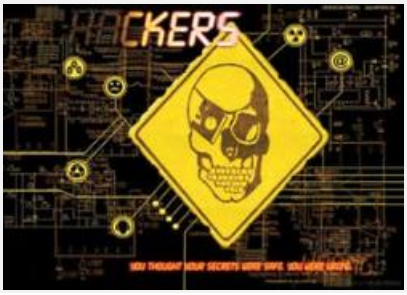

سه شنبه 25 مرداد 1390 - 09:26

دوران سرگرمي بودن هک

5 2سال پس از اینکه اولین ویروس رایانه ای ساخته شد، می گذرد، در حالی که صنعت بدافزارها روز به روز پیشرفته تر شده و در دستان گروه های تبهکاری یا دولت های قدرتمندی قرار گرفته که می توانند به راحتی از آنها در اجرای برنامه های مختلف استفاده کنند.

چرا هکرها ویروس مي سازند؟
دوران سرگرمي بودن هک
جام جم آنلاین: 25 سال پس از اینکه اولین ویروس رایانه ای ساخته شد، می گذرد، در حالی که صنعت بدافزارها روز به روز پیشرفته تر شده و در دستان گروه های تبهکاری یا دولت های قدرتمندی قرار گرفته که می توانند به راحتی از آنها در اجرای برنامه های مختلف استفاده کنند.
به گزارش مهر، چرا هکرها رایانه ها را هک می کنند؟ چرا کرم هایی را خلق می کنند که از طریق ایمیل تمامی دوستان و افراد لیست آدرس های یک کاربر را آلوده می کنند؟ چرا تروجان‌هایی را می سازند که تمامی اطلاعات را پاک می کنند؟ به خاطر شرارت؟ پول؟ یا دلیلی کاملا متفاوت؟

این سوالاتی است که «میکو هیپونن» یکی از متخصصان افسانه ای امنیتی رایانه ها که برای 25 سال به شکار ویروس ها پرداخته به آنها پاسخ داده است. وی یکی از متخصصان ارشد شرکت F-Secure در فنلاند است. وی تا کنون توانسته تعدادی از مخرب ترین و مخفیانه ترین ویروس های جهان را شناسایی و شکار کند، ویروس هایی از قبیل Sasser، Sobig.F و کرم .Storm «هیپونن» به عنوان یکی از 50 فرد مهم در صنعت وب نیز شناخته می شود.

به گفته وی، اولین ویروس رایانه ای به نام Brain.a در سال 1986 توسط دو برادر پاکستانی وارد رایانه ها شد. این ویروس بخش مرتبط با بالا آمدن سیستم عامل رایانه های تحت DOS را تحت تاثیر خود قرار می داد. این دو برادر ادعا کردند ویروس را به منظور جلوگیری از تخلف نرم افزاری کاربران ساخته اند اما این ویروس به سرعت در سرتاسر جهان گسترده شد و عصر جدید بدافزاری را در صنعت رایانه آغاز کرد.

دوران سرگرمی بودن هک

«هیپونن» زمانی که پی برد این ویروس در آستانه 25 سالگی خود قرار دارد برای نمایش دادن این روز خاص تصمیم گرفت به آدرسی برود که برادران پاکستانی آن را در کد ویروس خود نوشته بودند.

وی در نهایت تعجب مشاهده کرد این دو برادر در همان آدرس اقامت دارند و در پاسخ به سوال «هیپونن» اعلام کردند هدف آنها از ساخت این ویروس اثبات آسیب پذیری سیستم عامل IBM و بالاتر بودن ایمنی سیستم عامل ویندوز بوده است.

از نظر این دو برادر سیستم عامل DOS بسیار ضعیف و قابل نفوذ بود از این رو این دو تلاش کردند تا کدی از این سیستم عامل را به سیستمی دیگر انتقال دهند تا ضعف آن را به نمایش بگذارند. این ویروس کاملا موفق عمل کرد و در پی این دو برادر، افراد دیگری انواع متفاوتی از این ویروس را ساختند که قادر به وارد آوردن آسیب های جدی به رایانه ها نبودند.

پس از آن ایمیل وارد صنعت ارتباطات شد با ورود ایمیل هکرهایی که تا کنون به این پدیده به چشم سرگرمی نگاه می کردند، دریافتند می توانند از این کار درآمدزایی داشته باشند.

