بدافزار موبایلی آموزش فال تاروت

در بررسی‌های فضای مجازی در زمینه بدافزارهای اندرویدی، نمونه جدیدی از بدافزار اندرویدی در قالب برنامه فال با نام **فال تاروت** مشاهده می‌گردد که توسط کانال‌های ناشناس و منابع ناامن دانلود نرم‌افزار انتشار می‌گردند. این برنامه که در چندین نسخه ارائه شده‌است قابلیت ارسال پیامک ارزش افزوده و عضویت کاربر در آن سرویس‌ها را دارد. همچنین با ایجاد دسترسی در سیستم امکان ارسال نوتیفیکیشن را دارا می‌باشد. شکل زیر نمونه‌ای از تبلیغ برای دانلود این بدافزار را نشان می‌دهد که در کانال‌های ناشناس توسط افراد سودجو ارائه می‌گردد. مقدار مشاهده شده برای این بدافزار زیاد بوده و می‌تواند تعداد بیشتری از سیستم کاربران را آلوده کند.

شکل ۱ – پیام دانلود برنامه در شبکه‌های مجازی

شناسایی در آنتی ویروس‌ها

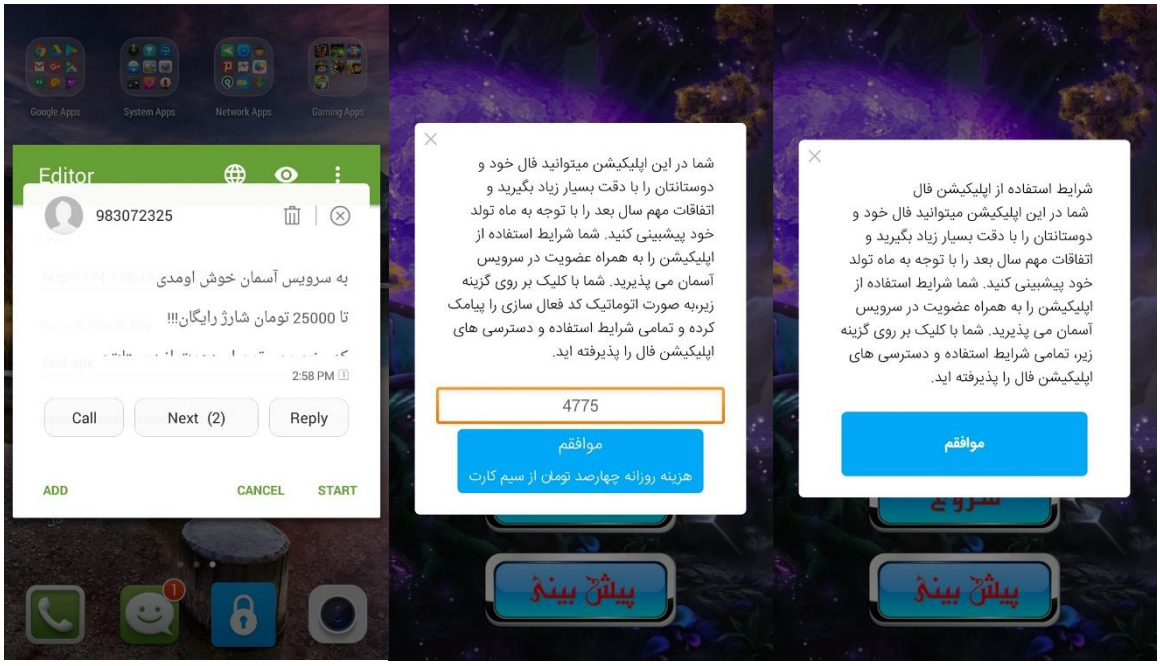
وضعیت تشخیص این فایل توسط آنتی‌ویروس‌های مشهور همراه با علت تشخیص به‌عنوان بدافزار در شکل شماره ۲ قابل مشاهده می‌باشد.

