禪

---

بدافزاری که تنها اطلاعات سرقت میکند

# تروجان **SpyDleaer** میتواند از **40** برنامه اندرویدی جاسوسی کند



پژوهشگران شرکت امنیتی پالوآلتو موفق شدهاند بدافزار خطرناکی به نام SpyDealer را شناسایی کنند . بدافزاری که به گفته این شرکت قادر است اطلاعات حساس کاربران را از 40 برنامه کاربردی معروف همچون ویچت، تلگرام، فیسبوک، اسکایپ، واتسآپ، تانگو و مرورگر فایرفاکس به سرقت ببرد .

بدافزار فوق برای دسترسی به این اطلاعات از سرویس دسترسپذیری اندروید استفاده کرده و به این شکل اطلاعات موجود در برنامههای کاربردی را سرقت میکند . این بدافزار از ابزار تجاری Baidu Easy Root به منظور روت کردن دستگاههای اندرویدی و دسترسی به امتیازات سطح ریشه برای سرقت اطلاعات استفاده میکند .

مطلب پیشنهادی



راهاندازی سرویس DDoS

یک دانشآموز **18** ساله انگلیسی متهم به اجرای حمله **DDoS** شد

کارشناسان این شرکت امنیتی اعلام داشتهاند که بدافزار فوق تنها روی نسخههای 2.2 تا 4.4 اندروید قادر است به دستگاهها نفوذ کند . بهطوری که در مجموع قادر است 25 درصد از دستگاههای اندرویدی را در معرض تهدید قرار دهد . زمانی که این بدافزار روی دستگاههای همراه اندرویدی نصب میشود در اولین مرحله دو گیرنده همپخشی (broadcast) را روی دستگاه نصب کرده تا این توانایی را داشته باشد همه رخدادها و وضعیت ارتباطات شبکهای دستگاه قربانی را مورد استراق سمع قرار دهد .



[redacted] • Public Oct 11, 2015

What the hell?

Show original text

Originally shared by ****

The residence is TCP network hijacked, the initial symptoms for the first time to open a new page will jump to a page advertising a 56ican and refresh before being accessed, at first thought a big problem, but the last two months began to appear all .apk files Downloads are reset / replace, the default download a 537.19K Trojans, but the most bizarre is the name of the Trojan program] is [zhenjianghua.apk spelling of my name. If the download is .zip, .exe, .rar, .7z will download an additional dll virus installation package.

Once the idea to try to resolve DNS hijacking, hostage-IP is 211.98.70.194 and 211.98.70.195 through dns nslookup used to verify the operator, to add it to the router's firewall and replacement dns. But only to resolve the problem domain hijacking error correction system, download the hijacking of no effect.

(a) Network hijacked and the user was infected by this malware



[redacted] has been denied superuser permissions:

cp /data/misc/wifi/wpa_supplicant.conf /data/data/xico.quxmcdp.qdqemb/wpa_supplicant.conf

[redacted] has been denied superuser permissions:

chmod 777 /data/data/xico.quxmcdp.qdqemb/wpa_supplicant.conf

[redacted] has been denied superuser permissions for an interactive shell

(b) The malware took screenshot and accessed the connected Wi-Fi information

اگر این بدافزار موفق نشود دستگاه کاربر را روت کند، بازهم این توانایی را دارد تا بخش اعظمی از اطلاعات را به سرقت ببرد . هکرها همچنین قادر هستند از راه دور و با استفاده از پروتکلهای UDP و TCP و پیامهای کوتاه دستگاه کاربر کنترل کنند . بدافزار فوق ضمن آنکه اطلاعات حساسی همچون پیامهای کوتاه، تاریخچه تماسها، مخاطبان، موقعیت مکانی کاربر و اطلاعات مرتبط به شبکههای بیسیم را به سرقت میبرد، این توانایی را داشته تا به تماسهای تلفنی که از شمارههای خاصی وارد میشوند پاسخ داده، مکالمات صوتی را ضبط کرده و درست همانند یک ابزار جاسوسی به ایفای نقش بپردازد .

مطلب پیشنهادی



دو آسیبپذیری بحرانی

آسیبپذیری روز صفری در روترهای **Humax** کشف شد

جالب آنکه بدافزار فوق میتواند به دوربین دستگاه دسترسی داشته و همچنین اسکرینشاتهایی را نیز تهیه کند . اولین نسخه از این بدافزار در اکتبر سال 2015 میلادی شناسایی شد و دومین نسخه در می 2017 شناسایی شد. این موضوع نشان میدهد که بدافزار فوق نزدیک به 18 ماه است که فعال بوده است. پژوهشگران پالوآلتو میگویند : «این بدافزار در مرحله توسعه قرار دارد . تاکنون نگارشهای مختلفی از این بدافزار شناسایی شدهاند که در تمامی این بدافزارها محتوای فایلهای پیکربندی و تقریبا تمامی رشتههای مورد استفاده از سوی این بدافزار کدگذاری و رمزنگاری شدهاند . زمانی که این بدافزار روی دستگاه قربانی نصب میشود در اولین کار اطلاعات پیکربندی همچون آدرس IP را از سرور کنترل و

فرماندهی و از یک فایل متنی به نام readme.txt بازیابی میکند . این بدافزار از کانالهای متنوعی به منظور برقراری ارتباط با مرکز کنترل و فرماندهی استفاده کرده و همچنین قادر است از 50 دستور مخرب استفاده کند .»

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
23:13 - 20/04/1396
برچسب:
امنیت - بدافزار - اندروید - SpyDleaer - ویچت - فیسبوک - تلگرام - اسکایپ - واتس‌آپ - فایرفاکس - Baidu Easy Root

---

نشانی
:https://www.shabakeh-mag.com/security/8642/%D8%AA%D8%B1%D9%88%D8%AC%D8%A7%D9%86-spydleaer-%D9%85%DB%8C%E2%80%8C%D8%AA%D9%88%D8%A7%D9%86%D8%AF-%D8%A7%D8%B2-40-%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D9%87-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF%DB%8C-%D8%AC%D8%A7%D8%B3%D9%88%D8%B3%DB%8C-%DA%A9%D9%86%D8%AF