Network Traffic Analysis Report

Objective

This report documents the investigation into suspicious network activity detected on the ANZ network. A laptop was flagged due to suspicious internet traffic, and an analysis was performed to determine what images were viewed, and what files were accessed and downloaded by the user. The provided packet capture file (pcap) was examined using Wireshark and a Hex editor to identify and extract artifacts contained within the network traffic.

Tools Used

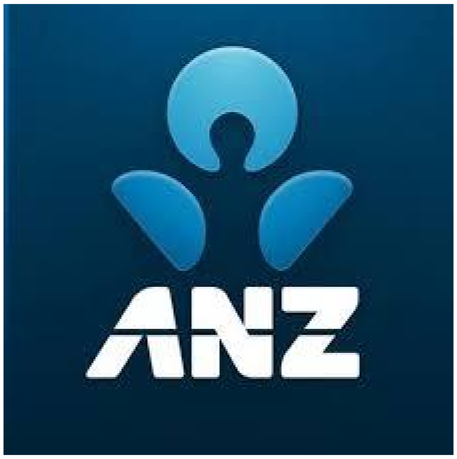
1. **Wireshark** - Used for capturing and analyzing network traffic.
2. **HxD Hex Editor** - Used for analyzing and reconstructing file data from network packets.

Procedure and Findings

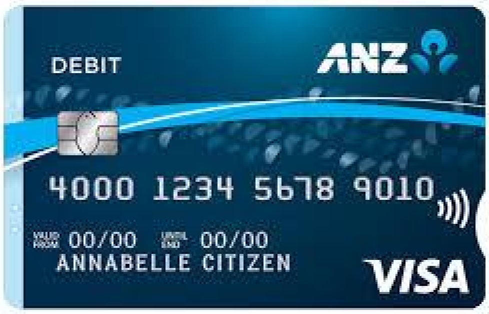
Sub-task 1: Extract anz-logo.jpg and bank-card.jpg

- **Process**:
    - Filter the HTTP traffic in Wireshark for anz-logo.jpg and bank-card.jpg.
    - Use the Follow TCP Stream feature to reconstruct the images.
    - Save the images by exporting the HTTP objects.
- **Findings**:
    - Successfully extracted anz-logo.jpg and bank-card.jpg.
- **Images**:

