charles SCHWAB

Advisor Services

Ransomware

Schwab Cybersecurity Update

The FBI recently warned of an uptick in ransomware, an increasingly popular—and for the victims, expensive—way for cybercriminals to extract money from unsuspecting computer users. As the name of the threat suggests, cybercriminals break into your computer and, once there, hold your data hostage until you pay a ransom. These attacks have infected thousands of computer users. According to the FBI, there were nearly 2,500 reported instances in 2015, costing victims $24 million in ransom. This does not include the thousands of unreported attacks.

The break-in. Cybercriminals rely on common techniques to break into computers, including deceiving users into clicking on links to compromised websites from either an email or a pop-up ad or by opening an email attachment containing malware. Once inside the computer, the hacker locks the user out, holding the data hostage by encrypting it and providing the decryption key once the ransom is paid. And, if the victim stalls or refuses to pay, cybercriminals may threaten to distribute personally identifiable information.

The payment. Victims may be told to send the ransom payment via money order, prepaid credit card or, increasingly, with bitcoins, where the hacker gives instructions to the victim on how to first purchase bitcoins and then make the payment via Bitcoin Wallet transfer. Cybercriminals using Locky, a ransomware responsible for a spate of recent attacks, demand payment of three bitcoins (valued at roughly $1,200) in exchange for a decryption key. Many experts disagree with paying ransoms, arguing that it encourages future attacks.

The target. Ransomware victims include home computer users, but increasingly small and medium-size businesses, financial institutions, government agencies, academic institutions, and other organizations have been impacted. In these instances, hackers will hold hostage confidential information about a company's customers, the loss of which would be detrimental to the business.

Recent examples include a February 2016 attack targeting a large medical center located in California. Cybercriminals infected the hospital's computer systems with malware that blocked access to patient electronic health records and demanded a ransom payment of 40 bitcoins (valued at $17,000). The incident lasted nearly a week, and many patients missed treatments. Once the hospital paid the ransom, the hackers provided a decryption key which allowed the hospital to regain control of its systems. In similar cases, public safety and law enforcement agencies in Massachusetts, Maine, and Illinois have also fallen victim to ransomware attacks, paying hackers in bitcoin to get their systems back online.

How to protect your computer and firm from ransomware

- ☐ Update your antivirus software
- ☐ Use a pop-up blocker
- ☐ Have strong passwords, use them once
- ☐ Store backed-up data offline
- ☐ Enable automated patches
- ☐ Download only from sites you know and trust
- ☐ Conduct regular system back-ups
- ☐ Use these precautions on your cell phone
- ☐ Don't open attachments or click on URLs in unsolicited emails, even from those you know

Additional resources

To avoid ransomware attacks, firms should remain vigilant and follow the FBI's recommendations found at https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise.

If you receive a suspicious or malicious email, please report it to the Anti-Phishing Working Group (APWP) at http://www.antiphishing.org/report-phishing/overview/.