ویروس رایانه ای شمعون که چهار سال پیش صنایع انرژی عربستان را هدف قرار داده بود، مجدد بازگشته و اتهامات علیه ایران را نیز بازگردانده است.

شرکت‌های امنیتی آمریکایی ادعا می‌کنند نسخه جدیدی از ویروس مخرب شمعون (Shamoon) که چهار سال پیش ده‌ها هزار رایانه شرکت‌های انرژی کشورهای خاورمیانه را هدف قرار داده بود، دو هفته پیش مجدداً در رایانه‌های عربستان سعودی مشاهده شده است.

کرود استرایک (CrowdStrike)، پالوآلتو نتورکز (Inc Networks Alto Palo) و سیمنتک (Corp Symantec.) روز 30 نوامبر 2016 از حملات جدید این بدافزار خطرناک خبر دادند. آن‌ها از هیچ‌یک از قربانیان نسخه جدید ویروس شمعون، که اطلاعات مستربوت رایانه ها را که برای راه‌اندازی آن‌ها استفاده می‌شود پاک می‌کند، نام نبردند. آن‌ها همچنین از میزان خسارات وارده و یا شناسایی هکرها اطلاعاتی منتشر نکردند.

ظهور مجدد ویروس شمعون از آن نظر موردتوجه است که نمونه‌های موفق چندانی از بدافزارهای پاک‌کننده دیسک سخت موجود نیست. از دیگر نمونه‌های این‌گونه بدافزارها می‌توان به مورد استفاده‌شده در استودیو فیلم‌سازی هالیوودی سونی اشاره کرد. بدافزارهای تخریب هارددیسک ازآن‌جهت موردتوجه دولت‌ها و شرکت‌ها است که بازیابی دستگاه‌های خسارت‌دیده، اگر ممکن باشد، بسیار زمان‌بر و هزینه‌بر است.

در نسخه اصلی ویروس شمعون، هکرها تصویری از پرچم در حال سوختن ایالات‌متحده را روی رایانه‌های شرکت آرام کو عربستان (Aramco Saudi) و رأس گس (Ltd Co RasGas) که از بزرگ‌ترین شرکت‌های فعال در حوزه نفت و گاز هستند نمایش می‌داد. به گفته محققان ویروس شمعون 2 یک کارت ویزیت نیز از خود به‌جا می‌گذارد، تصویری از آلان کوردی، پناه‌جوی 3 ساله سوری، که سال گذشته در سواحل مدیترانه غرق شد.

به ادعای دیمیتری آلپروویچ (Alperovitch Dmitri)، مدیر فناوری کرود استرایک، به‌احتمال‌زیاد گروه‌هایی از جانب ایران پشت سر حملات سال 2012 بوده است؛ البته هنوز بسیار زود است که بگوییم همان گروه شمعون 2 را راه‌اندازی کرده است. انگیزه این حملات هنوز روشن نیست.
گروه واکنش شرکت سیمنتک گفت:« چرا شمعون پس از 4 سال ناگهان پیدایش شده، هنوز معلوم نیست، با وجود این، با توجه به محموله خطرناک این ویروس، مشخص است که هکرها دوست دارند اهدافشان منتظر بنشینند و مترصد حرکات بعدی آن‌ها باشند.»

شرکت های امنیتی خبر دادند که این بدافزار به نحوی تنظیم شده بود تا حدود 8:45 بعدازظهر به‌وقت محلی روز پنج‌شنبه 17 نوامبر حمله خود را آغاز کند. با توجه به اینکه هفته کاری عربستان روز پنج‌شنبه پایان می‌یابد، به نظر می‌رسد این بدافزار برنامه‌ریزی شده بود تا هنگامی‌که افراد شرکت‌ها را ترک می‌کنند فعال شود و از فرصت تعطیلات آخر هفته برای مخفی ماندن و افزایش آسیب‌ها استفاده کند.

به گفته یکی از محققان پالو آلتو، احتمالاً این بدافزار تمام آخر هفته را برای گسترش فرصت داشته است.