



گزارش بررسی بدافزار اندرویدی اینستا پلاس
com.miladaziziapps.instaplus

فهرست مطالب

۱- مقدمه	۳
۲- معرفی برنامه	۳
۲-۱- بررسی ترافیک برنامه	۴
۳- نتیجه گیری	۵

۱- مقدمه

یکی از مسائلی که در دنیای تلفن‌های هوشمند همواره جای نگرانی بوده، موضوع حریم خصوصی است که در این رابطه، کارشناسان آزمایشگاه امنیت موبایل مرکز ماهر با رصد شبکه‌های اجتماعی یک بدافزار اندرویدی تحت عنوان «اینستا پلاس» را کشف کردند که IP کاربر را برای یک وب‌سرور ارسال می‌کند و موقعیت مکانی او را دریافت می‌کند. در ادامه به توضیح نحوه عملکرد این برنامه می‌پردازیم.

۲- معرفی برنامه

این برنامه در ابتدا دسترسی‌های موقعیت مکانی، تماس تلفنی و خواندن و نوشتن در حافظه گوشی را از کاربر می‌گیرد. اما بدون اطلاع کاربر، IP او را ارسال می‌کند و در پاسخ موقعیت مکانی کاربر را دریافت می‌کند. لازم به ذکر است این برنامه در مایکت ۶ هزار نصب فعال دارد و از طریق آدرس "https://myket.ir/app/com.miladaziziapps.instaplus" با عنوان «اینستا پلاس» در دسترس است (شکل ۱).



شکل ۱ برنامه اینستا پلاس در مایکت

در بخش بعدی با بررسی ترافیک برنامه به شرح درخواست‌های ارسال شده توسط برنامه به وب‌سرور می‌پردازیم.

۱-۲- بررسی ترافیک برنامه

پس از نصب برنامه، در بازه‌های زمانی نامشخص، IP کاربر برای یک وب‌سرور به آدرس "http://ip-api.com" ارسال می‌شود (شکل ۲).

```
GET /json/78.38.151.226
fields=country,region,regionName,city,status,isp,org,lat,lon HTTP/
1.1
Host: ip-api.com
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Origin: http://js.adad.ir
User-Agent: Mozilla/5.0 (Linux; Android 9; SM-J330F Build/
PPR1.180610.011; ww) AppleWebKit/537.36 (KHTML, like Gecko) Version/
4.0 Chrome/77.0.3865.116 Mobile Safari/537.36
Accept: */*
X-Requested-With: com.miladaziziapps.instaplus
Referer: http://js.adad.ir/adad-client/js/%3Fdevice
%3Dj3y171te%26androidid%3Db72eabc9330bf490%26token
%3D1ad900c4cab04c9eb47c86e40cba6856%26network%3D4G%26data
%3D0%26bazaarversion%3D702202%261%3D1%26car%3D43211%26j
%3D1ncWfzakV6ytf6ULYz406G5IK2txPPW51%2FAhmQ3Ywi2dQvQ9Uw21anMHj%2BoR
%2F35Bv4iLivFUGg%2BPfMU17o3zgyBYdvX1qMDLBh13toV%2Bw%2BUb7P9YWr
%2FB6T7E%2BN9M6SYIk6B8GW4wB7zYcqE1bfL7RdaQXFCoRgC%2BdBqa4qzC5Rc%3D
%26brand%3Dsamsung%26package%3Dcom.miladaziziapps.instaplus%26test
%3Dfalse%26version%3D6%26lang%3Den%26android%3D28%26adadversion%3D3
.1%26guid%3DA9a69f82e-a5d7-44f0-97a5-775ca7a0d444%26mode1%3DSM-J330F
%26library%3DAndroid%26dpi%3D320
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

شکل ۲ بسته‌ارسالی توسط برنامه به ip-api.com

در مرحله بعدی اطلاعات موقعیت مکانی کاربر از سمت وب‌سرور دریافت می‌شود (شکل ۳).

```
{
  "status": "success",
  "country": "Iran",
  "region": "12",
  "regionName": "Semnan Province",
  "city": "Semnan",
  "lat": 35.███,
  "lon": 53.███,
  "isp": "Iran Telecommunication Company PJS",
  "org": "Semnan University"
}
```

شکل ۳ بسته‌دریافتی از سمت وب‌سرور ip-api.com

سپس یک بسته حاوی اطلاعات گوشی کاربر مانند نام، مدل گوشی و ... به آدرس "http://adad.ir" ارسال می‌شود (شکل ۴).

```

GET /adview/?digest=e50d3f7bf3580054c7f62fdf8a33b836f5e4&device=
j3y171te&androidid=b72eabc9330bf490&token=1ad900c4cab04c9eb47c8
6e40cba6856&network=40&data=0&bazaarversion=702202&deviceid=jydrjh
dm-iwmq-rnfl-zgdshrnbnbbu&l=1&car=43211&j=q50vTcvVubDtp%2Fzq3%2B2j
jzrnPFcUQvgZb04ZjLlEvFw0nZwj7KFguVf9jaMKgwfl5e8wSBHG8jVo6VpjMgxuJ
nHSrjsam7zEY15ogkFCYE28ygY%2BQXVqWIE%2BVKLFFZmetXfEqAYN4z3y0Zf
zfxRjhFZ2wPaNkreZ070B4rsc%3D%26brand=samsung%26package=com.milada
z1z1apps_instaplus%26test=0&version=60&time=1.574937071625E12%26lang
=en%26android=28&adadversion=3.1&adid=&uid=A9a69f82e-a5d7-44f0-97
a5-775ca7a0d444&model=SM-J330F&library=Android&dpi=320&orientat
ion=1&js_version=2&adType=banner&scrWidth=360&scrHeight=640 HTTP/
1.1
Host: adad.ir
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Accept: */*
Origin: http://js.adad.ir
User-Agent: Mozilla/5.0 (Linux; Android 9; SM-J330F Build/
PPR1.180610.011; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/
4.0 Chrome/77.0.3865.116 Mobile Safari/537.36
X-Requested-With: com.miladaz1z1apps_instaplus
Referer: http://js.adad.ir/adad-client/js/%3Fdevice
%3Dj3y171te%26androidid%3Db72eabc9330bf490%26token
%3D1ad900c4cab04c9eb47c86e40cba6856%26network%3D40%26data%3D0
%26bazaarversion%3D702202%26l%3D1%26car%3D43211%26j%3Dq50vTcvVubDtp
%2Fzq3%2B2jzrnPFcUQvgZb04ZjLlEvFw0nZwj7KFguVf9jaMKgwfl5e
8wSBHG8jVo6VpjMgxuJnHSrjsam7zEY15ogkFCYE28ygY%2BQXVqWIE
%2BVKLFFZmetXfEqAYN4z3y0ZfzfxRjhFZ2wPaNkreZ070B4rsc%3D%26brand
%3Dsamsung%26package%3Dcom.miladaz1z1apps_instaplus%26test%3Dfalse
%26version%3D6%26lang%3Den%26android%3D28%26adadversion%3D3.1%26uid
%3DBPC7itZQ1RbepG1XogbSScw%26model%3DSM-J330F%26library%3DAndroid
%26dpi%3D320
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

```

شکل ۴ بسته ارسالی برنامه به سمت وب سرور adad.ir

۳- نتیجه گیری

در این گزارش به معرفی بدافزار اندرویدی «اینستا پلاس» پرداختیم. این برنامه IP کاربر را برای یک وب سرور ارسال می کند و موقعیت مکانی کاربر را دریافت می کند. سپس اطلاعات گوشی کاربر را به وب سرور "http://adad.ir" ارسال می نماید.