ویروس ها

در ماجرای ساسر، این نخستین بار بود که یک شرکت رایانه ای

درحد و اندازه مایکروسافت برای به دام انداختن یک ویروس

نویس وارد عمل می شد.

به نظر می رسید آنچه شرکت مایکروسافت را وادار به حضور در

عرصه های امنیت رایانه ای در مقابله با خرابکاران رایانه ای کرد،

ضربه های متعددی بود که خصوصا طی چند ماه اخیر بر سیستم

عامل های این شرکت وارد آمده است.

شاید به همین علت است که آنها با تعیین میلیون دلار جایزه عملا

به تیم های تحقیقاتی سیا و اف.بی.آی پیوستند و نتایج فعالیت آنها

به دستگیری نویسنده ویروس ساسر انجامید.

نوجوان ساله آلمانی پیش از آن که ماموران پلیس بخش هانوفر

را جلوی در منزل خود ببیند، هیچ گاه تصور نمی کرد کرم رایانه

ای که او آن را منتشر کرده و طی مدت کوتاهی میلیون ها رایانه

در سرتاسر جهان را آلوده کرده، بتواند به این سادگی صاحب

خود را گرفتار پلیس کند.

هرچند این کرم کوچک رایانه ای در ابتدای شناسایی خود از طرف

شرکتهای ضدویروس کم خطراعلام شد، اما کمی بعد با گسترشی

شتاب گونه، ناگهان در سرتاسر جهان پخش شد و درنقاطی هم

بعضی فعالیت های حیاتی را متوقف ساخت.

هرچند مقامات شرکت مایکروسافت ازاین ابتکار خود در قرار

دادن جایزه که منجر به دستگیری این پسرک آلمانی شد راضی به

نظر می رسند، اما خود آنها هم می دانند ویروس نویسان همواره

چند پله جلوتر ازشرکت های رایانه ای بوده اند.

بنابر گزارش خبرگزاری ها آنچه منجر به دستگیری این پسر

آلمانی شد، اطلاعاتی بود که توسط همشهری این ویروس نویس ،

به مایکروسافت و مقامات پلیس ارائه شده بود. شیوه ای که

مایکروسافت در برخورد با این کرم در پیش گرفت ، به گونه ای

مقابل قرار دادن متخصصان امنیتی با حتی ویروس نویسان با هم

است.

به این ترتیب وظیفه پیداکردن یک خرابکار صرفا به دانش چند

متخصص امنیت شبکه در یک کشور خاص محدود نمی شود،

کسب ۵ میلیون دلار آنقدر وسوسه انگیز است که یک آلمانی

نویسنده ویروس ساسر را به امریکایی ها معرفی کند.

چرخه ویروس های رایانه ای طی چند سال اخیر نشان می دهد

همگام با پیشرفت راههای امنیتی مبارزه با حملات اینترنتی این نرم

افزارهای کوچک موذی نیز خود را با محیط تطبیق داده و به

اصطلاح هوشمندتر و مخرب تر شده اند. مثلا کرم **Code Red**

که درسال مطرح شد، قادر به تکثیر خود به میزان ۲۵۰هزارمرتبه

درمدت زمان ۹ ساعت است.

همچنین ر زمان تکثیر به میزان قابل ملاحظه **Code Red**کرم

ای سرعت ترافیک اطلاعاتی روی اینترنت را کند می کرد. هر

نسخه از کرم فوق پیمایش اینترنت به منظور پیداکردن سرویس

یا را آغاز می کرد و هر زمان که یک **NT**دهندگان ویندوز

سرویس دهنده نا امن (سرویس دهنده ای که روی آن آخرین

نرم افزارهای امنیتی مایکروسافت نصب نشده بود) پیدا می شد،

کرم نسخه ای از خود را روی سرویس دهنده تکثیر می کرد و

نسخه جدید هم در ادامه عملیات پیمایش برای پیداکردن

سایرسرویس دهندگان کار خود را آغاز می کرد.

با توجه به تعداد سرویس دهندگان نا امن، یک کرم قادر به ایجاد

صدها و هزاران نسخه از خود است.

ایجادکنندگان ویروس های رایانه ای افرادی آگاه و باتجربه بوده

و همواره از آخرین حقه های موجود استفاده می کنند.

یکی از این حقه ای مهم در خصوص قابلیت استقرار در حافظه و

استمرار وضعیت اجرای خود در حاشیه است (البته تا زمانی که

سیستم روشن باشد) ، به این ترتیب امکان تکثیر این نوع ویروس

ها با شرایط مطلوب تری فراهم می شود.

