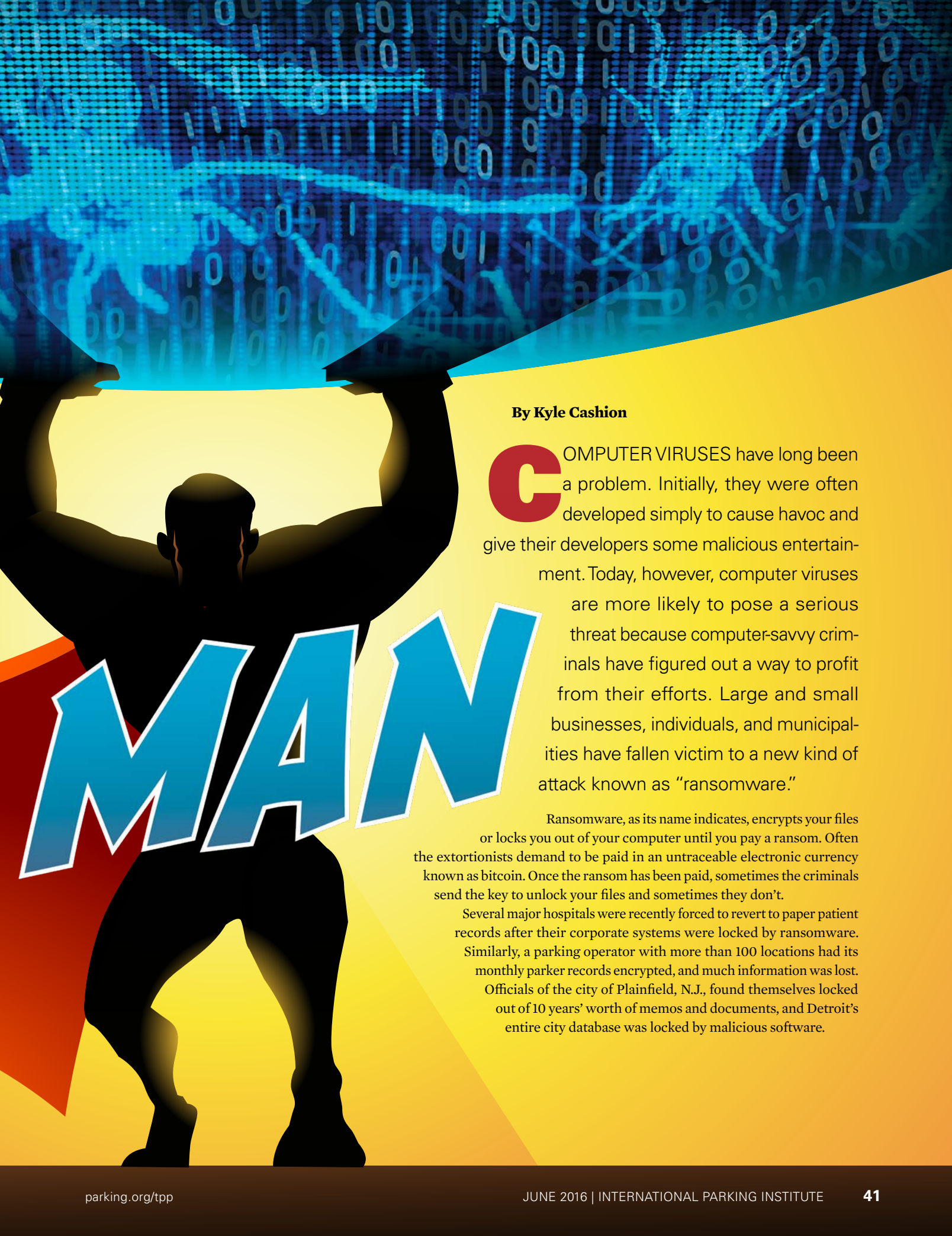




Becoming **CYBER-SUPER**

How to transform into a superhero and battle back evil (and dangerous) ransomware.



By Kyle Cashion

COMPUTER VIRUSES have long been a problem. Initially, they were often developed simply to cause havoc and give their developers some malicious entertainment. Today, however, computer viruses are more likely to pose a serious threat because computer-savvy criminals have figured out a way to profit from their efforts. Large and small businesses, individuals, and municipalities have fallen victim to a new kind of attack known as “ransomware.”

Ransomware, as its name indicates, encrypts your files or locks you out of your computer until you pay a ransom. Often the extortionists demand to be paid in an untraceable electronic currency known as bitcoin. Once the ransom has been paid, sometimes the criminals send the key to unlock your files and sometimes they don't.

Several major hospitals were recently forced to revert to paper patient records after their corporate systems were locked by ransomware. Similarly, a parking operator with more than 100 locations had its monthly parker records encrypted, and much information was lost. Officials of the city of Plainfield, N.J., found themselves locked out of 10 years' worth of memos and documents, and Detroit's entire city database was locked by malicious software.



According to the FBI, the Bureau received more than 2,400 complaints concerning ransomware in 2015; it is suspected that most victims don't bother reporting the crime. The threat is so serious that the U.S. Department of Homeland Security and the Canadian Cyber Incident Response Centre recently released a joint alert (TA16-091A) to help educate the public.

Ransomware is often spread via malicious attachments to an email, but a computer may also be infected by visiting a website. Ransomware attacks on smartphones are not yet common but do exist. These devices are most often infected when the user opens an app that pretends to be helpful but actually contains malicious programming.

