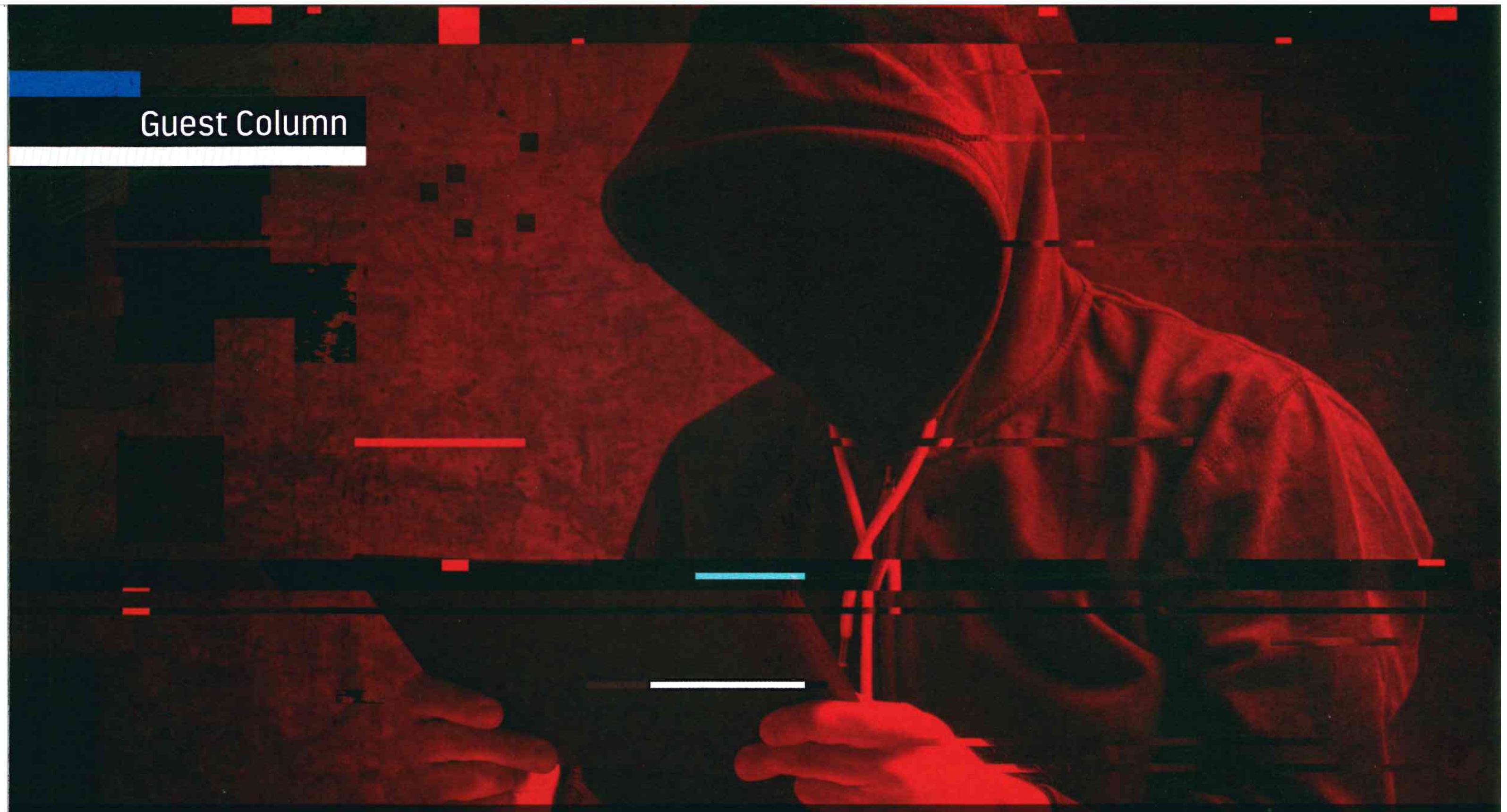
Guest Column



Ransomware *on the Rise*

by Barry Miller and Curt Graham, Mazanec, Raskin & Ryder Co., LPA

The message on your computer seems friendly — almost as if it were offering help. "Your data has been encrypted," it says. "But don't worry; it can be decrypted. All you need is a decryption key, which we are happy to sell you."

