بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

گزارش فنی

گزارش بدافزار Goldoson

شناسه سند ..... Goldoson _ Malware _Report
نوع سند ..... گزارش فنی
شماره نگارش ۱
تاریخ نگارش ۱۴۰۲/۰۱/۳۰
طبقه‌بندی سند ..... عادی

فهرست مطالب

۱ شرح بدافزار Goldoson

تیم تحقیقاتی موبایل McAfee یک کتابخانه نرم‌افزاری به نام Goldoson را کشف کرده است که فهرستی از برنامه‌های نصب شده و تاریخچه اطلاعات دستگاه‌های Wi-Fi و بلوتوث، از جمله مکان‌های GPS را جمع‌آوری می‌کند. این کتابخانه مجهز به این قابلیت است که با کلیک بر روی تبلیغات در پس‌زمینه، بدون رضایت کاربر، کلاهبرداری تبلیغاتی انجام دهد. این کتابخانه مخرب در ۶۰ برنامه مورد استفاده قرار گرفته و بیش از ۱۰۰ میلیون بار دانلود از طریق گوگل پلی و ۸ میلیون بار از طریق ONE store در کره جنوبی داشته است.

نکته قابل توجه این است که این کتابخانه مخرب توسط شخص دیگری توسعه داده شده است، و توسعه دهنگان برنامه، بدون آگاهی از مخرب بودن آن، در برنامه های خود استفاده کرده‌اند.

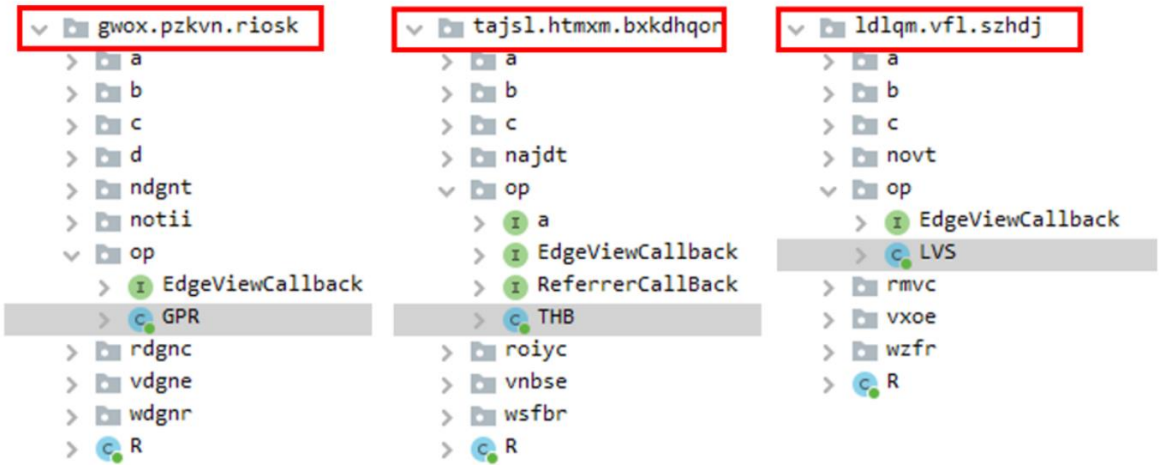
McAfee Mobile Security این تهدید را به‌عنوان Android/Goldoson شناسایی می‌کند و از مشتریان در برابر این تهدیدات و بسیاری دیگر از تهدیدات موبایل محافظت می‌کند. Mcafee لیست این برنامه های مخرب را به گوگل داده و گوگل به توسعه دهندگانش اطلاع داده است که برنامه های آنها سیاست های گوگل پلی را رعایت نمی‌کند و در نتیجه برخی از آنها حذف شدن و برخی توسط توسعه دهندگان بروزرسانی شدن تا شامل این کتابخانه مخرب نباشد.

