Why ransomware is on the rise

February 25 2016, by Joe O'connell

Credit: Luis Delgado/Northeastern University

A California hospital recently had its patients' records held hostage. But the perpetrators did not commandeer a room full of paper files. They were in fact hackers who restricted access to the electronic records and demanded a ransom of $17,000 in Bitcoins in exchange for stopping the attack.

This was the most recent example of ransomware, a form of extortion where hackers use malware to remotely take control of a computer or network–either by locking the computer or encrypting your files–and deny you access to your information. And the only way to remove the restriction is to pay a ransom, which the California hospital did.

We asked two Northeastern professors–cybersecurity experts Engin Kirda and Guevara Noubir–to explain what has spurred the recent ransomware attacks and what you can do to keep your information safe.

Why is ransomware becoming more prevalent and how has it evolved over the years?

Noubir: Ransomware malware have been around since the late 1980s. Concepts underlying public key crypto-based ransomware were conceived as an effective money extortion mechanism in the 1990s. The emergence of privacy infrastructure, such as the anonymity network Tor, and cryptocurrencies, such as Bitcoin, make it possible for an adversary to commit such cybercrimes and get away with it.

How is ransomware impacting cybersecurity?

College of Computer and Information Science professor Guevara Noubir. Credit: Brooks Canaday/Northeastern University

Noubir: Recent ransomware novelty lies is in the anonymous monetization/payment-exchange method. This is still not well studied but the rise of the attacks are driving the implementation of traditional security measures from awareness and policies to secure platforms and tools.

Kirda: Ransomware is not special. In the general cybersecurity landscape, it is yet another scam and means for using malicious code for making money. In fact, I would claim that no security professional has been surprised by the advent of ransomware because conceptually it uses very similar techniques as traditional malware to infect and spread.

Who is most likely to be a victim of ransomware and why? Do attacks tend be more random or are victims specifically selected?

Noubir: Victims are similar to traditional malware. While in the past extortion typically targeted companies and organizations, digital currencies are making it easier to automate against average users.

Kirda: The people who become victims of ransomware are also typically the victims of other types of malware as well. In most cases, ransomware attacks are random, but there might be a reconnaissance phase in some of the attacks where the attackers may choose to explore a potential target before launching something more large-scale.

The latest ransomware attacks against hospitals, for example, seem to have had a component that was targeted to a certain degree. Note that this fact, though, is also typical for any type of malware attack.

What are some best practices people can adopt to avoid being victims of ransomware?

Kirda: Ransomware attacks the victim's data. People pay up because they are afraid they will otherwise lose their information. A good defense mechanism is to make sure to always have current, remote backups. The cloud, for example, is a good place for backups for most users.

Of course, if a victim is not infected in the first place, it would be ideal. Organizations and users need to make sure they have current defenses in place and users need to learn not to open suspicious files or click on suspicious URLs.

Why are the ransom demands typically made in Bitcoin? Why not demand currency?

Noubir: It is difficult to trace Bitcoins because they are typically shuffled using online mixing services.

Provided by Northeastern University