پنجشنبه 18 آذر 1389 - 08:01

معرفی بزرگترین حملات سایبری جهان

به گفته "آرون سود" نایب رئیس مرکز بین المللی سایبری در دانشگاه "جورج میسون" اگر یک هواپیما را ببینید می دانید که به نیروی هوایی کشوری تعلق دارد، اما اگر به شما حمله سایبری شود حتی نمی توانید بفهمید از کجا به شما حمله شده است.

به گفته "آرون سود" نایب رئیس مرکز بین المللی سایبری در دانشگاه "جورج میسون" اگر یک هواپیما را ببینید می دانید که به نیروی هوایی کشوری تعلق دارد، اما اگر به شما حمله سایبری شود حتی نمی توانید بفهمید از کجا به شما حمله شده است.
متخصصان امور امنیت رایانه ای در جهان با بررسی پنج نمونه از بزرگترین و جدیدترین حملات سایبری در کشورهای مختلف، کرم استاکس نت را که به شکلی گسترده قصد تحت تاثیر قرار دادن ایران را داشت یکی از پیچیده ترین حملات سایبری جهان می دانند.

به گزارش خبرگزاری مهر، ما در جهان سایبری زندگی می کنیم، از بانکداری گرفته تا ارتباطات و یا خرید، تقریبا تمامی فعالیتهای روزانه بشر به سوی اینترنت گرایش یافته است، متاسفانه هرچه بشر بیشتر بر تکنولوژی تکیه می کند بیشتر در معرض خطر حملات سایبری قرار می گیرد.

شاید بزرگترین نگرانی درباره آنچه افراد مختلف آن را "پنجمین میدان جنگ" می خوانند (چهار میدان دیگر زمین، دریا، هوا و فضا هستند) نامرئی بودن آن است. به دلیل اینکه حملات سایبری از طریق شبکه های پیچیده رایانه ای و معمولا از جانب منابع درجه دو یا سه انجام می گیرند، تعیین منشا اصلی برخی از این حملات تقریبا غیر ممکن است.

به گفته "آرون سود" نایب رئیس مرکز بین المللی سایبری در دانشگاه "جورج میسون" اگر یک هواپیما را ببینید می دانید که به نیروی هوایی کشوری تعلق دارد، اما اگر به شما حمله سایبری شود حتی نمی توانید بفهمید از کجا به شما حمله شده است.

حملات سایبری دامنه متنوعی دارند، از شوخی های معمولی گرفته تا کرمهای مخرب رایانه ای که به واسطه حافظه های قابل حمل جا به جا شده و امنیت کلی کشوری را به خطر می اندازند. از آنجایی که امروزه تمامی زندگی ما به تکنولوژی، رایانه ها و اینترنت گره خورده است اطمینان از ایمن بودن این ابزارها بسیار حیاتی است.

متخصصان با بررسی حملات سایبری پیشین به بررسی سازه هایی پرداخته اند که بیشترین آسیب پذیری را در برابر حمله های تبهکارانه سایبری داشته اند تا راه حلی مناسب به دست آورند. در ادامه پنج نمونه خبرساز از حملات سایبری را که در میدان جنگ پنجم رخ داده اند و برخی راهکارها برای مقابله با چنین نمونه هایی را مشاهده می کنید:

کرم استاکس نت - 2010

به گزارش مهر، این کرم در سال جاری کشف شد و متخصصان این کرم را به عنوان یکی از پیچیده ترین کرمهای رایانه ای که تا به حال مشاهده شده می شناسند. این کرم به سیستمهای رایانه ای صنعتی که سیستمهای ماشینی نیروگاه ها و کارخانه ها را تحت کنترل دارند، حمله می کند. این کرم با بهره برداری از چهار نقطه ضعف که پیش از این در سیستم عامل ویندوز ناشناخته باقی مانده بودند، فعالیت می کند. برای مثال یکی از آسیب پذیری های ویندوز به استاکس نت کمک می کند در میان شبکه های محلی گسترش پیدا کند، دیگری به پخش شدن کرم در میان سخت افزارهای قابل جا به جایی از قبیل حافظه های USB و یا درایورهای CD کمک می کند.

به گفته متخصصان قابلیتهای این کرم در استفاده از بیش از یک نقطه ضعف سیستم عامل رایانه ها کاملا بی سابقه است و نشان از حمایت دولتی و پشتیبانی مالی شدید از این کرم رایانه ای دارد. با وجود اینکه هنوز تعیین قطعی هدف اصلی استاکس نت امکان پذیر نیست اما حملات این کرم به شکلی مشخص و نامتناسب به سوی ایران متمرکز بوده است. هر چند که این عملیات ناموفق بود.