شکل زیر ۹ برنامه که بیشترین نصب را داشته را نشان می‌دهد :

شکل۱: ۹ اپلیکیشن برتر که قبلا توسط Goldoson در گوگل پلی آلوده شده اند

چگونه بر کاربران تأثیر می گذارد؟

وقتی کاربر یک برنامه آلوده به این کتابخانه رو اجرا میکند، کتابخانه دستگاه رو رجیستر کرده و پیکربندی را از سرور C2 دریافت میکند. نام کتابخانه و دامنه سرور برای هر برنامه ای متفاوت و مبهم شده است. اسم Goldoson هم از روی اولین دامنه ای که پیدا کردن گرفته شده است.



پیکربندی دریافتی شامل پارامترهایی از عملکردهای برنامه است و اینکه هر چند وقت یکبار آنها را اجرا کند. براساس این پارامترها ، کتابخانه به صورت دوره ای دستگاه را بررسی میکند و سپس اطلاعاتش را استخراج میکند و اونها را به سرور C2 ارسال میکند. تگهایی مانند ads_enable یا collect_enable نشان دهنده فعال بودن عملکردها است و سایر پارامترها شرایط و دسترسی آن عملکردها مانند تاخیر بین عملکرد را مشخص میکنند.

```
{
    "code": 0,
    "data": {
        "bdls": "H4sIAAAAAAAAA4uOBQApu0wNAgAAAA==",
        "config": {
            "ads_cpc_update_interval": 3600000,
            "ads_cpi_display_percentage": 100,
            "ads_cpi_update_interval": 3600000,
            "ads_cps_max_delay": 1200000,
            "ads_cps_none_max_delay": 1800000,
            "ads_cps_none_update_delay": 1500000,
            "ads_cps_update_delay": 900000,
            "ads_enable": "Y",
            "ads_popup_interval": 14400000,
            "ads_spremiums_delay": 2000,
            "ads_spremiums_pull_count": 20,
            "ads_spremiums_pull_interval": 100,
            "ble_rssi_limit": -79,
            "collect_app_interval": 80280000,
            "collect_clear_count": 100,
            "collect_enable": "Y",
            "collect_fg_clear_count": 100,
            "collect_fg_enable": "N",
            "collect_fg_inner_initial_interval": 300000,
            "collect_fg_inner_interval": 30000,
            "collect_fg_interval": 600000,
            "collect_fg_limit_count": 60,
            "collect_fg_low_enable": "N",
            "collect_fg_noti_enable": "Y",
```


بارگذاری صفحات بدون اجازه کاربر:

داده‌های جمع‌آوری شده به صورت دوره‌ای هر دو روز یک‌بار ارسال می‌شوند، اما دوره ارسال ممکن است توسط فایل پیکربندی تغییر کند. این اطلاعات حاوی برخی از داده های حساس از جمله لیست برنامه های نصب شده، تاریخچه موقعیت مکانی، آدرس MAC بلوتوث و وای فای و غیره است. این ممکن است به افراد اجازه دهد که در هنگام ترکیب داده ها شناسایی شوند. شکل زیر نمونه ای از داده های جمع آوری شده روی دستگاه تست محققین را نشان می‌دهد:

شکل۳: نمونه ای از داده های جمع آوری شده روی دستگاه تست محققین

گوگل پلی جمع آوری لیست برنامه ها رو به عنوان داده های حساس و شخصی کاربر در نظر میگیرد و بنابراین برای دسترسی نیاز به تعریف مجوز (Permission) خاصی است. اندروید ۱۱ و نسخه های بالاتر در برابر جمع آوری داده ها عملکرد بهتری را دارند. محققین McAfee دریافتند که حتی در نسخه های اخیر اندروید، ۱۰ درصد از برنامه هایی که دارای این کتابخانه مخرب هستند ، مجوز QUERY_ALL_PACKAGES را دارند و امکان دسترسی به اطلاعات برنامه ها رو می دهند.

