TELCO UNITED CYBER

12 Steps To Protect Against Ransomware

Introduction

According to the National Cyber Security Center, in 2021 there was a huge increase in the amount of ransomware attacks reported globally. Supply chain attacks increased dramatically, double extortion enabled hackers to export stolen data to separate locations, and unpatched vulnerabilities continued to be one of the most common exploits hackers used to steal data. To top it off, the US Treasury credited $5.2 billion in bitcoin transactions to ransomware.

Unfortunately, ransomware is showing no signs of slowing down. In the first half of 2021, the average ransom payment was $570,000, which was an 83% increase from the previous year's findings, reported at $312,000. With ransomware on the rise, attacks will continue to infect schools, businesses, hospitals, banks, and government offices, to name but a few. Hundreds of new strains of ransomware continue to flood the internet daily, so how are you supposed to better protect your businesses?

At ThreatLocker we want to help you build a cybersecurity stack that is resilient to any cyber-attack that comes your way. We understand how important it is to not only protect your business but also those you look after. To help you on your journey, we have put together this eBook. Inside you will find 12 steps that will help you win the war on cyber threats, whilst keeping you protected against ransomware. You'll also see why the need for a policy-driven, Zero Trust, endpoint security solution has never been greater.

The US Treasury credited

$5.2 billion

in bitcoin transactions to ransomware

In the first half of 2021 ransom was said to be

$570,000

an 83% increase from 2020

TELCO UNITED CYBER

What is ransomware?

Ransomware is a type of malware that infects your computer, network systems, and the data held on them. The data becomes encrypted by the hacker, with access blocked until the ransom has been paid. While you might expect to regain access to your data once the ransom has been paid, there have been numerous cases where the data has not been returned. In a recent report conducted by Sophos, it was reported that 65% of people who paid the ransom got their data back, leaving 35% without all their data restored.

Ransomware is a money-making scheme, generated by hackers to exploit vulnerabilities and trick users into paying for their data to be returned. There are many variations and ways to distribute ransomware, however, the majority of ransomware is distributed via targeted attacks and phishing. No matter the strain, ransomware needs a path to follow in order to gain access to the user's data. By clicking on a suspicious link, opening an email from an unknown user, or downloading malicious files, the ransomware strain will gain direct access to the computer and data.

Once the machine has been infected, the malware will begin to encrypt the data. Typically a pop-up will cover the user's screen demanding a payment to be made to a cryptocurrency wallet. Here they will be instructed to pay the ransom in the form of a cryptocurrency, such as Bitcoin, Monero, and Zcash. Cybercriminals often threaten to release or withhold, the stolen data if the payment has not been made causing extreme amounts of damage and downtime. It is important to assume you will be hit at some point, and ensure your cybersecurity stack is strong enough to protect your business and those you look after.

Ransomware is malicious. It will strip your business of the ability to function, destroy your data, and cripple your funds. The need to better protect your business and those you protect has never been greater. In the following pages, you'll learn how to do just that. With the help of the ThreatLocker solution and our team of Cyber Heroes, we can help you win the war on cyber threats.

STEP #1

Allowlisting

Did you know that most employees use between 5-10 applications to perform their job functions? With that in mind, operating systems are left wide open leaving your business vulnerable to zero-day or new trending malicious malware, including ransomware. When you don't restrict which applications can run, you leave yourself exposed to vulnerabilities or the misuse of legitimate software. Although you might have software such as antivirus, this can often fail and leave you exposed.

Starting with an Allowlisting approach will enable any application to be blocked regardless of whether it is known or unknown malware. Default Deny has long been considered the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, Default Deny puts you in control over what software, scripts, executables, and libraries can run on your endpoints and servers. This approach not only stops malicious software but also stops other unpermitted applications from running. This process greatly minimizes cyber threats and other rouge applications running on your network.