Anz-logo

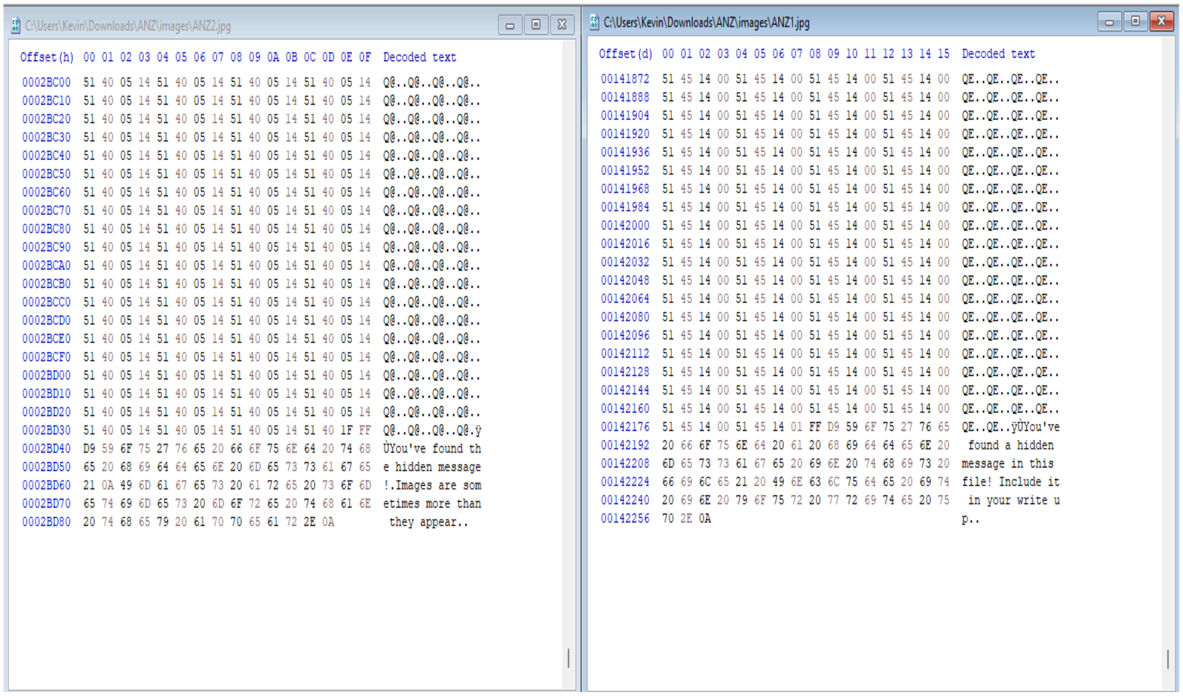


bank-card



Sub-task 2: Extract ANZ1.jpg and ANZ2.jpg

- **Process**:
  - Filter HTTP traffic for ANZ1.jpg and ANZ2.jpg.
  - Extract and analyze the images using Wireshark.
  - Inspect these images using the hex editor to compare file sizes and identify hidden metadata or any anomalies.
- **Findings**:
  - Successfully extracted both ANZ1.jpg and ANZ2.jpg. The files contain different hidden messages located within their decoded text besides their obvious visual differences.
  - ANZ1 hidden message “You've found a hidden message in this file! Include it in your write up”.
  - ANZ2 hidden message “You've found the hidden message! Images are sometimes more than they appear”.

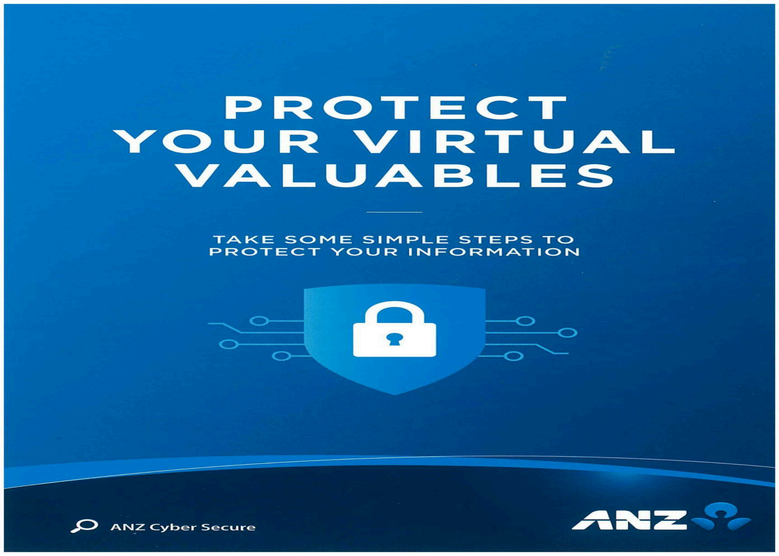


```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

0002BC00   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BC10   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BC20   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BC30   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BC40   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BC50   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BC60   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BC70   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BC80   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BC90   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BCA0   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BCB0   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BCC0   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BCD0   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BCE0   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BCF0   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BD00   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BD10   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BD20   51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14  Q@..Q@..Q@..Q@..
0002BD30   51 40 05 14 51 40 05 14 51 40 05 14 51 40 1F FF  Q@..Q@..Q@..Q@.ÿ
0002BD40   D9 59 6F 75 27 76 65 20 66 6F 75 6E 64 20 74 68  ÙYou've found th
0002BD50   65 20 68 69 64 64 65 6E 20 6D 65 73 73 61 67 65  e hidden message
0002BD60   21 0A 49 6D 61 67 65 73 20 61 72 65 20 73 6F 6D  !.Images are som
0002BD70   65 74 69 6D 65 73 20 6D 6F 72 65 20 74 68 61 6E  etimes more than
0002BD80   20 74 68 65 79 20 61 70 70 65 61 72 2E 0A         they appear..
```

