چهار شنبه 04 مرداد 1391 - 01:47

# کنترل حمله سایبری جدید علیه ایران از سرورهای جمهوری آذربایجان و کانادا

تروجان یا بد افزارهای مخرب "مهدی ؛ مسیح" با تمرکز بر اسلام، زبان فارسی، و درگیری های میان اسرائیل و ایران به صدها رایانهٔ شخصی در خاور میانه نفوذ کرده است

/خبرگزاری آران

خبرگزاری آران/سرویس آذربایجان

تروجان یا بد افزارهای مخرب "مهدی ؛ مسیح" با تمرکز بر اسلام، زبان فارسی، و درگیری های میان اسرائیل و ایران به صدها رایانهٔ شخصی در خاور میانه نفوذ کرده است.

بولتن نیوز:به گزارش محققان "سیمانتک"، سرور دستور و کنترل بد افزارهای مخرب "مهدی ؛ مسیح" در آذربایجان یافت شده است.

این در حالی است که "سکیولرت" بعضی از این سرور ها را در کانادا نیز یافته بود. بنا بر گزارش های منتشره، قبل از این بد افزارهای "شعله" و "استاکس نت" نیز توسط ایالات متحده و اسرائیل تولید و راه اندازی شده است که هدف آنها ایجاد اختلال و انفجار در مراگز صلح آمیز هسته ای ایران است و احتمال این میرود موضوع حملات بد افزار "مهدی؛ مسیح" به رایانه های اسرائیلی ساحتگی بوده و پوششی باشد برای جلوگیری از زیر سوال رفتن دوباره آمریکاییها و اسرائیلیها در حملات سایبری به تاسیسات هسته ای ایران.

در این رابطه "الینور میلز" در سایت "بلاگ پست" نوشت: محققان اعلام کردند که یک تروجان (یکی از قوی ترین هکرها سارق اطلاعات) که قادر به سرقت داده ها ، ثبت ضربهٔ کلید ها، تصاویر و فایل های صوتی پخش یا ضبط شده و سرقت فایل های متنی و تصویری است، طی هشت ماه گذشته حدود800 رایانه شخصی را آلوده کرده که عمدتا در ایران و اسرائیل بوده اند.

به گزارش "بلاگ پست" از شرکت امنیتی سکیولرت مستقر در اسرائیل؛ این بد افزار مخرب، ملقب به "مهدی" (مَدی) به دلیل ارجاع به کدواژهٔ مهدی یا "مسیح اسلامی"، حاوی رشته هائی به زبان فارسی و تاریخ در قالب تقویم فارسی در ارتباط با یک سرور فرمان و کنترل یا حداقل یکی از انواع آن و سروری دیگری است که حداقل به مدت یک سفر داخلی یا یک فصل در ایران نصب شده است.

سیمانتک گزارش داد: قربانیان این بدافزار شامل شرکت های زیرساخت های حیاتی، سفارتخانه های دولتی و شرکت های خدمات مالی مستقردر ایران، اسرائیل، افغانستان، امارات متحده عربی، عربستان سعودی و دیگر کشورهای خاورمیانه، و همچنین ایالات متحده و نیوزیلند است.

محققان می گویند با وجود نوع قربانیان و کشورهائی که به ویژه تحت تاثیر این بد افزار قرارگرفته اند، هنوز معلوم نیست که آیا این حمله با حمایت دولت یا دولت هائی برنامه ریزی شده است یا خیر.

سکیولرت گفت : این مبارزات با مهندسی اجتماعی از طریق یک ضمیمه ایمیل آغاز شد. در یکی از تلاش ها ، فایل ضمیمه ، بدافزاری را اجرا کرده که حاوی یک سند وُرد از مقاله ای با عنوان "جنگ های الکترونیکی - راز طرح اسرائیل برای حمله به ایران" بوده است.

به گزارش محققان سیمانتک، که سرور دستور و کنترل مورد بحث را در آذربایجان پیدا کرده اند، در حالی که سکیولرت بعضی از این سرور ها را در کانادا نیز یافته بود ؛ دیگر اهداف این بد افزار مخرب فایل های ضمیمهٔپاورپوینت است که عکسها و ویدیوهائی را نمایش می دهد درآن موشکی یک هواپیما جت را منهدم می کند و یا یک جعبه گفتگو را نشان می دهد که از کاربر می خواهد تا اجازهٔ نصب و راه اندازی یک فایل اجرائی SCRرا به او بدهد.

به گزارش بلاگ پست کسپرسکی فایل پاورپوینت با ویژگی "محتوای فعال شده " می تواند بطورخودکار محتوای اجرایی را در داخل فایل پیوست راه اندازی کند و دانلود کننده هایی که داخل آن تعبیه شده خدمات مخفیانه ای را نصب و راه اندازی کرده و پیش ببرند.

یک نمونه از این فایل های اجرایی به نمایش اسلایدی پازل ریاضی گیج کننده ای فرستاده شد، در حالی که دیگری مجموعه ای از تصاویر طبیعت با مضمون های مذهبی، و پیام هائی به زبان انگلیسی و عبری ضعیف را نشان می داد.

شرکت کسپرسکی مستقر در روسیه گفت که این شرکت همچنین تصاویری را دیده که یک انفجار هسته ای را نشان می دهد و ویدئویی، که به احتمال زیاد برای فریب قربانیان طراحی شده تا آنها را به سمت این تفکربکشاند که هیچ حادثهٔ ناگوار و ناخواسته ای اتفاق نمی افتد.

این جدیدترین قطعهٔ تروجان با لینک به ایران است. شعله، استاکس نت و پسر عمویش "دوکو" همگی سیستم های کامپیوتری بسیار مهمی را در ایران و کشورهای همسایه هدف گرفته اند. بنا بر گزارش ها شعله و استاکس نت توسط ایالات متحده و اسرائیل تولید و راه اندازی شده است./خ

پایان پیام.