شنبه 15 فروردین 1388 - 07:09

انگشت هکرها هنوز بر روی ماشه است

چهارشنبه 12 فروردین روز دشواری برای متخصصان امنیت سایبر در سراسر جهان بود.

پیش‌بینی‌ها و اطلاعات تیم‌های امنیت سایبر نشان می‌داد که کرم کانفیکر که بیش از 15 میلیون کامپیوتر را آلوده ساخته است، در این روز آماده تغییر استراتژی و احتمالاً فعال‌سازی یک حمله گسترده می‌شود.

روز اول آوریل هم بدون هیچ حمله‌ای سپری شد و از هیچ‌کدام از کامپیوترهای آلوده (که بیشتر آن‌ها در قاره آسیا هستند) فعالیت غیرمتعارفی گزارش نشد.

البته هنوز خطر فعالیت کانفیکر از بین نرفته است و با توجه به ماهیت کرم‌هایی از این قبیل که اکثراً برای مقاصد کلاهبرداری و درآمدزایی طراحی می‌شوند، باید از وجود چنین عامل مخربی احساس خطر کرد.

ماشه‌های تاریخی!

بد نیست در اینجا یادی از کرم‌ها و ویروس‌هایی کنیم که دارای روز فعال‌سازی (Trigger/ ماشه) بودند و در تاریخ امنیت سایبر نام خود را ثبت کردند.

این کرم‌ها معمولاً در دهه 90 میلادی بیشترین توجهات را به سوی خود جلب کردند و هکرها از آن‌ها برای یادآوری وقایع تاریخی و یا منافع سودجویانه خود بهره می‌بردند.

• میکل‌آنژ (Michelangelo)

این ویروس که در سال 1991 شناسایی شد، روز ششم مارچ هر سال بار حمله‌ای مخرب (Malicious) بر روی سیستم عامل DOS اجرا می‌کرد. در سال 1997 مایکروسافت راه‌حلی برای جلوگیری از حملات این ویروس یافت و Michelangelo خنثی شد.

• چرنوبیل (CIH)

ویروس چرنوبیل تاریخچه جالبی دارد. روز تولد طراح تایوانی این ویروس 26 آوریل، مصادف با حادثه نشت نیروگاه اتمی چرنوبیل اوکراین است. به همین دلیل از این روز به عنوان تاریخ فعال‌سازی CIH استفاده شد تا بخش‌هایی از هارددیسک و BIOS کامپیوترهای آلوده را پاک کند.

• کلز (Klez)

در ماه فوریه سال 2002 میلادی از طریق ایمیل منتشر شد و از رخنه امنیتی سرویس Outlook مایکروسفات برای نفوذ به دفترچه آدرس کاربران و ارسال مجدد به کامپیوترهای دیگر استفاده کرد. Klez در روز ششم ماه‌های فرد سال میلادی فایل‌های ویندوز کامپیوترهای آلوده را پاک می‌کرد. شرکت‌های امنیت سایبر یک ماه بعد از نشر این ویروس، شناسه (Signature) آن را منتشر ساختند.

• بلستر (Blaster)

Blaster یا MS-Blast 11 آگوست 2003 منتشر شد و حدود سه هفته بعد مایکروسافت خبر از یک رخنه امنیتی در سیستم عامل ویندوز داد. Blaster برای سوءاستفاده از این رخنه برای کشیدن ماشه یک حمله(DoS (Denial Of Service به سرور به‌روزسانی ویندوز در 15 آگوست 2003 طراحی شده‌بود. در بخشی از کد این ویروس که بعدها کشف شد، خطاب به بیل گیتس گفته شده‌بود: "پول درآوردن را رها، و مشکلات نرم‌افزارت را برطرف کن! ". مایکروسافت برای جلوگیری از این حمله سرور وب به زوررسانی خود را از بین برد.

• مای‌دوم (MyDoom)

مای‌دوم در ژانویه سال 2004 کشف شد و برای فعال‌سازی حمله DoS به وب‌سایت شرکت SCO (سازنده سیستم UnixWare) بین روزهای اول و دوازدهم فوریه 2004 طراحی شده‌بود. SCO هم وب‌سایت خود را جابجا کرد تا از دست مای‌دوم در امان باشد. نوع دیگری از مای‌دوم حمله موفق(DDoS (Distributed Denial Of Service به وب‌سایت مایکروسافت انجام داد. گفتنی است که مایکروسافت و SCO برای کسانی که اطلاعات مفیدی در مورد طراحان مای‌دوم به این دو شرکت بدهند 250هزار دلار جایزه تعیین کردند. مایکروسافت جایزه مشابهی برای سر کانفیکر تعیین کرده‌است

• سوبر (Sober)

سوبر در نوامبر سال 2005 ظاهر شد و قرار بود روز پنجم را ششم ماه ژانویه سال 2006 که مصادف با هشتاد و هفتمین تأسیس حزب نازی است، حملاتی را انجام دهد. این ویروس توانایی دانلود کدهایی از سرور خود برای شکل دادن یک ویروس جدید را دارد. البته سوبر با شکست روبرو شد و حمله‌ای از سوی آن گزارش نشد.