Five ways to become a smaller target for ransomware hackers

April 5 2016, by Tami Abdollah

Hacking for ransom is on the rise—on pace to beat out last year's figures—and hits people where it hurts, locking them out of files, photos and critical records until they pay hackers a bounty to restore their access. Hackers bait users to click on infected email links or open infected attachments, or they take advantage of outdated and vulnerable systems.

Victims see important files scrambled into encrypted gobbledygook, as an electronic ransom note warns that if they ever want to see those files again in a readable format, they must pay money in virtual currency, known as bitcoin.

Last year's 2,453 reports of ransomware hackings totaled a reported loss of $24.1 million, making up nearly one-third of the complaints over the past decade. They also represented 41 percent of the $57.6 million in reported losses since 2005. Such losses are significantly higher than any paid ransoms because companies routinely include remediation costs, lost productivity, legal fees and sometimes even the price of lost data in their estimates.

What's priceless is avoiding the hack altogether.

Here are five tips to make yourself a less likely victim:

MAKE SAFE AND SECURE BACKUPS

Once your files are encrypted, it's nearly always game over. Backups often are out of date and missing critical information.

Ransomware has become increasingly sophisticated and effective at separating users from the contents of their computers. For example, sometimes it targets backup files on an external drive. You should make multiple backups—to cloud services and using physical disk drives, at regular and frequent intervals. It's a good idea to back up files to a drive that remains entirely disconnected from your network.

UPDATE AND PATCH YOUR SYSTEMS

The recent samsam virus-like attack takes advantage of at least two security vulnerabilities on servers, including one discovered in 2007. Updating software will take care of some bad vulnerabilities. Browsers such as Chrome will automatically update behind the scenes, saving you the time and deterring hackers.

USE ANTIVIRUS SOFTWARE

It's basic but using antivirus will at least protect you from the most basic, well-known viruses by scanning your system against the known fingerprints of these viruses. Low-end criminals take advantage of less savvy users with such known viruses even though malware is constantly changing and antivirus is frequently days behind detecting it.

EDUCATE YOUR WORKFORCE

Basic cyber hygiene such as ensuring workers don't click on questionable links or open suspicious attachments can save headaches. System administrators should ensure that employees don't have unnecessary access to parts of the network that aren't critical to their work. This helps limit the spread of ransomware if hackers do get into your system.

IF HIT, DON'T WAIT AND SEE

When hackers hit MedStar Health Inc., the hospital chain shut down its network as soon as it discovered ransomware on its systems. That action prevented the continued encryption—and possible loss—of more files. Hackers will sometimes encourage you to keep your computer on and attached to the network but don't be fooled.

If you're facing a ransom demand and locked out of your files, law enforcement and cybersecurity experts discourage paying ransoms because it incentivizes hackers and pays for their future attacks. There's also no guarantee all files will be restored. Many organizations without updated backups may decide regaining access to critical files, such as customer data, and avoiding public embarrassment is worth the cost.

The hackers, of course, are counting on that.