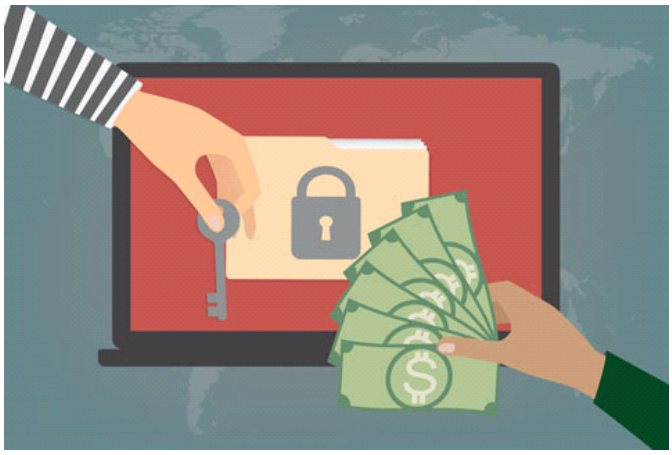
GROWERTALKS

Features

12/1/2020

Beware Ransomware

Chris Beytes



It was Super Bowl Sunday, February 2, 2020, a day the intruders assumed no one would be paying attention to the computer systems, when the first signs of the attack appeared. Information Technology (IT) staff from Ball Horticultural Company had done their monthly maintenance the night before. But around noon on Sunday, monitoring the system as they routinely do, they noticed some of the servers "misbehaving," as Chief Information Officer Mark Morris put it. So they investigated.

"We just assumed something went wrong during our maintenance on Saturday night," Mark recalls.

By the first quarter of the game, they knew it was not a glitch; it was some sort of malicious virus attack.

As part of Ball's cybersecurity planning, they had contracted with an Emergency Incident Response firm, a team of experts who, in the event of a disaster, would work with Ball's IT staff to recover their systems from backups. By halftime, they'd locked down the entire computer system so they could isolate the problem and prevent it from getting worse. By late that night, while the Chiefs were celebrating their win over the 49ers, they were even starting to bring a few systems back online.

But the damage had been widespread. The virus had completely encrypted the primary servers, as well as their remote backup disaster recovery facility. It impacted all business applications, including email, phones, Ball's WebTrack e-commerce platform, several remote locations and cloud applications … pretty much any system tied in to the "mothership" in West Chicago, Illinois.

As it turns out, the virus was a ransomware attack, specifically, the MedusaLocker virus.

"Literally, we saw the screens where they were asking for a certain amount of money and holding us ransom," Mark says.

MedusaLocker is a relatively new ransomware virus, but one that operates similarly to most others, encrypting computer data and requiring the victim to pay a ransom to get a decryptor key. They believe the hackers found an older, vulnerable machine somewhere in a greenhouse at one of their offshore farms. But to get into that machine,

they needed access, and the forensics team that studied the incident thinks the attack was the result of an employee's account being compromised due to a phishing attempt—an email requesting information or asking you to click on a link.

Thankfully, Ball had planned ahead; they had an emergency plan in place. They had experts on standby. They had backups of all their computer systems (and backups of the backups). They had a continuity plan in place for doing sales, inventory and all other business functions manually, without computers. This planning, plus tremendous efforts from employees, ensured that Ball kept taking and shipping orders even while systems were being recovered.

And they had cyber insurance. That company brought in their own "SWAT team" of experts Monday morning, one of whom "negotiated" with the hacker while the team worked on recovering the systems. They also provided legal advice.

Just two days later, Ball had virtually all of its systems up and running, with every device at every location around the world equipped with the latest antivirus software.

Oh, and they did not pay the ransom.

Why you should worry

Unfortunately, Ball's story isn't unique. Estimates are that that a business is attacked by a cybercriminal every 11 seconds, with damage costs from these attacks expected to reach $20 billion by 2021. And while many of these attacks target municipalities and health care providers, 20% of ransomware victims are small and medium-sized businesses. Several other horticultural firms beside Ball have been recent victims of ransomware.

Why did Ball want to share their story?

"Because the harsh reality is that it's not only possible, but it's likely to happen to everybody," Mark answered. "It's just a question of when, and how it impacts you, and how prepared you are to react to it."

Think about old computers that might be in your office or in a corner of a greenhouse, Mark says, running an old version of Windows and without current virus protection.

"Those are the very sorts of openings these guys look for, that let them get into the network and start these attacks," Mark points out.

