

نرم افزارهای مخرب و اصول مقابله با آن ها (قسمت ۲)

اغلب کاربران، تمام نرم افزارهای مخرب را با نام ویروس می شناسند و تفاوتی میان آن ها قائل نمی شوند. در حالی که انواع مختلفی از نرم افزارهای مخرب وجود دارند، این برنامه ها توسط افراد نفوذگر و بد اندیش به منظور رسیدن به اهداف مختلفی که در اکثر موارد، مخرب است نوشته می شود.

- (موضوع بحث هفته شانزدهم شنبه های سایبری **اسب های تروا (Trojans)** بودند و این هفته در ادامه بحث به ویروس ها می پردازیم.)

نمونه های متداول از نرم افزارهای مخرب در زیر نوشته شده است:

- **ویروس ها (Viruses)**
- **کرم ها (Worms)**
- **اسب های تروا (Trojans)**
- **جاسوسی افزارها (Spyware)**

معرفی انواع نرم افزارهای مخرب

۱- ویروس ها

ویروس ها برنامه هایی هستند که به منظور تخریب و آلوده سازی تعداد زیادی کامپیوتر برای اهداف خاصی طراحی می شوند. این برنامه های هوشمند، همراه برنامه های دیگر هستند تا در زمان و شرایط مناسب، زمینه آلوده شدن سایر برنامه ها را فراهم کنند. گونه ای از ویروس ها، بدون اطلاع کاربر از راه های مختلف وارد سیستم شده و اطلاعات را از کامپیوتری به کامپیوتر دیگر منتقل می کنند.

بسیاری از آن ها با هدف تخریب انواع مشخصی از فایل ها، برنامه های کاربردی و یا سیستم عامل نوشته شده اند که از منابع سیستم مانند فضای حافظه، دیسک سخت، توان پردازنده ای مرکزی و... بهره می گیرند و می توانند اعمال خطرناکی را انجام دهند. ویروس ها به دلیل بهره گیری از منابع سیستم سعی در تکثیر و آلوده سازی، سرعت را کاهش داده و سیستم را با خطا مواجه می کنند.

راه های انتقال برنامه های مخرب

برنامه های مخرب از جمله ویروس ها از راه های مختلف خود را به سیستم رسانده، در فرصت مناسب تکثیر شده و به اعمالی که بعضا جنبه تخریبی دارد می پردازند. برای جلوگیری از ویروسی شدن یا ورود برنامه های مخرب به سیستم، بهتر است از ورود آن ها جلوگیری شود. در این قسمت به چند نمونه از راه هایی که بیشتر توسط این نرم افزارها برای تهاجم مورد استفاده قرار می گیرد، اشاره می کنیم:

۱- اینترنت : دریافت فایل های که آلوده هستند.

۲- پست الکترونیکی : باز کردن نامه های آلوده یا نامه هایی که شامل فایل های پیوندی آلوده هستند. با باز کردن این فایل ها احتمال ویروسی شدن سیستم بسیار بالا است.

۳- برنامه ها : برنامه هایی که حاوی ویروس بوده و به محض اجرا شدن، دستگاه کاملا ویروسی می شود.

۴- دیسک های نرم CD و Flash ها : دریافت اطلاعات از طریق این امکانات از سیستم های آلوده باعث آلوده سازی سیستم به هنگام اجرا می شود. قبل از استفاده باید از سلامت آن ها اطمینان داشته باشید.

اصول تشخیص ویروسی شدن سیستم

هنگام کار با کامپیوتر آلوده به ویروس، کاربر با مشکلاتی مواجه خواهد شد. از جمله مواردی که بیشتر قابل توجه هستند می توان به کاهش حافظه، کاهش سرعت، باز نشدن و مخفی شدن فایل های موجود و صدور پیغام خطا اشاره کرد.

کاهش حافظه : چنانچه فضای آزاد در حافظه سیستم به طور غیر منتظره کاهش یابد، وجود ویروس را در سیستم گزارش می دهد.

کاهش سرعت در انجام کار : در این حالت سرعت اجرای برنامه ها کاهش یافته و فرامین به کندی انجام می شود، اگر از سلامت سیستم از نظر سخت افزاری اطمینان دارید این نشانه، وجود ویروس را تایید می کند.

باز نشدن یا مخفی شدن فایل ها : در صورت باز نشدن یک یا چندین فایل یا مخفی شدن آن ها می توان به آلوده بون سیستم پی برد.

نمایش تصادفی پیام های خطا : هنگام کار با کامپیوتر آلوده به ویروس، پیام های خطا به طور ناگهانی ظاهر می شود.

نمایش پیغام : گاهی ویروس ها اقدام به ارسال و نمایش پیام های معنی دار یا بی معنی خاصی می کنند.

Restart شدن سیستم: چنانچه سیستمی مشکل سخت افزاری خاصی ندارد و به طور ناگهانی راه اندازی مجدد شود نشانه ویروسی شدن سیستم است.

اصول مقابله با ویروسی شدن سیستم

همان طور که بیان شد، ویروس ها از راه های مختلف وارد کامپیوتر شده که در این قسمت به روش های جلوگیری از ورود نرم افزارهای مخرب می پردازیم:

نصب نرم افزار های ویروس یاب : این نرم افزار ها به منظور تشخیص ویروس ها و از بین بردن آن ها به کار می روند.

کنترل و حفاظت ورودی ها : اگر می خواهید از CD، دیسکت و ... استفاده کنید ابتدا باید از سلامت آن ها اطمینان حاصل کنید (از طریق نرم افزار های ویروس یاب).

استفاده از سیستم عامل های ایمن : از سیستم عامل ها با پوشش حفاظتی مناسب استفاده کنید. سیستم عامل Linux و Unix از جمله سیستم عامل های مناسب هستند.

حفاظت از ایمیل : از باز کردن ایمیل های مشکوک خود داری کنید.

به روز کردن نرم افزارهای ضد ویروس : تنها داشتن یک نرم افزار ویروس یاب کافی نیست. هر روزه ویروس های جدیدی عرضه می شوند که برای مقابله با آن ها لازم است که این نرم افزارها به روز شوند.

نکته پایانی

با نصب یک نرم افزار ضد ویروس مطمئن و به روز رسانی آن برای شناسایی ویروس های جدید، می توان درصد امنیت سیستم را تا حد زیادی افزایش داد.