


Ransomware Attack & Response Timeline

In this graphic we explore the series of events that were discovered during a ransomware Incident Response investigation that Ingalls performed in 2018, and the steps taken to resolve the attack.



User Receives Phishing Attack
Opens malicious Word Document with Macro, leading to infection
Day 1

PHASE 01 Reconnaissance

Day 2-20 
Attacker Performs Recon
Identifies computers that contain important data as well as where the backups are located

PHASE 02 Attack & Encrypt

Day 21 
Command Line Execution
Deletes all shadow copies of data

Day 21 
Data is Encrypted
Malware infection launches encryption attack against all servers & network shares

PHASE 03 System Outage & Ransom Demand

Day 22 
Victim Discovers Ransomware Attack
Employees start day & discover their data is missing
IT staff discover ransom note on servers

Day 25 
Ingalls is Contacted
Incident response team engages and deploys tools within hours

Day 25 
Containment & Recovery Begins
Forensic analysis identifies recoverable shadow copy data


Day 25 
Endpoint Protection Finds Malware
All malware found is immediately quarantined

Day 25 
Ransom Negotiations Begin
Attacker demands 50BTC, drops to 40BTC after initial communication with victim

PHASE 04 Recovery

Day 27 
Recovery Capability Confirmed
systems are restored as fast as shadow copies can be carved

Day 29 
Production Data Restored
majority of victim's workforce returns to normal schedule

Day 30 
Financial Data Restored
24-hour gap in restored data requires reentry, completed in 4-hours

Day 30 
Ransom Negotiations Drop
Price to 15BTC, ultimately end with attacker refusing to counter-offer of 1BTC after 95% of data is recovered



Containment Complete
Total of 243 files quarantined
Day 31