STEP #2

Add Dual Factor Authentication to Management Tools and Servers

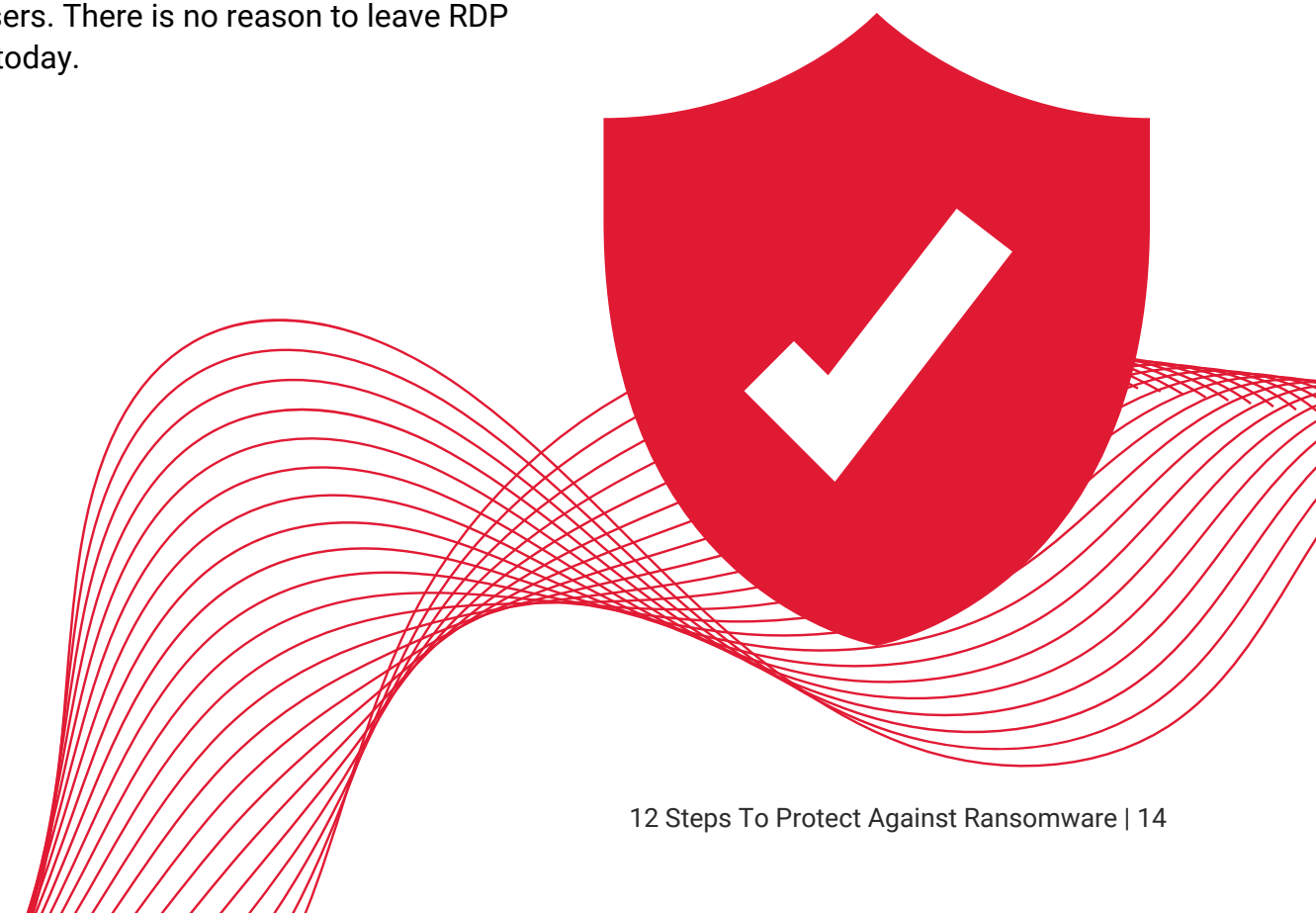
As an IT Professional, your aim is to protect business infrastructure from the inside out. However, all too often the tools needed to do this are being exploited. I.T. management, Remote Monitoring and Management (RMM), and other similar tools are extremely powerful. They make the job of I.T. professionals easier, but when used by an attacker, it can also make the deployment of malicious software easy. Add Dual Factor Authentication onto your RMMs, Antivirus, Remote Control Software, and any other platform that could allow access to both you and your customers' systems. Dual factor authentication should not be considered enhanced security for I.T. or MSP tools. It should be standard. Most platforms are free, so it makes it easy to enable this extra layer of security across all applications.

TELCO UNITED CYBER

STEP #3

Lock Down your Perimeter Firewall

Protecting your perimeter firewall helps to better protect you against hackers. When you leave ports such as RDP open you become vulnerable to malicious attacks. First and foremost you need to lock down all direct connections to Remote Desktop or similar services. If you do need to publish RDS, do so using a Remote Desktop Gateway server and protect the gateway with dual-factor authentication. There are many free Dual Factor applications available. DUO, for example, takes no more than 20 minutes to install and is free for up to 10 users. There is no reason to leave RDP open on the internet, if it is open, shut it down today.



