RANSOMWARE PROTECTION FOR MAC AND iOS

By Victoria L. Herring

Ransomware has been in the news lately, and, unfortunately, it already may have affected some of this article's readers. In a ransomware attack, malware is placed on a computer or in a network—through human error or owing to an intentional breach from a nefarious actor—locking up the computer or network by encrypting the data. A message arrives to pay the demanded amount or the lock will stay in place and the computer owner will lose the data. And the possibility exists that even if the ransom is paid, the lock will remain in place and the data will be lost forever.

iStock

For this reason, it is important *not* to pay the ransom. There is no guarantee you will get the encryption keys, and there is no way to trace any money sent with either Bitcoin or Green Dot cards (electronic payment methods). Those who rely on computerized data and records must take strong actions in advance of receiving a ransom message, not only to foil the criminal but to protect their systems.

Although it doesn't happen often, Apple devices can be subject to ransomware just as Windows-based PCs are. KeRanger was the first ransomware that attacked Apple devices. The attackers accomplished this by wrapping KeRanger into an installer for an application called Transmission, which is widely available free of charge. Apple does have some protections to keep us safe, the most prominent being the Mac App Store itself. If you download all your software from the App Store, there is little chance it is infected with malware because Apple screens both the software and the developers. Apple also uses a program called Gatekeeper, which scans new executable software for certificates and known developers. Gatekeeper didn't catch KeRanger immediately because of the way the malware used Transmission's valid certificate. This compromise didn't come from the App Store but the vendor's website directly. The attackers compromised the website, and a malicious file download was signed with a valid certificate (at the time). Apple was able to quickly stop the spread by revoking the certificate. Be leery of downloading any software from unknown sources, and always check the App Store first to see if you can get what you need there.

Apple or Mac machines can also be infected by malware or ransomware from Windows-based PCs connected to the same network and sharing the same files. An infection on a PC will spread to the shared files, causing an inability to access the data. The Mac itself may not be affected, but it can't get the data, and it might just spread the infection to others.

How do we combat this? My own practice is to never, never, *never* click on a link in an e-mail. Instead, I go to the original website and sign in. If you are using Mail on a Mac, you can safely click the caret to the far right of a link or URL, and it will show you a preview. It is rarely unwise to be overly cautious.

I also use Sophos (sophos.com) software on my machines, which monitors whether the websites I'm signing into are legitimate or not and keeps an eye on malicious attachments and sites. Sophos also produces general anti-virus software. Best practice dictates that all machines used in a work environment should have an anti-virus scan done at least weekly.

These measures can help protect you, but they may not do so entirely because you will at some point click on a link without thinking—assuming it's a message from your child, your spouse, or a trusted entity—only to find out it's a fake. I even get e-mails purportedly from Apple that initially look legitimate but that I know are not because of the e-mail address to which they are directed or other clues.

Because of threats such as malware, ransomware, social engineering, and simply human nature, backups are essential. Yes, backups can be infected with malware and ransomware, and in a networked system this is a major issue. However, if you maintain backed-up data on at least three different types of media and keep one copy at a different location, that's the safest backup method possible.

The different types of media needed for effective backups include external hard drives, online (cloud) backups, DVDs, and a NAS (network attached server). I have Time Machine (incremental backup software included with all macOS computers) back up to a hard drive connected to my main computer; SuperDuper! (shirt-pocket.com) bootable backup software that runs weekly to an external hard drive; and regular ongoing cloud backups via CrashPlan (crashplan.com). There are other pieces of software or services similar to these; do your own research before adopting anything. No matter what, make sure you understand them and use them religiously.

The off-location backup might be a physical drive moved to a safety deposit box or your home, or it could be a cloud backup at a data center. The idea is to have a copy of your data in a separate location from your computers in case a catastrophic event physically damages your systems.

A backup that is bootable is preferable and can save you much inconvenience when a tragedy occurs. When your main drive is infected or crashes, you can just boot from the bootable drive and operate temporarily from that clean drive until you repair the main problem.

With small businesses increasingly becoming more reliant on computers, and lawyers especially using them to save and scan documents, retain depositions in digital format, keep financial records in digital format, and avoid using paper, it is essential to have solid backups. Small businesses and small law firms using Apple computers can rely on Time Machine and a separate backup to a local NAS or external hard drives as a good first layer of defense.

John Moder of Crisp Solutions, LLC, suggests that in larger environments (i.e., with more than five users of computers on a network), time and storage space may be saved by just backing up the desktop folder and documents folders of each computer. In that circumstance, if there is an infection or catastrophic event, he can rebuild or replace everything else relatively easily.

There are more expensive and highly reliable methods of data protection available. John indicates that one is called Datto (datto.com), which is a hybrid onsite device with cloud-based replication. It is an industry-leading disaster recovery and backup solution. As a computer consultant to small business, he builds out custom solutions that are tailored to the client and to avoid overkill.

This whole discussion has been somewhat focused on Mac computers as opposed to iOS devices (iPhone, iPad, etc.). It's essential to protect yourself from infections of these devices as well. Evaluating what data on an iOS device needs to be backed up is important, especially because these devices rely mostly on backing up to cloud services. Cloud services can get infected, but there are many more precautions installed on these solutions. In most cases they are safe enough. My own practice is to physically connect my iOS devices to my computer and iTunes every now and then and back it up locally, rather than relying exclusively on automatic backup to iCloud.

There are anti-virus software products for both macOS and iOS machines. I use Sophos, as mentioned above, and it has provided me with some measure of comfort. But there are others that may be better for your situation.

Another layer of prevention is the use of a good firewall with unified threat management (UTM). This device is installed in your office network, often replacing your router, and allows for scanning of the network traffic, as well as other functionality. Although these devices often seem like overkill, and their high price tag discourages their deployment, they provide an excellent way to help prevent data loss because of external attacks, as well as scanning what is willfully brought into the network. A layered approach to security is always best, as it gives you more than one obstacle to put in the path of a bad actor.

As with most anything, true security depends on education, training, good practices, and human nature. From the discussion above, you can see that user error is the main cause of ransomware getting beyond technical protections. It's the clicking of links without thinking that typically leads to a problem.

Humans are likely to forget for a moment their training or the risks. This is why policies, education, and constant training are necessary. ■

Victoria L. Herring (vlh@herringlaw.com) practices in Des Moines, Iowa, in an office that has used only Apple/Macs since the early 1980s. She practices as a solo in the area of civil rights and employment discrimination. At present she is in the midst of retirement transformation, handling some cases but also engaging in fine art photography and co-owning an art gallery, Artisan Gallery 218. Thanks to John Moder, Crisp Solutions, LLC (crispsolutions.net), for his help in putting this article together; he has had to deal with the issue of ransomware in the real world and with small businesses.