CSN11123/4 Assessment Specification

Details

Module name:	Advanced Cloud and Network Forensics
Module number:	CSN11123/4
Session:	Semester 2, 2014/2015
Weighting:	50%
Submission:	Monday 27 April 2015

Coursework Assignment

Title: **Incident Response:** Investigation of Crytolocker

Outline Requirements

A company has reported that there has been some malicious activity within their company related to Cryptolocker-type activity. The critical incident response team has managed to get a virtual image of the host under suspicion (HUS), along with other traces of evidence that could be used for the investigation (this includes both host activity on the system and network traces).

It is thus your objective to investigate the virtual image, and produce a fair and unbiased report on the findings.

The VM image exists within the Napier DFET Cloud, which also contains the network trace, which can also be downloaded from:

https://dl.dropboxusercontent.com/u/40355863/crime.rar

The analysis should involve analysing the network trace for the connections from the hosts which connected to the host-under-suspicion (HUS). Along with this you should analyse and cross-correlate the activity within the logs on the HUS, and the trace of files left on the system. Evidence should also be gained from the applications which were used within the time window of interest. Please note that all other activity outside this window-of-interest should be ignored.

Host under suspicion: Production -> Crypto -> Crytpo_001, Crypto_002 …

Marking schedule

The coursework should be submitted via Turnitin, in a PDF format, if possible. It will be marked as follows:

- **Investigation Procedure** [20%]. This should outline your procedures for analysing the virtual image.
- **Findings** [45%]. This should outline the trail of evidence produced, and the findings from it.

- **Conclusions** [20%]. This should reflect the methods you have used in the report, and to assess their strengths and weaknesses, and any observations that you have gained.
- **References/Presentation** [15%]. All references must be defined in an APA/Harvard format, and should be integrated in the report.

The report should use the APA/Harvard format for all of the references, and, if possible, should include EVERY reference to material sourced from other places. Also, the report should be up to 20 pages long (where appendices do not count in the page count number).

An outline of this is given at:

https://youtu.be/PCMqrH8sFFY

Marking approach

There are multiple communications within the network trace, some of which have possible malicious intent, and others which are normal non-malicious content. As part of the analysis you should:

- In the report, define a strict methodology that you would apply in actually undertaking the investigation.
- Take reasoned judgments as to the nature of the trace of network activity.
- Where faced with suspect content, try to uncover the root of the evidence, such as cracking cipher codes. The methods tried should be clearly defined in the report.
- Define the timeline of activity involved in the possible malicious activity.
- Cross-corroborate the network traces with the system traces that appear on the host system (such as examining system logs, audit logs, and the file attributes), and report on any suspicious activities.

Each of the areas will be graded A+ (90%), A (80%), A- (70%), B+ (65%), B (60%), B- (55%), C+ (50%), C (45%), C- (40%), D (30%), E (15%) and F (0%). The mark will then be graded, and then reviewed to produce the final grade. All of the grades are indicative, and are used for the final assessment.