That message means the computer has been infected by ransomware, a type of software attack that is decidedly unfriendly, as it holds the user's data hostage for ransom. Users across the country have learned that the intent behind the message is anything but friendly. That includes local governments. Kentucky cities can take warning from their counterparts in other states, especially Ohio, which has been particularly hard hit in the past few years:

- In January, all government offices in Licking County, Ohio — 1,000 computers and a dozen servers — were shut down for nearly two weeks while the county determined whether it would pay the $31,000 ransom hackers demanded. The county ultimately decided that its backups were sufficient to rebuild its electronic records, which it did at the cost of more than $50,000 ($25,000 of which the county paid as a deductible on its cyber insurance policy).
- In April 2016, a fiscal officer in Vernon Township opened an email that was made to look like one from a shipping company. When she opened the email, the ransomware installed itself. The program demanded $200 for a decryption key, but because the township had good backups, it was able to restore the data.
- In October 2016, a ransomware attack affected as many as 17,000 voter records in Henry County, Ohio.
- A county court in eastern Ohio paid a $2,500 ransom to unlock its data because it did not have usable backups.

Kentucky is not immune to this alarming trend. In March, Methodist Hospital in Henderson declared itself in a state of emergency after an attack lasting five days. The hospital resolved the situation without paying hackers, but according to Mike Sunseri, deputy director of the Kentucky Office of Homeland Security, that experience may be an exception. "The bottom line is that these kinds of attacks are going to become more common because people are paying the ransom," Sunseri said.

He also related that a chain of hospitals in Kentucky, Virginia and West Virginia sustained ransomware attacks last year that left some of them resorting to pen and paper to do their work, reducing effectiveness to 20 percent.

Ransomware has evolved from spam attacks, broadcast to a large number of users, demanding $200 to $300. Many ransomware attacks are more targeted now and also demand more money. Hospitals were a logical target for such attacks because of the kind of work they do and their dependence on computer systems holding patient data. "There is a sense of urgency when lives are on the line," Sunseri said.

Because they hold sensitive information in their computer systems, and because they provide critical services, city governments and other local agencies are also logical targets for such attacks. "How long can your fire department be down?" asked Dave Mims, CEO and founder of Sophicity, an information technology company that partners with the Kentucky League of Cities. "How long can a city continue to offer electric service if it can't send out its utility bills?"

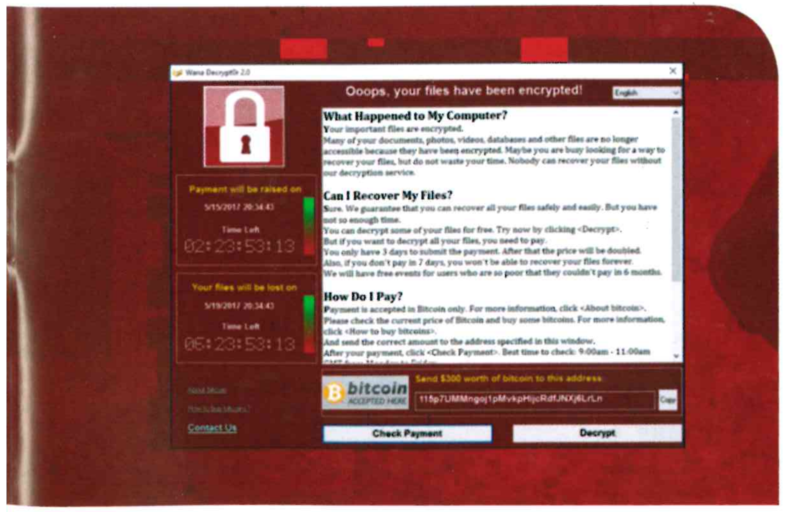
Because of budget constraints, local governments (especially smaller ones) may depend on legacy computer systems, which are more susceptible to all types of cyberattacks, including ransomware. The WannaCry Ransomware attack, first reported on May 12, 2017, affected more than 300,000 computers by the end of that month. That malware was built to take advantage of a vulnerability in older Windows operating systems.

How Does Ransomware Work?

Ransomware is most commonly distributed by emails that try to induce readers to click on a link — such as the "shipping" email sent to the Vernon Township fiscal officer. The type of deceit often depends on the season. Emails from purported shipping companies or retailers will often hit during the Christmas holidays. Others claiming to be from the Internal Revenue Service or accountants are prevalent in the weeks before April 15.

A user who clicks on a link or opens an attachment from one of these emails causes the download of an exploit kit, which installs ransomware on the affected computer. Once that installation is complete, the user is presented with a screen like the one below (from the WannaCry ransomware), which effectively is the ransom note.

