For data extortion victims, payoff may be only option

pressherald.com/2015/04/14/for-data-extortion-victims-payoff-may-be-only-option/

By J. Craig Anderson Staff Writer | @JCraigAnderson | 207-791-6390

Workers at the Lincoln County Sheriff's Office arrived early on March 21 to find they could not access any data on their computers. Instead, a digital ransom note appeared on their screens with a simple message: "Pay us 300 Euros, or you will be locked out forever."

Sheriff Todd Brackett said his immediate thought was that he would not even consider paying any amount to extortionists. Instead, his deputies would hunt them down and arrest them.

Then Brackett talked to the county's information technology service providers.

"They both said within the first two minutes of our conversation, 'Pay the ransom,' " he said. Brackett ultimately did pay, as did Houlton Police Chief Joe McKenna when his office computer was hit with a similar attack about two weeks later.

Cyber extortion isn't new, but the programs and methods that criminals use have become more sophisticated in recent years, data security analysts said. It has placed countless users – including some who work for government and law enforcement – in the uncomfortable position of having to decide whether to pay off criminals to recover their data.

PAYING OFFERS NO GUARANTEES

"You don't want to pay extortionists in any part of society," said John Forker, chief information security officer for the University of Maine System.

The reasons are obvious, he said. It encourages future extortion attempts, and there is no guarantee the criminals, once paid, will hold up their end of the bargain.

However, there are other considerations, Forker said, especially if the data being held for ransom is necessary to provide a vital public service such as law enforcement. "It would be unethical in some sense for them to not pay," he said.

Known as ransomware, the programs used by cyber extortionists can infect computers through malicious email attachments, websites and files downloaded from the Internet.

The malware takes over the computer and encrypts documents, photos and other files so they can no longer be opened without a digital key – a long string of numbers that only the extortionists know. To get the key, the victim must pay the ransom, which usually ranges from $100 to $1,500, according to cyber security training firm InfoSec Institute. Because the recipient remains anonymous, criminals often request payment via the digital currency bitcoin, which can be exchanged online for traditional funds.

McKenna, Houlton's chief, said he believes the ransomware on his computer was unleashed when he clicked on an email attachment that appeared to be a price quote on some equipment the department was interested in buying.

"When I opened up the attachment, there was no quote," he said. "I thought that was strange."

The next time McKenna turned on his computer and tried to use it, he couldn't open certain files. A window popped up with a countdown timer that instructed him to send about $500 in bitcoin to a certain email address within the allotted time, or the price would go up significantly.

McKenna couldn't remember exactly how long he was given to decide, but that it was about three or four days. He immediately shut down the computer and unplugged it.

After consulting with his IT provider and the FBI, McKenna said he decided to pay the ransom because his computer contained a decade's worth of important information such as personnel files. McKenna said he intentionally did not place those files on the department's shared server, which is backed up regularly.

His own desktop was not. Now, McKenna said, he plans to back up his own hard drive every three days.

"It's opened our eyes, and we're going to change a lot of our policies as a result," he said.

CYBER EXTORTION HARD TO TRACE

Lawyer Anthony Perkins, co-chair of the Intellectual Property and Technology Group at Bernstein Shur in Portland, said cyber extortion is a serious crime that is difficult to enforce, because the perpetrators are usually in countries that don't cooperate with U.S. authorities.

It is not illegal to pay the ransom, Perkins said, but users should avoid paying if at all possible, such as if they have backup copies of their recent data.

"It may be the better part of valor to pay it and then move on … (but) it encourages that behavior over and over," he said.

Although it is possible that criminals are targeting law enforcement specifically, ransomware generally is spread via mass emailings that attempt to trick the recipients into opening a file or visiting a website that triggers the malware, said Edward Sihler, technical director of the Maine Cyber Security Cluster at the University of Southern Maine.

The amount of the ransom is purposefully kept low to make it affordable to most victims, he said. Most people and organizations tend to approach the question of whether to pay in terms of a cost-benefit analysis, Sihler said.

"You've got to ask, 'How much data can you afford to lose?' " he said.

In Lincoln County, Brackett and other county officials decided the encrypted information was too valuable to lose. The infected server not only held sheriff's office data, but also data for the various departments of four municipalities, including the Damariscotta Police Department.

Damariscotta Police Chief Ronald Young said police keep information about criminals, arrests, traffic stops, court dates and other pertinent topics on the county's server.

Young said the department managed to function during the two-day data freeze by writing everything down on paper. Once the ransom was paid, the computer systems returned to normal, he said.

"As far as I can tell, everything was working appropriately," Young said.

Brackett said all of the county's data was being backed up regularly, but the backup software had malfunctioned, and two months' worth of data would have been lost. After two days of wrestling with his conscience, Brackett said, he did what he believed he had to do.

“It was the lesser of two evils – I don’t know how else to say it,” he said.

Share
Read or Post Comments

Were you interviewed for this story? If so, please fill out our accuracy form.

Send questions/comments to the editors.