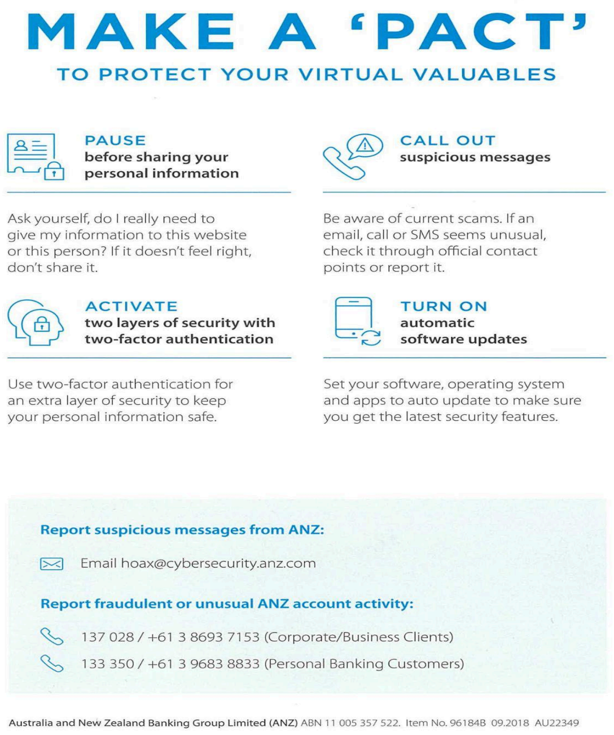
```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text

00141872   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00141888   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00141904   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00141920   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00141936   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00141952   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00141968   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00141984   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142000   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142016   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142032   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142048   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142064   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142080   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142096   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142112   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142128   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142144   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142160   51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00  QE..QE..QE..QE..
00142176   51 45 14 00 51 45 14 01 FF D9 59 6F 75 27 76 65  QE..QE..ÿÙYou've
00142192   20 66 6F 75 6E 64 20 61 20 68 69 64 64 65 6E 20   found a hidden
00142208   6D 65 73 73 61 67 65 20 69 6E 20 74 68 69 73 20  message in this
00142224   66 69 6C 65 21 20 49 6E 63 6C 75 64 65 20 69 74  file! Include it
00142240   20 69 6E 20 79 6F 75 72 20 77 72 69 74 65 20 75   in your write u
00142256   70 2E 0A                                         p..
```

- **Images**

ANZ1-


PROTECT YOUR VIRTUAL VALUABLES
TAKE SOME SIMPLE STEPS TO PROTECT YOUR INFORMATION
ANZ Cyber Secure
ANZ

ANZ2-



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

Report fraudulent or unusual ANZ account activity:

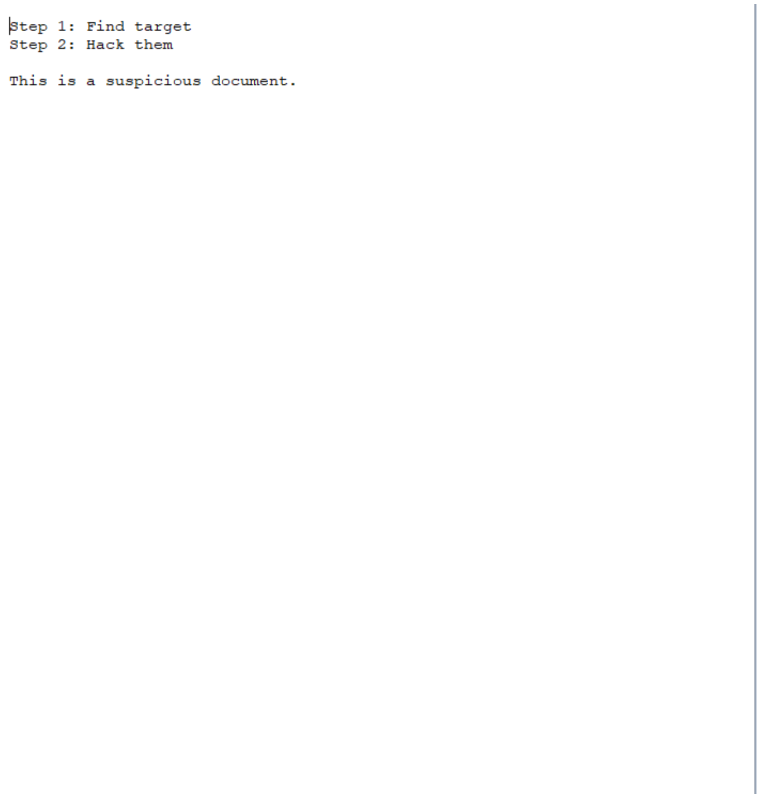
☎ 137 028 / +61 3 8693 7153 (Corporate/Business Clients)

