BIZ NET
BUSINESS - NETWORKS

Tech chronicle

August 2020

Ransomware

What is Ransomware?

Ransomware is a type of malicious software (malware) that is designed to hold your files or computer hostage, demanding payment for you to regain access. Ransomware has become very common because it is so profitable for criminals.

Like most malware, ransomware starts by infecting your computer, most often when you open an infected attachment or click on a malicious link in a phishing email. Once ransomware infects your computer, it encrypts files on your hard drive – possibly even your entire hard drive – or anything else connected to your computer, so you can no longer access your files. It then informs you that the only way you can recover your files is to pay the cybercriminal a ransom (thus the name ransomware). Sometimes, the criminals also threaten to release your files publicly if you don't pay the ransom. The criminals may demand payment in the form of untraceable digital currency, such as Bitcoin. If you pay the ransom, the criminals might give you access to your files, but there are no guarantees. Sometimes they will even take your money and still leave your computer infected without you knowing it or keep asking for more money.

Protect Against the Infection

You can protect your computer against a ransomware infection the same way you protect it against other forms of malware. Here are three key steps:

- **Update Your Systems and Software:** Cyber criminals often infect computers or devices by taking advantage of unfixed bugs (known as vulnerabilities) in your software. The more current

Marco's Corner

Keeping care of your clients is always important in all situations but becomes even more essential when your business is faced with a disaster, whether it be natural or man-made. Protecting the essentials in your business, whether it be the safety of your employees or your critical business data is paramount and there needs to be a plan in place to make sure that you know exactly what needs to be done when a disaster does occur. Disasters can be defined as anything that will disrupt your normal business operations, whether it be a fire, flood, theft, or Ransomware, which has been in the news quite a bit lately. Business data is essential for all organizations, so ensuring access to mission critical applications and the data it relies on is critical. I am sure you have heard the term "Business Continuity" before but what does it really mean? How do you apply its principles to keep your business running in the event of a disaster? More importantly, how do you take care of your clients when a disaster strikes your business? If you cannot continue to do business with your clients, the possibility of going out of business is very much a concern. How are you planning on running your business if you cannot get to your facility? How are you going to notify clients about how you are now going to conduct business during this period? **Business Continuity Planning is important for every business and Biz-Net can help you accomplish this. Call us at 775-850-7700.**

BIZ-NET
1325 Airmotive Way Suite 208
Reno, NV 89502

www.biz-net.com

This monthly publication provided courtesy of Marco Romero, President of Biz-Net, Reno NV

Our Mission: To provide the best possible service for our clients using the best tools available today. *As a business owner, I know you do not have time to waste on technical and operational issues. That's where we shine!*

your software is, the fewer known vulnerabilities it has, and the harder it is for cyber criminals to infect them. Therefore, make sure your operating systems, applications, and devices have automatic updating enabled.

- **Enable Anti-Virus:** Use up-to-date anti-virus software from a trusted vendor. Such tools are designed to detect and stop malware. However, anti-virus cannot block or remove all malicious programs, and usually it cannot recover your files after a ransomware infection. Cyber criminals are constantly innovating, developing new and more sophisticated infection tactics that can evade detection. In turn, anti-virus vendors are constantly updating their products with new capabilities to detect malware. In many ways it has become an arms race, with both sides attempting to outwit the other.
- **Be Vigilant:** Cyber criminals often trick people into installing ransomware and other forms of malicious software through phishing email attacks. For example, a cybercriminal might send you an email that looks legitimate and contains an attachment or a link. Perhaps the email appears to come from your bank or a friend. However, if you open the attached file or click the link, you could activate malicious code that infects your computer. If a message creates a strong sense of urgency or seems too good to be true, it could be an attack. Be vigilant – cyber attackers play on your emotions. — Common sense is often your best defense.

Back Up Your Files Before the Infection

Since it's impractical to assume that you'll always be able to prevent an infection, your best defense against ransomware is backups. If you have a backup of your important documents and other files, you have the option of recovering from backup instead of paying the ransom. It's important that you use some type of automated backup that regularly backs up all your files and that you test your restore procedures to make sure you can recover them if the need arises. There are numerous simple Cloud and local backup solutions that you can install on your computer that will securely and regularly back up all your files for you.

"Cyber criminals often trick people into installing ransomware and other forms of malicious software through phishing email attacks."

Major University In California Pays Large Ransom After Ransomware Attack

The University of San Francisco (UCSF) is the latest organization to fall victim to hackers, running afoul of a group utilizing the Netwalker ransomware strain.

UCSF is a research university whose recent efforts have been focused on health sciences generally and COVID-19-related research specifically. On June 3rd, 2020, Netwalker published a notice on a site they use for data leaks.

It stated they had successfully breached the UCSF network, publishing a sample of the files stolen during their attack. The sample included a number of student applications, complete with social security numbers, and screen shots of folder listings that appeared to contain financial information, medical studies, university employee information and the like. Later the same day that the post and samples appeared on the Netwalker leak site, UCSF confirmed the attack.

Their formal statement on the matter reads in part, as follows:

"As we disclosed on June 3, UCSF IT staff detected a security incident that occurred in a limited part of the UCSF School of Medicine's IT environment on June 1.

We quarantined several IT systems within the School of Medicine as a safety measure, and we successfully isolated the incident from the core UCSF network. Importantly, this incident did not affect our patient care delivery operations, overall campus network, or COVID-19 work.

The data that was encrypted is important to some of the academic work we pursue as a university serving the public good. We, therefore, made the difficult decision to pay some portion of the ransom, approximately $1.14 million, to the individuals behind the malware attack in exchange for a tool to unlock the encrypted data and the return of the data they obtained."

It's a staggering sum that underscores just how serious these kinds of attacks can be. Worse, over the last several months, UCSF is the third university to be successfully attacked. With months to go in 2020, they will almost certainly not be the last.

If 123456 Is Your Password, Change It Immediately

You probably aren't familiar with the name Ata Hakcil. He's a computer engineering student who recently conducted one of the largest password security surveys currently available.

To conduct his research, he collected a number of username and password "data dumps" from the Dark Web and analyzed the passwords he found there. Hakcil was able to analyze a massive collection of more than a billion passwords, looking for trends and commonalities.

IT Security Professionals have long known that password security is an area of persistent weakness that leaves companies of all shapes and sizes exposed. Hakcil was able to measure and assess just how bad that problem is. What he found was depressing.

The most commonly used password in the collection he analyzed was simply '123456,' which appeared in his dataset more than seven million times. It is the most widely used password in the world. Put another way, a staggering 1 person in 142 was found to have used that simple password. As you might suspect, that is laughably easy for a hacker to guess using the simplest of techniques.

In addition to that, Hakcil discovered that the average password length is 9.48 characters, which isn't great. Given the password referenced above, is better than you might have guessed.

Other relevant and intriguing statistics culled from this study include things like:

- Only 12 percent of passwords include a special character
- 29 percent of the passwords reviewed used alphabet characters only
- 13 percent used numbers only
- Given the above, fully 42 percent of all the passwords in the dataset were vulnerable to quick "dictionary style" attacks that would allow a hacker to gain access with minimal effort.
- The most common 1000 passwords unearthed by this research accounted for 6.607 percent of the total, which gives hackers a long list of low hanging fruit to work with.
- With the most common 1 million passwords, the hit rate is 36.28 percent. With the most common 10 million passwords, the hit rate is 54 percent. This makes most networks incredibly easy to breach.

If you're wondering why we keep reading about so many high profile data breaches month after month, the results of this research go a long way toward explaining it, and that's unfortunate.