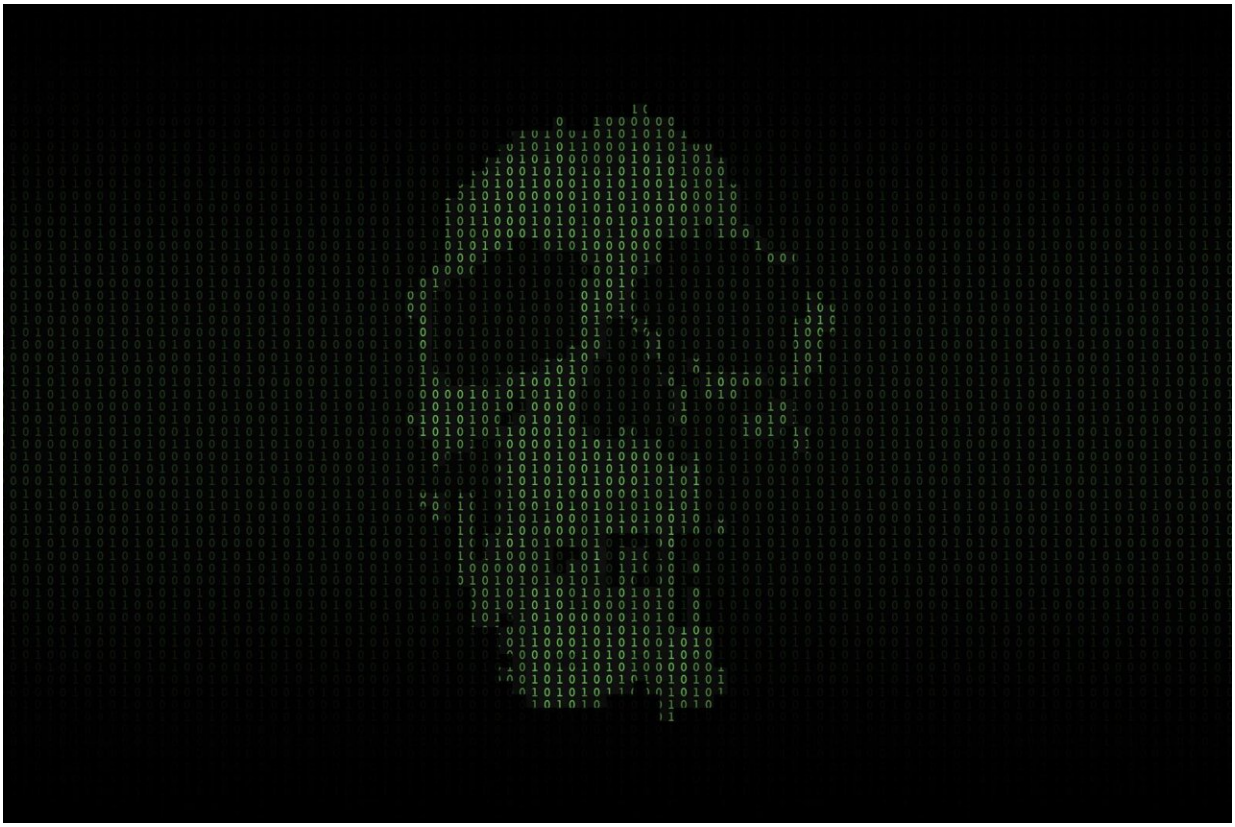
Understanding the rising threat of ransomware attacks

August 19 2021, by Lucie Rutherford



Credit: Ziniu Chen, University Communications

A rude awakening came to thousands of Americans in early May. Many motorists who had never seen the effects of a devastating ransomware attack found themselves scrambling to find a flowing gas pump, and

waiting in massive lines when they did.

This came after a suspected Russian-linked criminal group breached the computer network of the East Coast's largest oil supplier, Colonial Pipeline, shutting down its operations and threatening to leak stolen sensitive data if a $4.4 million ransom was not paid. Within days, pumps up and down the East Coast were taped off with "Out of Gas" signs.

