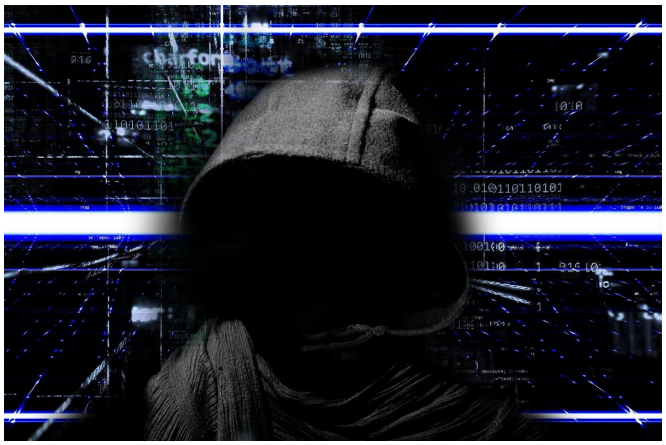
Expert discusses the Colonial Pipeline ransomware attack

12 May 2021, by John Thomas and Thomas Holt



Credit: CC0 Public Domain

On May 7, Colonial Pipeline announced that it fell victim to a ransomware attack and had shut down one of the largest fuel pipelines in the U.S. as a result. Thomas Holt, director and professor in Michigan State University's School of Criminal Justice, answers common questions about ransomware and how we can protect critical infrastructure from future attacks.

What exactly is ransomware?

Ransomware is a form of malicious software (or malware) that derives its name from its use: getting the target to pay a ransom. The attacker tries to get the victim to either download the malware via a phishing email or some other means, and once they click on the malware, it executes its payload. What that means is it installs a series of commands and software on the target system and effectively encrypts the user's files. Some ransomware can also spread to other systems within a network once it infects a target and further spread the damage it can do to system files. The payload also informs the victim of the encryption and tells them that they will only be able to decrypt their files once they pay a fee to a specific account, usually a Bitcoin or cryptocurrency wallet. Once paid, the attacker will typically decrypt the files and the system is restored, though there have been instances where that does not work.

What are the motives of hackers who use a ransomware attack? Are there any motives beyond money?

The typical motivation is economic gain as they're seeking payment from the victim. In some cases, one could argue it is also revenge or showing off, but largely it is about monetary gain. The attackers have increasingly targeted major corporations, sensitive systems, etc. because they believe the victims will pay. There have been two examples of ransomware being used by nation-states, WannaCry and NotPetya. These are unique in that WannaCry was less ransomware and more an attempt to get funds from victims. NotPetya appeared to be ransomware at first (specifically a variant called Petya) but turned out to be a kind of malware that essentially ruined the infected system (that's why it's called NotPetya).

How do companies and/or law enforcement generally handle these types of attacks?

Generally speaking, most individuals and companies pay the ransom. It is one of the few ways to get data back up and running. That is why ransomware attackers have escalated their targets from people to companies and larger targets over time—everyone pays, so the bigger your target (and the deeper their pockets) the more you stand to profit if they pay. There are different views on the ethics of paying ransoms but inevitably it is what most entities do when hit with ransomware. Some also hire third-party cybersecurity firms to do analyses of the attack, help with mitigation and aid any law enforcement investigations. However, the frequency of these attacks, coupled with their cost, means that there are more attacks than

investigators to successfully pursue actions through the justice system. Additionally, the fact that many cybercriminals reside in foreign countries makes it harder for investigators to take action as it takes time to get all legal agreements in place, and successfully arrest the perpetrator, let alone extradite them. So, there are relatively few prosecutions for ransomware.

What is the best way to protect yourself from these types of attacks?

At the individual level, the best things to do are to 1) not respond to suspicious emails or messages that you receive via your browser; and 2) keep your antivirus software up-to-date and regularly scanning your system. That helps reduce all sorts of attacks from being successful. At the corporate level, it is still largely about the individual users within your organization, though there are also system misconfigurations and vulnerabilities that can be targeted. So, having effective security professionals regularly managing your systems/updating and installing patches is important. For both groups, regularly backing up your data, and storing those backups somewhere secure is extremely important. That way you can increase the likelihood you don't lose anything in the event of a ransomware attack that is effective.

What do we need to do as a country to protect our infrastructure from these types of attacks?

The most important thing is to ensure we take cybersecurity seriously and actually use basic security practices. That will help reduce the likelihood that an attack is successful from the start. Second, taking more proactive efforts to pursue legal actions against ransomware operators and prosecute those actors would be helpful to start to deter their actions. Since many operate overseas, this makes detection, arrest and prosecution difficult. But more successful prosecutions may help to deter a portion of actors. Finally, there has to be some sort of resolution as to how to effectively avoid paying ransomware operators. As long as they get a payout, they will keep targeting systems. So finding technical solutions that could help defeat ransomware without paying the ransom might also help reduce the prevalence of these attacks.

Provided by Michigan State University