Module 1 Lab 1 guide: Widgets Plc

Case and screenshots are from <https://malware-traffic-analysis.net>.

# Lab 1: Malware incidents

You are the IT security team for Widgets Plc, a small manufacturer. On a Friday morning, you receive a call that none of the files on the file server are available. Every user who tries to access the files, gets an error message saying the file is corrupted.

You take a look on the share and find a number of files in each directory with the name *help\_your\_files*. You open a number of them and now your screen looks like the one below:

A screenshot of a social media post

Description automatically generated

The text is:

“Cannot find the files you need? Is the content of the files corrupt? It is normal because the files’ names, as well as the data is now encrypted for your protection with best 8192 bit encryption software.

Congratulations!!!

You have become a part of large community #Cryptowall.”

At this point, you know you have a problem. You look at all the files that have been changed, and notice that it was Jim from Human Resources who made the last changes to all the files. Jim is currently on leave to go on a bush walk and is currently outside of the range of mobile phone coverage somewhere deep in the Ureweras in New Zealand.

You check the email inbox belonging to Jim, and notice an email to Jim with the following resume:

A screenshot of a cell phone

Description automatically generated

You upload the attachment to virustotal and get the following report:

A screenshot of a social media post

Description automatically generated

In the meantime, the managing director has walked into your office, and demands to know what has happened. The broken file server has now stopped the business and access needs to be restored as soon as possible.

You are lucky. The backups were run yesterday, and worked. It will take four hours to retrieve the tapes and restore from backup.

**Incident resolution questions**1 What do you say to the director?  
2 The director says four hours to restore the files takes too long, and demands you pay the ransom to regain access more quickly. Is this wise?

**Indicator questions**

3 Who did this?

4 What indicators do you have from this incident?

5 How much time do they take to gather?

6 Where are they on the pyramid of pain?

**Scenario continued**

You are lucky again. Contacting the support channel for the ransomware, they say “It take six hours to get key”. The director now decides that restoring from backup is the best way to go. There are a few files that were changed between the time the backup was taken and now. Some of that data will be difficult to get back.

**Incident resolution questions**

7 Do you take a backup of the encrypted files before the restore? If so, why?

**Indicator questions**

8 What indicators do you have from this incident at this point?

9 How would you communicate them?

**Scenario continued**

You restore from backup and the business continues as usual. When Jim returns from holiday, you confirm that he did indeed open that email. Jim turns his computer on. At lunchtime the file server is encrypted again.

**Incident resolution questions**

10 What do you think happened?  
11 What can you do to prevent a recurrence of this in Widgets Plc?  
  
**Indicator questions**

12 What do you think happened?

13 How could you report this incident to a CERT? What would you supply?