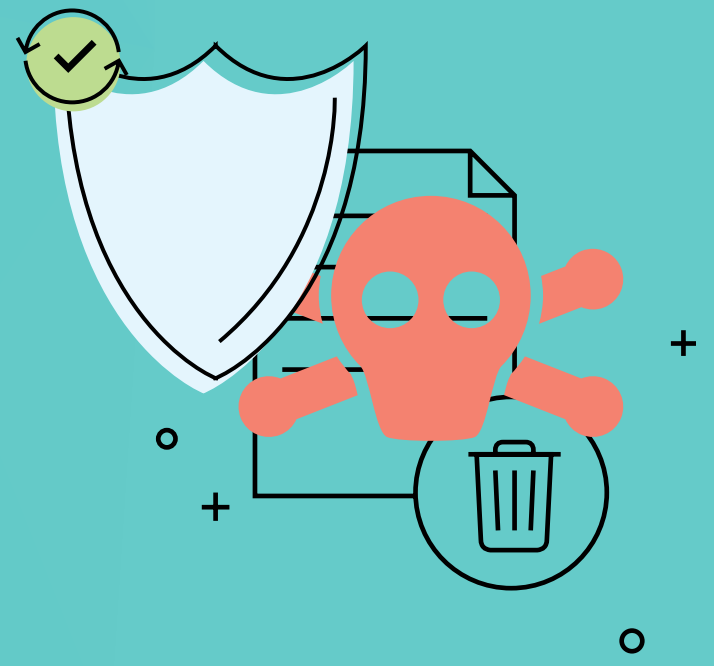
EBOOK

Enter-at

The Guide to CryptoLocker Protection And Removal



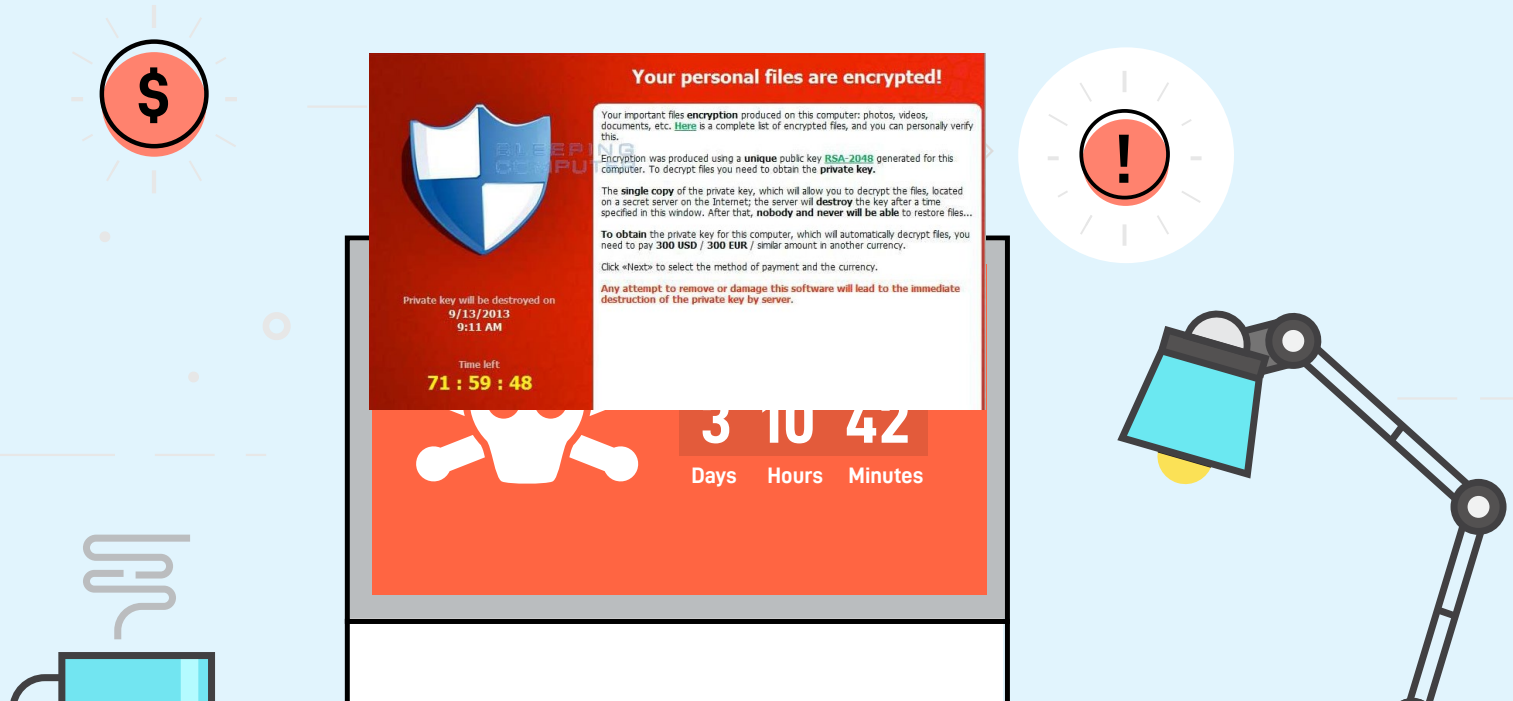
RAN*SOM*WARE (RANSƏMˌWE(Ə)R/)

