یکشنبه 16 مرداد 1390 - 11:32

جزئیات بزرگ‌ترین حمله سایبری جهان

کارشناسان شرکت امنیت رایانه‌ای مک‌آفی از بزرگ‌ترین مجموعه حملات سایبری تاکنون و نفوذ به شبکه ۷۲سازمان جهانی و بین‌المللی ازجمله سازمان ملل متحد پرده برداشته‌اند.

کارشناسان شرکت امنیت رایانه‌ای مک‌آفی از بزرگ‌ترین مجموعه حملات سایبری تاکنون و نفوذ به شبکه ۷۲سازمان جهانی و بین‌المللی ازجمله سازمان ملل متحد پرده برداشته‌اند.

گفته می‌شود چین در این پروژه جهانی هک و حمله سایبری دست داشته است.خبرگزاری رویترز به نقل از شرکت معتبر مک‌آفی که از هک‌شدن این ۷۲ سازمان، دولت و کمپانی در سراسر جهان پرده برداشته است، می‌گوید که «یک عامل دولتی» پشت این حملات بوده، اما از فاش کردن هویت این عامل خودداری کرده است. در همین حال این خبرگزاری از قول یک کارشناس امنیت رایانه که از جزئیات این پرونده خبر دارد می‌نویسد که همه شواهد از دست داشتن چین خبر می‌دهند. فهرست طولانی قربانیان این پروژه 5ساله، دولت‌های آمریکا، تایوان، هند، کره‌جنوبی، ویتنام، کانادا، سازمان آسه‌آن، کمیته بین‌المللی المپیک و همین طور چند پیمانکار دفاعی را دربرمی‌گیرد.

شرکت امنیتی مک‌آفی در گزارشی ۱۴ صفحه‌ای که اخیرا منتشر کرده می‌گوید: در مورد سازمان ملل، هکرها در سال۲۰۰۸ وارد شبکه رایانه این سازمان در شهر ژنو شده و نزدیک به 2سال بی‌آنکه شکی برانگیزند به مقدار فراوانی اطلاعات محرمانه دسترسی داشته‌اند.

به گفته جیم لوئیس، کارشناس سایبری در مرکز مطالعات بین‌الملل و استراتژیک، «بسیار احتمال دارد که دولت چین پشت این حملات سایبری باشد،چرا که برخی از قربانیان، اطلاعاتی داشتند که مورد توجه خاص پکن است. البته روس‌ها هم می‌توانستند باشند، اما بیشتر شواهد به چین اشاره دارند تا روسیه».

این نخستین بار نیست که نام دولت چین در یک پرونده هک و حمله سایبری در حد ملی و بین‌المللی مطرح می‌شود. مقامات چینی البته هر بار هرگونه اتهام در این زمینه را رد کرده‌اند. پیشتر، در خردادماه سال‌جاری نیز کمپانی گوگل هکرهای مستقر در چین را مسئول اقدام به سرقت اطلاعات از صدها کاربر جی‌میل از جمله مقامات دولت آمریکا، پرسنل ارتش، فعالان سیاسی مخالف دولت چین و روزنامه‌نگاران معرفی کرد.

دیمیتری آلپروویچ، معاون شرکت مک‌آفی، می‌گوید: حتی ما هم از تنوع و گوناگونی قربانیان و جسارت و گستاخی هکرها شگفت‌زده شده‌ایم.

به گفته آقای آلپروویچ، شرکت مک‌آفی تمام ۷۲ قربانی این حملات سایبری 5ساله را در جریان گذاشته و این حملات هم‌اکنون در سراسر جهان توسط مجریان قانون در دست بررسی است.

معاون شرکت مک‌آفی از ارائه جزئیات بیشتر در این زمینه، از جمله نام شرکت‌هایی که هدف هک قرار گرفته‌اند خودداری کرد.کارشناسان گفته‌اند که هکرها با استفاده از روش فیشینگ به کدهای شخصی کاربرانی که به اطلاعات دسترسی داشته‌اند، دست یافته‌اند. در روش فیشینگ یا به‌اصطلاح سرقت آنلاین، کپی دقیقی از یک وب‌سایت معتبر طراحی می‌شود و کاربر از طرق مختلف نظیر ای‌میل به این صفحه هدایت می‌شود. در ادامه از کاربر خواسته می‌شود تا اطلاعات مهمی نظیر نام کاربری و رمز عبور را وارد کند و به این ترتیب هکرها به این اطلاعات دسترسی می‌یابند. در این حملات نفوذگران پس از سرقت اطلاعات و با بهره‌گیری از خلأ امنیتی موجود در رایانه افراد با نصب نرم‌افزارهای مخرب کنترل رایانه را از راه دور در دست می‌گیرند.
در گزارش منتشره از سوی شرکت مک‌آفی، این حمله بزرگ سایبری بسیار تهدیدآمیزتر از حملات اخیر گروه‌هایی نظیر «ناشناس» شناخته شده است.

