



### Packet Capture Analysis:

I have analyzed the provided packet capture file using the free network analysis tool Wireshark. I was able to put "http" into the filter field in order to filter the network traffic to only see HTTP packets.

This view let me see some interesting http GET requests, which indicate that the user specifically requests information.

### Sub-task 1:

To find the images the user accessed called anz-logo.jpg and bank-card.jpg I followed the following process for both images:

First I filtered the packet capture for http traffic and looked through the remaining packets for the GET request that downloaded the image. I then right clicked the image and followed its TCP stream. In the TCP stream I saw what looked like image data. In order to view the data in hex format, I changed the view to 'raw', and then searched the hex data for a jpeg's file signature.

After finding the file signature "FFD8" at the top, and the file footer "FFD9" at the bottom, I copied everything between those two points into the hex editor HxD and saved it as a jpg image. Resulting in the image below.



Bank-logo.jpg



Bank-card.jpg

### Sub-task 2:

I followed the same process to extract these images as I did in sub-task 1, which was to view the TCP stream, identify the images hex data, then copy and save that as a jpg file.

The image for ANZ1.jpg :

# PROTECT YOUR VIRTUAL VALUABLES

TAKE SOME SIMPLE STEPS TO  
PROTECT YOUR INFORMATION



 ANZ Cyber Secure



ANZ1.jpg

The difference in the network traffic for this images download I discovered was a hidden message in the data after the end of the image.

The message said "You've found a hidden message in this file! Include it in your write up."

# MAKE A 'PACT'

## TO PROTECT YOUR VIRTUAL VALUABLES



**PAUSE**  
before sharing your  
personal information

Ask yourself, do I really need to give my information to this website or this person? If it doesn't feel right, don't share it.



**CALL OUT**  
suspicious messages

Be aware of current scams. If an email, call or SMS seems unusual, check it through official contact points or report it.



**ACTIVATE**  
two layers of security with  
two-factor authentication


Use two-factor authentication for an extra layer of security to keep your personal information safe.



**TURN ON**  
automatic  
software updates

Set your software, operating system and apps to auto update to make sure you get the latest security features.

### Report suspicious messages from ANZ:

 Email [hoax@cybersecurity.anz.com](mailto:hoax@cybersecurity.anz.com)

### Report fraudulent or unusual ANZ account activity:

 137 028 / +61 3 8693 7153 (Corporate/Business Clients)

 133 350 / +61 3 9683 8833 (Personal Banking Customers)

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Item No. 96184B 09.2018 AU22349

ANZ2.jpg

This network traffic also had a message hidden in the same way.

It was "You've found the hidden message! Images are sometimes more than they appear."

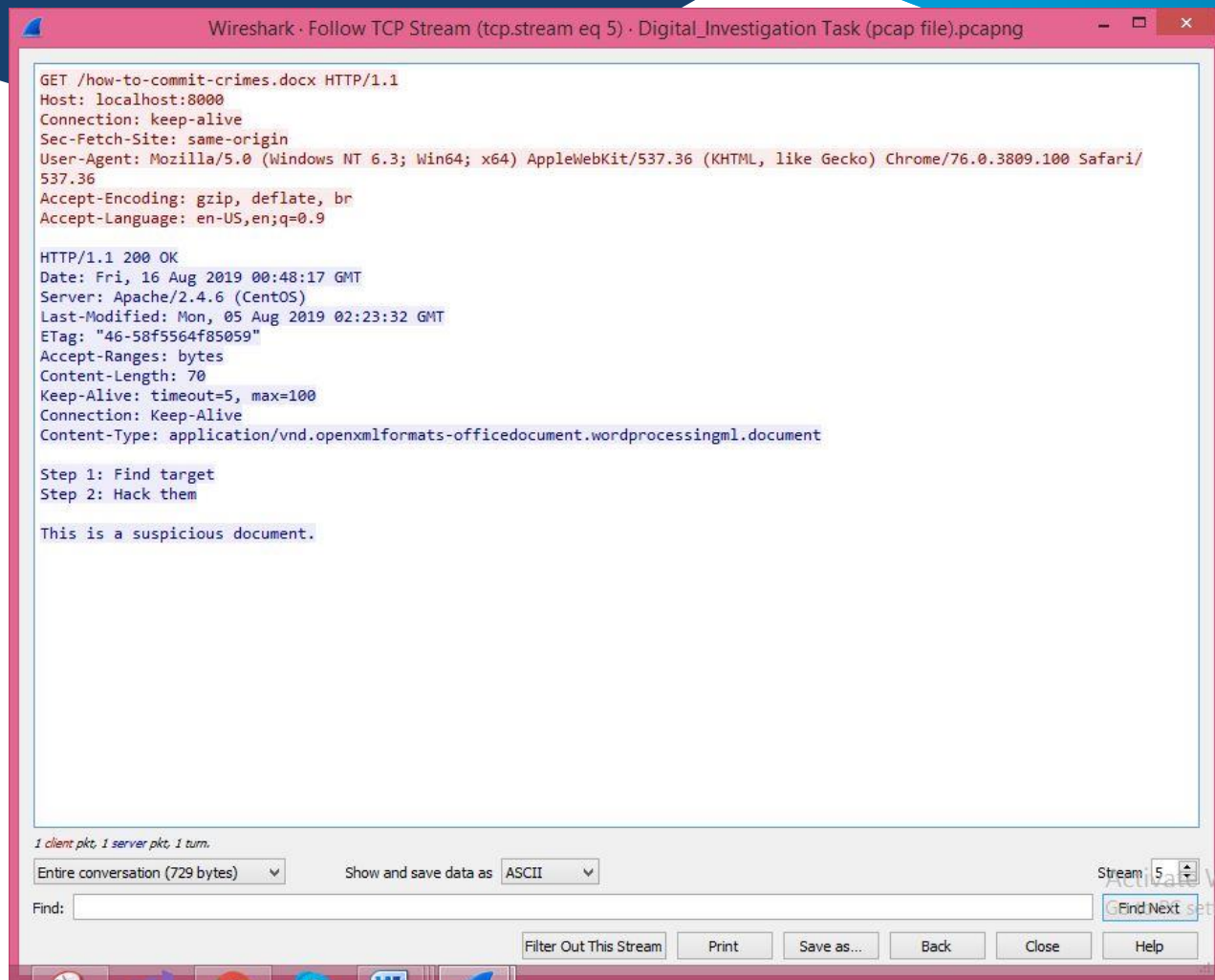
### Sub-task 3:

In order to find the contents of the document, I had to view the TCP stream of the http get request for the file. The documents contents were visible in the ASCII view.

Step 1: Find target

Step 2: Hack them

This is a suspicious document



### Sub-task 4:

In order to view these PDF's I viewed the TCP stream as usual, and found the file signature for a PDF, which was the hex data "25 50 44 46". I noticed in the ASCII view that the PDF data went until the very end of the TCP stream, so I copied all the hex data from the file signature onwards into HxD and saved it as a pdf file.

The same process worked for all three files:



VOLUME  
2

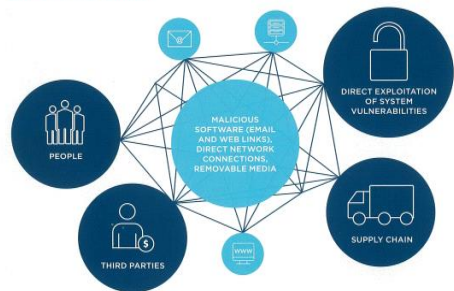
# CYBERSECURITY

WORKING TOGETHER TO KEEP YOUR  
ORGANISATION SAFE



## THE CHANGING CYBER THREAT LANDSCAPE

### COMMON ATTACK VECTORS



### AT A GLANCE

- Cybercriminals exploit any weakness in an organisation's people, process or technology infrastructure
- Using humans to infiltrate organisations is a common factor in most current cybercrime attacks
- Effective processes together with a risk management approach are crucial
- Organisations benefit from a multi-layered risk management strategy - 'defence in depth'
- The ability to know, control and adapt to new cyber threats will differentiate the strong from the weak
- Cyber resilience plans are essential - expect cyber disruption and prepare to deal with it while continuing to operate your business
- ANZ works with our clients to help keep them safe

## CYBERCRIME INNOVATION

Cybercrime continues to threaten the Australian business landscape, with cybercrime expertise improving and adapting to target specific businesses. The ACSC (Australian Cybersecurity Centre) reports the changing environment has seen more diverse and innovative attempts to compromise government and private sector networks, increasing numbers of DDoS incidents, deliberate targeting, and changes in the frequency, scale, sophistication and severity of cyber incidents.

Cybercriminals are increasingly sophisticated in their execution and can be equally opportunistic in who they target - from individuals through to large multi-national corporations, no one is immune from being attacked. This sophistication reflects the innovative methods used and speed of the execution. Cybercriminals innovate, make

decisions and execute faster than many organisations are equipped to deal with. Moreover, cybercrime is now a business in every respect, with services that mirror those of multi-national organisations including customer support and technical helpdesks to ensure their criminal products and services work as intended.

In order to protect your business, you must understand this changing landscape and adapt. Any modern corporate finance function is comprised of three main elements - people, process and technology. Cybercriminals look for and exploit any weakness in one or more of these elements to infiltrate the business to gain access to either information or syphon money, often millions of dollars at a time, into their international network.