TELCO UNITED CYBER

STEP #4

Restrict User Access

Human error is one of the biggest causes of successful ransomware attacks. Many employees are unable to tell the difference between a legitimate email, and a phishing email encrypted with ransomware. Hackers are very good at posing as employers within a company. A recent report from the FBI highlighted phishing as the most common cybercrime in 2020, and in a report from Verizon, 85% of breaches in 2021 were due to human error. So what can be done?

Training your employees around the risks associated with cyber threats, and showing them what not to click often isn't enough. We need to help them better protect themselves and with Ringfencing, you can do just that.

Ringfencing is a technique that is unique to ThreatLocker.

This technique is extremely effective at stopping attacks that live off the land. When businesses assign permissions to resources, they often do so at a user level. What we often do not realize is that every time we open an application on our computer, that application has full access to everything that we do. If an application that we are running is hijacked, exploited, or flawed, we want to be able to limit the amount of damage that the application can do.

Ringfencing allows you to define rulesets governing how an application can interact with other applications, and what resources an application can access. For example - If both PowerShell and Microsoft Office are required in your environment, that does not mean that Microsoft Office needs to be able to interact with PowerShell. Create Ringfencing policies to stop user frontend applications from interacting with system tools. Then create policies to stop applications like RegSRV32 and PowerShell from accessing the internet. This might sound complicated, but ThreatLocker has over 50 predefined policy sets that can be added in a few seconds.

STEP #5

Don’t Just Look for Malware, Look for the Footholds

Antivirus software often focuses on searching for active malware, but far too often dead services or scheduled tasks are left dormant causing no harm until a set date and time. Use additional layers such as threat hunting to detect and remediate these threats. “Cyber threat hunters bring a human element to enterprise security, complementing automated systems. They are skilled IT security professionals who search, log, monitor and neutralize threats before they can cause serious problems”, reports IBM. Threat hunters will dedicate their time to finding hidden malware so they can prevent a cyber-attack from happening. Not only does this add an extra layer of reliability to any cyber security stack, but it also minimizes the damage that the attack could have caused.

STEP #6

Set Default Lockout Group Policies

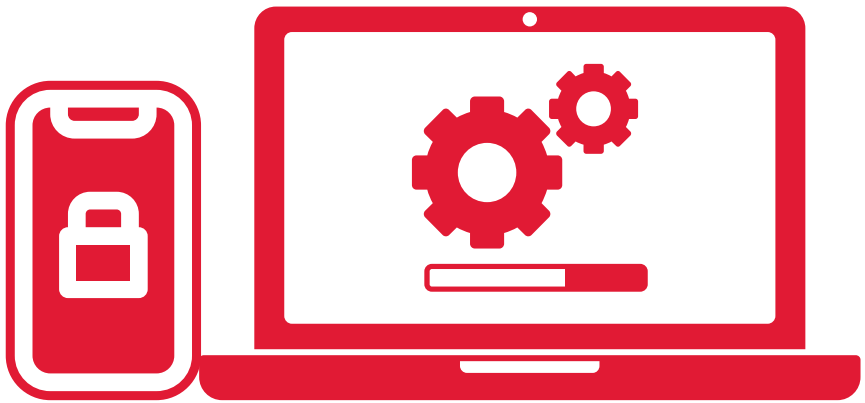
A lockout policy enables administrators to determine how long a user should be locked out of their account. For example, if a user were to forget their password a certain amount of times, the user would automatically be locked out. This enables the administrator to ensure that an attacker can't use a dictionary or a brute force attack to try and guess the user's password. This process is free and can be completed in no time at all. Admins need to simply set the default lock policy on computers to 10 minutes, or a reasonable number. Leaving machines unlocked, or forgetting your password will leave your machine vulnerable to cyber-attacks. Always assume hackers have the means to exploit any computer at any time and start locking your machine or setting lockout group policies.

STEP #7

Patch your Computers

Did you know, you can have the best security software in the world, and at best it will be 75% effective if your computers are not patched and up to date?

In 2017, Equifax were hit with a huge data breach. More than 143 million U.S consumers were affected, sensitive information was stolen, including credit card numbers, phone numbers, social security numbers, etc. The result? Equifax had to pay almost $1billion in legal fees and additional charges. Their reputation was compromised, their customers were fleeing, and their future was up in the air. During the investigation, it was discovered that the breach was the result of an unpatched web application. Hackers were able to get in and hijack their computer systems and network. As you can see, patching is not optional. Always make sure your machines are up-to-date and patched with the latest software.