یکی دیگر از حقه های موجود قابلیت آلوده کردن بوت سکتور

فلاپی دیسک ها و هارددیسک هاست. بوت سکتورشامل یک برنامه

کوچک به منظور استقرار بخش اولیه یک سیستم عامل در حافظه

است.

بااستقرار ویروس های رایانه ای در بوت سکتور اجرا شدن آن

تضمین خواهد شد. به این ترتیب یک ویروس بلافاصله در حافظه

مستقر و تا زمانی که سیستم روشن باشد، به حضور مخرب

خوددر حافظه ادامه خواهند داد.

ویروس های بوت سکتور قادر به آلوده کردن سایربوت

سکتورهای فلاپی دیسک های سالمی که در درایو ماشین قرار

خواهند گرفت هم هستند، در مکان هایی که رایانه به صورت

مشترک بین افراد استفاده می شود، بهترین شرایط برای تکثیر

ویروس های رایانه ای به وجود خواهد آمد ویروس سوبیگ هم

که چندماه پیش در اینترنت منتشر شد، فشار شدیدی به شبکه

اینترنت و سیستم های شرکتهای تجاری وارد آورد و بسیاری از

آنها را دچار کندی کرد.

این ویروس برای آن که توسطکاربران شناسایی نشود، مرتبا

موضوع پیغام های آلوده خود را تغییر می داد به این ترتیب

کاربران کم تجربه از ریسک بیشتری برای گشودن نامه های

آلوده به این ویروس برخوردار می شدند.

ویروسی مانند نت اسکای تغییر عنوان نامه را به اوج رساند به

نحوی که با تغییر نام و آدرس فرستنده ایمیل ، کاربران را دچار

این شک می ساخت که این نامه از طرف یک دوست برایشان

ارسال شده است.

که از ژانویه سال فعالیتخود را آغاز کرد، تنها **Mydoom**ویروس

طی ساعت میلیون ایمیل آلوده ایجاد کرد. این ویروس که از

ضعفهای سیستم عامل مایکروسافت بهره می برد، از طریق یک

فایل ضمیمه در نامه الکترونیکی منتشر می شد و به نشانی هایی

که از طریق ضعف مزبور روی یک سیستم یافته بود ایمیل آلوده

ارسال می کرد.

میزان آلودگی این ویروس به حدی بود که گفته می شدیکی از

هر ایمیل ارسالی را در بر می گرفت و در بیش از کشور جهان

مشاهده می شد.یک سال پیش ویروسی که شباهت آشکاری به

کردن رایانه ها می شد، **Reboot**ویروس ساسر داشت و باعث

تمام دنیای رایانه را به هم ریخت.

این ویروس که ام اس بلاست نام داشت ، بسرعت مشهور شد.

چرا که با دستور ساده خود مبنی بر راه اندازی مجدد ویندوز

عملا جلوی استفاده از دستگاه را می گرفت. این ویروس به گونه

هوشمندانه نوشته شده بود که بعد از آلوده کردن یک دستگاه به

دنبال دستگاه متصل به آن می گشت تا آنها را نیز آلوده سازد.

گفته می شد این ویروس در اوج فعالیت خود تنها ظرف ثانیه

رایانه های سالم را پیدا می کرد و تخمین زده می شد بیش از

هزار رایانه توسط انواع مختلف این ویروس آلوده شده است.

به عنوان نمونه ویروس ولچی یاناچی که از شیوه تخریبی ام اس

بلاست بهره می برد، نمونه ای از یک ویروس نیکوکار بود.این

ویروس بعد از ورود به سیستم تلاش می کرد بسته تازه نرم

افزارهای مایکروسافت راروی سیستم نصب کند و اگر کرم بلاستر

را روی سیستم می یافت ، آن را حذف می کرد. مشاور ارشد یک

شرکت ضدویروس نویسنده این ویروس نیکو کار را رابین هود

عالم اینترنت نامید که می خواهد ویروس پلید ام اس بلاست را

نابود کند.

به نظر می رسد ویروس های رایانه ای ماهیت دوگانه ای دارند،

آنها از یک سو تخریب می کنند و خسارت به بارمی آورند و از

سوی دیگر نتایج کار آنها جلوی تخریب های بیشتر و خسارت

سنگین تر رامی گیرد.

با چنین رویکردی آیا می توان آنها را به طور مطلق مفید یا مضر

خواند؟!