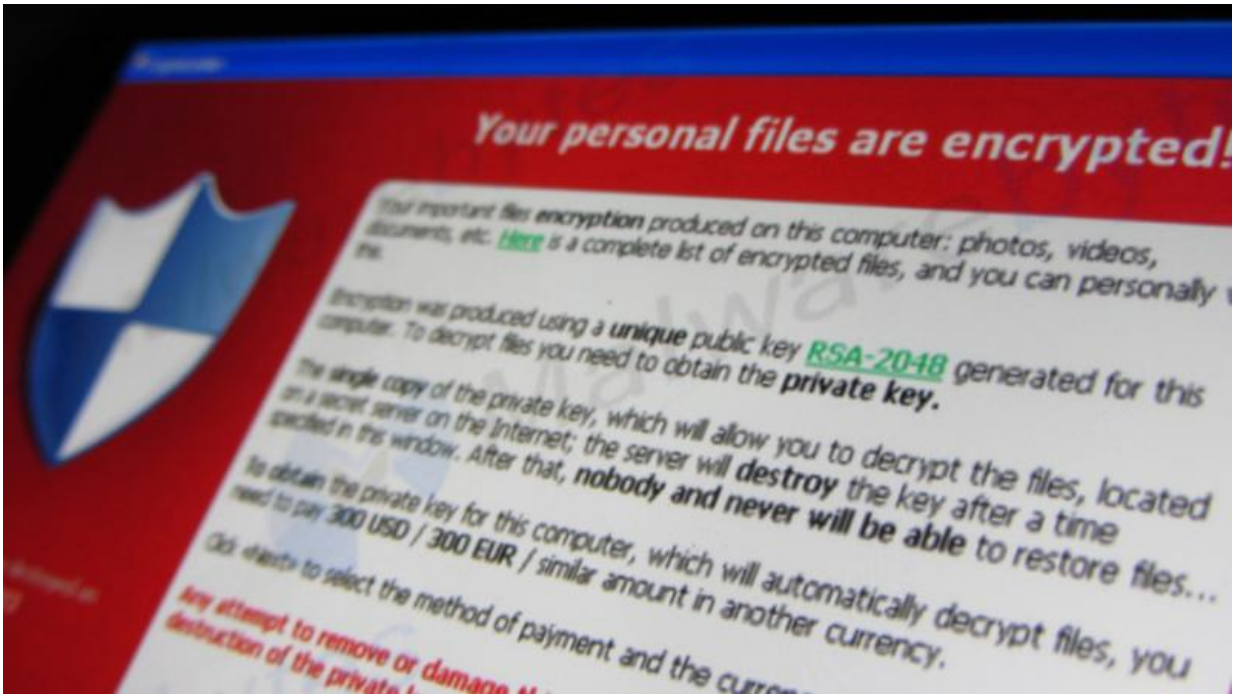
It's easier to defend against ransomware than you might think

May 24 2016, by Amin Kharraz



Try to make this the only time you see a ransomware warning notice. Credit: Christiaan Colen/flickr, CC BY-SA

Ransomware – malicious software that sneaks onto your computer, encrypts your data so you can't access it and demands payment for unlocking the information – has become an emerging cyberthreat. Several reports in the past few years document the diversity of ransomware attacks and their increasingly sophisticated methods.

Recently, high-profile ransomware attacks on large enterprises such as hospitals and police departments have demonstrated that large organizations of all types are at risk of significant real-world consequences if they don't protect themselves properly against this type of cyberthreat.

The development of strong encryption technology has made it easier to encode data so that it cannot be read without the decryption key. The emergence of anonymity services such as the Tor network and bitcoin and other cryptocurrencies has eased worries about whether people who receive payments might be identified through financial tracking. These trends are likely driving factors in the recent surge of ransomware development and attacks.

Like other classes of malicious software – often called "malware" – ransomware uses a fairly wide range of techniques to sneak into people's computers. These include attachments or links in unsolicited email messages, or phony advertisements on websites. However, when it comes to the core part of the attack – encrypting victims' files to make them inaccessible – most ransomware attacks use very similar methods. This commonality provides an opportunity for ransomware attacks to be detected before they are carried out.

My recent research discovered that ransomware programs' attempts to request access and encrypt files on hard drives are very different from benign operating system processes. We also found that diverse types of ransomware, even ones that vary widely in terms of sophistication, interact with computer file systems similarly.

Moving fast and hitting hard

One reason for this similarity amid apparent diversity is the commonality of attackers' mindsets: the most successful attack is one

that encrypts a user's data very quickly, makes the computer files inaccessible and requests money from the victim. The more slowly that sequence happens, the more likely the ransomware is to be detected and shut down by antivirus software.

What attackers are trying to do is not simple. First, they need to reliably encrypt the victim's files. Early ransomware used very basic techniques to do this. For example, it used to be that a ransomware application would use a single decryption key no matter where it spread to. This meant that if someone were able to detect the attack and discover the key, they could share the key with other victims, who could then decode the encrypted data without paying.

Today's ransomware attackers use advanced cryptographic systems and Internet connectivity to minimize the chance that a victim could find a way to get her files back on her own. Once the program makes its way into a new computer, it sends a message back over the internet to a computer the attacker is using to control the ransomware. A unique key pair for encryption and decryption is generated for that compromised computer. The decryption key is saved in the attacker's computer, while the encryption key is sent to the malicious program in the compromised computer to perform the file encryption. The decryption key, which is required to decrypt the files only on that computer, is what the victim receives when he pays the ransom fee.

The second part of a "successful" ransomware attack – from the perspective of the attacker – depends on finding reliable ways to get paid without being caught. Ransomware operators continuously strive to make payments harder to trace and easier to convert into their preferred currency. Attackers attempt to avoid being identified and arrested by communicating via the anonymous Tor network and exchanging money in difficult-to-trace cryptocurrencies like bitcoins.

Defending against a ransomware attack

Unfortunately, the use of advanced cryptosystems in modern ransomware families has made recovering victims' files almost impossible without paying the ransom. However, it is easier to defend against ransomware than to fight off other types of cyberthreats, such as hackers gaining unauthorized entry to company data and stealing secret information.

The easiest way to protect against ransomware attacks is to have, and follow, a reliable data-backup policy. Companies that do not want to end up as paying victims of ransomware should have their workers conduct real-time incremental backups (which back up file changes every few minutes). In addition, in case their own backup servers get infected with ransomware, these companies should have offsite cloud backup storage that is protected from ransomware. Companies that are attacked can then restore their data from these backups instead of paying the ransom.

Users should also download and install regular updates to software, including third-party plug-ins for web browsers and other systems. These often plug security vulnerabilities that, if left open, provide attackers an easy way in.

Generally, being infected with ransomware has two important messages for an organization. First, it's a sign of vulnerability in a company's entire computer system, which also means that the organization is vulnerable to other types of attacks. It is always better to learn of an intrusion earlier, rather than being compromised for several months.

Second, being infected with ransomware also suggests users are engaging in risky online behavior, such as clicking on unidentified email attachments from unknown senders, and following links on disreputable websites. Teaching people about safe internet browsing can dramatically

reduce an organization's vulnerability to a ransomware attack.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation