When your PC is held hostage

Troy Wolverton, San Jose Mercury News, 5/16/16, twolverton@bayareanewsgroup.com

A computer scam making the rounds could cost you hundreds of dollars or the ability to access your most precious pictures and sensitive files. It's called ransomware. It's a type of malware that locks up computers or computer files and won't allow users to access them unless they pay up. "It's heartbreaking," said Jeremy Buschine, the director of IT service and repair at ClickAway, a chain of computer repair shops headquartered in Campbell. "It's about as close to cyberterrorism as I've ever seen." Ransomware works like other types of malware. It's malicious software that typically gets onto users' computers when they open email attachments that have it embedded, visit infected Web pages or download certain software.

But unlike those other types of malware, ransomware uses encryption to scramble users' files. While they might be able to delete the ransomware after their machine's been infected, they often can't unscramble their data without the hackers' help.

Ransomware's been around for a while — the first prototype was described in the 1990s, according to security researchers — but it's become a huge problem in just the last six months. Security researchers have noted a huge uptick in the number of actual and attempted infections and in the types of ransomware circulating in the wild.

"Beginning this year, it really became an epidemic," said Ryan Naraine, head of the global research and analysis team at Kaspersky Lab, a security software company.

In recent months, hospitals, schools and even police offices have been hit with ransomware. In February, for example, Hollywood Presbyterian Medical Center in Los Angeles acknowledged that it paid cybercriminals $17,000 to unlock its computers after they were infected with ransomware.

But individuals as well as institutions are being affected. Helen Tindall, a retired county worker who lives in San Jose, recently had a computer get hit with a primitive form of ransomware.

Tindall, 75, allowed someone purporting to be a "Microsoft-certified technician" who reached her by phone to have remote access to her computer to supposedly fix the problems he said were coming from it. But instead of fixing any problems, the socalled technician installed software that flashed a message warning of other problems and gave a 1-800 number to call. When Tindall called the number, the helpful people who answered demanded $400 to remove the malicious software they had installed on her machine.

Fortunately for Tindall, the malware the hackers installed on her computer didn't encrypt her files, which included some art photographs she had taken. She was able to take her computer to an actual technician at the Geek Squad, Best Buy's in-house repair service, who was able to recover her files and delete the malware from her machine. But the ordeal cost her around $200 and a lot of stress.

"I couldn't go to sleep," she said. Others aren't so lucky. A local attorney who is a client of the Cheap Squad, a small computer repair shop in downtown San Jose, had his work computers with his case files on them infected with ransomware. Feeling like he didn't have a choice, the attorney paid the $500 ransom to get the key to unlock his files. But the key only unlocked the files for a limited time, which wasn't long enough for the attorney to recover them all. He ended up paying another $500 to get more time to transfer them.

Not that long ago, the Cheap Squad would only see about one case of ransomware every three months, said owner Jeremy Prader. Now, though, the shop is seeing about two cases every week.

"It's definitely jumped up a lot," Prader said. "And it's only going get worse."

Cybercriminals are glomming on to ransomware, because it often works and it makes them money, security experts say. And it's been boosted by two technical advances. In late 2013, CyptoLocker, a malware tool that encrypts the files of infected computers, started circulating. More recently, criminals have begun selling ransomware software on the so-called Dark Web, allowing even those without a technical background to get into the cyberransom game.

Windows users are the most at risk; the vast majority of ransomware targets PCs. But users of other devices aren't immune. Researchers have seen ransomware circulating on the Internet that targets Mac computers and Android smartphones and tablets.

Because there's often no way to treat a ransomware infected computer, the best way to defend yourself is to practice basic computer hygiene, including running anti-virus software, keeping that and other software on your computer up-todate and making frequent backups of your data to
a drive or service that is typically disconnected from your machine.

That last bit is important, because the latest versions of ransomware can infect not just your main hard drive, but any external drives that are attached and online storage services like Dropbox that appear to be external folders or drives. "A backup solves all sorts of ills," said Bruce Schneier, chief technology officer at Resilient Systems, an IBM-owned security company. "You can save a lot of money by building a better system before you're infected." Contact Troy Wolverton at 408-840-4285 or twolverton@bayareanewsgroup.com.

A GROWING PROBLEM

Ransomware has been around for years, but it's become particularly accuse in recent months, security researchers say.
By the end of 2014, there were only 16 main families, or types, of ransomware in the wild, according to Malwarebytes. Last year, there were 27 new ones. In the first quarter of this year alone there were 15 new families added.
About 60 percent of the malware infections encountered by anti-virus company Malwarebytes are now ransomware.
The number of ransomware infections detected by Enigma Software's SpyHunter software in the United States jumped by 158 percent just between March and April of this year.
n In the first quarter of this year, Kaspersky's anti-virus software blocked ransomware from installing on the computers of 372,602 users, up by 30 percent from the previous quarter.
Some 2,453 ransomware complaints were filed with the FBI's Internet Crime Complaint Center last year, with reported losses tallying more than $25 million.
Source: Mercury News research

PROTECTING YOURSELF FROM RANSOMWARE

Ransomware is dangerous, pernicious and becoming widespread, but you can take steps to minimize the risk that your computer will be infected.

Update: Make sure your software, operating system and plug-ins like Java and Flash are kept up-to-date by turning on their automatic update feature. Some hackers are exploiting vulnerabilities in those programs to install ransomware automatically when consumers visit hacked websites.

Back up your data: If your files are locked by ransomware, the only way to recover them without paying the ransom is typically from backup copies. If you aren't yet doing regular backups, you should start. If you already back up your computer, you may need to change how you're doing it. Some ransomware can find and encrypt files on anything that looks to the computer like an attached drive, including external hard drives you may have connected, drives you may have on your local network or cloud services like Dropbox. Experts advise you to use cloud backup services like Carbonite or an external hard drive that you disconnect after each backup. Ideally, they say, you should back up your data in multiple places or on to multiple drives.

Run anti-virus software: Assuming you keep it up-to-date and have it set to scan for viruses automatically, anti-virus software can usually detect and block known ransomware. Unfortunately, such programs typically struggle to identify and protect your computer from new versions of ransomware, so they're not a perfect solution. Some antimalware programs can act as a kind of backup, allowing you to undue changes ransomware and other malware have done to your computer.

Think before you click: Be skeptical of links or documents sent to you in email and be wary of clicking on them. Criminals have gotten good at creating messages that look like they come from legitimate sources.

WHAT TO DO IF YOUR COMPUTER IS INFECTED

Here are some tips on dealing with ransomware **if you don't have a backup**.
1. **Disconnect your computer**. In some cases, if you detect the infection early enough, you can minimize the damage by taking your PC offline.
2. **Determine the scope of the infection**. If you stop the infection in time, the ransomware may not lock up all your files. If you can live without the ones you lost, backup what's left and clear the infection.

3. **Look for a countermeasure**. If you determine the type of ransomware, you can sometimes find software that will decrypt your files.
4. **Consult with a computer technician or repair shop**. A technician may be able to help you recover your files, particularly if the malware attack is relatively unsophisticated.
5. **Pay the ransom**. This should be your last resort. The FBI advises against it, warning it only encourages criminals. And there's no guarantee if you pay the ransom that the hackers will give you either the key needed or sufficient time to recover all your files. But if you can't get access to your files any other way and your business depends on them or they include irreplaceable items, like the first video of your kid walking, you may have no other choice.