بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

گزارش بدافزار daam روی نسخه آلوده اندرویدی

نوع سند ..... گزارش فنی

شماره نگارش ۱

تاریخ نگارش ۱۴۰۲/۰۲/۱۶

طبقه‌بندی سند ..... **عادی**

تهران، خیابان شهید بهشتی بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک ۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴

(۰۲۱) ۸۸۱۱۵۷۲۴

cert.ir

فهرست مطالب

۱ شرح بدافزار

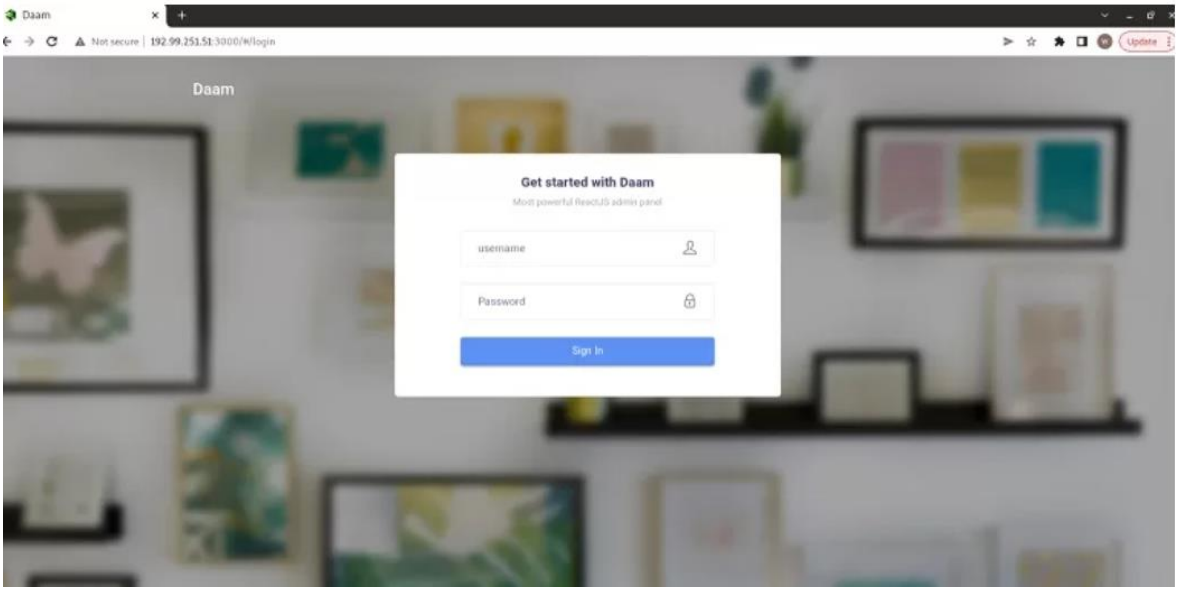
در سال‌های اخیر، استفاده گسترده از دستگاه‌های اندرویدی، آنها را به یک هدف اصلی برای مجرمان سایبری تبدیل کرده است. باتنت اندروید یک نوع معمول از نرم‌افزارهای مخرب است که مجرمان سایبری برای دستیابی به دستگاه‌های هدف استفاده می‌کنند. این دستگاه‌ها به صورت از راه دور کنترل شده و برای انجام فعالیت‌های مخرب مختلف استفاده می‌شوند مانند باج افزار و سرقت اطلاعات. آزمایشگاه‌های تحقیق و اطلاعاتی Cyble به تازگی یک باتنت اندرویدی را که توسط تیم MalwareHunter به اشتراک گذاشته شده بود را تحلیل کرد. گزارش فنی در خصوص نسخه آلوده برنامه Psiphon بنام PsiphonAndroid.s.apk را منتشر کردند که با بدافزار DAAM Android Botnet پیوند شده است. درواقع نمونه مخرب مذکور، نسخه تروجان شده از برنامه Psiphon است و به عنوان باتنت اندرویدی DAAM شناخته شده است که امکانات زیر را فراهم می‌کند:

- کی‌لاگر
- باج‌افزار
- ضبط تماس‌هایVOIP
- اجرای کد در زمان اجرا
- جمع‌آوری تاریخچه مرورگر
- ضبط تماس‌های ورودی
- سرقت داده‌های حساس PII
- باز کردن آدرسهای URL فیشینگ
- گرفتن عکس
- سرقت داده‌های کلیپ‌بورد
- تغییر وضعیت WiFi و Data

DAAM Android botnet یک سرویس APK binding است که امکان پیوند دادن کدهای مخرب را با یک برنامه قانونی فراهم میکند. با توجه به شکل ۱ این بدافزار به سرور C2 زیر وصل میشود.

شکل۱ : اتصال به سرور c2

شکل ۲ نیز نمایی از پنل ادمین DAAM Android botnet را نشان می‌دهد:



شکل۲: نمایی از پنل ادمین DAAM Android botnet

این سرور C2 از ابتدای آگوست ۲۰۲۱ در بدافزارهای مختلف دیده شده است و در شکل زیر نشان می دهد که این بات نت از سال ۲۰۲۱ عملیاتی شده و کاربران اندروید رو هدف قرار داده است.

192.99.251.51

Communicating Files (8)

Scanned	Detections	Type	Name
2022-01-09	20 / 61	Android	Currency_Pro_v3.2.6.apk
2023-04-19	22 / 62	Android	PsiphonAndroid.s.apk
2023-03-15	4 / 69	Win32 EXE	56dba611b57854bf1ff72ef004f2a0b9.virus
2023-04-16	15 / 64	Android	Boulder.s.apk
2022-03-30	21 / 62	Android	164a93b3ac1b0102344d721ff9ca3e6f.virus
2023-04-16	23 / 65	Android	Boulder.s.apk
2022-06-10	10 / 60	Android	1200927713f38e6cd18e71da96749db3.virus
2021-08-14	24 / 63	Android	045b8faac529696615cdaff2cda052f1.virus

آنالیز فنی بدافزار :

شکل زیر اطلاعات متادیتای این بدافزار را نشان میدهد:

شکل۳ : متادیتای بدافزار

اقدامات کاهشی:

مهاجمین علاقه دارند که از برنامه های قانونی ، برای هدف قرار دادن کاربران استفاده کنند. این کار باعث میشود تا قربانی کمتر شک کند. برای حفاظت در برابر این حملات روش های زیر پیشنهاد شده است:

- برنامه ها رو از طریق اپ استورهای رسمی مانند گوگل پلی و iOS App Store دانلود کنید.
- از یک محصول امنیتی معتبر (آنتی ویروس و ...) در دستگاه استفاده کنید.
- اطلاعات حساس مانند اطلاعات پرداخت با کسی به اشتراک گذاشته نشود.
- از رمزهای منحصر به فرد و قوی و ویژگی FA ۲استفاده کنید.
- از ویژگی های امنیتی بیومتریک مانند اثر انگشت برای باز کردن قفل دستگاهها استفاده کنید.
- از باز کردن لینک های ناشناس از طریق پیامک و ایمیل خودداری کنید.
- از فعال بودن Google Play Protect روی دستگاههای اندرویدی مطمئن شوید.
- دستگاه، سیستم عامل و برنامه ها را بروز نگه دارید.

IoCهای گزارش شده در جدول زیر نشان داده شده است :

نشانگرها	توضیحات
fdfbf20e59b28181801274ad23b951106c6f7a516eb914efd427b6617630f30۰	Currency_Pro_v3.2.6.apk
/hxxp://192.99.251[.]51:3000/socket.io	C&C server
d900a545a2d545ab96fa6dd7b46f881a1a80ed134db1c65225e8fa902b۱۸۴۳۵۶	PsiphonAndroid.s.apk
d4c5a0ea070fe0a1a2703914bf442b4285658b31d220f974adcf953b041e1137	Boulder.s.apk

۲ مراجع

https://blog.cyble.com/2023/04/20/daam-android-botnet-being-distributed-through-trojanized-applications/