starcom.
A Node4 Company

5 WAYS THAT RANSOMWARE HOLDS YOUR BUSINESS HOSTAGE

Ransomware is a form of malicious software characterised by threats, demands and holding systems or data hostage. Once it has infiltrated hardware or networks, cybercriminals demand a ransom from the victim business, claiming that they'll restore access and data upon payment. Ransoms can range from the hundreds to thousands of pounds.

These types of attacks are having somewhat of a resurgence, in part thanks to the growing – and essential – digitisation of business. Here we reveal 5 ways that ransomware holds your business hostage and the preventative measures your IT team can take.

1 Dupes with phishing emails

Have you ever received an email that you thought twice about acting on? There's a chance this suspicious communication was an attempted ransomware attack. We call these "phishing" emails, and they distribute ransomware by enticing recipients to read an email and open a link or attachment which contains the software.

DID YOU KNOW ?

23% of recipients open phishing emails

11% actually open attachments

Nearly **60%** of ransomware attacks come from email

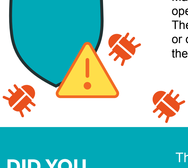
2 Hijacks open endpoints

Cybercriminals use shrewd tactics when deploying ransomware. They frequently access your systems via unused or vulnerable endpoints – internet-capable devices such as desktops, laptops and smartphones. From here, ransomware spreads until it reaches your data and business-critical systems.

DID YOU KNOW ?

Ransomware attacks are growing more than **350%** annually, and a business will fall victim every 14 seconds.

3 Exploits well-known vulnerabilities



Many attacks are based on known weaknesses in operating systems, web browsers and applications. These vulnerabilities are often caused by unpatched or out of date systems. Savvy cybercriminals exploit these gaps to launch ransomware attacks.

DID YOU KNOW ?

The WannaCry attack was designed to infiltrate unpatched or outdated Windows operating systems. Nearly all of the **200,000 computers** infected were end of life.

4 Fakes its way with malvertising

You may have unsuspectingly been exposed to malvertising and had a lucky escape. This form of ransomware sees attackers infiltrate networks and insert malware-laden ads into legitimate websites. Those who click will have their system infected with ransomware.

DID YOU KNOW ?

Malvertising is becoming more sophisticated and cost the ad industry **$1.1billion** in 2018.

5 Sneaks in via external devices

External devices, such as USB drives, are used to store and transfer files — making them targets for spreading ransomware. Some of these files contain an advanced feature that is used by hackers to launch ransomware when a file is opened.

DID YOU KNOW ?

Australian police issued a warning about USB drives containing ransomware appearing in mailboxes. The USBs masqueraded as a promotional Netflix app, then once opened deployed ransomware.

Without intelligent, tailored and trustworthy cybersecurity, it's worryingly easy to become a ransomware attack victim.

In just a matter of minutes, your business could be left in dire straits. But don't worry – risk can be mitigated by taking a proactive approach to protection.

Contact the Starcom team on 0844 579 0800 to book a Health Check.