Protecting US critical infrastructure from cyberattacks

November 3 2021, by Stephanie Jones

Credit: Pixabay/CC0 Public Domain

Over the past year, there has been a sharp increase in cyberattacks using malware to target the systems of critical infrastructure such as utility companies, government agencies and organizations that provide services and products that we rely on daily. According to a report from the cybersecurity firm CheckPoint Software, in the first half of this year, there was a 102 percent increase in these types of attacks compared to

2020.

"In years past, a lot of internet attacks were done for fun, but these days they are all for profit," said Guofei Gu, professor in the Department of Computer Science and Engineering at Texas A&M University. "The most popular, and profitable, type that we see nowadays is ransomware."

Ransomware is an advanced type of malware that installs itself onto a user's machine or device undetected, encrypts their data files, rendering them inaccessible, and demands a ransom payment to decrypt them. But even if the ransom is paid, the decryption process to get the files back to normal is a slow one.

"These groups will put several locks on the data," said Dilma Da Silva, professor and holder of the Ford Motor Company Design Professorship in the department. "While you may be able to get through them all with the key that they give you, it is going to take the computer a long time to get through them all. And there's always a possibility they will leave an extra hack behind for themselves or to sell to other cybercriminal groups."

Cybercrime is a growing business. The FBI reported that in 2020, despite most of the country being focused on the COVID-19 pandemic, they received a record number of complaints about cybercrimes, which cost Americans about $4.2 billion in losses. Cybersecurity Ventures predicts that by 2025, that number could grow to $10.5 trillion per year worldwide.

What is malware?

Malware is an umbrella term for any malicious software such as viruses, worms and spyware that is intentionally designed to cause harm or damage computers, computer systems, devices and networks. It can get

into a system through various methods, including email attachments, infected applications and USB drives, phishing emails, text messages and malicious advertisements.

Recent malware attacks have a couple of new features that set them apart from past attacks. The first is that the malware is a sophisticated software written by highly skilled professionals. It explores a computer's software vulnerabilities that even the owner of the system has not discovered. The second new feature is that these professional groups have begun targeting more profitable victims.

One of the nation's most vital infrastructure systems—utilities—are among the most vulnerable to cyberattacks. Many large utility companies run on very old systems and software and have highly constrained resources. The reason why these out-of-date platforms are still in use is because they were created to perform specific tasks and they still work. When a vulnerability is found, updating the system it is not a simple process. In addition, if one element of it is changed, then it can affect other parts of it in unpredictable ways and result in more issues. They are also not able to run additional software alongside it to protect it.

Better protecting critical infrastructure systems

When it comes down to developing solutions to improve the strength of these systems to protect from future cyberattacks, there is a dilemma. Unlike the computer systems that we use every day, like Windows or Linux, many of these critical infrastructure systems are highly closed to outsiders, including cybersecurity experts.

"On the one side, these organizations want their systems to be secure, but at the same time they are not able to achieve the level of security they need," Gu said. "They either cannot use existing solutions or they are unwilling to open their systems for experts to assess for possible

vulnerabilities."

While there may be good reasons to keep the details of their systems hidden, it makes collaborating with security experts who want to help difficult. To help improve communications between these organizations and cybersecurity experts, Gu suggests the solution could be designing these systems to be more open.

"A lot of the time, an open design is actually more secure because a lot of experts will be able to analyze it," he said. "If they are not able to find any problems or break them, it typically means that the system's security is good. It's all about finding a good balance between openness and security."

Cybersecurity research at Texas A&M

Texas A&M is one of only a handful of colleges and universities in the nation designated as a Center for Academic Excellence in all three National Security Agency focus areas: cyberoperations, cyberdefense and research. Da Silva's work, which is funded by the National Security Agency, centers around making computer systems more suitable for security work.

"It is essentially about the computational power to be able to process data very quickly," Da Silva said. "When there is a lot of data coming into a system at a rapid pace, the system needs to be able to consume that data very quickly and run algorithms that run closer to where the data is produced. We're really refining and specializing the things that Google and Facebook, for instance, use to process a lot of data but for cybersecurity, specifically."

Gu's research is focused on achieving defense in depth, which is a security approach that utilizes several layers of defense mechanisms that

are thoughtfully placed throughout a computer network to protect the valuable data within it from a variety of threats. In the event that a mechanism fails, then another will immediately step up to stop the attack.

"We've done a lot of work in terms of how we can proactively prevent, detect and recover from cyberattacks," Gu said. "For example, we built a system to detect new vulnerabilities inside a computer system's software that needs to be fixed before a cybercriminal could get in and explore the system."

As cybersecurity is virtually its own ecosystem that covers a lot of different aspects of our society, a wide breadth of expertise is needed to cover them all. The Texas A&M Cybersecurity Center is building a team of faculty and students that work on various aspects of security such as in the Internet of Things, cloud computing, blockchain and software.

Provided by Texas A&M University

Citation: Protecting US critical infrastructure from cyberattacks (2021, November 3) retrieved 17 April 2024 from https://techxplore.com/news/2021-11-critical-infrastructure-cyberattacks.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.