This screen demands a $300 payment for the decryption key. A typical feature of ransom screens is the countdown, as shown on the left-hand side of the pictured screen. It tells the victim when the initial demand will double after the countdown expires. A second countdown tells the victim when the files will be locked forever.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 20:34:43
Time Left
02:23:53:13

Your files will be lost on
5/19/2017 20:34:43
Time Left
06:23:53:13

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Ransomware is a program loaded on victims' computers via a phishing email or by exploiting vulnerabilities in the computer's operating system. Once loaded and executed, the ransomware encodes files on the affected computer, locking them from use. The data can only be made readable again by using the correct decryption key. The ransomware will also try to propagate itself onto networks to which an affected computer connects.

One logistical issue is that the demand usually requires payment in Bitcoin, an untraceable digital currency that is not backed by any government or central bank. A victim who decides to pay the ransom must figure out how to obtain and transfer Bitcoin.

Who Is Behind Ransomware?

Ransomware programs generally are written by overseas criminal enterprises, most often Russian and Eastern European. Those enterprises sell software kits to would-be extortionists, sometimes for a nominal amount but usually for a price that includes a percentage of the ransom the buyer can harvest. The buyers of the software are responsible for its distribution. The enterprises that sell the software compete on features and even on "customer service" they provide to the victims who download their product. (Some versions of ransomware may even offer a reduced ransom to victims who leave a positive review of their experience.)

In a strange way, the success of ransomware is built on trust — the victims' belief that if they pay the ransom, they actually will receive a key that will decrypt their files and allow the victims to regain access to their data. Because the typical ransom demand is relatively small, the distributors are relying on receiving many such payments, which will not happen if it becomes known that they do not deliver what they promise upon payment.

But there is no guarantee that if you pay the ransom, you will regain access to your data. The perpetrators of WannaCry have been unable to distribute decryption keys fast enough to meet demand. Other ransomware hackers simply never have any intention of returning the data. Even if they do, Mims warned, there is no guarantee the data will be accurate. And Sunseri added that there also is no guarantee that, even if they return your data, hackers won't build a back door into your computer network. So paying ransom is not without risk.

Still, some take that risk because the larger risk of being without access to their data is more worrisome. Sunseri understands that. "Our general position is we never encourage anyone to pay the ransom, but it is always the choice of the individual or organization," he said.

How Can I Protect Against Ransomware?

Ransomware is most often introduced into a computer or network via email, when a user clicks on a link or opens a document that causes the computer to download malware. But WannaCry illustrates that defending against ransomware attacks is not a matter of adopting a single strategy. While it can be initiated through an email, once within a network, it attacks connected machines without requiring users to open attachments or click links.

So dealing with ransomware involves more than one strategy.

Educate Users

Teach computer users to be very wary of emails that contain links and attachments. Emails claiming that the reader may be the beneficiary from the death of an overseas prince are no longer the concern. Today's phishing emails are more sophisticated and are designed to reach users at times when they may be most susceptible to clicking on a link, such as the Christmas shipping email. Users must be constantly vigilant and should never click a link or open an attachment if there is the slightest doubt about where the email came from or without verifying the sender's email address.

Bitcoin was created by an anonymous internet user in 2009. This "cryptocurrency" can be used to purchase a variety of goods online, and the number of merchants accepting Bitcoin increases by the day. Notably, Bitcoin can also be transferred from one person to the next anonymously.

Owners keep Bitcoins in a digital wallet. They can spend them on online, or they can trade their Bitcoins on exchanges. All Bitcoin transactions are recorded in a "blockchain," an online ledger that verifies each transaction's validity. Some collectors are holding Bitcoin, hoping the value of this cryptocurrency increases. The market is volatile. As of the writing of this article, a single Bitcoin is worth more than $2,000 (up from a 2016 high of $807). Although the price fluctuates, Bitcoin is designed to be insulated from inflation as the supply of Bitcoin is limited to 21 million.

The ability to transfer Bitcoins anonymously has led to it being the currency of choice for cybercriminals and for ransomware hackers. Cybercriminals need not worry about the payment being traced back to them. Payments between citizens of different countries is simplified because Bitcoins are not tied to any country's currency. Currently, Bitcoins are also effectively unregulated, meaning we are in the Wild West phase of Bitcoin's existence.

> Ransomware or other invasive malware cannot spread to other parts of a network if there is no communication between them. Instruct your IT department or vendor to employ network segmentation.

