F A C T S H E E T

Australia & New Zealand's National Identity & Cyber Security Support Service

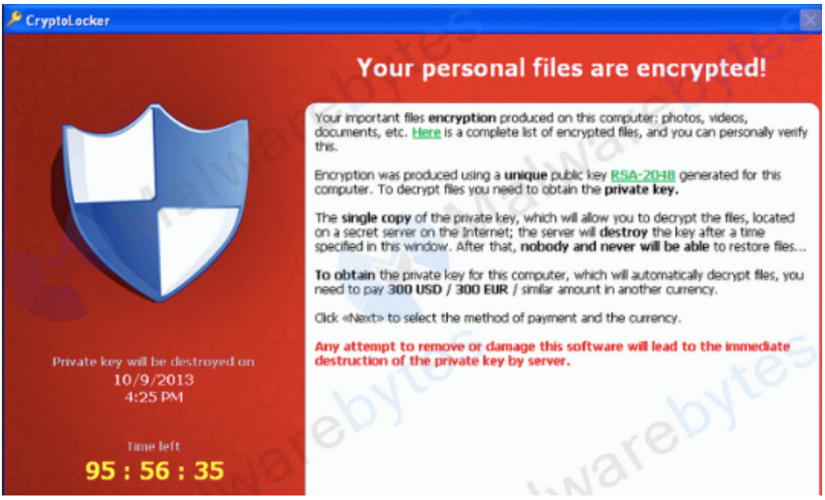
iDcare

# FACT SHEET: RANSOMWARE

**Ransomware** is a form of malware (a virus) that encrypts files, or denies the ability for a user to access their device, or both. There are many forms of ransomware, but they all lead to a demand for payment of a ransom for access to be allowed. Attacks typically come in the form of phishing emails, downloading free software, and remote access scams (someone being provided access to another person's device and installing ransomware whilst in control). Once the ransomware has been executed, such as by clicking on links or attachments, the criminals have largely automated their whole process. Pop-ups or other screen messaging will result that alerts the user to "a virus" or "encryption" or "computer being locked". A contact point will be provided, then typically a short timeframe is given to respond to the ransom demand.

## Detecting Ransomware

There are two ways to detect ransomware: (1) prior to executing the malware and (2) after executing the malware. The best way of detecting it before it's executed is through anti-virus. Make sure you run anti-virus on all devices frequently. The other way is when it's been executed and a demand is made.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

**Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.**

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

## Preventing Ransomware

- Ensure you back-up all of your data.
- Run anti-virus frequently and make sure it's the most recent version – millions of viruses are created each year so your anti-virus needs to keep up with these.
- Turn off your cloud storage when you are not using it (like Google, DropBox, OneDrive etc).
- Keep your operating system and apps/ software updated.
- Consider blocking ads and pop-ups, and think twice before downloading freeware (free downloads) without checking their security first!
- Become familiar with how to spot phishing emails and never provide remote access to your device when someone calls or emails you first.

## Responding to Ransomware

There are hundreds of ransomware types, but unfortunately most cannot be decrypted. Ransomware does the encrypting and the criminals using it have the tools to decrypt. Before you think about paying, you may want to try the following:

- EUROPOL and a number of software security vendors have launched a free decryption check called CRYPTO SHERIFF that can be accessed at <www.nomoreransom.org>.
- Decryption services – these are by no means a guaranteed result and most cost money.
- Assess what's at risk and would be lost. If there's too much at stake you may have to consider paying but be careful, you're dealing with criminals.

**For personalised support call IDCARE on 1300 432 273 (Aust) 0800 201 415 (NZ) or email contact@idcare.org**

***Disclaimer***

*© 2017 Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this FACT SHEET, IDCARE disclaims any liability to any person in respect to any actions performed or not performed as a result of the contents of the alert or any accompanying data provided. Note our service is free to the community and our Counsellors will never ask you to provide your personal information and credentials if we make contact with you.*