[redacted]

[redacted]

[redacted]

شکل 1: [illegible]

[illegible]

[illegible]

شکل 2: [illegible]

1- *AP* [illegible] *PSK* [illegible]

2- [illegible] *PTK* [illegible]

3- *AP* [illegible] *PTK* [illegible] *GTK* [illegible]

4- [illegible] *ACK* [illegible]

استراق سمع شبکه

برای سرقت اطلاعات شخصی شما همه آنچه یک مهاجم نیاز دارد، یک برنامه استراق سمع است که کل ترافیک قابل مشاهده روی شبکه را جمعآوری میکند . اگرچه WPA2 هر اتصال بین یک شبکه وایفای و کاربر را رمزنگاری میکند، اما اگر یک مهاجم فرآیند دست دادن چهارطرفه را شنود کند و به PSK دست یابد، قادر خواهد بود همه ترافیکی را که به دستگاه شما مربوط است، تا زمانی که PSK مجدد عوض شود، رمزگشایی کند . حتی اگر یک مهاجم به PSK دسترسی نداشت، ممکن است دادهها را شنود کند و بر اساس آن کلید را حدس بزند . کیفیت PSK که یک مدیر شبکه بیسیم آن را انتخاب میکند (نظیر طول، تنوع حروف، بهکارگیری نمادها یا واژههای شناخته شده)، میتواند بر سختی یا سادگی حدس زدن کلید تأثیر بگذارد .

جمعآوری دادهها توسط دیگران

حتی بدون حضور هکرهای فعال داده ضمانتی برای حفظ حریم خصوصی شما در حین اتصال به یک شبکه وایفای عمومی وجود ندارد . بزرگترین رخنه در حریم خصوصی شما بیشتر توسط تشکیلاتی ایجاد میشود که وایفای رایگان در اختیار شما قرار میدهد . برخی اوقات وایفای برای شناسایی مشترکان بالقوه که در مجاورت نقطه دسترسی حضور دارند و گاهی برای دنبال کردن وبسایتهایی که یک کاربر برای اهداف تبلیغاتی مشاهده میکند، مورد استفاده قرار میگیرد . این گونه جمعآوری دادهها توسط طرف سوم جدا از اهداف خرابکارانه ممکن است به کند و کاو در حریم خصوصی ما نیز منجر شود . در ادامه، روشهای متداولی بیان شده است که برنامهنویسان هاتاسپات برای فراهم کردن اطلاعات درباره کاربران وایفای بهکار میگیرند :

1- از مراجعان تقاضا میشود شماره تلفن یا ایمیل خود را بهمنظور ارائه پین برای دسترسی به اینترنت در اختیار آنها قرار دهند .

2- از مراجعان تقاضا میشود فایلی را در شبکه اجتماعی به اشتراک بگذارند یا دسترسی برنامه به هویت اجتماعی آنها را فراهم کنند .

3- چند نقطه دسترسی بر اساس قدرت سیگنال وایفای برای کاربر فراهم میکنند (برای مثال، بهمنظور دنبال کردن مسیر کاربران در یک فروشگاه یا برای شناسایی شبکهای که بیشترین کاربر را دارد).

4- تزریق کوکیها به مرورگر آنها بهمنظور بررسی تاریخچه صفحههای وب مشاهده شده توسط کاربران (بهمنظور نمایش تبلیغات مورد نظر).

مشتری
سرور DNS
شمایی از یک DNS نرمال
صفحه وب

شکل *3:* شمایی از یک *DNS* نرمال

نقاط دسترسی خرابکارانه

در حالی که چند شبکه مختلف برای دسترسی وجود دارد، شما اغلب حدس میزنید کدام هاتاسپات به محل مورد نظر شما تعلق دارد . برخی کاربران وایفای بهسادگی حتی به یک شبکه کاملاً ناشناخته متصل میشوند؛ تنها به دلیل اینکه دسترسی به آن رایگان است . واضح است این کار خطراتی در پی دارد، بهویژه اگر نقطه دسترسی خرابکارانه باشد یا توسط یک مهاجم آلوده شود . یکی از بزرگترین خطرات جعل صفحه است که در آن نقطه دسترسی خرابکار نام دامنه را تحت کنترل درمیآورد (نام دامنه طی یک فرآیند به نشانی IP معادل آن تبدیل میشود). در یک فرآیند عادی تبدیل DNS کاربر بهمنظور اتصال به اینترنت به سرویسدهنده متصل میشود.