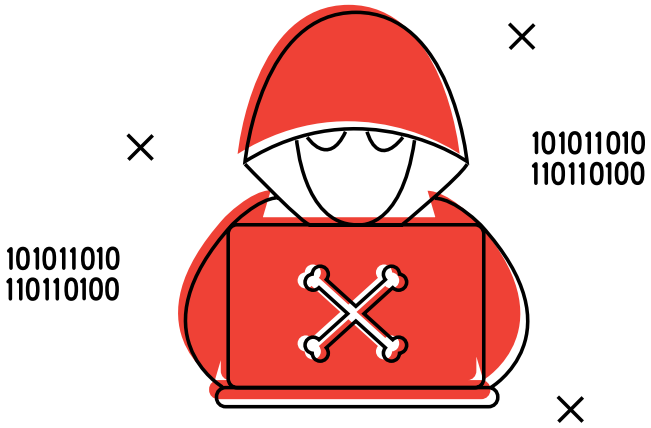
NOUN

A type of malicious software used by a cyber criminal to block access to a computer system until a sum of money is paid.

WHAT IS RANSOMWARE?

In order to discuss CryptoLocker, first we must have a handle on ransomware. According to the definition offered by the US Department of Homeland Security, ransomware is a type of malware that infects computer systems, restricting users' access to the infected systems. Ransomware variants, such as CryptoLocker, extort money from victims by displaying an on-screen alert stating that the user's systems have been locked or files have been encrypted. Unless a ransom is paid, access will not be restored.





CryptoLocker is one of the most common strains of ransomware attacking companies around the world **every single day.**

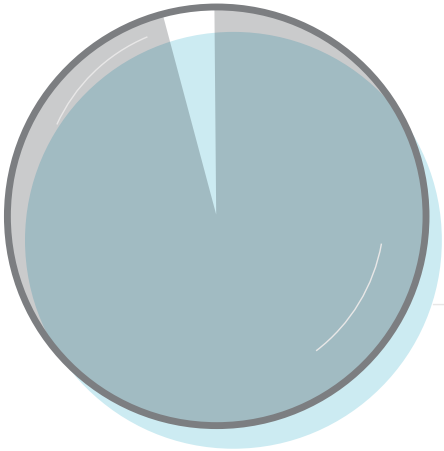
CryptoLocker is one of the most common strains of ransomware attacking companies around the world every single day. In a recent global survey of over 1,000 IT service providers, 95% reported recent encounters with CryptoLocker infecting small business clients. CryptoLocker renders it's victim's files unreadable using encryption, then demands payment to un-encrypt them. This variant is considered one of the top cybersecurity threats to businesses today.

Typically, CryptoLocker ransom demands are not particularly high—usually in the range of £200 to £500. However, the cost of downtime associated with ransomware can add up quickly, especially if the malware spreads beyond a single computer and onto your company's network. Recent statistics report that 63% of small-to-midsized businesses have suffered business-threatening downtime as a result of a successful ransomware attack.

Businesses in particular can (and should) minimise the impact of CryptoLocker and other forms of ransomware. This guide offers an overview of what you can do to protect yourself from these cyber attacks and how to recover quickly in the (not so rare) case you do fall victim.

CRYPTOLOCKER PROTECTION

Preventing a CryptoLocker infection is obviously the best possible way to avoid downtime. However, there is no single defense solution currently on the market that can 100% guarantee ransomware prevention for businesses. Instead, step up your data protection game with these leading recommendations for increasing your front line of defense.



