آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

پنجشنبه هشتم خرداد ماه ۱۳۹۹

کشف یک بدافزار[1] جدید در شبکه‌های اجتماعی مبتنی بر اندروید[2]

نسخه ۱,۰,۰

نویسنده : مونا رضا زاده **سردبیر :** محمد پیشدار

[1]-Malware (a portmanteau for malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network

[2]-Android is a mobile operating system developed by Google.

شبکه‌های اجتماعی مبنتی بر اندروید مورد هدف بدافزار وُلف.رَت[1] قرار گرفته‌اند

تاریخ: ۱۹/ مِی/ ۲۰۲۰

بررسی اجمالی :

اخیرا محققان حوزه امنیت اطلاعات موفق به کشف گونه جدیدی از بدافزار دِن.دی.روید[2] در سیستم‌عامل اندروید شده‌اند. گونه جدیدی که اطلاعات قربانیان را از طریق پیام‌رسان‌های معروفی مانند واتس‌آپ[3] و فیسبوک[4] جمع‌آوری می‌کند. این بدافزار "وُلف.رَت" نام داشته و به اعتقاد محققان در حال توسعه بیشتر است [۱].

نگاه کلی :

سیستم‌های آسیب‌پذیر	پیام‌رسان واتس‌آپ و فیسبوک
راه‌های نفوذ	ارسال پیام‌های فیشینگ[5] از طریق پیامک
هدف مهاجمان	سرقت اطلاعات کاربران در شبکه‌های اجتماعی

توضیحات بیشتر :

چند تن از اعضای امنیتی شرکت سیسکو تالوس[6] به نام‌های وارِن مِرسِر[7]، پال راسکاگِنرِز[8] و وینترو وِنترا[9] در مورد این بدافزار در محیط سیستم‌عامل اندروید می‌گویند [۱] :

---

[1]-WolfRAT
[2]-Dendroid is malware that affects Android OS and targets the mobile platform.
[3]-WhatsApp Messenger is a freeware and cross-platform messaging and Voice over IP (VoIP) service owned by Facebook.
[4]-Facebook, Inc. is an American online social media and social networking service company based in Menlo Park, California.
[5]-Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.
[6]-The Talos Security Intelligence and Research Group (Talos) is made up of leading threat researchers supported by sophisticated systems to create threat intelligence for Cisco products that detects, analyzes and protects against both known and emerging threats.
[7]-Warren Mercer
[8]-Paul Rascagneres
[9]-Vitor Ventura

"محتوا و سوابق گفتگو پیام‌رسان‌ها (مانند واتس‌اَپ) حاوی اطلاعات حساسی بوده که بسیاری از کاربران این نکته را حین تعاملات خود با گوشی فراموش کرده و به برنامه‌های دیگر اجازه دسترسی به آن‌ها را می‌دهند. براساس گزارشات بطور خاص پیام‌رسانی‌هایی نظیر لاین[1] با قابلیت رمزنگاری مورد هدف بدافزار وُلف.رَت قرار گرفته‌اند. این نشان می‌دهد که حتی یک کاربر محتاط با آگاهی از رمزنگاری سراسری گفتگوها می‌تواند تحت سلطه بدافزار وُلف.رَت قرار بگیرد."

بر اساس اعلام مدیر بخش فنی سیسکو تالس (وارِن مِرسِر) این بدافزار از طریق لینک‌های فیشینگ (فیشینگ از طریق پیامک) به دستگاه قربانی منتقل شده و از دامنه‌هایی با نام غذاهای تایلندی برای فریب کاربران استفاده می‌کند. براساس گزارشات محل قرارگیری خدمات‌رسان‌های فرمان و کنترل[2] این بدافزار در تایلند واقع شده است [۱].

وُلف.رَت بعد از بارگذاری، به شکل سرویس‌های مُجاز مانند برنامه‌های کاربردی گوگل‌پِلی[3] یا بروزرسانی فِلَش[4] بوده و بطور عادی و بدون هیچ تعاملی با کاربر به فعالیت خود ادامه می‌دهد. بطور مثال این بدافزار با استفاده از نام com.google.services خود را عنوان یک برنامه‌کاربردی گوگل‌پِلی معرفی می‌کند [۱].

تاکنون چهار نسخه از بدافزار مذکور با قابلیت‌های جدیدی نظیر ضبط فیلم از صفحه نمایش گوشی هنگام اجرای واتس‌اِپ شناسایی شده است. علاوه براین نسخه‌های جدیدتر، دسترسی‌های بالاتری مانند ACCESS_SUPERUSER (در اندروید ۵ به بعد منسوخ شده است) و DEVICE_ADMIN (در اندروید ۱۰ به بعد منسوخ شده است) را از دستگاه قربانی درخواست می‌کنند [۱]. آخرین نسخه کشف شده بدافزار وُلف.رَت در زمان فعالیت برنامه‌های فیسبوک، واتس‌اَپ و لاین از صفحه نمایش عکس گرفته و فایل مربوطه را برای خدمات‌رسان فرمان و کنترل خود ارسال می‌نمایند. بدافزار مذکور فعالیت خود را از ژانویه ۲۰۱۹ شروع کرده اما یکی از دامنه‌های (ponethus[.]com) خدمات‌رسان فرمان و کنترل آن در سال ۲۰۱۷ ثبت شده است [۱].

پیوست اجرایی:

- عدم کلیک بر روی لینک‌های ناشناس
- اطمینان از نصب برنامه‌های امن با استفاده پویشگرهای امنیتی
- دریافت نرم‌افزار از طریق فروشگاه‌های مشهور

منابع :

1. Threatpost Website
https://threatpost.com/wolfrat-android-malware-whatsapp-facebook-messenger/155809/

[1]-Line (styled as LINE) is a freeware app for instant communications on electronic devices such as smartphones, tablet computers, and personal computers.
[2]-A command and control server (C&C server) is a computer that issues directives to digital devices that have been infected with rootkits or other types of malware, such as ransomware.
[3]-Google Play is a digital distribution service operated and developed by Google.
[4]-Flash