☎ 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

Sub-task 3: Extract how-to-commit-crimes.docx

- **Process**:
  - Search for how-to-commit-crimes.docx in the filtered HTTP traffic.
  - Extract the file using the Follow TCP Stream" option.
  - Open the .docx file in a document editor to view the contents.
- **Findings**:
  - The document is suspicious due to its content, which outlines steps for committing cyber crimes.
  - No irregularities were found in the file’s hex data, suggesting it hasn’t been tampered with or hidden within another file.
- **Document Content**:

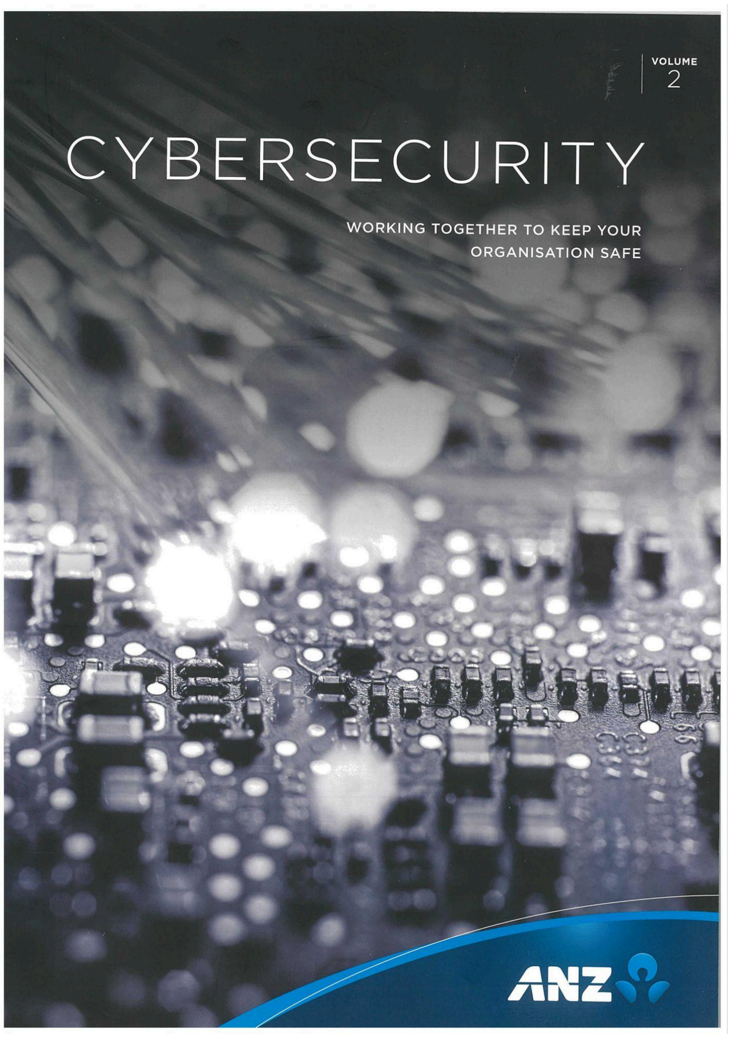


```
Step 1: Find target
Step 2: Hack them

This is a suspicious document.
```

Sub-task 4: Extract PDF Documents (ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf)

- **Process**:
    - Filter traffic to locate ANZ_Document.pdf, ANZ_Document2.pdf, and evil.pdf.
    - Extract the files using Wireshark and save them.
    - Screenshot the pdfs.
- **Findings**:
    - ANZ_Document.pdf and ANZ_Document2.pdf appear legitimate; however, evil.pdf contains a suspicious message stating "More suspicious stuff good job!" No irregularities were found in their hex code.
- **PDF Screenshots**:

