بدافزار شمعون اطلاعات مهم شرکت نفت و گاز در ایتالیا را از بین برد - دیجیاتو

مانی میرجوادی | جمعه، ۲۳ آذر ۱۳۹۷

طبق گزارشات گونه‌ی جدیدی از بدافزار شمعون در سیستم‌های شرکت نفت و گاز ایتالیا که -تحت قرارداد با ساایپم، شرکت ایتالیایی پیمانکار صنعت نفت و گاز هستند- پیدا شده که حدود ۱۰ درصد از فایل‌های موجود در کامپیوترهای ساایپم را از بین برده است.

بیشتر سیستم‌های آلوده شده به بدافزار شمعون در خاورمیانه قرار دارند، جایی که ساایپم بیشترین فعالیت را دارد. اما آلودگی به این بد افزار از هند و اسکاتلند نیز گزارش شده است.

شمعون یکی از خطرناک‌ترین بدافزارهای شناخته شده در دنیا به شمار می‌رود. این بدافزار ابتدا دو بار آرامکو، بزرگترین شرکت تولید نفت عربستان را هدف قرار داد.

در این دو اتفاق که یکی سال ۲۰۱۲ و دیگری در سال ۲۰۱۶ به وقوع پیوست، بدافزار یاد شده فایل‌های مهم شرکت نفتی آرامکو را حذف کرد و آن‌ها را با عکس‌هایی از پرچم آتش گرفته‌ی آمریکا و تصاویری از بدن بی جان آلان کردی (کودک سوری) جایگزین نمود.

حملات سال ۲۰۱۲ نیز به نوبه‌ی خود تاثیرات مخرب زیادی بر جای گذاشت. این حملات اطلاعات ۳۰ هزار کامپیوتر شرکت آرامکو را از بین برد و هفته‌های متمادی مانع فعالیت این شرکت شد.

حملات جدیدی که علیه ساایپم اتفاق افتاده نیز به نظر بی ربط با حملات آرامکو نیست. ساایپم یکی از اصلی‌ترین شرکای خارجی آرامکو به حساب می‌آید.

نسخه‌ی جدید بدافزار شمعون پیش از این دیده نشده بود. این بدافزار ابتدا روی VirusTotal آپلود شد که آی پی آپلود کننده از کشور ایتالیا بود، جایی که دفتر مرکزی سایپم در آن بنا شده است. نسخه‌های دیگر از این بدافزار روزهای بعد از آدرس آی پی‌هایی در هند آپلود شدند که پیش از این سایپم گزارش‌هایی از آلوده شدن سیستم‌هایش در این کشور را نیز دریافت کرده بود.

به گفته مسئولان سایپم این نسخه از بدافزار شمعون بر خلاف نسخه‌های قبلی فایل‌ها را جایگزین نکرده و صرفا آن‌ها را کدگذاری کرده است. اما یک متخصص امنیت بعد از بررسی این بدافزار از VirusTotal اعلام کرد که اطلاعات منتشر شده از این مسئول درست نیست.

این متخصص بر این عقیده است که فایل‌ها کدگذاری نشده‌اند. بلکه حذف شده و با فایل‌های مخرب و بیهوده‌ی دیگری جایگذاری شده‌اند که حتی با داشتن کلید و بعد از رمزگشایی فایل‌های اصلی شرکت نفت و گاز سایپم بازگشت داده نخواهند شد.

البته لازم به ذکر است که بدافزار شمعون جلوی کسب و کار را از سایپم نگرفته و تنها تعداد خاصی از لپتاپ‌ها و سیستم‌های این شرکت به این بدافزار آلوده شده‌اند و تجهیزات اصلی این شرکت آسیبی ندیده‌اند.

در حال حاضر ساییپم بسیاری از سیستم‌های آلوده‌ی خود را بازیابی کرده و در تلاش است تا با بازیابی فایل‌های بکاپ شده فعالیت عادی خود را از سر بگیرد.

دیجیاتو