

شناسایی بزرگترین حمله سایبری تاریخ

متخصصان امنیتی به تازگی دریافته اند که «عملیات موش مرموز» بزرگترین مجموعه حملات سایبری در سرتاسر جهان بوده که تا کنون در تاریخ به ثبت رسیده است.



جام جم آنلاین: متخصصان امنیتی به تازگی دریافته اند که #171 عملیات موش مرموز» بزرگترین مجموعه حملات سایبری در سرتاسر جهان بوده که تا کنون در تاریخ به ثبت رسیده است.

به گزارش مهر، این عملیات برای پنج سال متوالی ادامه داشته و 72 سازمان جهانی را هدف قرار داده است. به گفته متخصصان امنیت شبکه، این بزرگترین سری حملات سایبری بوده که تا کنون شناسایی شده و طی آن اطلاعات 72 سازمان جهانی از قبیل سازمان ملل متحد، دولتهای مختلف و شرکتهای بین المللی مورد حمله سایبری قرار گرفته اند.

گزارش مک کافی از #171 موش مرموز»

شرکت امنیتی مک کافی که این حمله سایبری وسیع را کشف کرده اعلام کرد گمان می رود در پس این حمله گسترده سایبری یک #171 مهره دولتی» حضور داشته باشد اما این شرکت نام دولت یا مهره ای که در آغاز و اجرای حمله دست داشته است را اعلام نکرد، اما از سویی دیگر متخصص دیگری که از این حمله سایبری آگاهی داشت شواهدی از حضور دولت چین را ارائه کرده است.

لیست طولانی و بلند بالای قربانیان پنج ساله این حمله سایبری شامل اسامی از قبیل سازمان ملل متحد، دولت ایالات متحده آمریکا، تایوان، هندوستان، کره جنوبی، ویتنام، کانادا، اتحادیه ملتهای جنوب شرقی آسیا، کمیته بین المللی المپیک، آژانس جهانی مبارزه با دوپینگ، و تعدادی از شرکتهای وابسته به فعالیتهای نظامی و فناوری است.

بر اساس گزارش رویترز، هکرها در سال 2008 توانسته اند به رایانه دبیرخانه سازمان ملل متحد در ژنو نفوذ کرده و برای مدت دو سال به صورت مخفیانه در آن باقی بمانند و به دریایی از اطلاعات محرمانه دسترسی پیدا کنند.

#171#؛ دیمیتری آلپروویچ» قام مقام مک کافی می گوید: تنوع گسترده شرکتهایی که توسط هکرها غافلگیر شده اند بسیار شگفت انگیز است. سرنوشت این حجم از اطلاعات به سرقت رفته هنوز نامشخص است اما به هر حال اگر بخش کوچکی از این اطلاعات منجر به ساخت محصولات بهتر توسط یک شرکت رقیب و یا شکست دادن یکی از مذاکره کنندگان اصلی در یک مذاکره مهم سیاسی شود، این حمله سایبری می تواند منجر به وارد آمدن خسارت بزرگ و غیر قابل جبرانی شود.

اولین نشانه های نفوذ موش مرموز

سازمان امنیت داخلی آمریکا در 24 سپتامبر 2011 این حمله سایبری را مورد بررسی قرار داد. مک کافی نیز در ماه مارچ سال جاری زمانی که محققان این شرکت در حین بازبینی محتویات یک سرور متعلق به شرکتهای دفاعی نشانه های حمله را مشاهده کردند، پی به شدت گستردگی این حمله سایبری برد. این سرور در سال 2009 و حین تجسس برای یافتن آسیب پذیری های شرکتهای دفاعی کشف شده است.

گفته می شود عملیات موش مرموز در اواسط سال 2006 آغاز شده است با این همه هنوز احتمالاتی از حملات زود هنگام تری که تا کنون ناشناخته باقی مانده اند وجود دارد. عبارت RAT به معنی موش صحرائی که در نام این عملیات به کار برده شده است در واقع مخفف عبارت #171؛ ابزار دسترسی از راه دور» است، نوعی نرم افزار که هکرها و متخصصان امنیتی برای دسترسی به شبکه های رایانه ای از آن استفاده می کنند.

بر اساس گزارش مک کافی، برخی از این حملات تنها یک ماه ادامه داشته اند اما برخی دیگر مدتی طولانی در حال اجرا بوده اند که نمونه بارز آن حمله سایبری به کمیته المپیک یکی از کشورها بوده که نام آن اعلام نشده و برای 28 ماه ادامه داشته است. به گفته آلپروویچ شرکتهای و آژانسهای دولتی هر روز و به صورت ناشناخته مورد حمله و تجاوز قرار می گیرند، فرصتهای اقتصادی خود را از دست می دهند و اسرار مالی آنها در اختیار رقبایشان قرار می گیرد.

وی می گوید این بزرگترین انتقال دارایی در قالب مالکیت معنوی کشورها در تاریخ بشر است و مقیاس این انتقال بسیار، بسیار ترسناک است.

