Long Island
BusinessNEWS
MAY 26-JUNE 1, 2017 | VOL. 64 | NO. 21 | $2.00 | LIBN.COM

GONE IN 60 MILLISECONDS

How hackers take companies hostage by 'ransomware,' and what's being done

By CLAUDE SOLNIK

Photo by Jenna Macri

COMPUTER CARE: LIBN Editor Joe Dowd talks with cyber security experts (L-R) Nicole Della Ragione, Peter DiSpirito and Nicholas Barone.

It was the kind of heist that might make a good movie or a TV series, only it was very much reality and not reality TV. There was no getaway car and no way to mark off the location with yellow crime scene tape.

A hacker with the Machiavellian moniker "thedarkoverlord" broke into Larson Productions' computers and stole the upcoming Season 5 of Netflix's Orange is the New Black. Next came the ransom request.

The Dark Overlord threatened to release the season if Netflix didn't pay the equivalent of $50,000 in bitcoin, an online currency.

Netflix refused and the hacker posted the season on Pirate Bay, a website urging viewers to hide their Internet address – and stream bit torrents.

While motorists are sometimes taken hostage on remote Third World roads, the most common hostage situations these days have been high-tech attacks on the Information Highway. The high-profile cases get international attention, but the problem has spread to Long Island companies who, in turn, have employed a new breed of security specialist.

Disney recently revealed it had been hit with a ransom request regarding the digital theft of a movie widely reported to be the latest installment in the Pirates of the Caribbean series.

And a virus known as "WannaCry" hit thousands of computers worldwide, leading to chaos in many countries on computers that hadn't used a Microsoft patch.

Hackers are causing electronic epidemics via ransom ware, software that shuts down servers or encrypts data until you pay for the cure.

They're also using phishing emails seemingly from co-workers and friends to get people to transfer money as the doors to data replace bank doors as targets for theft.

The Web really is the Wild West, but the most common targets have names of which you've never heard.

A Long Island medical practice's server was taken over and used to send malicious email around the world. A local accounting firm's electronic records, including its clients' data, were stolen.

"They got hacked. They are going through a tremendous amount of pain," Matt Brown, a vice president at IT and cyber security firm NST in East Northport, said. "They stole all their information. Every single one of their accounts received a letter that looked like it was from the IRS, asking them to call the number, asking them to finish their tax return."

The Big Breach

While big breaches make big news, the smaller ones, sometimes complete with ransom requests, may be the overlooked, if under reported, issue.

"Where is the next wave coming from? The big companies are aware of it," Nicholas Barone, a director in EisnerAmper's consulting services group, said. "We have a lot of small to middle-market companies. They have big issues in little companies. No one is immune."

Brown agreed that small and medium-sized businesses, if only because there are so many of them, are becoming prime hacking targets.

"I think those are the ones being attacked the most," Brown said. "Those are the ones where you see the phishing emails."

Small companies that do business with the government now must be certified as secure, leading them to hire IT firms to test and fix any flaws.

"They're being investigated like they're the enemy," Brown said. "Well, they could be."

All sorts of small companies are finding thieves attacking, and sometimes penetrating their systems. And sometimes, those "phishers" are leaving with a catch.

Barone mentioned a small medical practice with 30,000 patients whose records were stolen and whose server was taken over to attack Microsoft and eBay.

"Here is a three-doctor office practice," Barone said. "Suddenly, you're getting lawyers from Microsoft, Paypal and eBay saying your server is attacking us."

While medical information might seem of little value, medical records and healthcare billing are rife with valuable information beyond Social Security numbers.

"All that personal information a lot of times is used for prescription fraud. They can take this information and go in 25 different directions," Peter Maritato, professor of engineering, science and electrical technology at Suffolk County Community College, said. "You can get Social Security, credit card, health information, prescription information. You have everything in a one stop shop."

Hedge funds with only a few people managing billions of dollars also can prove sophisticated, if prime, targets.

"The SEC is concerned not about the big people, but the little people," Barone said. "The little people have access to billions of dollars under management."

