Local attacks highlight growing trend of cyber crimes

Posted by Jason Johnson | Jul 31, 2019 | Bay Briefs | 0 | ★★★★★

As two local companies continue to address cyber attacks on their networks, police and security consultants say the number of calls they're receiving about similar digital crimes has increased.

Springhill Medical Center was the victim of a cyber attack earlier this month that has sidelined a significant portion of its network for weeks. Then last Friday, steel producer Blastech Mobile confirmed it had been hit with an attack that "severely impacted [its] systems and operations."

Since then, reports from employees of both companies have suggested these were attacks that used ransomware — a form of malicious software designed to block access to data and/or systems until a certain amount of money is paid. Both companies are said to be investigating the incidents, though neither has confirmed any details about the attacks.

Calls from Lagniappe seeking input from Blastech were not immediately returned, and, so far, Springhill has only commented to confirm there was some kind of cyber attack on its network, which was then shut down to "contain the incident and protect data."

Recommended Stories

Municipal heartburn only getting worse
By **Rob Holbert**

When 'First' and 'Third World' problems collide
By **Ashley Trice**

Thank you for 17 years of support!
By **Rob Holbert**

We need our own Eagle to land
By **Ashley Trice**

Ivey an empty suit on environment
By **Rob Holbert**

However, reports from some hospital employees and others in the local medical community have suggested ransomware has encrypted or locked the hospital out of much of its network and that many digital functions were — and possibly still are — being conducted on paper.

Those details have not been confirmed, and a spokesperson for Springhill Medical Center has not responded to requests from reporters seeking an update. However, as of July 29, the hospital's website still appeared to be offline, and law enforcement is still investigating.

Glenda Snodgrass, president and lead consultant of local technology consulting firm The Net Effect, said ransomware attacks have become "rampant" across the United States in recent years and have started targeting all sorts of businesses and even individuals in some cases.

"Ransomware that encrypts data (crypto ransomware) and demands large payments in electronic funds gets the most press attention, as those incidents usually occur in larger organizations, but simple lock-out ransomware is extremely common on home computers and small businesses," Snodgrass said. "There is no particular size or type of business. From three employees to thousands, and in every vertical market — accounting firms, law firms, credit unions, medical offices, retail stores, manufacturers, nonprofit organizations — you name it."

That's not just an anecdotal observation. Within the past week alone, there was a major attack on the Georgia Department of Public Safety's network, and Lousianna declared a state of emergency after three public school systems fell victim to malware attacks.

According to the Internet Crime Report released by the FBI, it received a total of 351,936 complaints in 2018. Those represent losses exceeding $2.7 billion — a $1.9 billion increase over the past four years of data. Not all cyber attacks are reported to law enforcement, either.

Some of those complaints were about ransomware attacks, but despite getting a lot of news coverage, those are not the most common type of cyber attack. Many lucrative attacks from recent years fall under a category known as Business Email Compromise.

Those attacks target companies by spoofing the emails of high-level employees, and in some cases, actually compromising and using a real address. This type of scam was used to attack the Alabama State Port Authority in 2017, which led to the release of employees' tax information, and the Mobile Housing Board (MHB) in 2018 — an incident that cost MHB more than $480,000.

Kevin Levy, commander of the Mobile Police Department (MPD) Cyber Intelligence Unit, said he's also seen an increase in reports of various cyber attacks locally, though he did say there is more outreach and awareness about cyber security today than in the past.

While complex cyber attacks are handled by the FBI or U.S. Secret Service, MPD is uniquely situated because it's a partner at the Gulf Coast Technology Center — a joint operations facility that brings local, federal and state law enforcement agencies together under one roof.

"We're actually able to triage and respond to network intrusions and other incidents," Levy said. "That doesn't mean we'd take the ball and run with an investigation because that depends on the type of case and jurisdiction, but we do have the capacity to respond."

Levy said a quick response can help secure evidence, and in cases where perpetrators send out thousands of emails in a mass phishing attack, it can allow time to warn similar businesses.

Another troubling trend recently has been cyber crime victims choosing to pay ransoms instead of waiting on police or security consultants to restore or decrypt their data. For a company losing $500,000 a day, a ransom may be cheaper than going weeks without access.

"Oftentimes we see companies choose to pay the ransom demands when they do not have the ability to recover critical data that allows them to restore business operations back to normal. In many cases, the company does not have proper backups in place to recover," Snodgrass said. "Even when good backups exist, the extent of the infection is sometimes so great that the cost of downtime during an extended restoration period is too high to bear."

Last month, two cities in Florida opted to pay a combined ransom of $1.1 million to attackers that compromised their networks with malware. To the contrary, the city of Atlanta spent more than $2 million recovering from a 2018 attack that initially only sought $50,000 in Bitcoin.

However, many caution against paying ransoms because they can fund future attacks by those same actors and motivate others. Levy also said paying large sums of untraceable money to anonymous sources on the internet isn't always a safe bet, either.

"It's negotiating with people you don't or shouldn't trust," he said. "What if they take the money and then don't release your data?"

Snodgrass said it's important for businesses to be proactive and informed about cyber security and suggested making sure all software, systems anti-malware programs are up to date and that critical data backed up, encrypted and stored off-site. She said it's also just as crucial for businesses to make sure employees are educated about the threat of potential cyber attacks.

"When that email with an attachment carrying a brand-new malware gets past your technical defenses and lands in an employee's inbox, but that employee decides the email is suspicious and doesn't open the infected attachment, they've just saved your company from an attack," Snodgrass said.

Cyber-security consultant Drake Brignac also worked with Lagniappe on this report.Ä Graphic: