InfoTank

CYBERSECURITY CASE STUDY

Sophisticated Ransomware Attack Thwarted

March 2026

OVERVIEW

Earlier this week, the FBI contacted us about suspicious activity involving one of our Marietta clients. What they didn't know was that InfoTank had already identified and contained the threat three days earlier.

Our monitoring systems detected unusual lateral movement inside the network early Saturday morning. This type of activity is a strong indicator that an attacker has already gained access to the environment and is attempting to move from machine to machine in search of credentials, sensitive data, or opportunities to deploy ransomware.

This was the beginning stages of a ransomware attack, which would have spread and likely encrypted all devices.

INCIDENT DETAILS

Location

Marietta, GA

Industry

B2B Service Industry

Potential Loss

Complete Work Stoppage
100% Data Loss

Status

Contained – No Client Impact

MALICIOUS ACTIVITY IDENTIFIED

Security monitoring identified several indicators that an unauthorized actor had gained access to the network and was attempting to expand their presence. The following activity was detected:

- Unauthorized PowerShell remote session
- Attempts to modify Windows registry startup keys
- Remote Desktop firewall rule changes
- Credential harvesting activity
- Suspicious outbound network communication
- Attempts to interfere with endpoint protection

This type of activity is commonly associated with attackers attempting to establish persistence inside a network before launching a larger attack.

The FBI typically only contacts technology vendors when an incident involves a sophisticated threat actor they are actively tracking. This suggests the activity detected was likely part of a broader cybercrime campaign rather than a random or automated attack.



Immediate Response & Business Impact Prevented

- ☑ No Ransomware
- ☑ No Downtime
- ☑ No Data Loss
- ☑ No Monday Morning Crisis

- Machine isolated immediately
- Unauthorized software removed
- RDP access disabled
- Credentials reset
- SentinelOne tamper protection verified

POTENTIAL IMPACT IF THE INTRUSION HAD GONE UNDETECTED

Ransomware Deployment	Data Theft	Operational Shutdown
Attackers often move throughout networks silently before launching ransomware. If the intrusion had continued, the attacker could have encrypted company systems and demanded payment to restore access.	Once inside a network, attackers often search for sensitive data including financial records, credentials, and internal documents. If stolen, this information could be sold, leaked, or used in future attacks.	Many organizations experience days or even weeks of downtime following a successful cyberattack. Systems become unavailable, employees cannot work, and recovery efforts can take significant time.
This could have resulted in significant financial loss for the business.	**Client and company data may have been compromised.**	**Entire business operations could have been halted.**

For more information, visit www.infotank.com or call: 770-450-8783, Email: ali@infotank.com

InfoTank