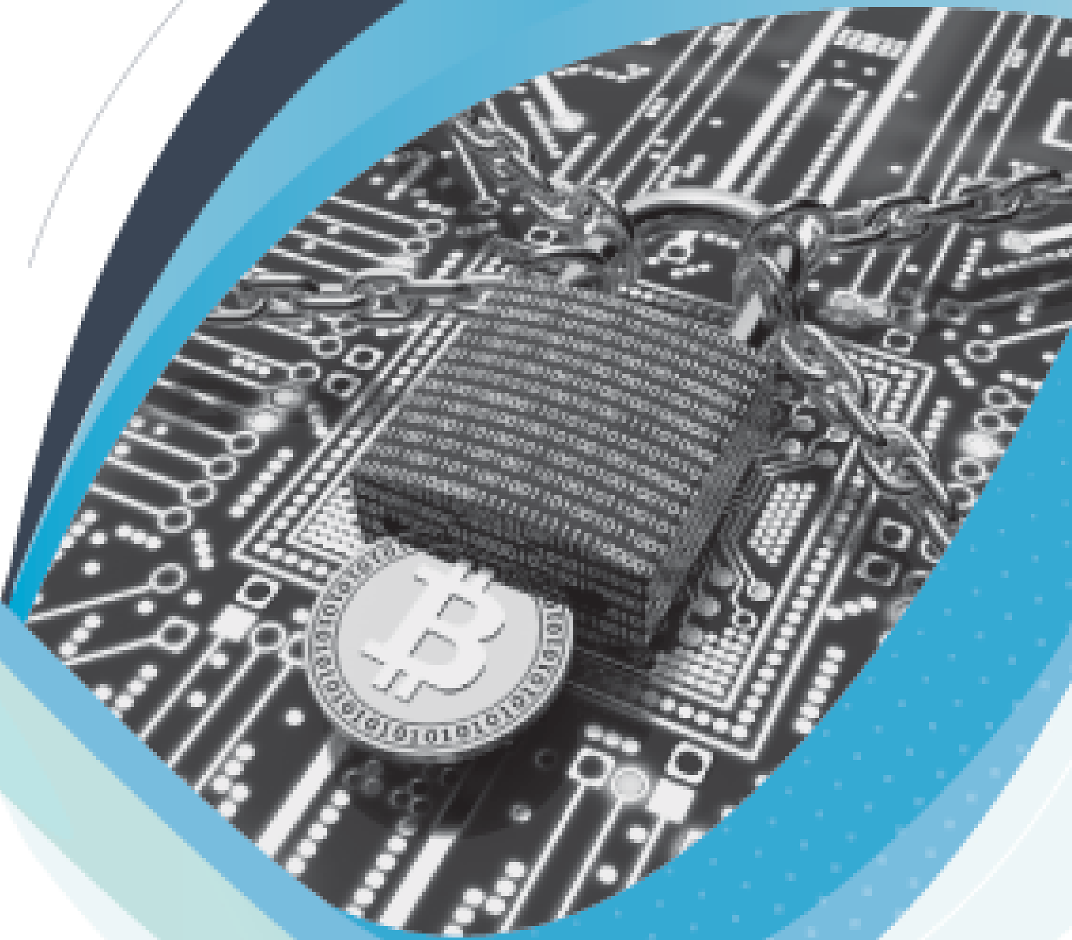
# 4 SIGNS

## you're under attack from ransomware

by:

brightflow TECHNOLOGIES

ABIDE



# You've probably heard a lot about **ransomware recently.**

This is the computer attack where a hacker locks you out of your systems and data. And you must pay a ransom, typically in Bitcoin, to get access again.

While it's not a new crime, it's one of the fastest growing crimes online. Because it's so lucrative to criminals.

And thanks to Covid and Work From Home, more and more businesses are unintentionally opening themselves up to the threat.

In fact, it's estimated there are more than a hundred calls to insurers every day relating to problems caused by ransomware.

Scary.

So unless you take necessary precautions, your business could fall victim at some point.

# But how do you know you're not already **under attack?**

Because here's something most people don't realize about ransomware.

If a hacker gets access to your systems today... they won't launch the attack straight away

It can take around 60 to 100 days - if not longer - from the time you're breached, to the delivery of ransomware.

So it's possible that you already have unwanted visitors hiding in your network. Now that's a scary thought .

You might be wondering why these cyber criminals spend such a long time launching their attack.

They spend weeks or more just looking around, investigating your network for weaknesses, and waiting for just the right time to maximize their profit.

Not only that, but weirdly, the longer they take, the harder it is for you to discover them.

# So how do you know if you're under attack? **And what do you do if you are?**

Here are 4 of the best ways for you (or preferably your IT service partner) to check that your network is safe and secure.