Ad-Aware	Android.Trojan.SMSSend.ARJ	AhnLab-V3	Android-PUP/SmsReg.9283f
Alibaba	A.W.Rog.Agent.BI	Arcabit	Android.Trojan.SMSSend.ARJ
Avast Mobile Security	Android:Evo-gen [Susp]	Avira	ANDROID/TrojanSMS.ANR.Gen
BitDefender	Android.Trojan.SMSSend.ARJ	CAT-QuickHeal	Android.Agent.ANZ
Cyren	ZIP/Trojan.YCZS-2	DrWeb	Android.SmsSend.1972.origin
Emsisoft	Android.Trojan.SMSSend.ARJ (B)	eScan	Android.Trojan.SMSSend.ARJ
ESET-NOD32	a variant of Android/TrojanSMS.Agent.CUJ	F-Secure	Android.Trojan.SMSSend.ARJ
Fortinet	Android/Agent.CSA!tr	GData	Android.Trojan.SMSSend.ARJ
Jiangmin	Downloader.AndroidOS.ada	K7GW	Trojan (0052cfa11)
Kaspersky	not-a-virus:HEUR:Downloader.AndroidOS.Ag...	MAX	malware (ai score=84)
McAfee	Artemis!00EE72E20638	McAfee-GW-Edition	Artemis!PUP
Symantec	Trojan.Gen.2	Symantec Mobile Insight	Other:Android.Reputation.1
Trustlook	Android.Malware.General	ZoneAlarm	not-a-virus:HEUR:Downloader.AndroidOS.Ag...
Zoner	Trojan.AndroidOS.SMSSend.T	AegisLab	Clean

شکل ۲ – وضعیت فایل در آنتی‌ویروس‌های مشهور

نحوه فعالیت بدافزار

برنامه بعد از نصب و راه‌اندازی در سیستم وضعیت و اطلاعات سیستم را بررسی می‌کند. با استفاده از اطلاعات سیم‌کارت ثبت شده اگر برای **همراه‌اول** باشد صفحه مربوط به همراه را نشان داده با استفاده از امکان ارسال پیامک کاربر را در سرویس **ارزش‌افزوده آسمان** با هزینه ۴۰۰ تومان برای هر پیامک ثبت نام کرده و برنامه‌ای با نام فال واقعی را برای کاربر دانلود و نصب می‌کند. ولی در صورتی‌که نوع سیم‌کارت مورد استفاده شده همراه‌اول نباشد ابتدا به آدرس اینترنتی متصل شده و از کاربر تقاضای ثبت شماره **ایرانسل** را دارد. بعد از ثبت شماره کاربر را در **سرویس پیامکی پرشتاب** با هزینه روزانه ۵۰۰ تومان ثبت نام کرده و برنامه فال واقعی را دانلود و نصب می‌کند.



شکل ۳ - عالیت برنامه و عضویت در سرویس پیامکی

شکل ۴ - محیط برنامه برای ثبت نام در سرویس پیامکی پرشتاب

پاکسازی بدافزار از سیستم

برای پاکسازی بدافزار از روی پوشی می‌توان مراحل زیر را انجام داد:

- در قسمت مدیریت برنامه در داخل تنظیمات گوشی، برنامه‌هایی با نام‌های فال، فال تاروت یا تاروت را حذف می‌کنیم.
- با شماره‌گیری #1*800* اطلاعات سرویس‌های پیامکی در صورتی‌که سرویسی (مانند سرویس-های **پرشتاب** و **آسمان**) فعال شده باشد با توجه به همان اطلاعات، اقدام به لغو آن‌ها می‌کنیم.
- آنتی‌ویروس سیستم را بروزرسانی کرده و سیستم را اسکن می‌کنیم.

راه‌های مراقبت و پیشگیری

برای اینکه گوشی موبایل خود را ایمن نگه داریم و از افشای اطلاعات و سواستفاده از آن مراقبت کنیم باید راهکارهای زیر را در نظر بگیریم:

۱- از آنتی‌ویروس‌های قوی و معتبر استفاده کنیم.

بیشتر برنامه‌های آنتی‌ویروس قدرت لازم را برای تشخیص یک فایل بدافزار را ندارند و فقط اسم یک آنتی‌ویروس را بر روی خود دارند. هنگام استفاده از آن‌ها، بعد از تحقیق مختصری در می‌توان یک آنتی‌ویروس موبایلی قوی و خوبی را انتخاب کرد.