عملیات آئورا - 2009

در سال گذشته میلادی، گوگل، آدوبی و در حدود 30 شرکت دیگر اعلام کردند قربانی حملات به شدت پیچیده سایبری شده اند. هکرها طی این حملات توانسته بودند با بهره برداری از نقطه ضعفی شناخته نشده در مرورگر اینترنت اکسپلورر، به اطلاعات حیاتی و خصوصی این شرکتها دست پیدا کنند. نام این حمله سایبری توسط نایب رئیس شرکت مک کافی، "دیمیتری آلپروویچ" انتخاب شده

است که با ردیابی فایلهای آلوده موفق به کشف واژه "آئورا" به معنی سپیده دم در میان فایلها شد. این بار هم با وجود اینکه امکان اطمینان یافتن وجود نداشت، باز همه نگاه ها متوجه چین شد و انتشار اسنادی درباره ارتباط دولت چین با این حمله سایبری توسط وب سایت جنجالی ویکی لیکز، فرضیه مقصر بودن چین در این حملات گسترده سایبری را تقویت کرد.

به گفته آلپروویچ این حمله مدل ذهنی که "در برابر چه کسی باید از خود محافظت کنیم" و "محرک هکرها چه می تواند باشد" را تغییر داد. نکته کلیدی دیگر نیاز به افزایش احتیاط در میان کارمندان شرکتهای چند ملیتی است تا در هنگام استفاده از رایانه های شرکت دقت کافی را به خرج دهند زیرا در شرکت گوگل یک کلیک کوچک و نا آگاهانه بر روی یک پیغام کوتاه منجر به بروز تمامی این مشکلات شد.

فرماندهی مرکزی ایالات متحده آمریکا - 2008

به گزارش مهر، برخی از سازمانها به ویژه سازمانهای دولتی رایانه های خود را از دسترس عموم و یا عضویت در شبکه های غیر ایمن خارج می کنند تا از بروز شکافهای امنیتی در آن جلوگیری کنند. در زبان رایانه ای این شکاف به شکاف هوایی شهرت دارد با این همه با ظهور رسانه های قابل حملی مانند حافظه های USB و یا CD ها تبهکاران سایبری فرصتی مناسب را برای نفوذ به درون شبکه های بسیار ایمن به دست آوردند. در سال 2008 وزارت دفاع آمریکا با چنین حملاتی مواجه شد که منبع اصلی آن یک حافظه USB غیر ایمن بود که به یک لپ تاپ وصل شده بود. این حافظه حاوی کدهای مخربی بود که در سرتاسر رایانه های وزارت دفاع آمریکا پخش شد و اطلاعات موجود در این رایانه ها را به سرورهای خارجی ارسال کرد.

از دیگر حملات سایبری ارتشی ناشی از حافظه های قابل حمل می توان به استاکس نت که به آن اشاره شد و کپی شدن فایلهای فوق سری ارتشی توسط سرباز "بردلی مانینگ" بر روی CD یکی از خواننده ها پاپ اشاره کرد که این اسناد و فایلها که حاوی تصاویر ویدیویی حمله آمریکایی ها به غیر نظامیان و 250 هزار مکالمه دیپلماتیک بود در نهایت توسط وب سایت ویکی لیکز منتشر شد. نکته قابل توجه در این حمله سایبری توجه به این نکته است که اگر افراد نسبت به آنچه در رایانه های خود ذخیره می کنند، دقت کافی به خرج ندهند، رعایت ایمنی برای پرهیز از شکاف هوایی ارزشی نخواهد داشت.

گرجستان - 2008

در سال 2008 و درست یک هفته پس از یورش روسیه به گرجستان، حمله ای سایبری دولت و وب سایتهای رسانه ای این کشور را دچار اختلال کرد. همانطور که در سال 2007 نیز جو سیاسی اقتضا می کرد کرملین دستور یک حمله سایبری را به استونی صادر کند. با این تفاوت که افرادی که به گرجستان حمله کردند سیستمهای رایانه ای سازمانی این کشور را نیز بی نصیب نگذاشتند. این حمله به "باتنت" شهرت داشته و به گونه ای است که هر شهروند روسی می توانسته است آگاهانه یا نا آگاهانه و با دانلود نرم افزاری سبک به ایجاد اضافه بار بر روی وب سایتهای دولتی و سازمانی گرجستان کمک کرده باشد.

استونی - 2007

به گزارش مهر، در این سال کشور استونی در معرض سیلی از حملات سایبری قرار گرفت که کل زیرساختارهای اینترنتی کشور را تحت تاثیر خود قرار دادند و البته هدف اصلی وب سایتهای دولتی و سازمانی، بانکها و روزنامه ها بودند. با توجه به زمانبندی حملات که در زمان مجادله این کشور و روسیه بر سر برداشتن یادبود شوروی از پایتخت استونی بود، مقامات استونی روسها را عامل اصلی این حملات می دانند. با این حال مثل همیشه امکان ردیابی منشا اصلی این نوع از حملات وجود نداشته و نخواهد داشت.