Armstrong Teasdale

February 19, 2016 • Advisory • www.atllp.com

RANSOMWARE: HOW IT WORKS AND WHAT YOU CAN DO

"Ransomware" is making big news, with reports that a California hospital paid $17,000 to regain access to its network after malware locked access to files. This is a case, however, of the news catching up to the facts. Ransomware has been one of the fastest growing forms of cyberattack over the last year. According to media reports, as many as 100,000 computers *per day* are being infected with ransomware.

These increasing ransomware incidents serve as the latest warning that companies need to take steps to protect against costly and damaging cyberattacks.

How Ransomware works

Without getting too technical, ransomware works by infecting a computer, then using modern cryptography methods to encrypt files. *Once encrypted, the files cannot be decrypted without the "key" that the hackers provide when you pay them ransom*. Since we are talking about encryption schemes that would take supercomputers years to break, there is (with one increasingly limited exception) no way to regain access to the encrypted files without paying for the key.

We mentioned an increasingly limited exception. A couple of years ago, when one ransomware ring was taken down by law enforcement, some of the private keys that ring used to decrypt were recovered. Thus, if the ransomware variant that infected your machine happens to be the increasingly outdated version that matches these keys, then you have a shot at getting your files back without paying the ransom. But, the hackers are very aware of this loophole, and more modern ransomware variants do not respond to the captured keys.

How Ransomware is spread

The delivery methods keep evolving, but almost all delivery mechanisms have something in common: human help. Common delivery methods include such human-machine interactions as opening infected email attachments, and visiting websites which inject the malware into the user's machine. While even the most innocent websites can be hijacked to deliver malware, the shadier websites are the most likely to give you an unwanted infection.

PEOPLE

Lucas Amodio, C|EH

Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES

Litigation

Intellectual Property

Data Innovation, Security and Privacy

These delivery methods have several implications which help explain ransomware's rapid proliferation. First, the hacker doesn't have to put any thought into making you a target. He or she just has to cast the malware about (much like throwing seed into the air), and then wait for you to call once you are infected. Second, ransomware has an extremely high ROI for the hacker's limited efforts. The hacker has to write (or buy) the ransomware once (and it's not expensive to acquire), seed it once, and then sit back and watch the profits roll in from thousands of infections.

What you can do
While nothing provides a bulletproof solution to this growing problem, implementing and strengthening several measures can lower your risk:

- Because much of this malware infects machines by tricking the user, raising user awareness of this problem is crucial. Users who are more resistant to clicking on suspicious email links and visiting shady websites are your best means of lessening exposure. You should realize that:

  - Inattentive users run a very real risk of bringing damaging cyber-infections into the company.
  - "Think before you click" on email attachments and imbedded links is an important defense. You are far better off having users who over-report suspicious links to IT than with users who are overly trusting.
  - Web browsing should be limited to those business sites that are necessary for your operations.
  - If your users have the ability to link to company systems from their personal computers or other devices, understand that applying these rules to their personal device use makes them, and the company, safer.
- Encourage prompt employee reporting of potential problems. Even the most diligent employee may fall prey to a malicious email. Employees who fear discipline or termination will be much less likely to swiftly report potential problems. You will eventually discover you've been compromised, but only after the damage has multiplied.
- Back up frequently. Losing a file to encryption is much less problematic if you have a clean backup copy. Review your backup procedures, and make sure you have a robust backup process.