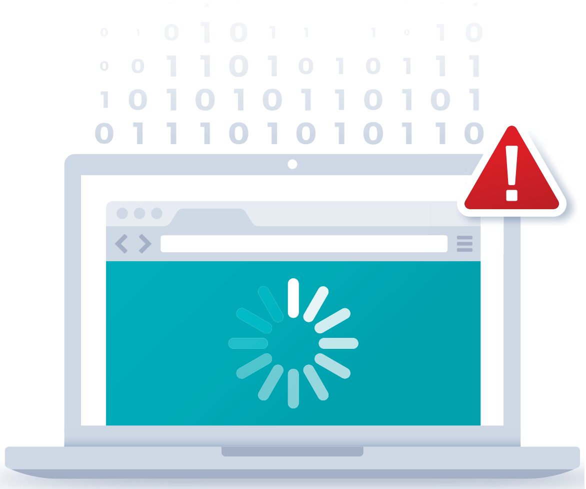
Redpoint
Cybersecurity LLC

REDPOINT INCIDENT RESPONSE USE CASE



THE PROBLEM

A large state & local government organization was faced with a large-scale ransomware attack. Sophisticated, worm-enabled malware infected 2,000+ computers in under two hours and deployed ransomware that encrypted data on systems across the network. The organization, unprepared for an attack of this magnitude, needed:

- **Containment and remediation of its critical services and capabilities with "hostile hosts".**
- **Digital forensics collection & analysis to construct a timeline of events and identify threats, patient zero, compromised accounts, movement, delivery method, and other criteria.**
- **Urgent disaster recovery planning and execution.**

TOOLS & TECHNIQUES

- **Emergency Response:** The event started at 7am and our team was engaged via text and phone calls within the first 30 minutes. We deployed an initial on-site team within 2 hours for immediate support.

- **Advanced Malware Analysis and Forensics:** Our team conducted malware reverse engineering and timeline analysis to confirm credential harvesting and primary propagation method.

- **Containment:** We coordinated with the organization's network engineering provider to contain active "hostile hosts" through routing updates, data center isolation, and targeted shutdowns of critical operations capabilities.

- **Discovery:** We analyzed the server environment to identify recoverable systems or configuration to facilitate the rebuild of critical infrastructure. We performed data integrity analysis on unencrypted data and exfiltrated data to shared storage solution for recovery after spinning up new server infrastructure.

- **Remediation:** Our team consulted with client leadership, technical staff, and 3rd-party providers to plan and execute migration to cloud-based server infrastructure with proper backup policies established and in use; we planned, organized, and executed a re-imaging procedure for client workstations statewide at all locations using the newly established infrastructure.

OUTCOMES

☑ **Rapid response** including initial engagement within the first hour and on-site personnel within two hours. We activated 7+ support staff within the first 24 hours and 15+ within
72 hours.

☑ **Established** critical “mass on target” within the first 12 hours.

☑ Systematically **identified and contained** “hostile hosts” while balancing business priorities.

☑ **Recovered** ~14TB of data following integrity analysis and exfiltration.

☑ **Remediation** of the client’s statewide workstation distribution.

CONTACT US TODAY

TAB BRADSHAW

tab@redpointcyber.com

Principal

Redpoint Cybersecurity

RUSSELL SAFIRSTEIN

russell@redpointcyber.com

President

Redpoint Cybersecurity

This contains information which is general in nature and based on sources which are believed to be authoritative. Specific applications would require consideration of all facts and circumstances by qualified professionals familiar with a taxpayer and therefore we are not liable for the application of any information contained herein. No part of this correspondence may be reproduced or utilized in any form or by any means without written permission from Redpoint Cybersecurity.