ANZ_Document.pdf



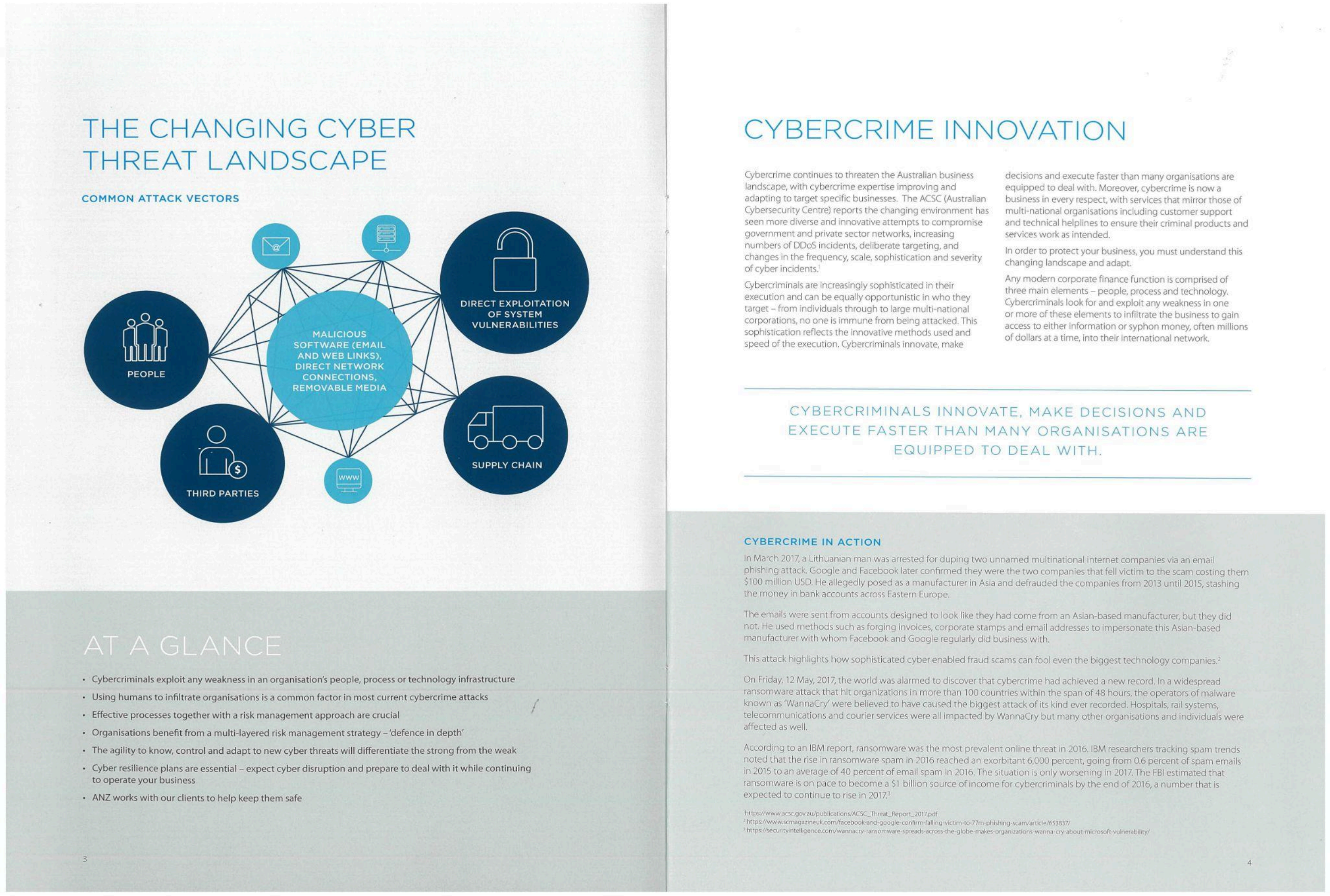
VOLUME 2

CYBERSECURITY

WORKING TOGETHER TO KEEP YOUR ORGANISATION SAFE

ANZ

ANZ_Document2.pdf



THE CHANGING CYBER THREAT LANDSCAPE

COMMON ATTACK VECTORS

MALICIOUS SOFTWARE (EMAIL AND WEB LINKS), DIRECT NETWORK CONNECTIONS, REMOVABLE MEDIA
DIRECT EXPLOITATION OF SYSTEM VULNERABILITIES
PEOPLE
THIRD PARTIES
SUPPLY CHAIN
WWW

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 agility 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.[1]

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 helplines 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 $100 million USD. He allegedly posed as a manufacturer in Asia and defrauded the companies from 2013 until 2015, stashing 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.[2]

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 organizations 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.

