July 2020 • The Monthly Security Awareness Newsletter for Everyone

Ransomware

What is Ransomware?

Ransomware is a type of malicious software (malware) that is designed to hold your files or computer hostage, demanding payment for you to regain access. Ransomware has become very common because it is so profitable for criminals.

Like most malware, ransomware starts by infecting your computer, most often when you open an infected attachment or click on a malicious link in a phishing email. Once ransomware infects your computer, it encrypts files on your hard drive – possibly even your entire hard drive – or anything else connected to your computer, so you can no longer access your files. It then informs you that the only way you can recover your files is to pay the cybercriminal a ransom (thus the name ransomware).

Sometimes, the criminals also threaten to release your files publicly if you don't pay the ransom. The criminals may demand payment in the form of untraceable digital currency, such as Bitcoin. If you pay the ransom, the criminals might give you access to your files, but there are no guarantees. Sometimes they will even take your money and still leave your computer infected without you knowing it or keep asking for more money.

Protect Against the Infection

You can protect your computer against a ransomware infection the same way you protect it against other forms of malware. Here are three key steps:

Update Your Systems and Software: Cyber criminals often infect computers or devices by taking advantage of unfixed bugs (known as vulnerabilities) in your software. The more current your software is, the fewer known vulnerabilities it has, and the harder it is for cyber criminals to infect them.

Therefore, make sure your operating systems, applications, and devices have automatic updating enabled.

Enable Anti-Virus: Use up-to-date anti-virus software from a trusted vendor. Such tools are designed to detect and stop malware. However, anti-virus cannot block or remove all malicious programs, and usually it cannot recover your files after a ransomware infection. Cyber criminals are constantly innovating, developing new and more sophisticated infection tactics that can evade detection. In turn, anti-virus vendors are constantly updating their products with new capabilities to detect malware. In many ways it has become an arms race, with both sides attempting to outwit the other.

Be Vigilant: Cyber criminals often trick people into installing ransomware and other forms of malicious software through phishing email attacks. For example, a cybercriminal might send you an email that looks legitimate and contains an attachment or a link. Perhaps the email appears to come from your bank or a friend. However, if you open the attached file or click the link, you could activate malicious code that infects your computer. If a message creates a strong sense of urgency or seems too good to be true, it could be an attack. Be vigilant – cyber attackers play on your emotions. — Common sense is often your best defense.

Back Up Your Files Before the Infection

Since it's impractical to assume that you'll always be able to prevent an infection, your best defense against ransomware is backups. If you have a backup of your important documents and other files, you have the option of recovering from backup instead of paying the ransom.

It's important that you use some type of automated backup that regularly backs up all your files and that you test your restore procedures to make sure you can recover them if the need arises. There are numerous simple Cloud and local backup solutions that you can install on your computer that will securely and regularly back up all your files for you.

Guest Editor

Lenny Zeltser is the CISO at Axonius, a cybersecurity asset management company. He also teaches malware combat and writing at the SANS Institute. Lenny is active on Twitter as @lennyzeltser and writes a security blog at zeltser.com.

Resources

Got Backups?: https://www.sans.org/security-awareness-training/resources/got-backups
Stop That Phish: https://www.sans.org/security-awareness-training/resources/stop-phish
The Power of Updating: https://www.sans.org/security-awareness-training/resources/power-updating
SANS FOR610 Course - Reverse Engineering Malware: https://sans.org/for610