It took an attack of this capacity, affecting lives so directly, for the average person to notice what can happen when data and software are held for ransom. The Colonial Pipeline attack was one of thousands each year, many of which go unnoticed despite the fact that millions of dollars are cumulatively spent in ransoms.

Between 2019 and 2020, ransomware attacks rose 158% in North America alone, and the collective cost of attacks reported to the FBI went up 200%, from $8.9 million to $29.1 million.

According to Don Brown, senior associate dean for research at the University of Virginia's School of Engineering, Quantitative Foundation Distinguished Professor in Data Science and W.S. Calcott Professor in the Department of Systems and Information Engineering, criminal acts of this nature are not going away anytime soon, especially if companies continue to pay ransoms.

As the looming threat plagues organizations—from national security agencies and Fortune 500 companies to schools and small businesses—UVA Today asked Brown to explain the nature, commonality, protections and future of ransomware attacks.

Q. What are ransomware attacks? What do they do?

A. Ransomware attacks penetrate data management software and then

encrypt access to the data using a key known only to the criminals. The original owners of the data can then no longer access it. Once the data is hijacked, the criminals then demand money to decrypt access to the data.

Q. Almost half of the East Coast's fuel supply was halted due to the Colonial Pipeline attack. How are perpetrators able to do this?

A. Ransomware attacks enter through a variety of methods, but the most common are through exploitation of simple passwords (e.g., "password"), through phishing attacks (i.e., posing as a legitimate site in order to obtain a password or log-in credentials), and through software (e.g., M.S. Windows) with known bugs that has not been updated.

Q. What other massive attacks has the United States seen?

A. The U.S. has seen a lot of attacks. There is the well-known attack on the Democratic National Committee in 2016, although that was a data breach, not ransomware. The same groups (they appear to be Russian) that attacked the Colonial Pipeline appear to have attacked many businesses worldwide over the last month through the exploitation of a security bug in the Kaseya software. Also, China is widely suspected of breaching the United States Office of Personnel Management in 2014 to obtain as many as 32 million records of government personnel and their families with security clearances.

Unfortunately, there are more than these.

Q. How often do smaller ransomware attacks go

unnoticed by the public? Where do these take place?

A. Since not everyone reports attacks, we don't know the full scope. But recent attacks exploiting the Kaseya bug have likely affected thousands of businesses worldwide. These attacks are against supply chain companies, but they have also targeted manufacturers, hospitals and health care providers, and even schools, since they know these organizations often have weak security and are critically dependent on their data.

Q. What are governments, organizations and companies doing to protect themselves? What are they not doing, or what should they be doing?

A. The Biden administration is currently in discussions with [Russian leader Vladimir] Putin, as you can see in the news.

The U.S. needs to decide on an overall policy regarding cyberattacks. Are these nation-state attacks? For instance, the attack on the Colonial Pipeline by criminals in Russia was not necessarily by the Russian government, but Russia has done nothing to stop these attacks on other countries, particularly Western countries. Also, the U.S. has condoned payment for exploits in commonly used software such as Windows and IOS. This creates a worldwide market for potential exploitation.

Q. Why should individuals be concerned about ransomware attacks? Can individuals do anything to protect themselves?

A. Clearly these attacks affect all of us, as we saw with lines at gas stations following the Colonial Pipeline attack. Attacks on hospitals and

schools may be local and not as visible or highly publicized, but could also have severe and rippling consequences.

The main thing individuals can do is to use strong passwords, be very cautious about opening email attachments or responding to emails that want personal information and keep software up to date.

Q. What does the future of ransomware attacks look like?

A. Unless governments agree to cooperate and go after the criminals, we're probably only going to see more ransomware attacks. Sadly, it could get much worse before it gets better.

Provided by University of Virginia