THREATLOCKER

12 Things You Should Have Done to Stop Ransomware

Over the last few years, we have signed up hundreds of MSPs. We like to ask every new customer why they are considering ThreatLocker. Generally, the need for policy-driven zero trust endpoint security is the main objective. This does not stop us from asking if they have had issues with ransomware, viruses, or any other malicious software in the past.

We have gathered what we've learned from our customers and compiled a list of **12 things you should be doing to stop ransomware from killing your business.** This guide includes security solutions that you should be implementing.

This is not a complete list, and the focus is on items that are not being implemented, rather than the protections that are usually already in place. Some readers will inevitably disagree and think many of these items are overkill. The hard truth is, the items on this list would have prevented a majority of the attacks we have investigated.

Default-Deny

Most employees use between 5-10 applications to perform their job functions. With that in mind, operating systems are pretty much left wide open, so any application, malicious or otherwise, can run, leaving your business vulnerable to zero-day or new trending malicious software, including ransomware. By not restricting what can run, you leave yourself exposed to vulnerabilities or the misuse of legitimate software. Antivirus software only attempts to block the bad stuff and oftentimes, it fails. If you start with a default-deny approach, any application will be blocked regardless of whether it is known or unknown malware.

Unfortunately, application whitelisting has a pretty bad reputation because of the complexities around managing deployment and updates. ThreatLocker has addressed these issues head-on, making application whitelisting not only feasible but extremely simple.

Not only can a default-deny approach be used to block access to unknown applications, but application whitelisting also be used to block access to tools such as Powershell and registry editors where they are not needed.

Lock Down your Perimeter Firewall

Leaving ports such as RDP open on the internet is somewhat of a laughing matter on many Facebook groups, Discord channels, and other social platforms. Although, it is not so funny when you talk to businesses who have lost all of their data from a ransomware attack.

First and foremost, 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 excuse to leave RDP open on the internet, if it is open, shut it down **TODAY!**

Add Dual Factor Authentication to Management Tools and Servers

Our job as I.T. professionals is to protect our infrastructure, but far too often, our tools are being used against us. I.T. management, Remote Monitoring and Management, 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, especially since many platforms cost nothing. Enable it on everything! Far too many MSPs and I.T. departments are getting breached, whether it be ScreenConnect, Kaseya, GoToAssist, or Teamviewer. Do yourself a favor and turn on dual-factor today!

Restrict User Access

It is nice to trust that your employees will not do something bad, however, far too many companies have colossal file shares that anybody can access. Even if you trust your employees, restrict access to files and folders based on what they need to perform their job functions. If they do somehow manage to run ransomware, at least the damage will be restricted to what they can access.

Ringfence your Applications.

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. I have already discussed reducing user permissions to file shares and making sure users are not administrators. 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.

A recent trending attack is the use of links and macros in Microsoft Word documents to spawn applications such as PowerShell or RegSRV to encrypt or copy your files to a remote host. If you can, block applications like PowerShell using Application Whitelisting, however, in many cases, these tools are needed to perform other functions.

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 loads of predefined policy sets that can be added in a few seconds.

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.

Set Default Lockout Group Policies

This is free and can be completed in no time. Go onto both your and your clients' domain controllers and set the default lock policy on computers to 10 minutes, or a reasonable number. It is not OK to presume an attacker has no way to get onto a computer. Assume the device will be compromised, and make sure that computers are not left running and unlocked.

Patch your Computers

This should not be up for debate. Patch your operating system and third-party applications. 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. I have seen far too many cases of old vulnerabilities like Eternal Blue used to create admin accounts on servers and push out ransomware. **Patching is not optional!**

Disable Macros

Macros were considered magic in the 1990's. We lived in a world of automatic documents and spreadsheets. Unfortunately, it wasn't long before attackers realized they could automate the same processes in order to attack our computers. As we quickly approach 2020, macros are seldom used, if you don't need them, disable them. You can disable macros by using Group Policy or manually on the computer.

Use Secure Passwords

I am amazed by the number of Managed Service Providers who sign up for ThreatLocker and complain about the password complexity requirements being too long. Our password complexity requirements are not long at all. Confirm that your users are using secure passwords, and be sure to use secure and unique admin account passwords.

Monitor your Domain Admins Groups

As the years go by, you will find more and more users have been added to the domain admin group on your domain controllers. Users should NEVER be running as a domain administrator! Check your domain admin groups, and remove everyone apart from a limited number of users. While you are at it, rename your default administrator accounts.

Turn on the Windows Firewall

For ransomware attacks to be successful, it needs to propagate across your network. One of the easiest ways for ransomware to propagate is by using push installers. Turn on your Windows Firewall, or another personal firewall. Perimeter firewalls are not enough, 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.

Don’t Make Users Local Administrators

This week we hired a new marketing manager, and she needed to install a printer. The installer required her to be a local administrator, and it would have been the easiest thing in the world to make her one. However, this simplicity comes at a severe cost. Users who are local administrators can knowingly and unknowingly make changes to their system that allow malware to get deep within the operating system.

Even worse than making a user a local administrator, is adding the domain users group to the Administrators group on the local computer. Not only does the user have system-level access to their machine now, but they also have system-level access to all computers on your 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.

Use ThreatLocker Storage Policies to Protect your Files

In addition to Ringfencing applications from running, you should also protect your files with policy-driven controls. Setting user permissions is a given. Still, you should also configure file share, USB, and other policies to restrict access to files, not only at a user level but also at an application level. A few examples of simple yet effective policies that can stop your files being encrypted by ransomware:

1. Block untrusted application access to your file shares. If you have a QuickBooks share, only allow the QuickBooks application access to this share. Not only will this stop ransomware from encrypting your files, but it will also prevent users from copying and pasting the data. It only takes a few minutes to limit application access to your shares and is very effective at stopping ransomware from crippling your system.

2. Stop users from saving untrusted file types to your servers. I saw a case recently where an attacker replaced an excel file with an .exe on a file server. The file has the same icon, and when the user ran the .exe, it opened the original spreadsheet. What the users did not realize is they also initiated a hidden malware attack. Make a list of file types that need to be saved to your server, and create a policy to stop any writes for anything else.

3. The worse case after a ransomware attack is the backup drives are also encrypted. Nothing is a replacement for an offsite backup that is not connected to your network. But you can also give your local backups an extra layer of protection. Configure a storage policy in ThreatLocker, to only allow your backup software to access your backup drives.

While this whitepaper is intended to help you reduce the risk of a ransomware attack, it does not substitute a comprehensive cybersecurity plan.

To learn more about ThreatLocker visit: **www.threatlocker.com**