**Successfully Deliver**

Below is a copy of my report:

COMP6441 2020T1 Awesome project z3290805

Project Proposal I achieved up to and including a HD criteria.

A computer virus or more specifically a spyware which logs keystrokes in Windows was created. The virus was implemented in Batch and Powershell script. They were compressed together and disguised as an image. It was uploaded to an AWS S3 bucket. The URL to the payload could be sent in a spoofing email. Once the payload is downloaded and extracted by a victim, opening the disguised image runs the script automatically. The script:

1. Hides the window running the scripts to the background
2. Copies the script to startup folder so they run every time the system starts
3. Sends requests to an AWS API Gateway which passes the request body to a lambda function running Node.js.
4. The lambda function saves the keystrokes to DynamoDB.

**Weekly blog post to demonstrate what has been achieved 50%:**

Week2: Research on the history and classification of computer viruses

Week3&4: Start building the script and come up with plans to capture the keystrokes with AWS services

Week5: Follow AWS documents to build the service as planned. Tested with Postman.

Week7: Update and debug scripts to make it work with AWS. Make it run as system boots.

Week8: Record a short video and make this report. Reflections.

**The virus code itself should be evaluated on 25%**:

lethality: The spyware records all keystrokes as soon as the system boots. If the victim login to any account in a browser then all ID and passwords would be compromised. If the virus runs on a public computer then it would affect everyone who uses the computer.

benefit: Everything is saved to DynamoDB for the attacker to review. The ID of the first tuples is randomly generated then the rest are sequential so as the attacker is able to group keystrokes collected from a single session. The attacker could use victim's credentials to access the compromised accounts.

survivability: The virus copies itself to the user's startup folder. Recall the default action of powershell is opening the script in an editor. It would be obvious when the script file is opened in

a window when the system starts. Hence, the Powershell script hides all cmd and notepad windows as it gets executed.

infectivity: The email is spread with the technique of Email From spoofing. It makes the email look like it is sent from a trusted person or entity. A social engineered email could increase the victim to run the payload further. At this time of change due to lockdown, people are vulnerable to information about course updates.

method of evaluation: The AWS infrastructure is decommissioned everytime testing is done (also to save cost). The virus only runs for 40 seconds, as a safety precaution. No code was uploaded to any repository.

**The quality of the final report 25%**: Given the limitation to 1 page, please refer to my blog posts and youtube video for details and references.