جاسوسی از مذاکرات هسته ای ایران به وسیله مجوزهای دیجیتالی فاکسکان صورت گرفته است - دیجیاتو

امیر مستکین | سه شنبه، ۲۶ خرداد ۱۳۹۴

کمپانی امنیتی کسپرسکی امروز اعلام کرد که با نگاهی عمیق تر به ویروس Duqu 2.0، توانسته به اطلاعات بیشتری دست پیدا کند. اکنون این کمپانی امنیتی روسی عنوان نموده که ویروس یاد شده برای جاسوسی، از مجوز های دیجیتالی کمپانی «فاکسکان» بهره برده است.

فاکسکان نامی آشنا برای دوستداران تکنولوژی به شمار می رود، سازنده ای تایوانی که کار اسمبل کردن محصولات مختلفی از آیفون و آیپد های اپل گرفته تا اکس باکس های مایکروسافت و همچنین پلی استیشن ۴ های سونی را بر عهده دارد. در ادامه با دیجیاتو همراه باشید.

نرم افزار مخرب Duqu 2.0 توانسته بود شبکه هتل های محل برگزاری جلسات شورای امنیت سازمان ملل متحد را آلوده کند. اکنون کسپرسکی می گوید نسل قبلی این ویروس به نام Duqu ۱.۰ و همچنین استاکس نت نیز از گواهی های دیجیتالی دزدیده شده از کمپانی های تایوانی بهره گرفته اند و این احتمال می رود که حمله کنندگان می خواسته اند اینگونه به نظر برسد که حملات از چین صورت گرفته اند.

مجله وایرد باور دارد که ویروس Duqu ۱.۰ و ۲.۰ به شکل کامل توسط رژیم صهیونیستی توسعه یافته اند و از آنجایی که هکرها برای اعمال مخرب خود به یک مجوز دیجیتالی (digital certificate) نیاز داشته اند، از مجوز های فاکسکان استفاده شده تا این اشخاص بتوانند درایورهای لازم را بر سرورهای امنیتی کسپرسکی نصب کنند.

نکته اینجاست که ویروس Duqu ۲.۰ پس از خاموش شدن کامپیوتر ناپدید می گردد و سپس یک درایور می تواند دوباره و پس از روشن شدن کامپیوتر، آن را نصب کند. هکر ها از همین درایور برای انتقال داده ها (که مشخصا آنها را دزیده اند) نیز بهره گرفته اند تا در نهایت شناسایی کلیت بدافزار به سطوح مشکل تری کشیده شود.

کاستین رایو (Costin Raiu) مدیر تیم تحقیق و بررسی بین الملل کسپرسکی اکنون باور دارد که حمله کنندگان از یک مجوز دیجیتالی متعلق به کمپانی فاکسکان بهره گرفته اند تا ضریب موفقیتشان بسیار بالاتر رود؛ وی همچنین عقیده دارد که چنین عملی بسیار نادر است.

چنین اتفاقاتی باعث گشته اند که شرکت امنیتی کسپرسکی نتواند در هنگام برگزاری مذاکرات، وجود چنین ویرویسی را تشخیص دهد تا اینکه بالاخره مدتی بعد مهندسانش به این رخنه ی امنیتی پی می برند.

رایو اکنون باور دارد که بدافزار یا ویروس های Duqu 1.0 و استاکس نت نیز در گذشته از مجوز های دیجیتالی مشکوک استفاده کرده اند.

دیجیاتو