The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- What Is Ransomware?
- Should You Pay the Ransom?
- Back Up Your Files
- Further Protective Measures

Ransomware

What Is Ransomware?

Ransomware is a special type of malware that is actively spreading across the Internet today, threatening to destroy victim's documents and other files. Malware is software--a computer program--used to perform malicious actions. While ransomware is just one of many different types of malware, it has become very common because it is so profitable for criminals. Once ransomware infects your computer, it encrypts certain files or your entire hard drive. You are then locked out of the whole system or cannot access your important files, such as your documents or photos. The malware then informs you that the only way you can decrypt your files and recover your system is to pay the cyber criminal a ransom (thus the name ransomware). Most often, the ransoms must be paid in some form of digital currency, such as Bitcoin. Ransomware spreads like many other types of malware. The most common method involves emailing victims malicious emails, where cyber criminals trick you into opening an infected attachment or clicking on a link that takes you to the attacker's website.

Guest Editor

Lenny Zeltser focuses on safeguarding customers' IT operations at NCR Corp and teaches malware combat at the SANS Institute. Lenny is active on Twitter as **@lennyzeltser** and writes a security blog at **zeltser.com**.

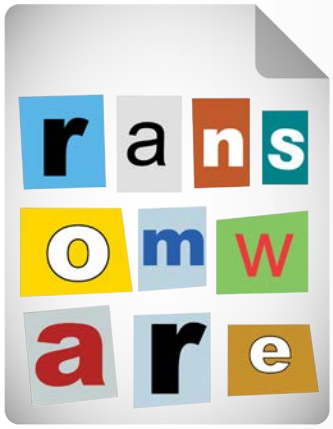
Should You Pay the Ransom?

That is a tough one. The problem is that the more often people pay these criminals when they are infected, the more motivated criminals are to infect others. On the other hand, you may have no other option to recover your files. Be warned though, even if you do pay the ransom, there is no guarantee you will get your files back. You are dealing with criminals; they may not decrypt the files, or even if they do provide you with a decryption method in exchange for payment, something may go wrong during the decryption process or your computer may be infected with additional malware.

Back Up Your Files

Perhaps the best way to recover from a ransomware infection and not pay a ransom is to recover your files from backups.

This way, even if you get infected with ransomware, you have a way of recovering files after rebuilding or cleaning up your computer. Keep in mind that if your backup can be accessed from the infected system, ransomware might delete or encrypt your backup files. Therefore, it's important to back up files to reputable cloud-based services or to store your backups on external drives that are not always connected to your system. In addition, a common mistake that many people make with backups is to assume that it works without testing whether they can actually recover files. Be sure to regularly test that your backups are working, and confirm that you can recover the files you need should your system become infected with ransomware. Backups are important, as they also help you recover when you accidentally delete files or your hard drive crashes.



Ransomware is a malware that, once it infects your computer, encrypts all the files on your computer, denying you access to them.

Further Protective Measures

Moreover, you can protect yourself from ransomware infections the same way you would against other types of malware: don't get infected. Start by making sure that you have up-to-date anti-virus software from a trusted vendor. Such tools, sometimes called anti-malware software, are designed to detect and stop malware. However, anti-virus cannot block or remove all malicious programs. Cyber criminals are constantly innovating, developing new and more sophisticated malware 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. Unfortunately, the bad guys are usually one step ahead, which is why you need to ensure you back up your files and employ these additional steps to protect yourself:

- Cyber criminals often infect computers or devices by exploiting vulnerabilities in your software. The more current your software is, the fewer known vulnerabilities your systems have and the harder it is for cyber criminals to infect them. Therefore, make sure your operating systems, applications, and devices are enabled to automatically install updates.

- On computers, use a standard account that has limited privileges rather than privileged accounts such as "Administrator" or "root." This provides additional protection by preventing many types of malware from being able to install themselves.
- Cyber criminals often trick people into installing malware for them. For instance, they 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 were to open the attached file or click on the link, you would activate malicious code that installs malware on your system. If a message creates a strong sense of urgency, is confusing, seems too good to be true, or has poor grammar, it could be an attack. Be suspicious, common sense is often your best defense.

Protect yourself from ransomware by remaining vigilant when opening email attachments or clicking on links, ensuring that you have updated anti-virus software, and confirming that your files are regularly backed up and can be restored.

An Easier Way to Manage Your Security Awareness Program

SANS Institute's new Advanced Cybersecurity Learning Platform (ACLP) makes deploying, maintaining, and measuring awareness programs easier and more effective. Learn more at https://securingthehuman.sans.org/u/jGf.

Resources

Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Encryption:	https://securingthehuman.sans.org/ouch/2016#june2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Microsoft Article:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610 Course - Reverse Engineering Malware:	https://sans.org/for610

License