A Q&A about the malicious software known as ransomware

8 April 2015, byJoyce M. Rosenberg

Ransomware is a growing threat to computer users, who can suddenly find they're unable to open or use their files when their machines are infected. The malicious software can attack any user—an individual, small business, Fortune 500 company or a government agency.

Some questions and answers about ransomware:

Q. What is ransomware?

A. It's a type of software used by hackers to extort money from computer and smartphone users. A program called CryptoLocker appeared several years ago, and made files like word processing documents and photos inaccessible to computer users unless they paid a ransom, usually $500 to $700. Law enforcement agencies shut Cryptolocker down in 2014, but there is a new generation, with versions called Cryptoware and Cryptowall.

Q. How does it work?

A. Ransomware infiltrates a computer after a user clicks on a link or attachment in an email. It can also attack when a user visits a website, including well-known ones with good security systems, according to technology consultant Greg Miller of CMIT Solutions of Goshen, New York. Once inside the computer, it encrypts or locks up files, making them impossible to use. It can also lock up a network of computers if it infects a server, a computer that links PCs.

Q. How does a user pay a ransom?

A. Bitcoins, an online currency that is hard to trace, are becoming the preferred way hackers collect ransoms, according to FBI Special Agent Thomas Grasso, who is part of the government's efforts to fight malicious software including ransomware.

Q. How many attacks have there been? And how many users pay a ransom?

A. During 2013, the number of attacks each month rose from 100,000 in January to 600,000 in December, according to a report last year by Symantec, the maker of antivirus software. Those are the most recent figures available, but cybersecurity experts say the attacks are growing.

The company estimates on average, 3 percent of users with infected machines pay a ransom.

Between June 1 and Dec. 31, 2014, the government's Internet Crime Complaint Center received 1,646 complaints about ransomware attacks, the FBI's Grasso says. From Jan. 1 to March 31 of this year, there were 629 complaints. Ransomware accounted for about 1 percent of complaints about all kinds of cybercrime. The majority of ransomware attacks go unreported because people or businesses are embarrassed about having been hacked or paid a ransom, Grasso says.

Q. Can you prevent an attack or limit how many files are infected?

A. Conventional anti-virus programs may not be able to prevent an attack because hackers continually change their software to stay one step ahead of protective measures. Large corporations use sophisticated programs to reduce their vulnerability, but it costs more than many smaller users can pay, says Liam O'Murchu, a security executive at Symantec.

Files should be backed up in a system not directly connected to a computer or network. Storing files in online systems like Google Drive or OneDrive aren't secure, however, because they are continually linked to what's on a PC. Users may want to invest in online storage that will be able to retrieve uninfected files.

And all users must be wary about any emails with links or attachments, even if they seem to come from a known sender.

Businesses should also create separate systems for different departments or functions, says Jonathan Fairtlough, a cybersecurity executive with the security company Kroll. That will help stop ransomware from spreading if a company is attacked.

In some attacks, only some files are infected, says Philip Banks, owner of Banks Technology Services, a Roanoke, Virginia-based technology consultant.

Q. How is an infected computer repaired?

A. If a ransom is paid, the hackers generally send users a computer code that unlocks the files one by one. Depending on how many files are infected, the process can take weeks.

If there is a backup, the machine must be stripped of all files and software and reset to what's called factory condition. That process will also remove the ransomware. New files and software are then installed from the backup.