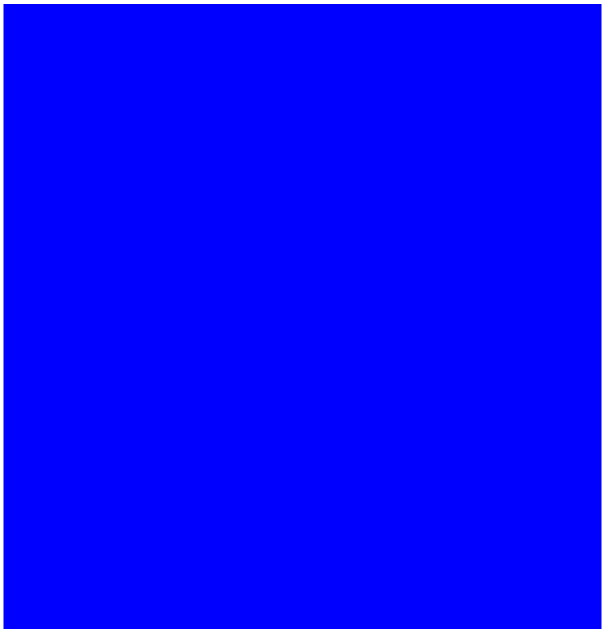
According to an IBM report, ransomware was the most prevalent online threat in 2016. IBM researchers tracking spam trends noted that the rise in ransomware spam in 2016 reached an exorbitant 6,000 percent, going from 0.6 percent of spam emails in 2015 to an average of 40 percent of email spam in 2016. 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.[3]

[1] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

[2] https://www.scmagazineuk.com/facebook-and-google-confirm-falling-victim-to-77m-phishing-scam/article/653837/

[3] https://securityintelligence.com/wannacry-ransomware-spreads-across-the-globe-makes-organizations-wanna-cry-about-microsoft-vulnerability/

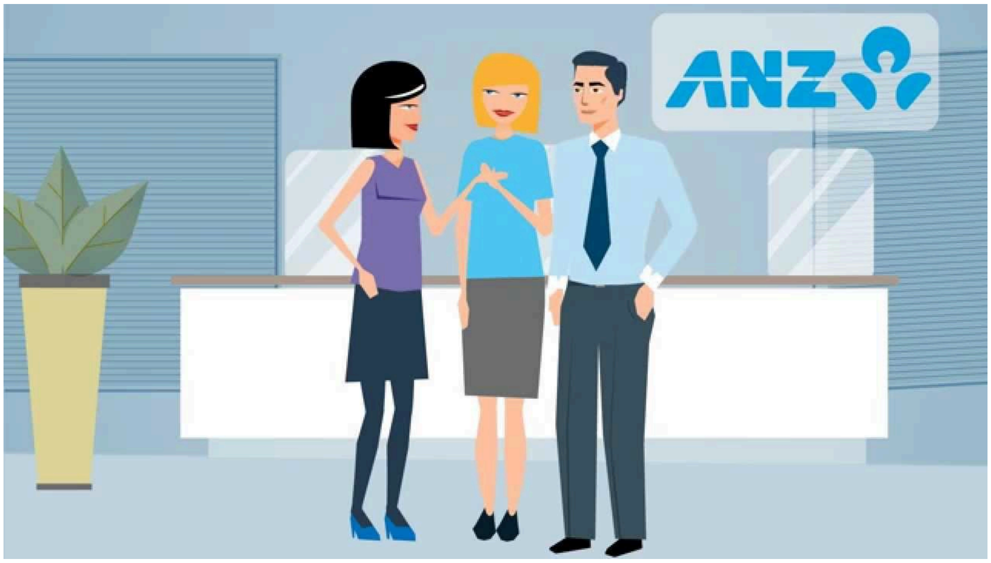
Evil.pdf



More suspicious stuff good job!

Sub-task 5: Extract and Analyze hiddenmessage2.txt

- **Process**:
  - Search for hiddenmessage2.txt in the network traffic.
  - Extract the file and open it in a text editor to reveal its contents.
- **Findings**:
  - After viewing the file in HxD hex editor, the data turns out to be encoded and based on its file signature, it turns out to be a jpg image.
- **Image converted from text**:

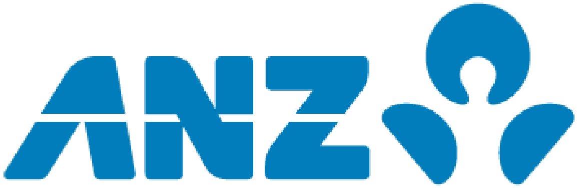


Sub-task 6: Analyze atm-image.jpg Traffic

- **Process**:
  - Locate atm-image.jpg in the traffic.
  - Extract the image and analyze it in a hex editor for additional data.
- **Findings**:
  - After extracting the image from the network traffic and loading it into the HxD hex editor, two distinct file signatures, both identified as jpg images, were detected by their unique segment header (FFD8) and footer (FFD9). The images were then separated by opening a new tab in HxD and pasting each segment of text individually.
- **Images**

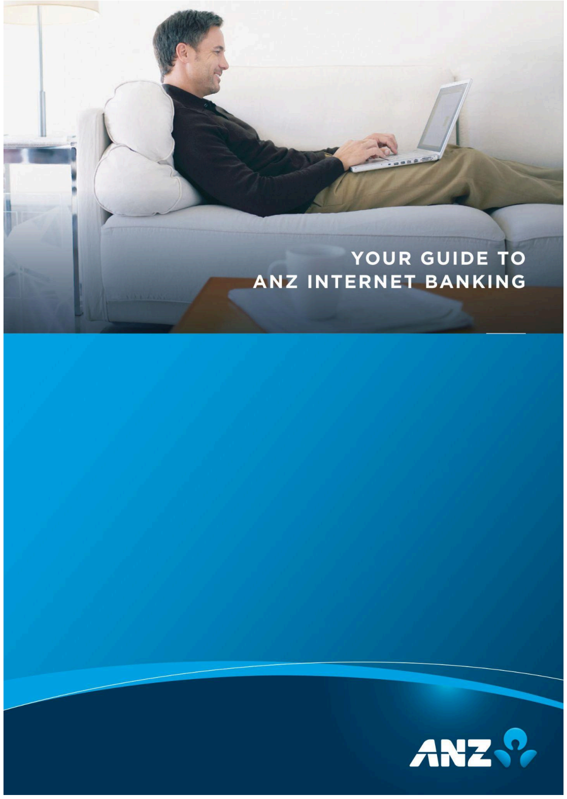
Sub-task 7: Extract broken.png Image

- **Process**:
    - Filter traffic for broken.png.
    - Extract the image.
- **Findings**:
    - After noticing the string was in base64, I used a base64 to image converter to extract the image.
- **Image**:



Sub-task 8: Extract and Analyze securepdf.pdf

- **Process**:
  - Search for securepdf.pdf in the HTTP traffic.
  - Extract and open the file.
  - Detail the steps taken to access the content.
- **Findings**:
  - After analyzing the traffic, I was able to infer that it was a zip file due to its file signature of 50 4B 03 04. I also noticed a password at the bottom of the stream. After going to the HTTP object list and extracting secure.pdf as a zip file, I extracted the file and was prompted to put in the password which then provided me with the images below.
- **PDF Screenshots**:



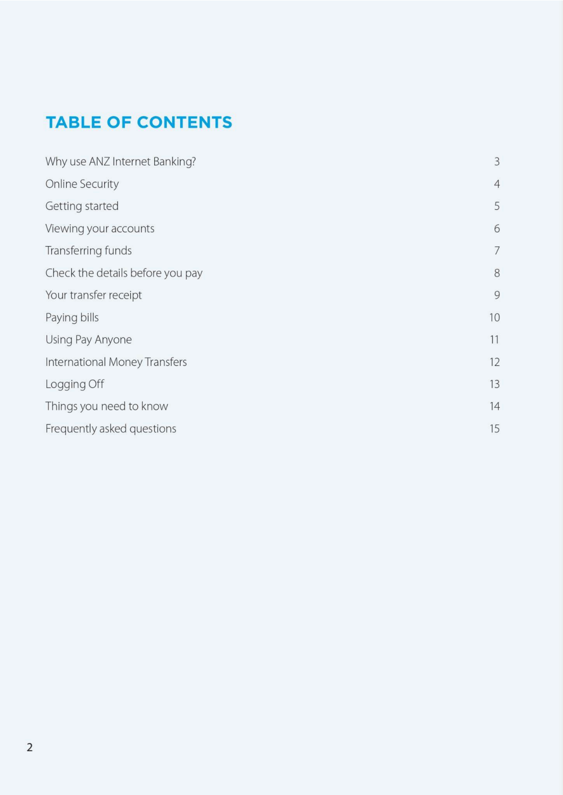


TABLE OF CONTENTS

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

2