TELCO UNITED CYBER

STEP #8

Disable Macros

Macros are automated input sequences used to imitate mouse action or keyboard clicks. These programmable patterns are then used to automate work and trim down the time it takes to complete tasks on programs such as Microsoft Excel and Word.

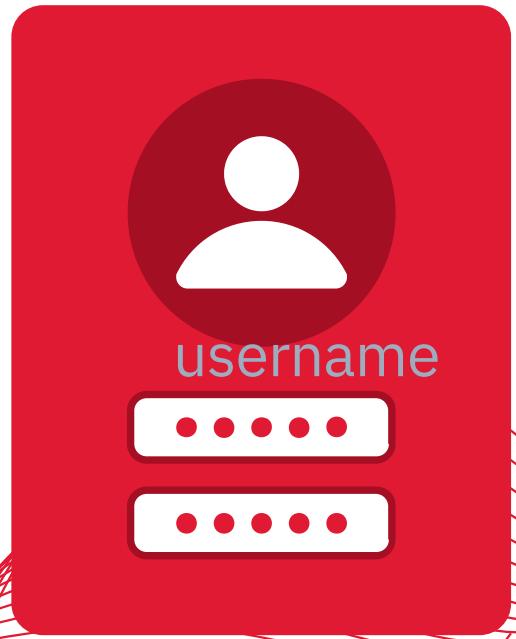
Unfortunately, hackers can exploit macros, turning them into malicious viruses that will hijack machines. With so many businesses across the globe now using automated programs to complete tasks, macro attacks are dramatically increasing. You can avoid macro attacks by simply disabling them on your machine using a group policy or doing it manually. If you don't need them, it's better to disable them before it's too late.

Adding Ringfencing to your cybersecurity stack will enable you to limit what approved applications can run on your network. In doing so, you will stop any malicious macros from talking to the other applications running on your machine. Before the macro has even been able to exploit your data, Ringfencing has seen it and stopped it. You can always reach out to one of our Cyber Heroes if you want to learn more about how Ringfencing can enhance your cybersecurity stack.

STEP #9

Use Secure Passwords

Using a strong and secure password is a vital step when it comes to better protecting your data. Hackers are extremely clever. They use software to crack passwords, enabling them to crack even the toughest of passwords. Having a long and complex password full of numbers, capital letters, special characters, etc, will help your data stay protected. There are a huge variety of password generator tools available, and password managers, which will help you generate an unhackable password and keep your data safe. The more you do to protect your data, the harder it will be for hackers to gain access to it.



TELCO UNITED CYBER

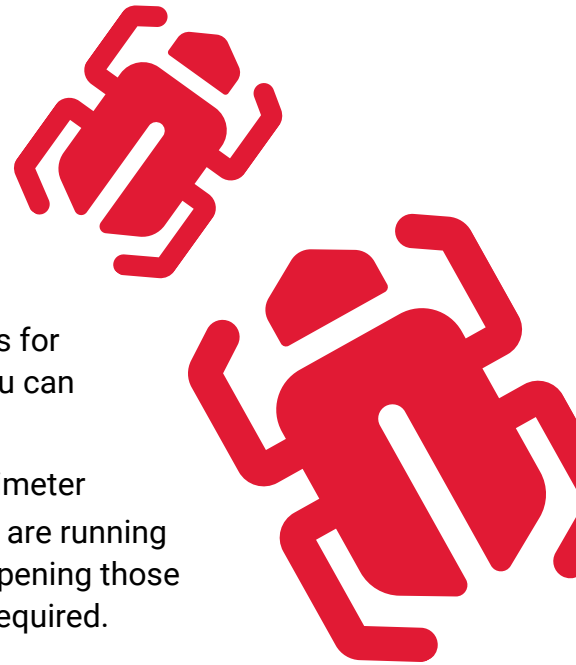
STEP #10

Monitor your Domain Admins Groups

Monitoring your domain admin group is a vital step to becoming better protected. It is important you know who operates within this group and when new users are added. If a user is added without permission, or without the need to be a domain admin, you will increase the risk of a security breach. Your group should be limited to the minimum and monitored closely for any suspicious activity. If a hacker already has access to your system, it won't take them long to insert themselves as a domain admin. In doing so they will have access to every machine, across every network. Once they carry out their attack, the effects will wreak havoc. Locking down your domain admin group will stop this from happening. It's important to get ahead of the game before the hacker even has the chance to win.

STEP #11

Turn on the Windows Firewall



Did you know that ransomware attacks can propagate across your network? One of the easiest ways for ransomware to propagate is by using push installers. As scary as this may sound, there are ways you can mitigate this type of attack from happening.

