https://www.cbsnews.com/news/ransomware-how-cybercriminals-hold-data-hostage-why-the-best-solution-is-often-paying-a-ransom-60-minutes-2019-08-25/

C:\one Drive\60 minutes\08-25-19 1900 How Cyber Criminals Hold Data Hostage, often Paying.pdf

CBS News / CBS Evening News / CBS This Morning / 48 Hours / 60 Minutes / Sunday Morning / Face The Nation / CBSN Originals Log In S

EPISODES OVERTIME TOPICS THE TEAM SUBSCRIBE

HOW CYBERCRIMINALS HOLD DATA HOSTAGE... AND WHY THE BEST SOLUTION IS OFTEN PAYING A RANSOM

Targets have included hospitals and municipalities, but the FBI says anyone on the internet should expect to be attacked by cybercriminals

2019 AUG 25 CORRESPONDENT SCOTT PELLEY

RECENT SEGMENTS

Former N Tim Gree with ALS

What hap when cybercrir hold data

Who's res for the op epidemic

Cleaning plastic in

The tool hack any smartph

Twenty-two towns, counties and police departments in Texas are recovering after their computer systems were taken hostage just over a week ago. The state of Texas says the attacks, which happened simultaneously, were ransomware and the FBI is investigating. Ransomware locks up a victim's files until money is paid or the users find another way to recover their data. More and more, critical public service networks are the targets. Before Texas, the city governments of Newark, Atlanta and Baltimore were hit and San Francisco's transit authority; the Colorado Department of Transportation and Cleveland's airport. As we first reported in May, 26% of cities and counties say they fend off an attack on their networks every hour. Perhaps even worse, dozens of hospitals have been held hostage all across the country.

Ransomware: Prevent your computer from being infected

In January 2018, the night shift at Hancock Regional Hospital watched its computers crash with deepest apologies. The 100-bed facility in the suburbs of Indianapolis got its CEO, Steve Long, out of bed.

Steve Long: We had never been through this before. And it's something that I read in the journals. And I say, "Oh, those poor folks. I'm glad that's never going to happen to us." But when you come in and you see that the files on your computer have been renamed and all of the files were renamed either "we apologize for files" or "we're sorry." And there was a moment when I thought, "Well, maybe they're not so bad. They said they were sorry." But, in fact, they had encrypted every file that we had on our computers and on the network.

Steve Long

Long told 911 to divert emergency patients to a hospital 20 miles away. His staff turned to pen and paper. Nothing electronic could be trusted.

Steve Long: This is a ransomware, so this is a virus that has gotten into the computer system. "Would it have the ability to jump to a piece of clinical equipment? Could it jump to an IV pump? Could it jump to a ventilator? We needed a little time just to make sure about that."

But time was a luxury not offered in the ransom demand.

Steve Long: "Your network has been encrypted. If you would like to purchase the decryption keys, you have seven days to do so or your network files will be permanently deleted." And then it gave us the amount that we would need to pay to get that back.

Scott Pelley: And that came to?

Steve Long: About $55,000.

That was the same price demanded of the city of Leeds, Alabama, three weeks after Hancock Hospital. Mayor David Miller was surprised his town of 12,000 would be a target; not much to notice in Leeds, at least not since Charles Barkley graduated from the high school.

David Miller: I didn't know that this malware attack was actually a ransomware attack. As soon as we found that out, that took it to a little different level.

Scott Pelley: How do you mean?

David Miller: Well, it was going to cost us some money.

Mayor David Miller

Like the hospital, the city of Leeds was cast back into the age of paper: no email, no access to its personnel files or financial systems.

Scott Pelley: Can all companies and local governments expect to be attacked?

Mike Christman: I think everyone should expect to be attacked.

The FBI's Mike Christman says cybercrooks know governments and hospitals are likely to pay because they can't afford not to. Until his recent promotion, Christman was in charge of the FBI's cybercrime unit.

Scott Pelley: You're waiting for the day that somebody says, "We have the 911 system held hostage in a major city and we need $10 million today"?

Mike Christman: I hope that day never comes, but I think we should prepare for that possibility.

Christman says in 2017, 1,700 successful ransomware attacks were reported but he figures that's less than half. Most businesses, he says, would rather pay than admit they were hacked.

Mike Christman: I'm aware of one ransomware variant that affected all 50 states that had some $30 million in losses, and over $6 million in ransom payments. I would tell you that the losses are very significant, and easily approach a hundred million dollars or more just in the United States.

That ransomware variant he's talking about is the one that held Hancock Hospital hostage. It's called "SamSam" after one of its file names. Experts told Steve Long "SamSam" is unbreakable.

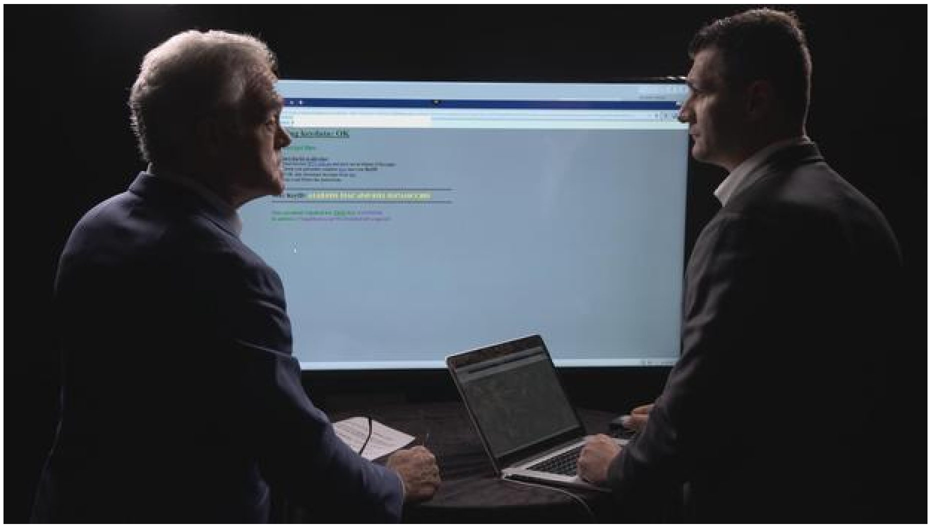
Steve Long: There was nothing that we could do to unlock those files. Our only choice was to wipe the system and hope that we had backups or to purchase the decryption keys.

