Infrascale™

STEPS TO MITIGATE RANSOMWARE DAMAGE

Code Red:
You've Been Compromised

Security experts predict that ransomware will be a $1 billion industry by the end of 2016. In most cases, the cost of the ransom is trivial compared to the cost of system downtime, missed sales, and lost credibility. And therein lies the incentive for victims of ransomware to pay off their anonymous blackmailers, so they can restore their systems and get their data back.

Complicating things for business is the rise of Bitcoin and other crypto currencies, which have made it possible, safe, and easy for cyber thieves to demand and receive payments and transfer money anonymously.

WHAT SHOULD YOU DO IF YOU GET CAUGHT IN A RANSOMWARE ATTACK?

How can you begin to mitigate the damage right now—as soon as the first ransomware symptom rears its ugly head? How do you avoid paying the ransom? What do you do after the attack to restore your data? Here are the ransomware mitigation steps the security experts recommend you take:

Minimizing the Damage

Steps to Take **During** a Ransomware Attack

01 Identify, isolate, and remove the infected computer(s)

Disconnect from the network immediately, so ransomware cannot spread to shared drives and connected systems.

02 Set the BIOS clock back

Resetting the BIOS clock back to a time before the ransom expiration window is up might help delay the expiration deadline. But the programmers are getting smarter, so this tactic may only work with certain strains of ransomware.

03 Determine when the infection started

Often you've been infected for weeks before the ransomware message appears. Before you can restore your clean files from backup, you need to know how far to go back to ensure a clean restore.

04 Inform employees

Ensure that all employees are aware that a ransomware attack is in process and direct them to the processes and procedures needed to protect their data and provide a timeframe for restoration of affected systems.

Restoring the Data

Steps to Take **After** a Ransomware Attack

01 Use System Restore & Decryption Tools

Enable System Restore on your Windows machine, as you might be able to take your system back to a known clean state. Also, see if your anti-virus solution offers free decryption tools that can help decrypt files.

02 Identify a safe point in time

Determine the point in time when ransomware infected your data. Restore the most recent clean files from a backup just prior to the infection date.

03 Restore infected systems

If a production database or mission-critical application has been infected, leverage a DRaaS solution to spin up an image or virtual machine in minutes -- ensuring your users stay productive.

Final note: A comprehensive backup and disaster recovery solution is your number one defense against ransomware. Be sure to practice restore processes and know that your actual data can easily be retrieved.

Learn More:

Read the FBI's outlook and recommendations on ransomware prevention — featuring detailed reports tailored to the separate interests of CEOs and CISOs.