Spooked by spike in cyber extortion, businesses are stockpiling bitcoin for payoffs

21 February 2017, by Tim Johnson, Mcclatchy Washington Bureau

U.S. corporations that have long resisted bending to the demands of computer hackers who take their networks hostage are increasingly stockpiling bitcoin, the digital currency, so that they can quickly meet ransom demands rather than lose valuable corporate data.

The companies are responding to cybersecurity experts who recently have changed their advice on how to deal with the growing problem of extortionists taking control of the computers.

"It's a moral dilemma. If you pay, you are helping the bad guys," said Paula Long, chief executive of DataGravity, a Nashua, N.H., company that helps clients secure corporate data. But, she added, "You can't go to the moral high ground and put your company at risk."

"A lot of companies are doing that as part of their incident response planning," said Chris Pogue, chief information security officer at Nuix, a company that provides information management technologies. "They are setting up bitcoin wallets."

Pogue said he believed thousands of U.S. companies had prepared strategies for dealing with hacker extortion demands, and numerous law firms have stepped in to facilitate negotiations with hackers, many of whom operate from the other side of the globe.

Symantec, a Mountain View, Calif., company that makes security and storage software, estimates that ransom demands to companies average between $10,000 and $75,000 for hackers to provide keys to decrypt frozen networks. Individuals whose computers get hit pay as little as $100 to $300 to unlock their encrypted files.

Companies that analyze cyber threats say the use of ransomware has exploded, and payments have soared. Recorded Future, a Somerville, Mass., threat intelligence firm, says ransom payments skyrocketed 4,000 percent last year, reaching $1 billion. Another firm, Kaspersky Lab, estimates that a new business is attacked with ransomware every 40 seconds.

"If you're hit by ransomware today, you have only two options: You either pay the criminals or you lose your data," said Raj Samani, chief technical officer at Intel Security for Europe, the Middle East and Africa. "We underestimated the scale of the issue."

Hackers often send out email with tainted hyperlinks to broad targets, say, an entire company. All it takes is one computer user in a company to click on the infected link to allow

hackers to get a foothold in the broader network, leading to hostile encryption.

"At least one employee will click on anything," said Robert Gibbons, chief technology officer at Datto, a Connecticut company that offers digital disaster recovery services.

Law enforcement counsels U.S. businesses not to succumb to ransom demands, urging them to keep backup copies of their data in case of hostile encryption.

"The official FBI policy is that you shouldn't pay the ransom," said Leo Taddeo, chief security officer for Cryptzone, a Waltham, Mass., company that provides network security. Until 2015, Taddeo ran the cyber division of the FBI's New York City office.

But practical considerations increasingly are dictating a different approach. "It's an option to pay the ransom to get back up and running. Sometimes it's the only option," Taddeo said.

"But it has downsides," he added. "Paying ransom just invites the next attack."

Moreover, 1 in 4 companies that pay ransoms never get their files restored, Gibbons said.

The idea of rewarding extortionists with payment makes some technologists see red.

"That makes me super mad," said Lior Div, chief executive of Cybereason, a Boston-area cybersecurity company. "There are things that are unacceptable, and we need to fight them."

Div and his company have done something about the extortion epidemic. They built a product called RansomFree that claims to detect 99 percent of all ransomware strains.

So far, the free software has been downloaded 125,000 times, the company says.

As extortionists get more sophisticated, researchers say, they are modifying their malicious code, their infection strategies and the way they collect payments.

Once they weasel their way into your network, they now take a look around.

"They'll actually explore your system to see how much money they can squeeze from you," said Andrei Barysevich, director of advanced collection at Recorded Future.

And they won't offer any sympathy, no matter how valuable the encrypted data, even if lives are at stake, say, in a health care network. They may even say they are doing nothing evil.

"They actually think they are on the moral high ground. They think the companies should have paid more for security," said Barysevich, who spoke at a presentation this week at the annual RSA cybersecurity conference in San Francisco, which bills itself as the world's leading gathering of cybersecurity specialists.

One of the reasons midsize and large companies are storing bitcoin for emergency use is that extortionists, once they succeed at penetrating a system, commonly give a deadline for payment before destroying data. But victims can't rush out and buy bitcoin in a day or two.

"It takes at times a week for (brokers) to process you," Barysevich said.

Setting up the wallet ahead of time, Pogue said, allows businesses an option that is quick, although perhaps repugnant.

"If they need to go to it, they are not spinning their wheels standing up a bitcoin wallet," Pogue said.