Scott Pelley: To pay the ransom.

Steve Long: Indeed. That is exactly what that means.

@import
"data:text/css;base64,LyogdGhpcyBmaWxlIGlzIG9ubHkgbmVlZGVkIHdoaWxlIFVWUC5qcyBkb2VzIG5vdCBzdXB

Protect your computer from ransomware



Correspondent Scott Pelley with Tom Pace

Tom Pace is vice president of Blackberry-Cylance, a leading security firm.

Scott Pelley: So this isn't a crook sitting in front of a desktop, breaking a sweat, trying to break into somebody's system. This is something they unleash that's automated, and they sit back and drink coffee until they get the results?

Tom Pace: That's certainly appears to be the rule, not the exception.

Making the coffee may be the hard part. Pace showed us a website that offers ransomware for rent. An attacker can use one of many illicit products here and the website takes a cut if ransom is paid.

Tom Pace: And something else that's interesting here is they actually provide you with basically a chat room where you can ask questions to the people who maintain this architecture for you.

Scott Pelley: Frequently asked questions for criminals.

Tom Pace: Exactly.

Tom Pace logged on to the site and used it to encrypt a network of his own.

Tom Pace: So all of the files that are on this system have now been successfully encrypted.

Scott Pelley: So this took you just slightly over five minutes and you didn't write a single line of code?

Tom Pace: Correct.

Scott Pelley: Off the shelf.

Tom Pace: Off the shelf. Ready to go.

Pace told us ransoms are typically modest, like at Hancock Hospital or Leeds, Alabama, $50,000 or so.

Tom Pace: If you're asking for millions from everybody, that's just everybody doesn't have millions to pay, right? So, finding that sweet spot and sticking to it has worked well.

Scott Pelley: And that's why the same ransom was asked of little Leeds, Alabama and great big Atlanta?

Tom Pace: Correct.

Three weeks after Leeds, SamSam slipped into Atlanta's city hall.

Howard Shook is a councilman and chair of the finance committee.

Howard Shook: 911 was up and running. But for a while, the police did not have the ability to do computer checks on license plates and, you know, cars they were pulling up on and that kinda thing, which was a concern.

Scott Pelley: What else crashed?

Howard Shook: The court system went down, which was a major inconvenience for the thousands of people cycling through municipal court.

SamSam demanded $50,000, but Atlanta refused to pay. Instead, the city spent $20 million to recover on its own. It took months and seven years of police dashcam video was never recovered.

Scott Pelley: Why did you think paying was a bad idea?

Howard Shook: At first it was just instinctive. I mean, if you're being violated I don't know why you should reward somebody for having done that.

Scott Pelley: It must gall the hell out of some of your clients to pay the bad guys.

Tom Pace: Absolutely. I mean, we have lots of clients who are incredibly angry. I mean, you have to imagine this is, for many of them, the worst day of their professional career and sometimes their life.

A day made even worse by the occasional high end ransom. Pace told us one of his clients paid almost a million dollars. Another paid up after receiving this threat.

Tom Pace: "Would it not be a shame if we leaked all of your internal data about your clients and customers? Sounds to us like a large lawsuit waiting to happen." So, they're extorting them in two ways. They're extorting them by actually encrypting all the files. And then they're extorting them by threatening to also release the data.

Scott Pelley: Once this transaction is completed and the client gets his files back, how does he know he's not going to be attacked again?

Tom Pace: There's no way to really prove that he will not be. We try and do a really good job of making sure we reduce all the vulnerabilities and entry points. But there is no guarantee that they won't come back to the same organization that they just successfully impacted though we haven't seen that happen very often. Though it has happened.

Last year the Justice Department said it unmasked SamSam. A grand jury indicted two Iranians, neither named Sam.

The FBI says the two Iranian suspects were in it for the money, not espionage. They collected $6 million before they went quiet after the indictment. Prosecutors say the suspects are in Iran where they can't be extradited. The most threatening ransomware tends to come from countries including Russia that the FBI can't reach.

Mike Christman

Scott Pelley: Is cybercrime becoming to the FBI what banks were in the 1930s?

Mike Christman: I think it is. Cybercrime has really become a way of life and connected to everything we do, and really every, every crime we see. And I know that by 2020, we expect to see 50 billion devices worldwide connected to the internet.

Scott Pelley: So the question becomes at what point does this ransomware come to our phones, where some crook says, "I've got your phone. Send me 50 bucks"?

Mike Christman: I think it's already on the doorstep for that. I think some of those devices that connect to the internet can not only be compromised, but they can be used to facilitate other attacks under the command and control of bad actors.

Scott Pelley: This can be, "I have your phone, I have your car, I have your house"? Anything that's connected to the internet?

Mike Christman: Absolutely.

Produced by Henry Schuster. Associate producer, Rachael Morehouse.

Scott Pelley
Correspondent, "60 Minutes"

Search...