۲- از دانلود و نصب برنامه از منابع نامعتبر خودداری کنیم.

برنامه‌هایی که در منابع دانلود معتبر همچون Google Play عرضه می‌شوند با استفاده از محافظ‌هایی یکبار برنامه‌ها را بررسی می‌کنند. ولی بیشتر این برنامه‌ها هم امن نیستند. منابع نامتعبر شامل کانال‌های تلگرامی، مارکت‌های غیررسمی و ناشناخته شده، دریافت برنامه از یک شخص دیگر از طریق برنامه‌های اشتراک‌گذاری و غیره می‌باشد.

۳- هنگام نصب برنامه‌های موبایلی به دسترسی‌های درخواستی دقت کنیم.

یشتر برنامه‌ها برای کار خاصی طراحی شده‌اند مثلا برنامه‌ای برای تبدیل عکس به نقاشی می‌باشد ولی در صورتیکه به دسترسی‌های آن نگاه می‌کنیم امکان ارسال و دریافت پیامک هم وجود دارد. این نوع دسترسی‌ها غیرمعقول می‌باشند. لذا هنگام نصب برنامه‌ها به دسترسی‌های درخواستی توجه کرده و در صورتیکه برنامه‌ای قبلا نصب شده باشد می‌توان در تنظیمات مربوط به برنامه، دسترسی‌های غیرعادی را غیرفعال کرد.

۴- پشتیبان‌گیری مداوم از فایل‌ها و اطلاعات

بیشتر بدافزارها از نوع باج‌افزار می‌باشند و می‌توانند فایل‌ها و اطلاعات موجود بر روی گوشی موبایل را رمز کرده و دسترسی به آن‌ها را ناممکن کنند و یا در برخی از بدافزارها امکان حذف یا خرابکاری بر روی اطلاعات وجود دارد. لذا برای درمان بعد از آلوده شدن به بدافزار به فایل‌های پشتیبان نیاز پیدا می‌کنیم. برای این‌کار بصورت مداوم (هفتگی یا ماهانه) از فایل‌ها و اطلاعات حساس و مورد نیاز فایل پشتیبان ایجاد کرده و آن‌ها را در یک دستگاه دیگر مانند کامپیوترهای شخصی نگهداری کنیم.

۵- عدم استفاده از نسخه‌های غیررسمی برنامه‌ها

برنامه‌هایی مانند تلگرام نسخه‌های غیررسمی زیادی مانند موبوگرام دارند که توسط توسط اشخاص دیگری توسعه داده شده‌اند و در منابع غیرمعتبر بیشتری ارائه شده‌اند. بیشتر این برنامه یک برنامه قانونی و امن نبوده و امکان آلوده‌سازی را دارند. لذا از نصب چنین برنامه‌هایی باید خودداری گردد و از نسخه‌های رسمی که توسط خود شرکت‌ها ارائه می‌گردد استفاده شوند.

۶- عدم دانلود برنامه‌هایی با عناوین گول‌زننده

برنامه‌های زیادی با استفاده از نام‌های گول زننده‌ای (مانند نمایش فیلم مستهجن) اقدام به پخش بدافزارهای خود می‌کنند لذا با توجه به محتویات بدافزاری این نوع از برنامه‌ها از دانلود و نصب خودداری کنیم.

۷- هشیار بودن در هنگام نصب برنامه‌هایی با حجم پایین

برنامه‌هایی مثل فال یا غیره که نیاز به ارائه اطلاعات برای کاربر دارند باید این اطلاعات را در درون خود ذخیره کنند لذا با این کار حجم برنامه مورد استفاده بالاتر می‌رود. برنامه‌هایی مانند فال تاروت که حجمی کمتر از یک مگابیت دارند نشان دهنده این می‌باشند که اطلاعاتی نداشته و برنامه‌های تقلبی می‌باشند.

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

شماره تماس: ۰۴۵ – ۳۱۵۰۵۷۱۸

آدرس اینترنتی: cert.uma.ac.ir

آدرس: اردبیل – خیابان دانشگاه- دانشگاه محقق اردبیلی – دانشکده فنی – مرکز آپا محقق اردبیلی