Keep Computer Software Up to Date

WannaCry attacked a vulnerability in Microsoft's Windows operating systems. Microsoft distributed a patch aimed at closing this vulnerability in March. The worm did not affect users who installed the patch. Microsoft has been criticized for its initial response to users of older Windows versions. Although it eventually distributed free patches to these users (Microsoft normally charges for the support of older versions of its software), that move came too late for some to protect themselves against WannaCry. Updating from older versions of software and timely applying patches (or setting up automatic patching) will help protect against similar attacks.

Test Your Systems

Cities can check the status of their systems and try to find (and remedy) vulnerabilities before hackers exploit them. Commercial vendors offer "penetration testing," where the vendor tries to infiltrate a computer network just as a hacker would. Hackers often begin their efforts by social engineering, calling users at an organization and trying to get information from them that can be used to gain access to a network. Security vendors can also try social engineering techniques to pinpoint users who may give up such information.

Kentucky offers assistance to cities and local government organizations, including free penetration testing, said Jason Childers, director of the Kentucky Intelligence Fusion Center (KIFC). The KIFC is a collaborative effort of the Office of Homeland Security, Kentucky State Police, and other state and federal agencies. Through a partnership with federal agencies, the Kentucky Office of Homeland Security can assist cities in performing a "cyber resilience review" of their computer systems.

Childers also noted that the Office of Homeland Security is part of the recently formed Kentucky Cyber Threat Working Group, which meets to discuss current threats and means of dealing with them. The working group meets at 1:00 p.m. on the second Monday of every month. Any city interested in sending a representative to the meeting can contact Childers at 502.564.2081 or at jason.childers@ky.gov.

Segment Networks

Not all parts of your network need to be in communication with each other at all times, Childers said. Ransomware or other invasive malware cannot spread to other parts of a network if there is no communication between them. Instruct your IT department or vendor to employ network segmentation.

Back Up Data

The ability of a ransomware victim to avoid paying ransom depends on how well the victim's computer systems are backed up. Through its partnership with KLC, Sophicity offers IT in a Box, which provides several services, including data backups and off-site data storage. Both can be critical in restoring computer systems without paying ransom. On-site backups will help a city recreate its data more quickly. Off-site backups may take longer but are part of a disaster response strategy, in the event a city's on-site backups are destroyed. "Other than someone's life being in jeopardy, data backup is our first priority," Mims said.

Share Risk by Insuring Against Cyberattacks

Traditional insurance products, such as a commercial general liability policy, or a public officials liability policy, generally do not cover cyber-related issues, such as ransomware attacks. But insurers now offer specific policies for cyber risks. KLC includes cyber coverage via an endorsement to its current policies. Other carriers offer cybersecurity insurance via separate polices. Whether the victim of a ransomware attack chooses to pay the ransom or to restore data, costs are associated with either choice. The right cyber insurance policy can pay or defray those costs and offer other resources for getting the insured back to full efficiency.

The difference between a natural disaster and a ransomware attack is that the latter is more predictable. "To think you're safe, that's false security," Mims said. "Ransomware is getting bigger because it's a huge moneymaker for bad guys."

If you are a victim of ransomware or any other kind of computer breach, Sunseri recommends immediately contacting the Kentucky Office of Homeland Security. "We have a system of resources through the state and federal agencies that can help." KC

About the Authors

Barry Miller

Curtis Graham

Barry Miller and Curtis Graham are attorneys with Mazanec, Raskin & Ryder, L.P.A, Lexington, which supports KLC through its awards program sponsorship.

Miller's practice focuses on insurance coverage opinions and litigation, including coverage issues related to municipal liability, bad faith and extra-contractual damages, and data management and cyber security law. He has considerable experience handling technology issues involving data breach defense and electronic discovery as well. He regularly provides instruction and counsel to a variety of groups, including attorneys and business owners, regarding preservation of digital evidence and insurance aspects of cyberliability. In 2017, he earned his accreditation as a Certified Information Privacy Professional/United States (CIPP/US), credentialed through the International Association of Privacy Professionals (IAPP). Contact: bmiller@mrrlaw.com or 859.899.8513.

Graham focuses his practice on civil rights and governmental liability issues, including the representation of police officers, municipalities, correctional institutions and city officials. In addition to his representation of governments and government officials, Graham is experienced in all aspects of insurance litigation, ranging from coverage and bad faith disputes to insurance defense litigation. He has also handled matters of commercial law, subrogation, collections, data security and cybersecurity law. Contact: cgraham@mrrlaw.com or 859.899.8516.