دانشکده مهندسی کامپیوتر

استاد درس: دکتر دیانت

بهار ۱۴۰۳

پروژه سزیم
امنیت سیستم های کامپیوتری

ستاره باباجانی - ملیکا محمدی فخار
۹۹۵۲۱۱۰۹ - ۹۹۵۲۲۰۸۶

---

۱ ویروس ملیسا

همزمان با رشد حجم داده ها و اهمیت تجاری آنها، استفاده از خدمات ابری برای مدیریتاین ویروس یکی از مخرب ترین ویروسهای کامپیوتری زمان خود به حساب می آید. و در طول بهار ۱۹۹۹ توسط شخصی با نام دیوید اسمیت از نیوجرسی نوشته شد. ویروس ملیسا به گونه ای طراحی شده بود تا بتواند از طریق پیامهای ایمیل از یک کامپیوتر به کامپیوتر دیگر منتشر شود. این ویروس نخستین بار در ۲۶ مارچ ۱۹۹۹ به وسیله برخی نرم افزارهای آنتی ویروس و شرکت های امنیت اینترنت شناسایی شد. ویروس ملیسا با سرعت بسیار بالا از طریق اینترنت منتشر و دردسرهای زیادی را برای بخش خصوصی و شبکه های دولتی به وجود آورد و بسیاری از سرویس های اینترنتی را مختل ساخت و شرکت ها را مجبور به متوقف ساختن موقت سرویس های ایمیل خود نمود. این ویروس توجه بسیاری را به خود جلب کرد که در نهایت به عنوان سریع ترین ویروس منتشر شده زمان خود شناخته شد.

۲ نحوه عملکرد ویروس ملیسا

ویروس ملیسا یک ویروس مبتنی بر مایکروسافت Word ۹۷ بود که با انتشار از طریق پیام های ایمیل عمل می کرد. این ویروس در صندوق پیام های دریافتی ظاهر می شد و به عنوان یک پیام مهم از فردی شناخته شده برای صاحب ایمیل، با یک فایل ورد ضمیمه خود را نشان می داد. این پیام با عنوانی همچون «فایل یا سندی که درخواست داده بودید. آن را به شخص دیگری نشان ندهید» فرد را وسوسه کرده تا فایل ضمیمه را باز کند، با این حال، به محض کلیک کردن بر روی فایل یا سند و فعال کردن آن، ویروس ملیسا خود را در اسناد دیگر ورد تکثیر یا تکرار کرده و همچنین خود را به عنوان یک ایمیل اسپم به ۵۰ آدرس ذخیره شده در اکانت ایمیل فرد گیرنده ارسال می کرد. این امر اغلب منجر به فاش شدن اطلاعات خصوصی و محرمانه موجود در اسناد ورد از طریق ایمیل می شد. به این دلیل که ملیسا جهت فعال شدن نیاز به تعامل با کاربر داشت به عنوان یک کرم اینترنتی در نظر گرفته نمی شد.

۳ علائم هشدار دهنده

تشخیص این ویروس سخت بوده و به راحتی برای کاربران کامپیوتر آشکار نمی شد و جهت شناسایی آن اغلب نیاز به افراد متخصص می بود. نحوه تشخیص آن از طریق برخی علائم مانند سیستم های از کار افتاده و معیوب شده ایمیل بود، بدین ترتیب که این سیستم ها اطلاعات خصوصی و محرمانه را از یک کامپیوتر آلوده ارسال می کردند. با این حال، پیشگیری بهترین راه متوقف ساختن این ویروس به حساب می آمد و تنها کافی بود که موضوع و نام فایل را شناسایی کرده سپس آن را به عنوان یک ایمیل اسپم نشاندار ساخته و بدین ترتیب کامپیوتر از خطر ابتلاء به ویروس حفظ می شد. یکی از تست های متداول بررسی ویروس به قصد اجرای فایل مشکوک زمانی بود که دقایق ساعت با روز آن ماه هماهنگ می بود.