همچنین در اندروید ۶ و بالاتر ، ممکن است در زمان اجرا از کاربر مجوزهایی مانند مکان ، فضای ذخیره سازی ، دوربین و ... خواسته شود. اگه کاربر مجوز مکان رو بدهد، برنامه نه تنها به داده های GPS دسترسی دارد بلکه به اطلاعات دستگاههای WIFI و بلوتوث اطراف دستگاه هم دسترسی دارد. براساس BSSID (Basic Service Set Identifier) و RSSI (Received Signal Strength Indicator) برنامه می تواند مکان دستگاه را دقیقتر از GPS بخصوص در یک مکان بسته شناسایی کند.

همونطور که بیان شد بخشی از عملکرد این بدافزار، کلاهبرداری تبلیغاتی است. برای اینکار بدافزار یکسری کد HTML رو بارگذاری میکند و به یه WebView مخفی و سفارشی تزریق میکند و با بازدید از URLها ترافیک جعلی و مخفی ایجاد می‌کند.

گزارش برنامه ها و دامنه های شناسایی شده (IoC):

دامنه های مخرب :

bhuroid.com	enestcon.com	htyyed.com
discess.net	gadlito.com	gerfane.com
visceun.com	onanico.net	methinno.net
goldoson.net	dalefs.com	openwor.com
thervide.net	soildonutkiel.com	treffaas.com
sorrowdeepkold.com	hjorsjopa.com	dggerys.com
ridinra.com	necktro.com	fuerob.com
phyerh.net	ojiskorp.net	rouperdo.net
tiffyre.net	superdonaldkood.com	soridok2kpop.com

برنامه های آلوده :

در ادامه لیست ۶۰ برنامه آلوده فهرست شده است ، اگه از این برنامه ها استفاده می شود، انها را بروزرسانی کنید تا نسخه آلوده را حذف کنید (update) و اگه نسخه بروزرسانی موجود نیست آنها را حذف کنید (Removed).

نام بسته	نام برنامه	دانلود GooglePlay	وضعیت
com.lottemembers.android	L.POINT with L.PAY	10M+	Update
com.Monthly23.SwipeBrickBreaker	Swipe Brick Breaker	10M+	Removed
com.realbyteapps.moneymanagerfree	Money Manager Expense & Budget	10M+	Update
com.skt.tmap.ku	TMAP-대리,주차,전기차 충전,킥보	10M+	Update
kr.co.lottecinema.lcm	롯데시네마	10M+	Update
com.ktmusic.geniemusic	지니뮤직 – genie	10M+	Update
com.cultureland.ver2	컬쳐랜드[컬쳐캐쉬]	5M+	Update
com.gretech.gomplayerko	GOM Player	5M+	Update
com.megabox.mop	메가박스(Megabox)	5M+	Removed

kr.co.psynet	LIVE Score, Real-Time Score	5M+	Update
sixclk.newpiki	Pikicast	5M+	Removed
com.appsnine.compass	Compass 9: Smart Compass	1M+	Removed
com.gomtv.gomaudio	GOM Audio – Music, Sync lyrics	1M+	Update
com.gretech.gomtv	곰TV – All About Video	1M+	Update
com.guninnuri.guninday	전역일 계산기 디데이 곰신톡–군인	1M+	Update
com.itemmania.imiapp	아이템매니아 – 게임 아이템 거래 …	1M+	Removed
com.lotteworld.android.lottemagicpass	LOTTE WORLD Magicpass	1M+	Update
com.Monthly23.BounceBrickBreaker	Bounce Brick Breaker	1M+	Removed
com.Monthly23.InfiniteSlice	Infinite Slice	1M+	Removed
com.pump.noraebang	나홀로 노래방–쉽게 찾아 이용하는 …	1M+	Update
com.somcloud.somnote	SomNote – Beautiful note app	1M+	Removed
com.whitecrow.metroid	Korea Subway Info : Metroid	1M+	Update
kr.co.GoodTVBible	GOODTV다번역성경찬송	1M+	Removed
kr.co.happymobile.happyscreen	해피스크린 – 해피포인트를 모으 …	1M+	Update
kr.co.rinasoft.howuse	UBhind: Mobile Tracker Manager	1M+	Removed
mafu.driving.free	스피드 운전면허 필기시험	1M+	Removed
com.wtwoo.girlsinger.worldcup	이상형 월드컵	500K+	Update
kr.ac.fspmobile.cu	CU편의점택배	500K+	Removed
com.appsnine.audiorecorder	스마트 녹음기 : 음성 녹음기	100K+	Removed
com.camera.catmera	캣메라 [순정 무음카메라]	100K+	Removed