Don the Costume

The most important protection is training your employees: Teach them not to click links or open attachments in unsolicited emails and to beware even of emails that appear to be legitimate. Before clicking a link, they should always check to see where the link will actually take them. Most email clients display the destination, known as a URL, most often at the bottom of the client or browser screen. If the URL doesn't match what you expect, assume it's a trap.

Teach employees not to enable macros in attached documents. One malicious program, known as Locky, is transmitted as an email attachment. The email advises you to enable macros if the data in the document don't look correct. However, the macro actually downloads the ransomware, which then encrypts your files and demands payment.

Train employees to use a healthy sense of skepticism before clicking any "You've got to see this" or "You won't believe this" link. These are called clickbait, and malicious websites often lurk behind them.

Shields Up

There are internet services that offer their opinion of whether a website is safe to use or not. Search for "reputation services malware" to find several companies that offer analysis of whether a website is a known host of ransomware or viruses.

Finally, teach employees to scan all attachments with antivirus software before opening them. Antivirus software, at least at the moment, is not tremendously successful at catching ransomware, but the situation is improving. Regardless of whether it detects a ransomware attack, scanning attachments will often stop other viruses.

Avoiding Kryptonite

In addition to employee training, there are several technical protections that your organization should employ:

- Use a script blocker in your web browser so websites can't run scripts in your browser or download programs unless you allow it. NoScript is a popular add-on for Firefox, and there are several popular blockers for the Chrome browser. Script blockers may be a bit of an annoyance until you build up the whitelist of sites that you allow but are well worth it for the trouble they prevent.
- Configure your email server to block dangerous types of email attachments, such as program files (those with an extension of .exe, .com, and .bat) and password-protected .zip files. Be certain your blocking software checks the actual content type of the attachments, not just the file type as indicated by the extension on the file name.
- Keep your operating system, antivirus program, and

The most important protection is training your employees: Teach them not to click links or open attachments in unsolicited emails and to beware even of emails that appear to be legitimate.

- firewalls patched with the latest updates. Your operating system and antivirus software should be allowed to update themselves automatically. Manufacturers regularly post updates to address newly discovered security threats.
- Restrict users to be able to access only the parts of your corporate servers that they need to do their job. Often in a small to medium-size business, it's easy to simply grant users access to the entire server rather than the drives and folders they actually need. Only the portion of a server that the user can see is in danger of being infected by them.
 - People who work as administrators for your server should have two logins: one for tasks that require administrative access and one for regular work. Only use the administrative login when doing something that absolutely requires it.
 - Use strong passwords for logins. There is some debate about the effectiveness of changing your passwords often, given that people tend to repeat the same patterns in their passwords. However, there's no doubt that using a strong password (at least eight characters, including upper and lower case letters plus at least one number and a special character) makes it much more difficult for your systems to be compromised.
 - Restrict physical access to your servers. Ransomware and viruses can be spread to a computer simply by inserting a thumb drive (USB stick) into one of its ports.
 - Consider restricting employees to using only work-related websites from work devices. This is often controversial, but a work computer is the property of the company and its use should be covered by your employee handbook. It is also possible to configure your firewall to prohibit connections to sites that are suspected of delivering malware.
 - Require that employees who bring their own computers from home must use the company-approved antivirus software and ensure it is up to date.

Heroes Back Up

It is impossible to overstate the value of backup and recovery plans. If your systems are compromised by

ransomware or a virus, your business' future is dependent upon the quality of your backups and the ability to recover using them.

Backups should be made both regularly and offline. For most operations, it's not possible from a practical standpoint to back up everything every day. This means you have to decide the length of time you're willing to recreate data for, and that determines how often you back up the data. This time will likely vary based on the type of data.

Backups should be made to media that is normally not accessible to users. This prevents your backups from being locked by ransomware. Additionally, making your backups to media that is offsite, either in the cloud or on media that you physically remove from the main office, protects you in the event of fire or flood.

Do not just depend on the operating system to create shadow copies of your important files. On a Windows server, the Volume Snapshot Service can automatically create a backup of a file, but this does you no good if the backup only contains files that have already been encrypted by ransomware.

A final note about backups: Encrypt them. Then you don't have to worry about the backup falling into the wrong hands.


Back at the Batcave

Make and test your recovery plan: Your IT support staff should document the backup procedures and the steps to recover your servers and data from these backups. These plans should begin with a list of all the applications that your staff uses, where the data for those applications is stored, how often this data should be backed up, and how long the backups should be kept.

The only way to verify that your backups can be read and that they contain all the information you need to recover from an infection is to test the plan. Have your staff pretend that the hard drive on the server has crashed, no data from it is recoverable, and that they have to restore your application and data from a backup. Tests like this often reveal the gaps in backup plans, starting with the failure to know how to reinstall applications if need be.

When Bad Guys Get Through

If your data is locked by ransomware, the FBI and many security firms recommend that you not pay the ransom. There's no guarantee that the criminals will give you access to your data, and paying them supports their so-called business. However, if you don't have a backup and the data is important to your business, it will be very tempting to pay and hope.

Your best bet is to train your users to reduce the chances of infection, then back up securely and often. An ounce of prevention is worth many pounds of cure. 



KYLE CASHION is a principal of IntegraPark, LLC. He can be reached at kyle.cashion@integrapark.com.