Emerald ICT
Complete Computer Solutions

June 2017

NEWSLETTER

WannaCry Ransomware Explained: Is Your Business At Risk?

You'd be hard-pressed to miss last week's biggest headline, the WannaCry cyber-attack sent shockwaves around the globe. Businesses of all sizes and even police departments found themselves crippled without warning.

Among the most prominent victims were many NHS hospitals in the UK, affecting up to 70,000 individual devices such as essential MRI scanners and blood-storage refrigerators. But by the time it hit the news, it was too late – either your system was protected, or it was infected. Here's how it all went so wrong.

What is WannaCry?

The WannaCry cyber-attack was a type of malware (the collective name for computer viruses & bad juju) called 'ransomware'. Just like the name suggests, it's actually a demand for money. Like all ransomware attacks, WannaCry encrypts your files and holds them hostage until you pay. In this case, the price was set at £300, payable with internet currency Bitcoin, and you had 3 days to pay before it doubled. If you didn't pay, the ransomware threatened to delete your files permanently. It's yet unknown how much money the WannaCry hackers have earned with their latest attack, but you can be sure plenty of people have paid the ransom. Even the FBI recommends paying the ransom, especially if the ransomed files are of a sensitive nature or weren't backed up.

How It Spread So Fast

It seems WannaCry may be a 'computer worm' that self-replicates and spreads, rather than a phishing attack that needs to be activated with a click. So far, no common trigger has been identified, as is normally the case with phishing links. WannaCry moved rapidly from system to system, spreading out through the entire network, including all connected backups and storage devices. At the same time, it spread out to infect other networks, who then spread it further, and so on. Given the nature of the internet, it was everywhere within hours.

Why Some Businesses Were Safe

WannaCry could ONLY infect systems that have fallen 2 months behind in their Windows updates. This is because it was created to take advantage of a specific vulnerability in Windows, one which Microsoft patched months ago. Without that patch, the ransomware could waltz right past the firewall, past the anti-virus and directly into the system (the NHS were reportedly running Windows XP – no longer supported). Those running Windows 10 or a fully patched, recent version of Windows were completely unaffected – the virus literally had no way in

It just goes to show the importance of staying up to date. We haven't seen a second spike in WannaCry attacks yet, but that doesn't mean there won't be one. A quick update could protect your business from weeks of downtime and lost revenue, making attacks like this a non-issue.

Emerald ICT
Complete Computer Solutions

With our managed services, we can make sure you stay up to date – and protected. Give us a call today at 0113 2579992

More than 150,000 computers worldwide have been infected by a new Ransomware called WannaCry. Learn more about it and how it affects your business in this month's newsletter.

Ransomware attacks can cost £150-£600 to get your files released, IF they honor your payment.

How Much Could A Ransomware Attack Cost You?

Have you ever thought about how much your data is worth? Information is possibly the most valuable part of your business – there's your client database, accounting software and inventory management, and of course, any intellectual property you may own. When the ransomware, WannaCry, tore through the world recently, many businesses were suddenly forced to re-assess the value of their data: was it worth saving, and what would be the deeper cost of the attack?

Most ransomware attacks cost £150-£600 to get your files released, but that's only IF the cyber-criminals honor the payment and actually give you the decryption key. Meanwhile, new client calls are still coming in and you may find yourself unable to operate with your systems down. Paying the ransom or restoring from an unaffected backup seems like a quick fix, but it doesn't end there. There's still the downtime involved to restore all your data – possibly days – and that's a lot of lost productivity. Plus, if word gets out that your data has been compromised, you may find confidence in your business plummets and your existing clients head elsewhere. That £150 ransom may end up costing well over £150,000!

Prevent Ransomware Attacks on your Business

Keep your systems up to date: WannaCry took advantage of a flaw in older versions of Windows, one that was since patched by Microsoft. But to be protected, businesses had to be up to date with their patches AND be running a supported version of Windows. Delaying patches and updates puts your business at risk - we can help you update automatically.

Lock down employee computers: Very few staff will require full administrator access to your business network. The higher their level of permissions, the more damage a person can do – either accidentally with a whoopsie click, or by inadvertently installing malware. By locking down your employee computers, you have a better chance of containing a malware attack to non-vital systems. Our experts can design an access management plan that gives you best of both worlds: flexibility PLUS security.

Educate your workplace: Most employees believe they're being cyber-safe but the reality is quite different. Many malicious links and embedded malware have become hard to spot in an instant – which is all it takes to click and regret. We can work with your staff to establish procedures around checking links for authenticity before clicking, awareness around verifying the source of attachments, and the importance of anti-virus scanning. We'll help get the message through!

Have a solid backup plan: When ransomware hits, a connected backup = infected backup. Unfortunately, synced options such as Dropbox immediately clone the infected files, rendering them useless. The only safe backups will be the ones both physically and electronically disconnected, with systems designed to protect against attacks like this. Our experts can set you up with a backup system that makes recovery a breeze.

Be proactive: The best way to avoid the financial cost of a ransomware attack is to prevent it from happening in the first place. Remember, many businesses were able to watch WannaCry from the sidelines, completely unaffected and seizing opportunities while their competitors were down.

Emerald ICT
Complete Computer Solutions

Our managed services can help protect your business against the next cyber-attack.

Call us at 0113 2579992 today.