Ransomware: A rapidly growing threat

A hospital paralyzed by hackers" is the headline of a recent article about a ransomware attack on servers at a Southern California hospital.[1] Hackers had used this new type of malware to encrypt patient records — and demanded money to make patient files available again. Meanwhile, patient care had come to a standstill.

Ransomware is a growing concern for companies large and small. The FBI's Internet Crime Complaint Center will soon release data showing that in 2015, there were 2,453 reported ransomware incidents in which victims paid $24.1 million total.[2] The actual number of incidents and losses may have been far greater.

To pay or not to pay

Ransomware is malicious software that blocks access to a computer system or files until the victim pays a monetary amount.

The hackers often want payment in bitcoin, a virtual currency that is publicly available, anonymous, and very difficult to track. If a ransom is paid, there's no guarantee that you'll regain access to your infected systems or that the hackers won't come back for more.

According to the FBI, the financial impact of this scheme goes beyond the ransom payment. There may also be an impact to business associated with the loss of sensitive or proprietary information, a disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation.

Best practices to reduce your risk from ransomware and other malware attacks

Companies have to be increasingly vigilant to prevent cyber-attacks. At a minimum, keep your antivirus software and operating systems up to date.

Additional best practices include training your employees at every level of the organization to:

- Back up critical data regularly — and store that data offline. Make sure your organization's business continuity plan includes the appropriate processes, skills, and relationships to address cyber-attacks and cyber terrorism.

- Unless you're certain they're from trusted senders, do not select links in emails or text messages, download attachments, or install programs. Be particularly cautious when opening unexpected emails from known or unknown senders.
- Never use a direct link in an email or text message to sign on to your banking portal. Instead, go directly to the sign-on page. Direct links may appear to be legitimate, but a slight difference in a URL could lead you to a malicious website.

What you should do today

Talk to your IT group now about the rising threat of ransomware, so they can ensure the appropriate security measures are in place for your company.

If you suspect fraud, contact your Wells Fargo representative, or call 1-888-937-9997, Monday through Friday, 5:00 a.m. to 7:00 p.m. Pacific Time, and ask to have a Wells Fargo Dealer Services Commercial Relationship Manager in your area contact you.

Extra resources/information

Staying prepared for and protected from ransomware (infographic)

FBI Internet Crime Complaint Center (IC3) link to website
Site provides information for filing complaint, FAQs, IC3 and ransomware brochures, etc.)

1. Kavah Woodell, "A Hospital Paralyzed by Hackers," *The Atlantic*, February 17, 2016.
2. Devlin Barrett, "FBI Says Threat From 'Ransomware' Is Expected to Grow," *The Wall Street Journal*, March 10, 2016.