ransomware Attack on Saturday Night

CLIENT:

Large-Scale Materials Handling Company

INDUSTRY:

Commercial and Industrial

CLIENT SCOPE:

500+ employees with multiple locations, providing products and services

ISSUE:

Active ransomware attack across all server platforms

TALON SERVICES DELIVERED:

Emergency virus remediation, IT Consulting, Complete Network Protection, Data Protection Solutions

PROCESS:

- Emergency call placed to Talon on Saturday night
- Remote and onsite IT engineers responded
- Disabled file shares and access across servers and the network to stop virus spread
- Identified root cause and entry of virus
- Restored data, reviewing backup files for signs of the virus
- Brought business-critical servers back online, reestablishing file shares, connections, and network environment
- Consulted on backup procedures to enhance redundancy and restoration policies
- Implemented a multiple server and storage area network

RESOLUTION:

The company involved is now a Talon Managed IT Services client.

Cryptoviruses, often called ransomware, differ from normal malware. While malware is certainly malicious, cryptoviruses have bad actors behind them, actively working to seize data and then demanding a ransom for its return. It's the 21st-century version of a holdup.

Late one Saturday night, Mike Linville (Talon President) and his wife were enjoying a horse and buggy ride in Memphis, TN when his cell phone rang. The CFO of a large materials handling company was on the call, saying his company's network was under attack with ransomware, crippling their network. It appeared to be getting worse as time passed.

Mike contacted Steven Norris (Vice President, Technical Services) who got Talon technical support on a call with the attacked firm's IT management, while Talon engineers were already en route. The Talon team promptly pinpointed the source of the attack, halted the spread of the virus, and restored the network and server environment to its original, healthy state.

After the immediate crisis was handled, Talon consulted on enhanced backup and security protocols to help prevent future ransomware attacks, including how to quicken the restoration of systems if needed. The company is now a Talon Managed IT Services client, regularly requesting additional project work as needed, including the configuration and rollout of a multi-server environment and storage area network.

"Even though we were not a regular client of Talon's, they still answered our call on a Saturday night at 10:30pm."