Ransomware

A Quick Guide

wanstor

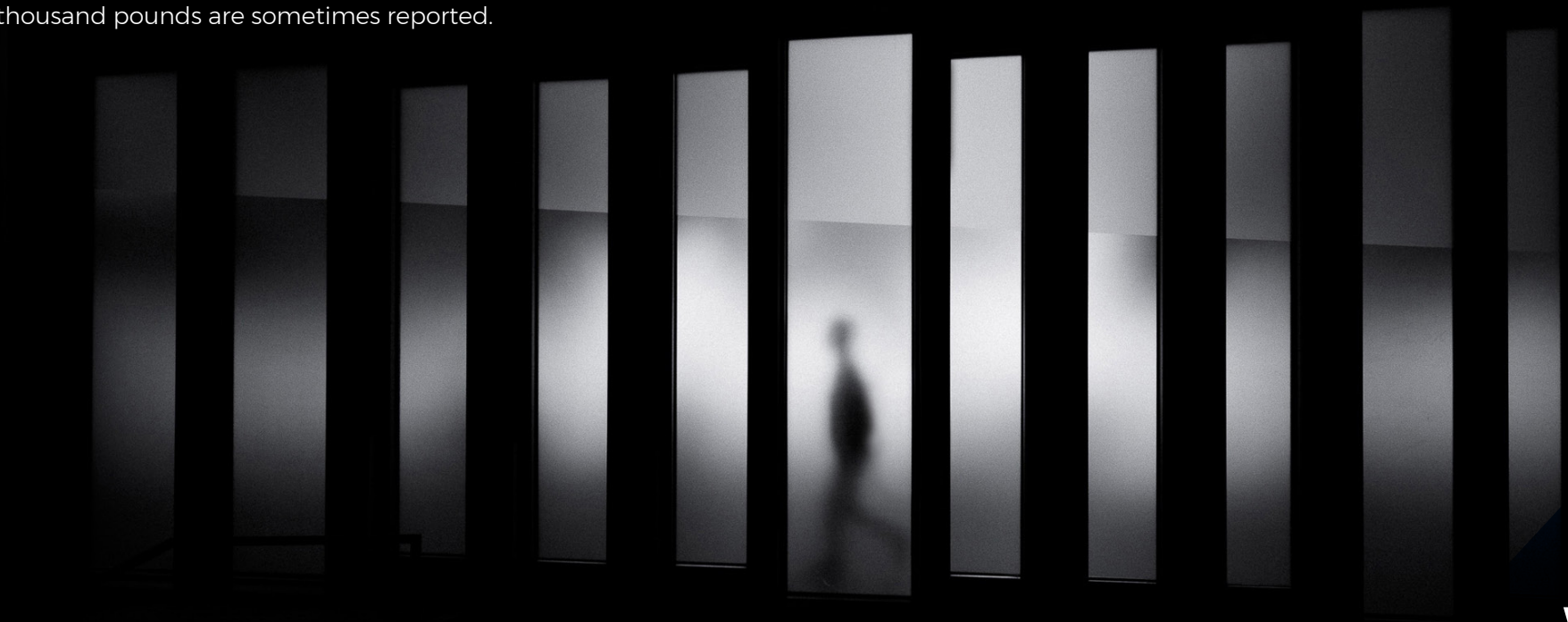
Ransomware can be crippling for an organisation if left unchecked as it is a type of malware that blocks access to a system, device, or file until a ransom is paid.

At Wanstor we understand a number of businesses and not for profit organisations have been hit recently by hackers using Ransomware. This almost always occurs when the ransomware encrypts files on the infected system (crypto ransomware), although a few variations are known to erase files or block access to the system using other methods (e.g. locker ransomware).

The cyber threat actors behind ransomware most commonly demand that the victim pays £200 - £1,000 in bitcoins, though other currencies, gift cards, and ransoms of up to several thousand pounds are sometimes reported.

From our extensive IT security understanding, we know that Ransomware almost always involves opportunistic targeting, with dissemination through false advertising or spam emails containing malicious attachments.

In the past several months, Wanstor has become aware of several ransomware variants that include additional independent components, such as data exfiltration, participation in distributed denial of service (DDoS) attacks, and anti-detection components.



wanstor

AT WANSTOR, WE SUGGEST ALL IT TEAMS TAKE ON BOARD THE FOLLOWING RECOMMENDATIONS:

Securing Networks & Systems

+ Identify devices connected to and running on your network, keeping hardware, OSs, applications and software updated and patched

+ Use antivirus software with automatic signatures and updates, firstly checking existing anti-virus software licence is valid and supported

+ Ensure the IT team perform regular backups of all systems to limit impact of data loss, and store backups offline; some ransomware can encrypt backup files if visible on the network.

+ Put in place a backup system that allows multiple iterations of backups to be saved, in case any copy contains encrypted or infected files. Verify backups are operational. Rebuilding or reimaging an infected system from a known good backup or fresh installation is the only known way to guarantee infection has been removed from any system.

+ Implement an anti-spam solution to help stop phishing emails from reaching the network. Consider adding a warning banner to all emails from external sources that reminds users of the dangers of clicking on links and opening attachments.

+ Consider the use of a proxy server for Internet access and / or ad blocking software.

+ Implement software restriction policies or other controls to prevent unauthorized programs from executing, especially when stored in locations frequently used by malware, such as temporary folders.

+ Where possible, use virtual environments as they help provide isolation and enable faster recovery.

+ Vet and monitor third parties that have remote access into the organisation's network and / or your connections to third parties.

+ Also make sure they are as diligent as your IT team is when considering cybersecurity best practices.

+ Consider disabling user access to personal webmail and social media accounts.

+ Make sure staff know where and how to report suspicious emails and possible infections.

Securing the End User

+ Provide employees with social engineering and phishing training. Urge them not to open suspicious emails, not to click links contained in such emails, not to post sensitive information online, and to never provide usernames and/or passwords to any unsolicited request.

Responding to a Compromise or Attack

+ Unplug infected systems from the network to prevent further infection.

+ Restore files from regularly maintained backups.

To find out more information about Wanstor's IT Security solutions and how they can help protect your organisation from attack, please contact us on 0333 123 0360, email us at info@wanstor.com or visit us at www.wanstor.com

wanstor