Gone phishing

Although many systems may seem safe, Barone said hackers sometimes steal data when it's being transferred online from one source to another.

"For that brief moment moving it from one security environment to another, you see the content," Barone said. "That is the Achilles heel of the credit card industry."

Even if fire walls prevail, physical breaches also are possible. The data in a missing computer can prove to be worth more than its weight in gold.

"A simple lost computer can result in millions of names being exposed," Barone said. "There's the loss of an asset. That's just as important in cyber protection."

People can steal data on premises, whether it's the cleaning person, an HVAC maintenance person alone at night, the pizza delivery person or an employee.

Even though one school had some top cyber security staff, someone broke into the president's office and stole data by plugging a USB drive into his computer, Brown said.

"He worked in a locksmith's place," Brown said. "He jimmied the lock, put in a data sniffer on the secretary's computer, took it off and had every password."

Brown said the only reason he got caught was that he began ordering food at 2 a.m. through the president's computer.

Risky business

Possibly the worst thing, though, isn't just that data can be stolen. Even if it isn't taken, the cost of being breached can be massive, due to requirements to notify those affected.

"When we have a breach, when we know somebody has been in here, the question is how much information was stolen," Barone said. "You're guilty until proven innocent once in network."

Regulators have special requirements, adding more costs to notify those possibly affected and cure a breach in which it's impossible to determine the exact extent.

"The law compounds the expense and the loss and impact," Barone said. "They want to be protective, to protect everybody's data."

Risks are only likely to grow, as people spend more time on the Web – and electronic communications become more pervasive.

"Millenials are more likely to create data incidents. They were born to networks. They were born into this technology," Barone said. "Why does an insurance carrier ask how many miles you drive? The theory is the more miles you drive, the higher your risk."

Peter DiSpirito, Flushing Bank's chief information security officer, said hackers may penetrate a server – and essentially settle in for months – stealing data or using its web addresses to wreak havoc elsewhere.

"All you need to do is get in there at one point, find that data," DiSpirito said. "Nobody will know you're in for a year. Sift it out slowly."

Fighting back

Nobody thinks they'll be breached, even if computers are turning into a kind of mechanical Maginot Line. But the threat of shutting down a company, even without taking data, can be the equivalent of a potential fire or flood.

"Businesses don't understand the risk of operating on the Internet. They need to use a layered approach to security," DiSpirito said. "The threat landscape is continually evolving. The thieves are getting more sophisticated. A company needs to keep evolving their preventive measures."

Firms can use anti-malware, anti-spam and email filtering along with what DiSpirito called perimeter security, endpoint security, employees' security awareness and good risk analysis.

"We are transitioning our businesses to more of a security practice and doing the IT as an add-on," Brown said. "Typically we were always doing IT. Now we've slowly become security experts. Every single meeting I go to, whether it's an existing or a new account, security is the primary topic."

The Internet is a little bit like an Information Highway where everyone is speeding or where the limit is as fast as you can go. But you can reduce risk.

"We're still not at a point when we're thinking about how to fix this worldwide," Maritato said. "We can require this and this to be done. It's such a level of complexity."

Even cars have been hacked, which could become a bigger problem as software is used to drive vehicles. The Internet of things, meanwhile, is turning into a new horizon for hackers.

"It's been reactive," Maritato said. "Everybody thinks it's not going to happen to me. The Internet of things has gotten to the point where we have opened so many doorways."

Nations such as Russia and North Korea, criminals and mischief makers all hack, sometimes selling data to people who try to cash in. Governments, of course, also are being hacked: The next shot heard around the world may be fired electronically.

"We're living on borrowed time," Maritato said. "This may be the next world war."

Secrecy often envelops attacks: Firms don't want to admit what occurred. "It's very embarrassing for them to release they've been hacked," Maritato said of a law firm that was hit.

A kind of game of cat and mouse is going on. The problem, Maritato said, is that the hackers often seem to be one step ahead of the protectors. In other words, it's hard to tell who's the cat and who's the mouse.

"Whatever is built can be broken into," Maritato said. "If a system is built, it can be hacked."