In a recent survey, **95% of IT service professionals** reported recent CryptoLocker attacks against small buinesses.

- Install reputable anti-virus and firewall technology;
- Ensure all applications are patched and up-to-date;
- Proceed with caution when opening emails; Do not click links or open email attachments you aren't expecting; verify the contents of the attachment first.
- PRO TIP: Right click the link and copy the URL then paste it into a new browser window to be certain that the link doesn't lead to a malicious website; and
- Ensure that all employees are trained on these email best practices—phishing scams are the #1 cause of ransomware's success today.

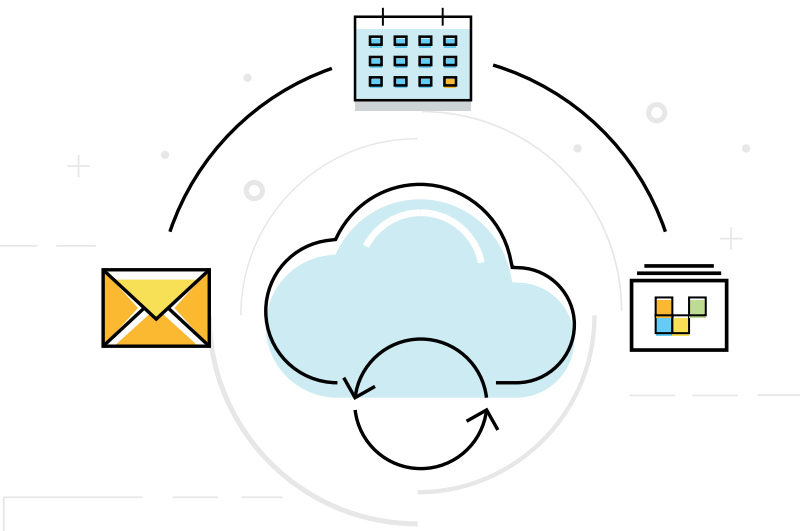
CRYPTOLOCKER RECOVERY

Like many of the leading ransomware strains today, CryptoLocker code is constantly being adapted to avoid detection by the leading solutions of defense available. In fact, 93% of IT service providers report ransomware infiltrating anti-virus and anti-malware software in the past 12 months and 77% report it infiltrating email and SPAM filters. The social engineering tactics cyber criminals employ to dupe their victims continue to be highly effective, likely due to the void in cybersecurity training within businesses.

So, let's say the worst has happened and you are staring CryptoLocker in the screen. To recover, you must be able to restore your data to a point-in-time that is *before* the attack occurred.

Here's the bottom line. It is essential to deploy a modern backup and recovery solution, such as Datto, to protect all of your critical data, files and folders. Taking proper backups is the best way to ensure you'll be able to recover files fully and quickly without paying ransom or worse, suffering from downtime.

Don't neglect the vulnerable data that lives in cloud-based applications, such as Office 365 and Google Apps. Despite popular belief, **ransomware targets these SaaS solutions as well.**



And, when I say "all of your data," I mean it. Don't neglect the vulnerable data that lives in cloud-based applications, such as Office 365 and Google Apps. Despite popular belief, ransomware often targets these SaaS solutions as well. So, if your business is in the cloud, it is essential to deploy a cloud-to-cloud backup solution such as Datto Backupify.

Finally, you need to be certain your systems are completely free of CryptoLocker before restoring any data.

Here are the basics to CryptoLocker recovery:

- Take independent backups that store files on an alternate system;
- Set up and stick to a regular backup schedule;
- Choose a backup solution that takes backups periodically throughout the day to minimise data loss;
- Choose a backup solution that offers fast restore times to minimise application downtime;
- If you rely on a cloud-based offerings such as Office 365 or Google Apps, invest in a industry-leading cloud-to-cloud backup solution; and
- Use a ransomware removal tool to be sure your systems are clean before restoring data.

CONCLUSION

There is no question that CryptoLocker and other forms of ransomware are a major threat to all businesses today. However, you can mitigate the impact by putting the right technologies and strategies in place. As there is no single solution that answers the ransomware problem, a layered approach is best. Security and backup are both important in protecting your business from data loss whether it be from ransomware or something else. It is also important to observe cybersecurity best practices by educating all employees on how to recognise suspicious emails, ads and websites.

For more information please contact:

Richard Henderson | Director
Phone: 01869 220280
Email: Richard@enter-at.co.uk
Enter-at | enter-at.co.uk