دوران تبهکاری هکرها

با آغاز قرن جدید هرزنامه ها به یکی از بزرگترین تجارت ها تبدیل شده بودند اما برای ارسال تعداد زیادی هرزنامه به تعداد زیادی رایانه نیاز خواهد بود و برای اینکه هکر قابل شناسایی نباشد نباید این رایانه ها متعلق به وی باشند، دراین شرایط بود که عبارت «باتنت» مفهوم پیدا کرد.

ویروس ها به هکرها امکان می دادند تا کنترل رایانه کاربران را از راه دور به دست بگیرند، هکرها از رایانه های آلوده برای به دام انداختن دیگر رایانه ها استفاده می کردند و با شیوه های مختلف به حساب های بانکی و اطلاعات مالی کاربران دسترسی پیدا می کردند. در سال 2005 مفهوم بدافزار نویسی به کلی متحول شد زیرا از مرحله اثبات کاربردی بودن به مرحله درآمدزایی رسیده بود.

دلیل دیگری نیز برای اوج گرفتن بدافزار نویس ها وجود دارد: سیستم عامل ویندوز XP، سیستم عاملی قدیمی که هنوز به شکلی باورنکردنی مورد استفاده کاربران جهان قرار دارد، این سیستم عامل بر روی بیش از 50 درصد از رایانه های متصل به اینترنت وصل شد در حالی که بسیار غیر ایمن است.

«هیپونن» می گوید ویندوز XP یکی از غیر ایمن ترین سیستم های عامل در جهان است در حالی که بیشتر رایانه ها در جهان از این سیستم عامل استفاده می کنند.

به گفته وی، امروزه 99 درصد از منابع بدافزارها گروه های تبهکاری هستند که در گذشته هیچ نگرانی درباره آنها وجود نداشت اما اکنون گروه های سازماندهی شده تبهکاری وجود دارند که زمانی که متخصصان عملیات آنها را متوقف می کنند، این گروه ها به خوبی هویت متخصصان را شناسایی می کنند، این به آن معنی است که متخصصان امنیت شبکه همواره در خطر قرار دارند.

این یک خطر فرضی نیست، اوایل سال جاری پسر «اوگن کسپراسکای» فردی که مالک برترین لابراتوار آنتی ویروس در جهان است در خیابانهای مسکو ربوده شد که هنوز دلیل این آدم ربایی مشخص نشده است، آنچه که آشکار است امروز متخصصان امنیت شبکه در جایی میان گروه های مافیایی و مقادیر زیادی پول ایستاده اند، جایی که به هیچ وجه برای ایستادن امن نیست. البته این پایان کار نیست، اکنون منبعی جدید، مرگبارتر و قدرتمند تر برای ویروس ها شماسایی شده اند: دولت ها!

دولت ها هم هکر شده اند

هیپونن یک نسخه از ویروس استاکس نت را همواره به همراه دارد، پیچیده ترین ویروسی که تاکنون در جهان مشاهده شده با قابلیت آلوده سازی محیط های ویژه برنامه ریزی شده مجهز به کنترل کننده های منطقی قابل برنامه ریزی مشخص، تنظیمات مشخص، و موقعیت مشخص که در نهایت آشکار شد این موقعیت یکی از نیروگاه های اتمی در ایران است.

این ویروس در زمان فعال بودن می تواند چندین روز از فعالیت یک نیروگاه را ذخیره کند و سپس اطلاعات ذخیره شده را بر روی نمایشگرها پخش کند و از سویی دیگر منجر به تخریب ساختارهای حیاتی نیروگاه شود.

«هیپونن»، دولت آمریکا را عامل اصلی ساخت این ویروس مخرب می داند، در حالی که هیچ اثباتی برای حرفش ندارد. این ویروس بر خلاف دیگر ویروس ها در اینترنت منتشر نشد بلکه با استفاده از USB از رایانه ای به رایانه ای دیگر منتقل شد. با این همه هنوز مشخص نیست این ویروس چگونه به ایران رسیده است.

استاکس نت ویروسی است که آغاز گر دورانی جدید از زندگی بدافزارها است. امروزه حمله ویروس های پیچیده به اندازه ای دقیق و حساب شده هستند که می توانند تنها یک دستگاه و یا یک فرد را مورد هجوم قرار دهند و دولت ها، سازمان ها و گروه های تندرو هم اکنون درگیر این پدیده هستند.