در یک تهاجم جعل صفحه، هکر نسخه جعلی یک وبسایت را ایجاد میکند. برای مثال، ممکن است از شما خواسته شود قبل از اینکه به اینترنت دسترسی پیدا کنید، چیزی را در فیسبوک لایک کنید و سپس مستقیم به صفحه جعلی مربوط به ورود به حساب کاربری فیسبوک متصل خواهید شد که کاملاً مشابه نسخه اصلی آن است . به محض اینکه وارد حساب کاربری خود شوید، اطلاعات شما ذخیره میشوند و با پیغام خطا در ورود به حساب کاربری مواجه و سپس به صفحه واقعی فیسبوک هدایت میشوید تا دوباره برای ورود به حساب کاربری تلاش کنید . به این ترتیب، قبل از آنکه از آنچه اتفاق افتاد با خبر شوید، اطلاعات حساب کاربری شما به سرقت رفته است.

حمله DNS Spoofing
مشتری
سرور DNS
صفحه وب
صفحه وب تقلبی
مهاجم

شکل*4:* حمله *DNS Spoofing*

روش دیگر که به آن «حمله دوقلوی شیطانی» گفته میشود، یک نقطه دسترسی جعلی برای هک کردن دادههای شما ایجاد میکند . این روش بیشتر در اماکن عمومی نظیر پارکها یا سایر محیطهای بزرگ که تحت کنترل سازمان خاصی نیستند، به کار میرود . یک مهاجم با استفاده از یک لپتاپ مجهز به کارت شبکه قادر است یک نقطه دسترسی دوقلوی شیطانی با نام مشابه ایجاد کند . فرض کنید در یک مکان عمومی هستید و آیپاد شما

حمله دوقلوی شیطانی
مشتری
اینترنت
نقطه دسترسی
مهاجم دوقلوی
شیطانی

:5 [illegible]

[illegible]

[illegible]

1- [illegible]

2- [illegible]

3- [illegible]

راه ویروسها وارد کامپیوتر شما شوند . برای مثال، یک حمله متداول این است که به کاربر اعلام میکند مرورگر شما به نسخهای از نرمافزار فلش Adobe نیاز دارد و سپس شما را به یک وبسایت جعلی هدایت میکند که در اصل با نصب برنامه از این وبسایت، کامپیوتر شما به ویروس آلوده خواهد شد .

4- روش مناسب کسب اطمینان از حفظ امنیت اطلاعات کاربر در حین اتصال به یک وایفای عمومی استفاده از شبکههای اختصاصی مجازی است. اساساً یک شبکه اختصاصی مجازی بین دستگاه شما و سرور شخص سوم تونلی ایجاد میکند . همه دادههای ارسال و دریافت شده از طریق این تونل رمزگذاری میشوند و به این ترتیب هم از سرویسدهنده وایفای و هم هر شخص دیگری که تلاش میکند شبکه را شنود کند، مخفی خواهند شد.

اگر نتوانید از طریق شرکت خود به شبکه اختصاصی مجازی دسترسی پیدا کنید، یک شبکه اختصاصی مجازی طرف سوم مطمئن نظیر وایفای نصب کنید که از IPSec یا Open SSL استفاده میکند . اتصال به یک شبکه وایفای عمومی بسیار ساده است. هاتاسپاتهای عمومی رو به رشد و متعاقباً هکرهای این گونه شبکهها نیز در حال افزایش هستند . بهترین راه محافظت شما در مقابل سرقت دادهها درک وضعیت وایفای و آسیبپذیری آن و پیروی از توصیههای امنیتی خواهد بود .

مترجم:
مرضیه سادات کیایی
منبع :
نتورک ورلد
دسته بندی:
فناوری شبکه
تاریخ انتشار :
17:42 - 25/03/1394
برچسب:
شبکههای بیسیم - وایفای عمومی - امنیت وایفای - امنیت شبکه بیسیم

منبع: https://www.shabakeh-mag.com/networking-technology/864