**This guide is a little more technical than the ones we normally write**. We'll explain the concepts in a way anyone can understand, of course.

But we must tell you about some specific technical things and software that can be signs of an impending attack.

## 01 CHECK FOR OPEN RDP LINKS

What's an RDP link and how do you open or close it?

We don't want to get too techy here, so put simply, an RDP (or Remote Desktop Protocol) is Microsoft technology that allows a local computer to connect to and control a remote PC over a network or the internet.

You're probably utilizing this kind of thing if you've had any of your people working from home this year, as it makes remote access a lot easier.

But RDP links left open to the internet are a very common route for cyber criminals to enter your network.

Scan for open RDP ports regularly, and utilize multi-factor authentication for your links (multi-factor authentication is where you generate a code on a separate device to prove it's really you).

Or have them behind a VPN (Virtual Private Network), which gives you a private network from a public internet connection.

This really is a specialist job. Your IT service partner should be able to do it for you.

## 02 LOOK FOR UNEXPECTED SOFTWARE

One of the methods ransomware gangs use to take control of your system is certain software tools. It's important that you use a Network Scanner to check exactly what's running and who's running it.

Often, cyber criminals will take control of just one PC first, perhaps using a phishing email to persuade someone to click on a bad link without realizing it.

Once they have control of one PC, they can then target the entire network.

Sometimes, tools such as AngryIP or Advanced Port Scanner are used to do this. Check your network for tools like these. If they are present and your IT people haven't installed them, it's possible you have a problem.

Criminals also utilize tools to steal your passwords and log in credentials. Tools such as Mimikatz and Microsoft Process Explorer.

If you spot anything unfamiliar anywhere in your system, get in touch urgently with your IT support partner, who can investigate further.

## 03 MONITOR YOUR ADMINISTRATORS

Your network administrators typically have the authority over which applications are downloaded to your network.

So what's the best way for hackers to download the applications they need? They create a new administrator account for themselves.

Then they can download whichever tools they need to compromise your network.

You need to be aware of software such as Process Hacker, IOBit Uninstaller, GMER and PCHunter. These are all legitimate tools which could be used by any IT specialist.

But in the wrong hands they can be dangerous. And hackers can use them to disable your security software.

## 04 CHECK FOR DISABLED TOOLS AND SOFTWARE

Once the cyber criminals have administrator rights, they can locate and disable your security software.

You can tell that an attack is close to being launched if Active Directory and your domain controllers are disabled.

Next, any backup data the criminals have found will be corrupted. And any systems that automatically deploy software will also be disabled, to stop your attempts to  update your computers after an attack.

Something called PowerShell will then be used to spread everything across your network.

It's worth remembering that this will all be done slowly.
Your hackers will take their time, because that makes it much harder to detect them.

Many security tools only record traffic for a set period of time,  and are then reset. This means that there is no data held on the entry. Which disguises the attack until it's ready to launch.

Once an attack has been launched and your data held to ransom, most of the time there's little you can do other than attempt to restore backups. Or pay the ransom.

The hackers have normally been so thorough with their preparation that even the best IT security specialists have few options open to them.

brightflow TECHNOLOGIES

# So, once you've detected that something might be wrong, **what can you do to stop an attack from being launched?**

The most important step is to regain control of your RDP sessions – remember, the remote access we mentioned earlier on.

This will stop attackers coming in again. And will also cut off their control access.

You can force a password change across your core systems, which will also throw your attackers out. However, it's worth noting that this is pointless if your RDP access is not cut off and controlled, as the attackers will just re-enter.

Monitor your administrator accounts. This may sound like a simple step, but you'd be surprised at how often it's neglected. You should also monitor and limit who can use PowerShell within your organization. Without getting into the details of what PowerShell is; just know it's a powerful tool you don't want the wrong people playing with.

Keep all of your software and security patched and updated. It's very tempting to click 'later' on updates. But saving a little time now is not worth the huge amount of time and money that you'll lose should you become the victim of a ransomware attack.

Implement multi-factor authentication across all of your applications, if you haven't already. This adds another level of security for your network and helps to prevent unauthorized access.

Finally, build your security from the ground up, and make sure every member of staff throughout the business – from CEO to entry level worker – has regular security training. If everyone is aware of the risks and how to avoid them, it could stop a potential attack in its tracks.

Because this is such a highly technical subject, it's not something you or your team should tackle on your own. You need IT security specialists to take preventative action, and monitor your systems regularly for early signs of problems.

# This is what our team does. **We're the experts you can trust.**

Let us look at your current data security arrangements and advise you on ways you can improve it. Trust us, you'll sleep a lot better at night.

www.brightflow.net
704.893.8445

brightflow
TECHNOLOGIES