Computer users face hard choice—pay ransom or lose files

April 8 2015, byJoyce M. Rosenberg

In this Wednesday, April 1, 2015 photo, Jeff Salter, CEO of Caring Senior Service, poses for a photo in his company office building in San Antonio. Last December, the network of nearly 30 computers at Caring Senior Service were invaded by ransomware, software hackers use to try to extort money from people and businesses that can't open or use documents, pictures, spreadsheets and other files. (AP Photo/Matthew Busch)

It's a chilling moment: A message appears on a computer screen, saying the files are encrypted and the only way to access them is by paying a ransom.

It happened at Jeff Salter's home health care business last December. The network of nearly 30 computers at Caring Senior Service was infected with ransomware, malicious software that hackers use to try to extort money from people and businesses by preventing them from opening or using documents, pictures, spreadsheets and other files. If computer users don't pay, there's no way they can access their files.

Ransomware is one of the fastest-growing forms of hacking, cybersecurity experts say. Anyone from a home computer user to a Fortune 500 company can be infected. It can also attack smartphones. The smaller the users, the more vulnerable they are to losing their files—unless they have a secure backup for their system or go through the complicated process of paying cybercriminals.

Salter thought he was prepared for such an invasion. Most of his files were backed up in a place hackers couldn't access, and he was able to restore his information. But one machine wasn't; it contained marketing materials for his San Antonio-based franchise chain with 55 locations. Salter paid a $500 ransom.

"It would have cost us $50,000 to try to spend the time to recreate the stuff," Salter says. "It would have been pretty devastating if we'd lost all that."

EVERYONE'S AT RISK

Like many hackers' tools, ransomware can arrive in emails with links or attachments that, when clicked on, unleash software into files. Attacks can also occur when users visit websites; cybercriminals can attach computer code even to well-known sites operated by tech-savvy companies, says technology consultant Greg Miller of CMIT Solutions of Goshen, New York.

Anyone can be hit: individuals, big and small companies, even government agencies. The Durham, New Hampshire, police department was attacked by ransomware in June when an employee clicked on a legitimate-looking email. The department's 20 computers were cleared of the ransomware and files were restored from a backup system. The Swansea, Massachusetts, police department, meanwhile, had to pay a $750 ransom after it was attacked.

In this Wednesday, April 1, 2015 photo, Jeff Salter, CEO of Caring Senior Service, poses for a photo in his company office building in San Antonio. Last December, the network of nearly 30 computers at Caring Senior Service were invaded by ransomware, software hackers use to try to extort money from people and businesses that can't open or use documents, pictures, spreadsheets and other files. (AP Photo/Matthew Busch)

"We certainly are seeing ransomware as a common threat out there," says FBI Special Agent Thomas Grasso, who is part of the government's efforts to fight malicious software including ransomware.

Attacks are generally random, but specific companies and people can be targeted. Many small businesses and individuals are at risk because they lack technology teams and sophisticated software to protect them from hackers, says Keith Jarvis, a vice president at Dell SecureWorks, a security arm of the computer maker. Many don't have secure backup systems that will allow them to retrieve uninfected files.

Hackers can invade computers at large companies, as seen in attacks at companies like retailer Target Corp. that stole customer information. Big companies' risks from ransomware are relatively low; they have backups and separate computers for departments like sales or accounting, Jarvis says. An email click in one department could infect one or more computers, but likely wouldn't spread elsewhere.

Cyber criminals are starting to target small businesses more than in the past because they're vulnerable, says Liam O'Murchu, a security executive at antivirus software maker Symantec Corp. Symantec and other companies involved in cybersecurity work with the government to try to identify hackers.

One way hackers fool small businesses is by attaching realistic-looking invoices to emails, O'Murchu says.

It's not known who the hackers are, he says. A version of ransomware called Cryptolocker was shut down in 2014. None of the hackers or groups of hackers have been caught.

In this Wednesday, April 1, 2015 photo, Jeff Salter, CEO of Caring Senior Service, poses for a photo in his company office building in San Antonio. Last December, the network of nearly 30 computers at Caring Senior Service were invaded by ransomware, software hackers use to try to extort money from people and businesses that can't open or use documents, pictures, spreadsheets and other files. (AP Photo/Matthew Busch)

ATTACKED AND NO BACKUP

A computer user gets a message saying files have been encrypted and is given instructions to pay a ransom, often between $500 and $700. Ransoms must be paid in bitcoins, an online currency.

If files are backed up securely, users can remove infected files and software from a computer and reset it to what's called factory condition. Files from the backup sites are then restored to the computer.

In this Wednesday, April 1, 2015 photo, Jeff Salter, CEO of Caring Senior Service, poses for a photo in his company office building in San Antonio. Last December, the network of nearly 30 computers at Caring Senior Service were invaded by ransomware, software hackers use to try to extort money from people and businesses that can't open or use documents, pictures, spreadsheets and other files. (AP Photo/Matthew Busch)

Freelance writer Sandra Gordon paid $637 when her computer was infected in January. Gordon, who faced losing files going back 16 years, decided to pay after technicians said there was nothing they could do. She didn't have a secure backup.

Typically, when the ransom's paid, hackers email a computer code to the user so the files can be released. But Gordon, based in Weston, Connecticut, didn't get her code for five days, and had to plead with the hackers via email to send it to her.

"It was very lonely and scary and hard to imagine even going forward as a business," she says.

Citation: Computer users face hard choice—pay ransom or lose files (2015, April 8) retrieved 20 March 2024 from https://phys.org/news/2015-04-users-hard-choicepay-ransom.html