Homework

IT's About Business 4.2

Ransomware

MIS

In early 2016 the Hollywood (California) Presbyterian Medical Center (**www.hollywoodpresbyterian.com**) experienced a cyberattack that encrypted some of the hospital's crucial information. In response, the hospital turned off its network so that the infection could not spread and began negotiations with the attackers, who demanded a rumored $3 million in bitcoins as ransom. Hospital employees resorted to pen, paper, telephones, and fax machines for many tasks normally carried out by information systems. Such tasks included accessing patient information and test results, documenting patient care, and transmitting laboratory work, X-rays, and CT scans. The hospital stated that the network shutdown did not affect patient care, although the hospital did send some patients to other facilities.

The hackers held the hospital hostage for 10 days until the hospital paid them approximately $17,000 worth of bitcoins to decrypt its key information.

Over Thanksgiving weekend in 2016, the public transit system in San Francisco would not accept riders' money. Attackers had compromised the agency's ticketing system, encrypted its data, and reportedly demanded 100 bitcoins (about $73,000 at that time) to send the decryption key. The agency refused to pay the attackers. Instead, the agency deactivated its ticketing machines and let riders go through the gates for free. The agency restored its ticketing machines and by Monday the system was operating normally, even if the agency missed two days of revenue.

The malicious software that infected the hospital and the transit system is called *ransomware*. Ransomware, or digital extortion, blocks access to a computer system until the system owner or operator pays a sum of money. Types of ransomware include Cryptolocker, Cryptowall, TeslaCrypt, CTB Locker, and Locky. The most current form of ransomware demands payment through the hard-to-trace cryptocurrency Bitcoin, and it uses the anonymizing Tor network (**www.torproject.org**). Some attackers are even taking a "freemium" approach: They decrypt some data for free to show victims that they can get the remainder of the encrypted data if they pay the ransom.

Ransomware is typically disseminated through established botnets and phishing attacks. Victims are told to pay the ransom in Bitcoin or through MoneyGram to untraceable gift cards in Eastern Europe. Ransomware attacks are growing rapidly. The average charge to decrypt data has grown from $294 in December 2015 to $679 by June 2016, according to security firm Symantec (**www.symantec.com**). The FBI estimated that the ransomware industry may have reached a total of $1 billion in ransom paid in 2016.

Many ransomware victims stated that the attackers were honoring their promise to decrypt the data if the victim complied with the terms within the specified time. This situation was an incentive for additional victims to pay the ransom rather than pursuing another, generally more costly, solution. In fact, security analysts estimate that almost half of ransomware victims pay the ransom.

Two recent ransomware variants appeared at the end of 2016. The first variant offers the decryption key to a victim if the victim provides a link to the ransomware to two other people or to companies that pay the ransom. With the second variant, hackers pretend to be job hunters in an effort to infect corporate human resources systems. The cybercriminals even submit cover letters to appear legitimate.

There are several possible solutions to the ransomware problem.

- The first line of defense is to back up crucial data and information often, preferably through an encrypted cloud-based storage company or an online backup service to make copies of your operating system and data. See, for example, iDrive (**www.idrive.com**), CrashPlan (**www.crashplan.com**), SOS Online Backup (**www.sosonlinebackup.com**), and Carbonite (**www.carbonite.com**). Your backup data storage must be connected to only your system when you are backing up the data.

  Canada's Ottawa Hospital averted a ransomware interruption because it had backed up the data encrypted on some of the hospital's computers. The hospital completely erased the hard drives of the infected computers, restored them, and returned them to service.
- Second, it is imperative to provide education and training so that users are aware of phishing and spear-phishing attacks and not click on any suspicious e-mails or suspicious links in e-mails.
- Third, employ a real-time monitoring system that can possibly stop ransomware almost immediately. Such a system, called CryptoDrop, was created by staff at the Florida Institute for Cybersecurity Research. CryptoDrop stops the ransomware encryption at the start of the process, ensuring victims have less reason to pay the ransom.
- Fourth, victims can pay the ransom, even though the FBI advises against this practice. However, one hospital administrator noted that she had no choice because patient safety was at risk.

Sources: Compiled from D. Palmer, "This Ransomware Targets HR Departments with Fake Job Applications," *ZDNet*, January 4, 2017; M. Heller, "Unique Threat Offers Victims Ransomware Decryption to Spread Infections," *TechTarget*, December 12, 2016; J. Stewart, "SF's Transit Hack Could've Been Way Worse—And Cities Must Prepare," *Wired*, November 28, 2016; J. Lee, "CryptoDrop: Prevent Ransomware Attacks by Stopping Encryption Early," *Ipswitch blog*, September 1, 2016; G. Fleishman, "Two Ways to Stop Ransomware in Its Tracks," *MIT Technology Review*, July 29, 2016; K. Zetter, "4 Ways to Protect Against the Very Real Threat of Ransomware," *Wired*, May 13, 2016; T. Simonite, "With Hospital Ransomware Infections, the Patients Are at Risk," *MIT Technology Review*, April 1, 2016; W. Ashford, "U.S. Hospital Claims to Have Fought Off a Ransomware Attack," *Computer Weekly*, March 23, 2016; M. Orcutt, "Hollywood Hospital's Run-In with Ransomware Is Part of an Alarming Trend in Cybercrime," *MIT Technology Review*, February 18, 2016; M. Heller, "Ransomware Attack Causes Internal Emergency at Hollywood Hospital," *TechTarget*, February 16, 2016; T. Simonite, "Hospital Forced Back to Pre-Computer Era Shows the Power of Ransomware," *MIT Technology Review*, February 16, 2016; P. Muncaster, "Over One-Third of Firms Hit by Ransomware Blitz," *InfoSecurity Magazine*, June 26, 2015; C. Stobing, "Ransomware Is the New Hot Threat Everyone Is Talking About; What Do You Need to Know?" *Digital Trends*, June 6, 2015; R. Lemos, "Ransomware Threat Drives Companies to Enforce Better Backup Habits," *eWeek*, May 26, 2015; R. Simon, "'Ransomware' a Growing Threat to Small Businesses," *Wall Street Journal*, April 15, 2015; R. Lemos, "How to Prevent Ransomware: What One Company Learned the Hard Way," *PC World*, March 26, 2015; L. Constantin, "Malvertising Campaign Delivers Digitally Signed CryptoWall Ransomware," *PC World*, September 29, 2014.

Questions

1. **Why is ransomware more than a nuisance?**
2. **Are your digital files adequately backed up? Why or why not?**