



BEATING RANSOMWARE

HOW TO PROTECT
YOUR PRACTICES
FROM RANSOMWARE

SUMMARY

- > What Is Ransomware?
- > Top Attack Vectors
- > Potential Practices Implications
- > Current & Emerging Ransomware Trends
- > Top Misconceptions Related to Ransomware
- > Best Practices for Prevention and Detection
- > Best Practices for Mitigation and Response



WHAT IS RANSOMWARE?



Ransomware
encrypts
data

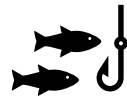


Attackers **demand**
payment for the
decryption code



No guarantee
of file
recovery

TOP ATTACK VECTORS



Email phishing



Unsecured RDP ports



Software/patching vulnerabilities



Malicious websites



Pop-ups/ads

POTENTIAL PRACTICES IMPLICATIONS



Downtime and disruption



Lost files, wages and equipment



High recovery costs



Reputation damage and loss of customers



Regulatory fines and ID theft costs



CURRENT & EMERGING RANSOMWARE TRENDS

- ⚠ Supply chain attacks
- ⚠ Double extortion techniques
- ⚠ Ransomware-as-a-Service (RaaS)
- ⚠ SMBs increasingly targeted

TOP MISCONCEPTIONS RELATED TO RANSOMWARE

*My backups will get me
back up and running.*

*My antivirus software
provides complete
protection.*

*If my practices gets hit,
I'll pay the ransom and
move on.*

*My practices isn't a
target for ransomware
attacks.*



BEST PRACTICES FOR PREVENTION AND DETECTION

- Install latest patches
- Don't click on links or open attachments
- Back up data regularly
- Security awareness training



BEST PRACTICES FOR PREVENTION AND DETECTION

- Endpoint detection and response
- Good password hygiene
- Routine vulnerability scanning
- Network monitoring and segmentation



BEST PRACTICES FOR

MITIGATION AND RESPONSE

- Don't power down or shut off any affected systems
- Isolate the compromised portion of your network
- Secure backups
- Don't trust the entire network system



BEST PRACTICES FOR

MITIGATION AND RESPONSE

- Collect and secure partial portions of ransomed data
- Collect all available log information
- Change online account and network passwords after removing the system from the network
- Use the oldest backup to restore the system

LET'S KNOCKOUT RANSOMWARE



CONTACT US TODAY.