Emerald Spectrum Advisory
Malissia Johnson, CFP®, AAMS, CMFC
5300 Maryland Way, Suite 303
Brentwood, TN 37027
615-369-0690
esateam@emeraldspectrum.com
www.emeraldspectrum.com

EMERALD SPECTRUM
ADVISORY
"An Extraordinary Planning Experience"

Hostage Data: Ransomware and Protecting Your Digital Information

On May 7, 2021, the Colonial Pipeline, which carries almost half of the East Coast's fuel supply from Texas to New Jersey, shut down operations in response to a ransomware attack. Colonial paid a $4.4 million ransom not long after discovering the attack, and the pipeline was reopened within a week. While there was enough stored fuel to weather the outage, panic buying caused gasoline shortages on the East Coast and pushed the national average price of gasoline over $3.00 per gallon for the first time since 2014.1

Ransomware is not new, but the Colonial Pipeline incident demonstrated the risk to critical infrastructure and elicited strong response from the federal government. Remarkably, the Department of Justice recovered most of the ransom, and the syndicate behind the attack, known as DarkSide, announced it was shutting down operations.2

The Department of Homeland Security issued new regulations requiring owners and operators of critical pipelines to report cybersecurity threats within 12 hours of discovery, and to review cybersecurity practices and report the results within 30 days.3 On a broader level, the incident increased focus on government initiatives to strengthen the nation's cybersecurity and create a global coalition to hold countries that shelter cybercriminals accountable.4

Malicious Code

Ransomware is malicious code (malware) that infects the victim's computer system, allowing the perpetrator to lock the files and demand a ransom in return for a digital key to restore access. Some attackers may also threaten to reveal sensitive data. There were an estimated 305 million ransomware attacks globally in 2020, a 62% increase over 2019. More than 200 million of them were in the United States.5

The recent surge in high-profile ransomware attacks represents a shift by cybercriminal syndicates from stealing data from "data-rich" targets such as retailers, insurers, and financial companies to locking data of businesses and other organizations that are essential to public welfare. A week after the Colonial Pipeline attack, JBS USA Holdings, which processes one-fifth of the U.S. meat supply, paid an $11 million ransom.6 Health-care systems, which spend relatively little on cybersecurity, are a prime target, jeopardizing patient care.7 Other common targets include state and local governments, school systems, and private companies of all sizes.8

Ransomware gangs, mostly located in Russia and other Eastern European countries, typically set ransom demands in relation to their perception of the victim's ability to pay, and high-dollar attacks may be resolved through negotiations by a middleman and a cyber insurance company. Although the FBI discourages ransom payments, essential businesses and organizations may not have time to reconstruct their computer systems, and reconstruction can be more expensive than paying the ransom.9

Protecting Your Data

While major ransomware syndicates focus on more lucrative targets, plenty of cybercriminals prey on individual consumers, whether locking data for ransom, gaining access to financial accounts, or stealing and selling personal information. Here are some tips to help make your data more secure.10

Use strong passwords and protect them. An analysis of the Colonial Pipeline attack revealed that the attackers gained access through a leaked password to an old account with remote server access.11 Strong passwords are your first line of defense. Use at least 8 to 12 characters with a mix of upper- and lower-case letters, numbers, and symbols. Longer and more complex passwords are better. Do not use personal information or dictionary words.

One technique is to use a passphrase that you can remember and adapt. For example, Jack and Jill went up the hill to fetch a pail of water could be J&jwuth!!2faPow. Though it's tempting to reuse a strong password, it is

Emerald Spectrum Advisory
Malissia Johnson, CFP®, AAMS, CMFC
5300 Maryland Way, Suite 303
Brentwood, TN 37027
615-369-0690
esateam@emeraldspectrum.com
www.emeraldspectrum.com

safer to use different passwords for different accounts. Consider a password manager program that generates random passwords, which you can access through a strong master password. Do not share or write down your passwords.

No easy answers. Be careful when establishing security questions that can be used for password recovery. It may be better to use fictional answers that you can remember. If a criminal can guess your answer through available information (such as an online profile), he or she can reset your password and gain access to your account.

Take two steps. Two-step authentication, typically a text or email code sent to your mobile device, provides a second line of defense even if a hacker has access to your password.

Think before you click. Ransomware and other malicious code are often transferred to the infected computer through a "phishing" email that tricks the reader into clicking on a link. Never click on a link in an email or text unless you know the sender and have a clear idea where the link will take you.

Install security software. Install antivirus software, a firewall, and an email filter — and keep them updated. Old antivirus software won't stop new viruses.

Back up your data. Back up regularly to an external hard drive. For added security, disconnect the drive between backups.

Keep your system up-to-date. Use the most recent operating system that can run on your computer and download security updates. Most ransomware attacks target vulnerable operating systems and applications.

If you see a notice on your computer that you have been infected by a virus or that your data is being held for ransom, it's more likely to be a fake pop-up window than an actual attack. These pop-ups typically have a phone number to call for "technical support" or to make a payment. Do not call the number and do not click on the window or any links. Try exiting your browser and restarting your computer. If you continue to receive a notice or your data is really locked, contact a legitimate technical support provider.

For more information and other tips, visit the Cybersecurity & Infrastructure Security Agency website at us-cert.cisa.gov/ncas/tips.

1–2, 11) Vox, June 8, 2021
3) U.S. Department of Homeland Security, May 27, 2021
4) The Washington Post, June 4, 2021
5) 2021 SonicWall Cyber Threat Report
6) The Wall Street Journal, June 9, 2021
7) Fortune, December 5, 2020
8) Institute for Security and Technology, 2021
9) The New Yorker, June 7, 2021
10) Cybersecurity & Infrastructure Security Agency, 2021

While major ransomware syndicates focus on more lucrative targets, plenty of cybercriminals prey on individual consumers.