Mark lists several things you can do to help protect your business from a cyberattack and to help bring your systems back online if one occurs.

The first is having up-to-date computers running up-to-date virus protection software. Internet providers offer basic protection and at a minimum you should talk to your carrier to see what sort of protection they offer, he says. But he adds that it's worth the investment to find a local IT person or company to give you some personalized advice about protecting your particular computer network.

Firewalls and virus protection software are essential, "but you can spend hundreds of thousands on that, and if you have one employee click a link, it's all for naught," Mark says. That's why the second step in cybersecurity is staff training.

"The FBI said when they looked at our case that, more than likely, somebody clicked on a link and gave [the hacker] access to the system. People, at the end of the day, are the weakest link," he said.

Ball does routine cyber safety training for its staff on how to recognize suspicious emails. They also send out test phishing emails. Any employee who falls for one is in for extra training.

An added layer of protection is cyber insurance (see sidebar). In addition to the IT and legal resources provided during the attack, the insurance company's experts looked over the upgrades to the system after the event to make sure it was secure against a future attack.

Have a continuity plan for running your business without your computer system in case you incur an extended computer system outage. In a larger operation, have each of your departments develop such a plan. Maintain a call list for your managers, facilities crew and employees who you'll need to contact during an emergency. Include personal email addresses and phone numbers. This should be on paper so it's accessible even if you have no computer or email.

Lastly, never let down your guard, says Mark.

"Unfortunately, as quickly as we come up with new virus protection and backup strategies, the thieves are out there trying to beat us and find a way in."

Cyber Insurance

"It doesn't matter whether you're a garden center, greenhouse grower, landscaper or retail florist, data breaches will always be an ongoing threat to your business," warns Dan Zastava, Director of Corporate Underwriting & Product Development for Sentry Insurance, which provides insurance solutions to horticulture businesses through its Hortica brand. Sentry offers specialized cyber insurance coverage for a wide range of threats, from ransomware to "fraudulent impersonation," which happens when a cyber attacker impersonates a vendor, making them appear legitimate, says Dan.

"They'll then ask a member of your team to adjust a payment process related to a bank or routing number," he explained. "If the impersonator is successful, you may be sending funds to what you thought was your vendor, only to find out later (when the real vendor calls and asks why your payment is overdue) that the money was sent elsewhere."

Although cyber insurance has been available for several years, it's not standardized across the industry. One carrier may provide broad coverage, while another carrier may offer a narrower scope.

While the coverage terms may vary, cyber insurance will typically respond in computer security events where a third-party hacker is able to infiltrate your computer system. Following are some of the more common coverage offerings today:

• The cost of a cyber forensic analyst to determine how the hacker got into the system and what data was accessed

• The services of an attorney to identify state-by-state notification requirements pertaining to an individual's personally identifiable information being exposed

• The use of a public relations firm

• Liability coverage, if you're sued as the result of a covered breach event

• Payment card industry fines or penalties

• Business interruption

• The physical loss of sensitive information such as HR files

• Cyber extortion (ransomware)

• Social engineering (phishing) and fraudulent impersonation

Your carrier may also have tools and resources to help you reduce your risks, such as response plan templates, webinars, training modules and federal- or state-specific information that horticulture businesses should be aware of.

Lest you think your business is too small to justify a cyber insurance policy, Dan says if your small businesses doesn't have an IT department to identify and address a cyberattack, your insurance company can help you secure such services, typically at lower negotiated rates than you could on your own.

Todd Frauendorfer, Treasurer of Ball Horticultural Company, stated, "As with most insurance policies, one of the biggest benefits is access to experts when something goes wrong. Even a policy with low limits and high deductibles can be of great value. Most insurance companies have negotiated lower rates with attorneys, IT professionals and other experts. In the end, it can save you time and money."

Just as important, the claims team can assist you with navigating what can be an emotional time for a small business owner. To that end, business interruption coverage related to cyber incidents can assist the business owner with replacing some of the lost profits associated with a covered event.

Costs will vary by each carrier, but it's usually based on several factors, such as the size of the company, the controls that they've established, the industry sector they're in, and the level of coverage and limit they're seeking.

As we all look to the future, the level of reliance on Internet and connected devices will continue increasing, which only creates more exposures for horticulture businesses, large and small. That's why Dan suggests that all horticulture businesses explore the option of adding cyber coverage.

"The results of a data breach can be costly and have lasting impacts on your business, so it's important to have that additional protection that many standard property or liability policies may not cover." **GT**