What Happened

- 11 pm: IT received notice of server issue and began investigating the problem.
- **Dharma** - type of ransomware
- The hacker demanded ransom in exchange for the decryption key

What Happened

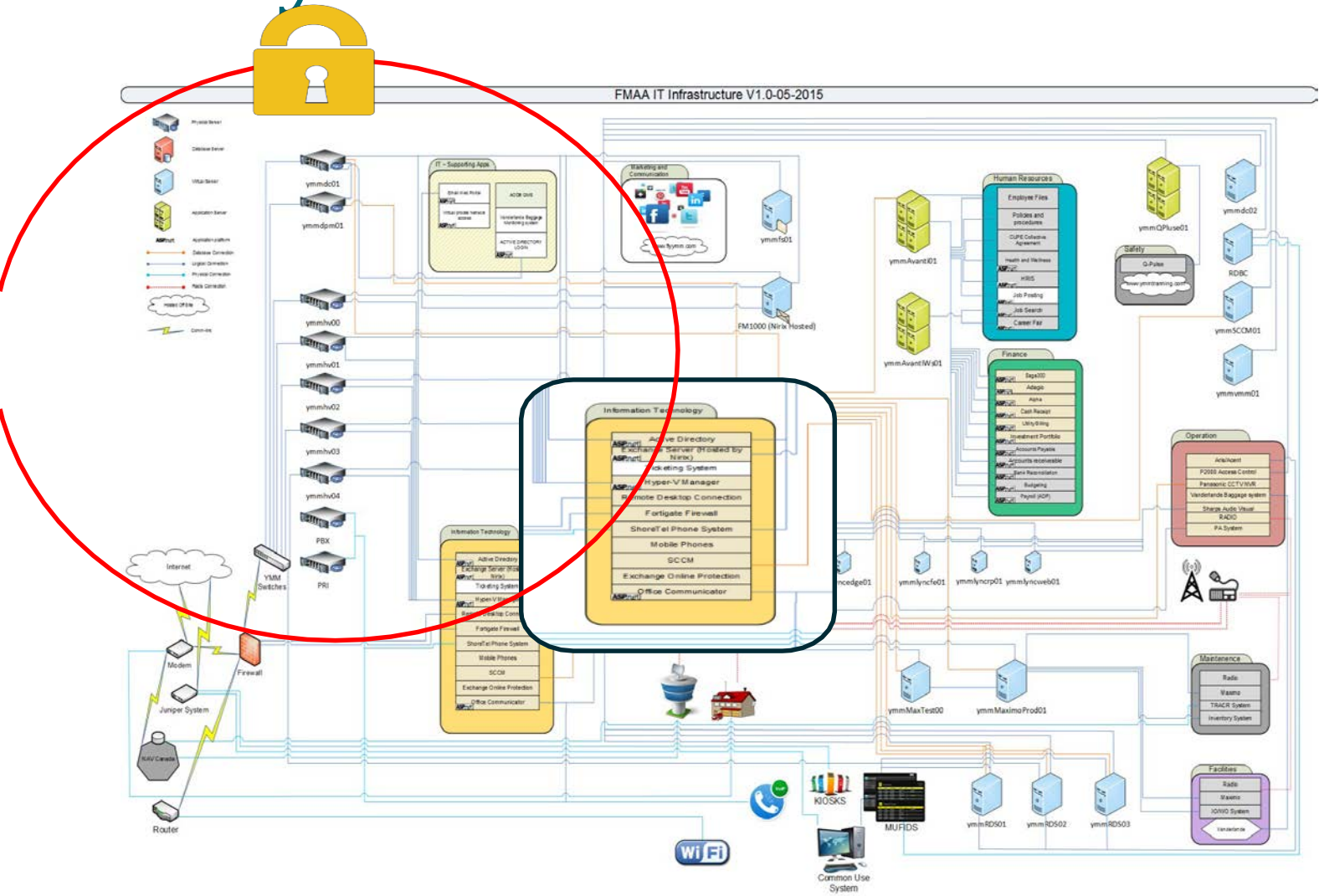
Affected

- Administration files were encrypted
  - All windows system files
  - 90% of the server
  - 100% of workstations
  - Finance
  - Accounting
  - Payroll
  - Marketing
  - Human Resources

Not Affected

- Airlines
- Communication medias, including emails, phones, radios
- FIDS
- CCTV
- Access Control
- Parking booth
- baggage system
- CATSA
- RAIC

Entry Point



- Enter system thru a vulnerability with VPN access
- Once the hacker got into the system through the server infrastructure, they were able to access all files and folders with administrative credentials
- They encrypted all the data, leaving organization unable to access files & services

Impact

- Administration Employees shut down for a total of 9 business days (April 4th - April 17th)
- System rebuild and reprogramming 6 - 8 weeks to full restore
- No DATA lost or compromised
- Total Damages - $375,000

Aftermath Fortification

- Completed network vulnerability scan by cyber security expert
- Strengthened our all network security policies
- Upgraded anti virus with both Signature based and Behavior based
- Implemented CryptoGuard system
- Updated 2 factor authentication for VPN
- Implemented Intrusion detection system
- Updated Intrusion Prevention System

“Put Cyber-security on the agenda before it becomes the agenda”