For instance, always make sure you turn on your Windows Firewall, or another personal firewall. Perimeter firewalls are not enough, you need to always assume your perimeter has been breached. Even if you are running servers that require dangerous ports to be opened, develop the habit of turning on the firewall and opening those ports. Most servers do not need RPC ports to be opened, and if they do, only open them where it is required.

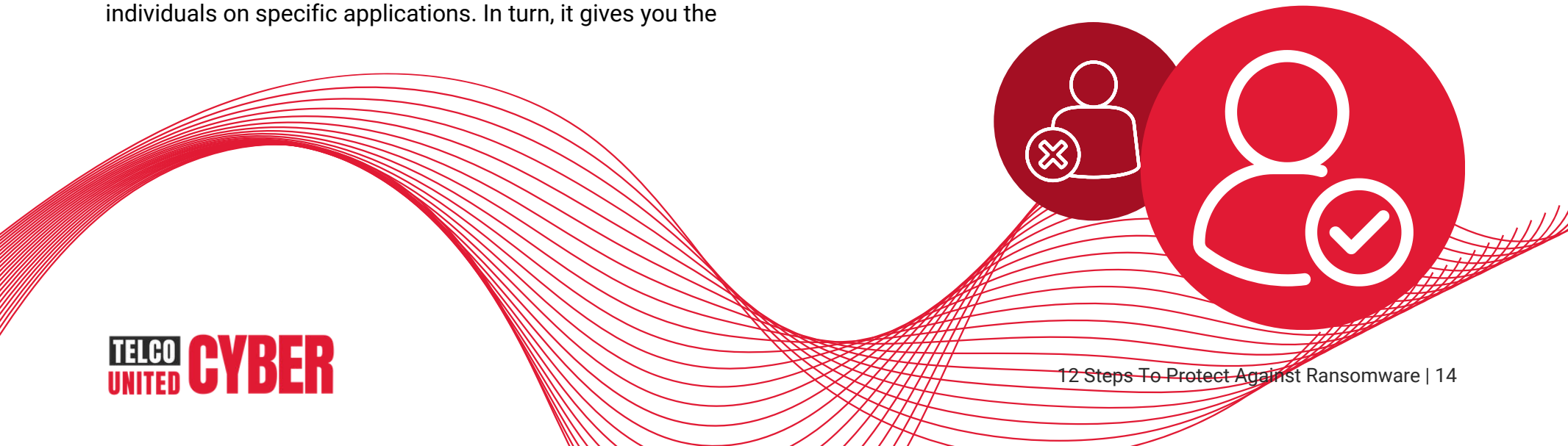
STEP #12

Don’t Make Users Local Administrators

It is important to note that users who are local administrators can knowingly and unknowingly make changes to their system which can allow malware to infect the operating system. It is also worth noting that you probably won’t want to add domain user groups to the administrator group. If an attack is going to happen, doing the above will enable the attack to wreak havoc on your machines and network. Make sure you remove regular user accounts from the local administrator’s group. That includes your own account. If you need administrator access, use a second login.

ThreatLocker Elevation Control can help you do this. It connects to its cloud-based Application Control Suite to add an extra layer of security by creating access policies for individuals on specific applications. In turn, it gives you the ability to approve or deny an individual’s administrator access to specific applications within an organization even if the user is not a local administrator.

There are many ways in which Elevation Control can help you monitor user activities. If you’re thinking of adding a solution like this to your cybersecurity stack, why not meet with a Cyber Hero and let them show you exactly how it will benefit you and your business.



TELCO UNITED CYBER

Conclusion

Ransomware is continuously evolving. Unfortunately, it is impossible to predict exactly when a cyber-attack might occur, but it is vital you remain prepared. By implementing these 12 steps, your business will have all of the necessary tools needed to either stop an attack from happening, or stop it from spreading any further. It is also worth noting that all of your employees should be made aware of these steps, so they can take the time to educate themselves around the importance of cybersecurity. Employees tend to be the weakest link, so getting them up to speed, and trained on the latest security software will only help strengthen your efforts. The great news is, defense solutions are on the rise, and it has never been easier to better protect yourself.

By implementing the ThreatLocker solution, you can help secure all of the data that lives within your business and stop it from becoming encrypted. Adding a Zero Trust, policy-driven security solution to your endpoints will help you better protect yourself against imminent cyber-attacks. You are the only person who should decide what happens to your data, and we can give you the tools you need to ensure it never falls into the hands of a hacker.

TELCO UNITED CYBER