Beware the Rise of Ransomware

Kim Boatman
Find Under: Threats

The latest spin on a ransom note isn't composed of letters clipped out of a newspaper. Increasingly, criminals are unleashing brash attacks on your PC and its data through a type of malicious software called ransomware.

It's exasperating enough when your computer is sluggish because of a virus, but what if the virus installs embarrassing pornography on your screen or encrypts your data so you can't read it? Ransomware attacks often use these tactics to demand you pay a ransom to remove the pornography or to access your files.

Ransomware on the rise
"There's more and more documented evidence that this is going on," says Ori Eisen, founder and chief innovation officer of fraud prevention company 41st Parameter. "It's more prevalent in the United Kingdom, which is sort of a staging or testing ground. It's starting there and getting more momentum."

The FBI recently issued an alert about the broader category of rogueware, which include ransomware and fake antivirus scareware scams. According to the FBI, criminals are netting an estimated $150 million a year through these scams. "Ransomware is actually scarier" than the scareware scams, says Robert Siciliano, a Boston-based identity theft expert. "There's nothing worse in the field of technology than having a criminal in control of your network. When a ransomware attack occurs, it can easily elevate from a potential data loss to potential identity theft to a data breach in the form of extortion."

How ransomware works
These aggressive assaults begin in a similar manner to scareware. You're duped into clicking on an infected popup advertisement or you visit an infected website. However, instead of just trying to trick you into buying fake antivirus software, the bad guys hold your computer hostage and attempt to extort payment.

In some instances, ads for pornographic websites appear on your screen each time you try to click on a Web page. The ads cover a portion of the page you're trying to view. "Just imagine you're sitting at work and that happens to you," says Eisen. One ransomware attack puts time pressure on the victim, stating that a piece of your data will be destroyed every 30 minutes if you don't pay up. Another attack attempts to force you to purchase a program to de-encrypt your data.

The criminals often ask for a nominal payment, figuring you'll be more likely to pay to avoid the hassle and heartache of dealing with the virus. They may ask for as little as $10 to be wired through Western Union, paid through a premium text message or sent through a form of online cash.

Protect yourself from ransomware
As with other attacks, you can work to avoid ransomware. Experts advise taking these steps to avoid attacks or protect yourself after an attack:

1. *Use reputable antivirus software and a firewall.* Maintaining a strong firewall and keeping your security software up to date are critical. It's important to use antivirus software from a reputable company because of all the fake software out there.
2. *Back up often.* If you back up files to either an external hard drive or to an online backup service, you diminish the threat, says Eisen. "If you back up your information, you should not be afraid to just turn off your computer and start over with a new install if you come under attack." Eisen backs up his data regularly, so every six months, he simply restores his computer's system to default and starts afresh. "I would highly recommend it," he says.
3. *Enable your popup blocker.* Popups are a prime tactic used by the bad guys, so simply avoid even accidentally clicking on an infected popup. If a popup appears, click on the X in the right-hand corner. The buttons within a popup might have been reprogrammed by the criminals, so do not click on them.
4. *Exercise caution.* Don't click on links inside emails, and avoid suspicious websites. If your PC does come under attack, use another computer to research details about the type of attack. But be aware that the bad guys are devious enough to create fake sites, perhaps touting their own fake antivirus software or their de-encryption program.
5. *Disconnect from the Internet.* If you receive a ransomware note, disconnect from the Internet so your personal data isn't transmitted back to the criminals, says Eisen. He recommends simply shutting down the computer. If you have backed up your data, you can re-install software. If you don't feel comfortable doing so or you are unable to start fresh, you may need to take your computer to a reputable repair shop, says Eisen.
6. *Alert authorities.* Ransomware is a serious form of extortion. "Local police are probably not equipped to deal with this," explains Siciliano. "However, the local FBI would want to know about it."

Don't be tempted to give in and pay the ransom, warns Siciliano. "Paying them would be a mistake because they will further extort you and most likely not release your information." Taking precautions to protect your information and maintaining vigilance are the best solutions to avoid becoming a victim in the first place.