بعضی از این حملات تنها در عرض یک ماه انجام گرفته اما در برخی موارد دیگر نظیر نفوذ به سایت‌های کمیته ملی المپیک چندین کشور آسیایی در آستانه بازی‌های المپیک سال۲۰۰۸ پکن، هکرها به‌مدت ۲۸ماه به‌طور نامتناوب مشغول جمع‌آوری اطلاعات محرمانه بوده‌اند.

سازمان امنیت داخلی آمریکا در 24 سپتامبر 2011 این حمله سایبری را مورد بررسی قرار داد. مک‌آفی نیز در ماه مارس سال‌جاری زمانی که محققان این شرکت حین بازبینی محتویات یک سرور متعلق به شرکت‌های دفاعی نشانه‌های حمله را مشاهده کردند، پی به‌شدت گستردگی این حمله سایبری برد.

این سرور در سال2009 و حین تجسس برای یافتن آسیب‌پذیری‌های شرکت‌های دفاعی کشف شده است. گفته می‌شود عملیات موسوم به «موش مرموز» در اواسط سال2006 آغاز شده است با این همه هنوز احتمالاتی از حملات زودهنگام‌تری که تاکنون ناشناخته باقی مانده‌اند وجود دارد. عبارت RAT به معنی موش صحرایی که در نام این عملیات به کار برده شده است در واقع مخفف عبارت ابزار دسترسی از راه دور است؛ نوعی نرم‌افزار که هکرها و متخصصان امنیتی برای دسترسی به شبکه‌های رایانه‌ای از آن استفاده می‌کنند.

به گفته آلپروویچ، معاون شرکت مک‌آفی، شرکت‌ها و آژانس‌های دولتی هر روز و به‌صورت ناشناخته مورد حمله و تجاوز قرار می‌گیرند، فرصت‌های اقتصادی خود را از دست می‌دهند و اسرار ملی آنها در اختیار رقبایشان قرار می‌گیرد.
وی می‌گوید: این بزرگ‌ترین انتقال دارایی در قالب مالکیت معنوی کشورها در تاریخ بشر است و مقیاس این انتقال بسیار بسیار ترسناک است.

راج سامانی، ازمقامات مک آفی، نیز به بی‌بی سی گفت: این حملات همچنان ادامه دارند و برعکس حملات سایبری اخیر، بسیار عظیم هستند و طیف وسیعی از شرکت‌ها را دربرمی‌گیرند. وی افزود که نمی‌داند با اطلاعات به سرقت رفته چه کار کرده‌اند. یک ای‌میل به فردی در سازمان مورد نظر که به اطلاعات محرمانه دسترسی دارد فرستاده می‌شود که به پیوست آن برنامه‌ای ضمیمه شده که پس از بازشدن ای‌میل در رایانه به اجرا درمی‌آید و دسترسی به اطلاعات آن سازمان را برای سارقین امکان‌پذیر خواهد کرد. آنها قبل از اینکه شناسایی و دستگیر شوند تمامی اطلاعات را سرقت می‌کنند.

با این حال، گراهام کلولی، کارشناس امنیت رایانه می‌گوید: هرازگاهی یک سرقت اطلاعاتی گزارش می‌شود و انگشت اتهام همیشه به سوی چین نشانه می‌رود. ما نمی‌توانیم مقصر بودن این کشور را اثبات کنیم اما نباید ساده‌انگارانه هم به این قضیه نگاه کنیم. هر کشوری در جهان احتمال دارد در اینترنت جاسوسی کند. مؤسسات مختلفی در چند ماه اخیر مورد حمله Lulz Sec یا افرادی ناشناس قرارگرفته‌اند.

پس نباید بلافاصله یک کشور را متهم کرد. گاهی اوقات مسئله دزدیدن کیف پول یا اطلاعات شخصی یک فرد نیست بلکه موضوع سرقت پنهانی و بی‌سروصدای اطلاعاتی است که ارزش بسیار بالای سیاسی، نظامی و حتی اقتصادی دارند.