ادعا شده بخشی از بدافزار مورد استفاده این گروه را شرکت «**محک رایان افزار** » در تهران که وابسته به**سپاه پاسداران** است تکمیل کرده است.

سرویس مطبوعاتی شبکه «فیسبوک» اعلام کرد؛

سرویس مطبوعاتی شبکه «فیسبوک» در اعلامیه ای از مسدود کردن دویست حساب کاربری گروهی از هکرهای مستقر در ایران خبر داد.

به گزارش اسپادانا خبر و به نقل از اسپوتنیک، این حساب‌ها بخشی از یک عملیات جاسوسی سایبری بودند که بیشتر کارکنان نظامی ایالات متحده و کسانی را که برای شرکت‌های دفاعی و هوافضایی کار می‌کنند هدف می‌گرفت.

در اعلامیه فیسبوک آمده است:

گروه هکری که کارشناسان امنیتی به آن نام «تورتس‌شل» Tortoiseshellداده‌اند از افراد ساختگی آنلاین برای تماس با هدف‌هایش بهره می‌گرفت و گاهی طی ماه‌ها در آن‌ها ایجاد اعتماد می‌کرد و بعد آن‌ها را به سایت‌هایی هدایت می‌کرد تا با کلیک کردن لینک‌های مخرب، دستگاه‌های‌شان را به بدافزارهای جاسوسی آلوده کند.

گروه تحقیق فیسبوک نیز نوشته است:

«این فعالیت نشانه‌های عملیاتی با منابع و استمرار کافی را داشت و بر تدابیر نیرومند عملیاتی امنیتی استوار بود تا هویت عوامل آن را پنهان کند. این گروه در چندین شبکه اجتماعی پروفایل‌های جعلی ساخته بود تا به نظر معتبرتر برسد و اغلب به در نقش کارفرماهایی ظاهر می‌شدند که می‌خواهند کارکنان شرکت‌های هوافضایی و دفاعی را استخدام کنند. این گروه از ایمیل، پیام‌رسانی و خدمات تعاملی استفاده می‌کرد تا بدافزار توزیع کند. می‌شود. هکرها از دامنه‌هایی که به طور اختصاصی برای جذب هدف‌هایشان طراحی شده بود استفاده می‌کردند از جمله وبسایت‌های استخدام برای شرکت‌های دفاعی به گونه‌ای که مشابه وبسایت کاریابی وزارت کار ایالات متحده بود. هکرها عمدتا اشخاصی را در آمریکا، بریتانیا و اروپا هدف قرار داده بودند».

این گروه پیشتر عمدتا بر بخش‌های اطلاعات و صنایع دیگر در خاورمیانه متمرکز بود. در جریان تحقیقات روشن شد که بخشی از بدافزار مورد استفاده گروه را شرکت «محک رایان افزار» در تهران که وابسته به سپاه پاسداران است تکمیل کرده است.

برچسب ها: شبکه های اجتماعی [1]
تروریسم [2]
سپاه پاسداران [3]