

Ransomware Attacks May Blindside Unsuspecting Users

When internet users have their hackles up waiting for a cyber attack, they often expect the attackers to sneak in through the proverbial back door, sneaking in a stealthy, covert, and hidden manner. But in cyber space, nothing is certain. While the victim is busy looking over his shoulder, the attacker may just run up and whack him over the head – metaphorically, of course. The threat of ransomware is a good example of a direct attack. Unlike a stealth attack such as keylogging, in which the victim is extorted via logged keystrokes that capture passwords, account numbers, and other personal and financial information without their knowledge, ransomware is more direct. Ransomware is an attack in which perpetrators use malicious code to hijack the victim's computer files and encrypt them, rendering them unreadable and useless. For the kicker, the attackers then contact the victim, demanding a ransom in the form of a payment or online transaction in return for a decryption password. Ransomware has not been a very widespread issue, but as hackers and users both become more sophisticated, it may be used to blindside more and more people who are only worried about phishing or keyloggers. Luckily, the same techniques used to prevent users from falling victim to those widely known scams are the same: 1. Do not open email or attachments from unknown sources. 2. Do not follow links to unknown sites. 3. Do not download games, files, or software from unknown sources. 4. Install antivirus and anti spyware software and update it daily. 5. Install a firewall and popup blocker and keep them turned on. 6. Make sure all browsers and system software is updated regularly. 7. Back up all system files and computer files on a separate machine, online, or on disk, so that the hard drive can be wiped if necessary without sacrificing important files or programs. When faced with the loss of their computer data, some people may panic and instinctively hand over the payment. However, many may find that they paid for no reason at all. One ransomware program, known by the moniker Ransom.A, is actually not destructive – on the contrary, it relies on empty threats to extract payment. In addition to randomly activating pornographic popups on the user's computer, Ransom.A threatens to destroy a file every 30 minutes until the user wires a conveniently low payment of \$10.99 to the attackers in return for an "unlock code." But Ransom.A does not have the ability to delete or encrypt files; all it does is rely on the user's need for a fast, cheap fix to what is, essentially, not a real problem. There are, however, ransomware programs that actually will do harm, such as Trojan.Archiveus, which, according to antivirus company Kaspersky Lab, copies, scrambles, and deletes all the files in the user's "My Documents" folder. A ransom note is then sent to users offering the decryption password in exchange for a purchase from an online Russian pharmacy. Drive-by downloading is thought to be the main way Archiveus is spread. However, according to Symantec Corp., the password to unlock the encryption is: mf2lro8sw03ufvnsq034jfowr18f3cszc20vmw – apparently, the decryption password was found in the code, offering an example of the fact that hackers are as susceptible to human flaw as the most inexperienced user. Though the threat of ransomware is relatively low, it is still a good idea to back up all computer files and take the necessary steps to prevent receiving one of the nasty little notes. And, if you should find yourself in that position, contact law enforcement officials before making any payments to your attackers.

About the Author

If you are a participating pharmacy, please go to instructions to download the icon. Drug World Pharmacies Duane Reade Eckerd Corporation.

Source: <http://www.productsherbal.com>