فیسبوک: گروه هک ویتنامی APT32 در نقاب یک شرکت IT فعالیت می‌کند - دیجیاتو

پیمان حسنی | یکشنبه، ۲۳ آذر ۱۳۹۹

فیسبوک مدعی شد یک گروه هک در ویتنام با نقاب یک شرکت IT فعالیت کرده و توسط دولت این کشور پشتیبانی می‌شود.

تیم امنیتی فیسبوک مدعی پیدا کردن هویت واقعی یک گروه هک با اسامی APT32 و OceanLotus شد. این گروه دستکم از سال ۲۰۱۴ فعال است و شرکت‌های خصوصی در صنایع مختلف و همچنین دولت‌های خارجی، سازمان‌های دفاع از حقوق بشر و آژانس‌های خبری را در جنوب آسیا و جهان هدف قرار داده است.

گروه مورد بحث از تاکتیک‌های متعدد از جمله فیشینگ و بدافزارهای اختصاصی برای آلوده کردن سیستم‌ها استفاده می‌کند و برای جلب اعتماد قربانیان وب سایت‌های جعلی با نقاب سازمان‌ها و افراد حقیقی و قانونی توسعه می‌دهد. محققان امنیتی اوایل سال جاری میلادی هشت اپلیکیشن اندرویدی مخرب در گوگل پلی شناسایی کردند و آنها را به این گروه مرموز ربط دادند.

حال فیسبوک می‌گوید شرکت فناوری اطلاعات CyberOne Group که به طور قانونی در شهر «هو شی مین» ویتنام فعالیت می‌کند به گروه هک OceanLotus با APT32 ربط دارد. یکی از مدیران

صفحه فیسبوک این شرکت که حالا غیرفعال شده در پاسخ به سوال رویترز گفت: «اشتباه شده، ما گروه Ocean Lotus نیستیم.»

فیسبوک در گزارش خود اشاره نکرد که چگونه شرکت CyberOne Group را به گروه هک OceanLotus ربط داده، اما گفت ارائه جرئیات بیشتر باعث می‌شود تا گروه‌های هک مشابه از روش‌های شناسایی باخبر شوند و ردیابی آنها مشکل‌تر شود.

محققان امنیتی در گذشته نیز گروه‌های هک را به شرکت‌ها و سازمان‌های تحت حمایت دولت‌ها ربط داده‌اند. سال ۲۰۱۳ محققان شرکت امنیتی Mandiant یک ساختمان ۱۲ طبقه در شانگهای چین را به عنوان مقر گروه هک Comment Crew شناسایی کردند که در طول ۷ سال گذشته مسئول حمله سایبری به بیش از ۱۴۰ ارگان بوده است.

به گفته محققان این ساختمان مقر اصلی یکی از واحدهای سری ارتش آزادی‌بخش خلق چین به نام «واحد ۶۱۳۹۸» است که دولت آمریکا آن را متهم به دست داشتن در عملیات‌های هک و جاسوسی سایبری از صدها سازمان بین المللی کرده است. آوریل ۲۰۱۸ نیز شرکت امنیتی FireEye اعلام کرد بدفزار Triton که سبب از کار انداختن نیروگاهی در خاورمیانه شد در آزمایشگاهی در روسیه توسعه داده شده است.

دیجیاتو