CYBERCRIMINALS INNOVATE, MAKE DECISIONS AND EXECUTE FASTER THAN MANY ORGANISATIONS ARE EQUIPPED TO DEAL WITH.

### CYBERCRIME IN ACTION

In March 2017, a Lithuanian man was arrested for duping two unnamed multinational internet companies via an email phishing attack. Google and Facebook later confirmed they were the two companies that fell victim to the scam costing them \$300 million USD. He allegedly posed as a manufacturer in Asia and defrauded the companies from 2013 until 2015, siphoning the money in bank accounts across Eastern Europe.

The emails were sent from accounts designed to look like they had come from an Asian-based manufacturer, but they did not. He used methods such as forging invoices, corporate stamps and email addresses to impersonate this Asian-based manufacturer with whom Facebook and Google regularly did business with.

This attack highlights how sophisticated cyber-enabled fraud scams can fool even the biggest technology companies.<sup>2</sup>

On Friday, 12 May 2017, the world was alarmed to discover that cybercrime had achieved a new record. In a widespread ransomware attack that hit organisations in more than 100 countries within the span of 48 hours, the operators of malware known as WannaCry were believed to have caused the biggest attack of its kind ever recorded. Hospitals, rail systems, telecommunications and courier services were all impacted by WannaCry but many other organisations and individuals were affected as well.

According to an IBM report, ransomware was the most prevalent online threat in 2016. IBM researchers tracking spam trends noted that the rise in ransomware spam in 2016 reached an exorbitant 6,000 percent, going from 0.6 percent of spam emails in 2015 to an average of 40 percent of email spam in 2016. The situation is only worsening in 2017. The FBI estimated that ransomware is on pace to become a \$1 billion source of income for cybercriminals by the end of 2016, a number that is expected to continue to rise in 2017.

<sup>1</sup>[https://www.acsc.gov.au/publications/ACSC\\_Threat\\_Report\\_2017.pdf](https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf)

<sup>2</sup><https://www.mcafee.com/au/resources/articles-and-whitepapers/whitepapers/2017/05/16/2017051601.htm>

<sup>3</sup><https://www.cisco.com/middleware/2017/05/16/2017051601.htm>

ANZ\_document2.pdf (extracted image)

More suspicious stuff good job!

Evil.pdf(extracted image)

### Sub-task 5:

I viewed the TCP stream of this file, and noticed that instead of being plain text it was encoded data and when viewed as hex it had the same file signature as a jpg image. So I copied and saved the hex data with HxD as I have for other images, and discovered that the text file was actually this image.



#### Sub-task 6:

I viewed the TCP stream as normal when investigating this traffic, and found two sets of jpeg file signatures. In the TCP stream I saw what looked like image data. In order to view the data in hex format, I changed the view to 'raw', and then searched the hex data for a jpeg's file signature. After finding the file signature "FFD8" at the top, and the file footer "FFD9" at the bottom, I copied everything between those two points into the hex editor HxD and saved it as a jpg image.

I tried extracting both sets of data, and got two different images. Resulting in the image below.

First image:



Second image:





So the thing that is different about this traffic is that a single GET request performed by the user downloaded two images.

#### Sub-task 7:

To find the images the user accessed called *broken.png* I followed the following process for both images:

First I filtered the packet capture for http traffic and looked through the remaining packets for the GET request that downloaded the image. I then right clicked the image and followed its TCP stream. In the TCP stream I saw what looked like image data. In order to view the data in hex format, I changed the view to 'raw', and then searched the hex data for a jpeg's file signature. After finding the file signature "89 50 4e 47 0d 0a 1a 0a" I copied everything after that point to end and then copy into the hex editor HxD and saved it as a png image. The image as follow:



#### Sub-task 8:

After investigating TCP stream for securepdf.pdf I discover following thing:

The data there was not for a PDF. The bottom of the file contained the hidden message: Password is "secure"  
It contained the file signature for a zip file, meaning that the the user downloaded was actually a zip file.

So I copied the hex of the zip file into HxD and saved it as a zip file. I opened this zip file, and found it contained a pdf file called rawpdf.pdf. When opened, the pdf prompted for a password. The password 'secure' shown in the tcp stream worked and the PDF opened. It was the first two pages to a guide for internet banking.



YOUR GUIDE TO  
ANZ INTERNET BANKING



TABLE OF CONTENTS

Why use ANZ Internet Banking?	3
Online Security	4
Getting started	5
Viewing your accounts	6
Transferring funds	7
Check the details before you pay	8
Your transfer receipt	9
Paying bills	10
Using Pay Anyone	11
International Money Transfers	12
Logging Off	13
Things you need to know	14
Frequently asked questions	15