Expert discusses ransomware attacks and how to prevent them

June 15 2021, by Eric Stann

Credit: CC0 Public Domain

The recent ransomware attack on a major oil refinery in the United States, followed weeks later by another hack that affected a large meat supplier, have again brought the issue of cyberattacks to the forefront of

people's minds, followed closely by a renewed push toward building better cyber defenses to help prevent critical data from being stolen and held hostage by cybercriminals. Furthermore, these attacks have caused a ripple effect in the nation's economy, most notably with sudden rises in gasoline and food prices, gasoline shortages and delays with shipping and logistics of goods and services.

Cybersecurity expert Prasad Calyam is the director of the Cyber Education and Research Center (Mizzou CERI), and an associate professor in the Department of Electrical Engineering and Computer Science. Here, he explains what ransomware attacks are, and shares some ways people and businesses can protect their digital information from being stolen online.

What does it mean when a company or business is a victim of a ransomware attack?

It means that the victim experiencing a ransomware attack has had its internal computer and network systems compromised by an intruder, and the intruder has taken control of a valuable asset, such as a database, software program, hardware device or network element. If the victim has been notified by the hacker about the compromise, then the victim is making a difficult decision to either pay the ransom or not pay the ransom and reset the compromised system to a safe state.

Most common ransomware attacks target business-critical data, and the hackers will encrypt the data. A ransom payment is demanded to avoid permanent data loss—destruction of the encryption key—or to avoid undesired data exposure by making protected intellectual property or confidential information public.

What can businesses do to protect their information

from being held ransom by hackers, especially as more data is being moved into cloud-based data storage systems?

If critical data is moved to cloud-based platforms versus hosting them in-house, the businesses will have access to highly diverse and capable tools to secure the data; however, necessary expertise needs to be present in the business to suitably leverage data security capabilities of cloud-based platforms.

What are some basic actions people can take to protect their information from being stolen by hackers, even if they aren't personally targeted but are involved in an organization-level data breach?

Any business is always at a risk of being impacted by a ransomware attack, and it's just a matter of 'when' and not an 'if." Therefore, every business should prepare a plan involving three scenarios—you are a victim, you will soon be a victim, and you will eventually be a victim. The plan is critical because the time to react or make difficult decisions will be short as the hacker will put pressure to have the victim pay up. In order to defend against ransomware or any other modern cyberattacks, the plan should focus on training employees on not falling victim to social engineering attacks, such as disclosing passwords. The plan should also feature policies to backup datasets that can be recovered quickly, and setup strict access control for critical assets to deter an intruder to easily gain control of the valuable assets. Furthermore, the business should invest in an on-going monitoring strategy to ensure that the risk of falling victim or recovering from a ransomware attack is minimized to the extent possible.

To learn more about how to prepare a cybersecurity plan to defend against ransomware and other modern cyberattacks, businesses,

especially small businesses, please see a five-part webinar series that Calyam recently created with funding from the Small Business Administration in collaboration with the Missouri Small Business Development Center.

Why do you feel there has been a recent increase in the number of reported cyberattacks, such as the major gas pipeline and a large meat-production company? Do you feel this trend will continue?

Ransomware attacks have been used by hackers for many years. Early on, ransomware attacks were "commodity" attacks that indiscriminately tried to infect computer systems in the hope of finding vulnerable organizations. If a victim was found, many times either the victim would not agree to pay a ransom or was not technically adept to make a bitcoin transaction as demanded by the hackers. More recently, hackers have started launching "targeted" attacks using sophisticated methods to find organizations that can be victimized for getting big ransom bitcoin payments in market segments such as healthcare, finance and utilities. The trend of these attacks will continue and is highly dependent on how the bitcoin value fluctuates. However, we are seeing government agencies finding ways to recover bitcoin ransom payments, which will hopefully add to deterrence along with organizations becoming more aware as well as prepared to defend against ransomware attacks.

Provided by University of Missouri