در صورت انجام این کار، ویروس متنی را در فایل ورد باز شده، به این مضمون وارد می نمود: «بیست و دو امتیاز، به علاوه پنجاه امتیاز به خاطر استفاده از تمام حروف من. بازی تمام شد».

۴ خسارت وارد شده

گرچه ویروس ملیسا موجب از کار افتادن یا پاک شدن هیچ فایلی نمی شد، اما یک نقض جدی امنیتی به حساب می آمد که اثرات مخرب بسیاری از جمله بارگذاری اضافی سرورهای ایمیل برجای می گذاشت که باعث شد شرکت هایی مانند مایکروسافت و اینتل برخی از سرویس های خود را به طور موقت تعطیل سازند. این ویروس صدها هزار کامپیوتر را تحت تأثیر خود قرار داد. این کامپیوترها عموماً آنهایی را شامل می شدند که برنامه های WORD MS و OUTLOOK را بر روی ویندوز ۹۵، ۹۸ و NT و سیستم عامل های مکینتاش نصب کرده بودند. این امر موجب بروز هرج و مرج در اینترنت شد بطوری که که سازمان های تحقیقاتی نظیر اف بی آی، پلیس ایالت نیوجرسی و برخی خدمات رسانهای اینترنت جهت یافتن مجرم دست به کار شدند. این حملات همچنین منجر به وارد آمدن خساراتی معادل ۲.۱ میلیارد دلار و اختلال در ارتباطات چندین شرکت خصوصی شد. گرچه این ویروس اینترنت را به طور کامل مختل نمی ساخت اما نخستین ویروسی بود که پوشش خبری و رسانه ای گسترده ای به خود اختصاص داده و توجه عموم را به خود جلب نمود.

۵ نحوه متوقف ساختن این ویروس

نویسنده این ویروس فایل آلوده را بر روی برخی گروه های خبری معروف به عنوان فهرستی از پسوردهای وب سایتهای مختلف قرار می داد. ردیابی این پست برای بازرسان از طریق آدرس ایمیل و آدرس آی پی کامپیوتری که از آن فرستاده شده بود کار ساده ای بود. آنها از این اطلاعات جهت یافتن محل اختفاء و دستگیری دیوید اسمیت استفاده نمودند. به محض آنکه اسمیت دستگیر و متهم به ارتکاب جرم شد، محاکمه طولانی و گسترده ای از او به عمل آمد. با این حال، اسمیت مجرم شناخته شده و پس از اقرار به ساخت و نحوه ایجاد ویروس ملیسا به ۱۰ سال زندان محکوم شد که تنها ۲۰ ماه از آن را در زندان گذراند و علاوه بر آن ملزم به پرداخت مبلغ ۵۰۰۰ دلار جریمه شد. او همچنین از دسترسی به شبکه های کامپیوتری بدون اجازه از دادگاه منع شد. علی رغم آنکه نویسنده و طراح این ویروس به دام افتاد، اما این ویروس ماه های زیادی به کار خود ادامه داده تا اینکه تولید کنندگان نرم افزار در نهایت موفق به ساخت نرم افزارهایی جهت توقف تقریباً کامل رشد و توسعه این ویروس شدند. امروزه موارد بسیار نادری وجود دارد که در آنها فایل های آلوده به ویروس ملیسا از طریق ایمیل دیده می شود. هرچند طراح ویروس ملیسا آن را به دلیل منافع مالی ایجاد ننمود و برخلاف اکثر ویروس هایی که امروزه وجود دارند، تنها به قصد شیطنت دست به این کار زد. اما این روزها دلیل طراحی ویروسها کلاه برداری و بدست آوردن پول

های هنگفتی است. اما کاربران می توانند با به روز کردن مداوم نرم افزار آنتی ویروس خود و رعایت احتیاط به هنگام گشت و گذار در اینترنت از ویروسی شدن سیستم خود جلوگیری نمایند.