com.cultureland.plus	컬쳐플러스:컬쳐랜드 혜택 더하기 …	100K+	Update
com.dkworks.simple_air	창문닫아요(미세/초미세먼지/WHO …	100K+	Removed
com.lotteworld.ticket.seoulsky	롯데월드타워 서울스카이	100K+	Update
com.Monthly23.LevelUpSnakeBall	Snake Ball Lover	100K+	Removed
com.nmp.playgeto	게토(geto) – PC방 게이머 필수 앱	100K+	Removed
com.note.app.memorymemo	기억메모 – 심플해서 더 좋은 메모장	100K+	Removed
com.player.pb.stream	풀빵 : 광고 없는 유튜브 영상 …	100K+	Removed
com.realbyteapps.moneya	Money Manager (Remove Ads)	100K+	Update
com.wishpoke.fanciticon	Inssaticon – Cute Emoticons, K	100K+	Removed
marifish.elder815.ecloud	클라우드런처	100K+	Update
com.dtryx.scinema	작은영화관	50K+	Update
com.kcld.ticketoffice	매표소–뮤지컬문화공연 예매& …	50K+	Update
com.lotteworld.ticket.aquarium	롯데월드 아쿠아리움	50K+	Update
com.lotteworld.ticket.waterpark	롯데 워터파크	50K+	Update
com.skt.skaf.l001mtm091	T map for KT, LGU+	50K+	Removed
org.howcompany.randomnumber	숫자 뽑기	50K+	Update
com.aog.loader	로더(Loader) – 효과음 다운로드	10K+	Removed
com.gomtv.gomaudio.pro	GOM Audio Plus – Music, Sync l	10K+	Update
com.NineGames.SwipeBrickBreaker2	Swipe Brick Breaker 2	10K+	Removed
com.notice.safehome	안심해 – 안심귀가 프로젝트	10K+	Removed
kr.thepay.chuncheon	불러봄내 – 춘천시민을 위한 공공 …	10K+	Removed

com.curation.fantaholic	판타홀릭 – 아이돌 SNS 앱	5K+	Removed
com.dtryx.cinecube	씨네큐브	5K+	Update
com.p2e.tia.tnt	TNT	5K+	Removed
com.health.bestcare	베스트케어–위험한 전자기장, …	1K+	Removed
com.ninegames.solitaire	InfinitySolitaire	1K+	Removed
com.notice.newsafe	안심해 : 안심지도	1K+	Removed
com.notii.cashnote	노티아이 for 소상공인	1K+	Removed
com.tdi.dataone	TDI News – 최초 데이터 뉴스 앱 …	1K+	Removed
com.ting.eyesting	눈팅 – 여자들의 커뮤니티	500+	Removed
com.ting.tingsearch	팅서치 TingSearch	50+	Removed
com.celeb.tube.krieshachu	츄스틱 : 크리샤츄 Fantastic	50+	Removed
com.player.yeonhagoogokka	연하구곡	10+	Removed

مراجع

1- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/goldoson-privacy-invasive-and-clicker-android-adware-found-in-popular-apps-in-south-korea/