مگیت

موضوع این هفته ی مگیت

آشنایی با بدافزارها

IT Students Scientific Chapter

@itssc itssc.ir @itssc_society

تعریف بد افزار:

بد افزار به زبان ساده به یک برنامه ی مختلف گویند که برای کاربران اینترنت و دستگاه های دیجیتال با عملکردهایی مثل سرقت اطلاعات، به اشتباه انداختن کاربر، تغییر یا حذف داده ها ،کد گذاری (data encryption)نا خواسته روی داده ها و یا مانیتور کردن فعالیت (مشاهده وضعیت یک سیستم یا اطلاعات) کاربران درون محور او طراحی شده اند و با کمک عوامل انسانی یا به صورت خودکار ، به شیوه های خاص و رسانه های چندگانه در بین رایانه ها بیشتر میشوند.

یکی از رایج ترین راه انتشار و انتقال بد افزار ها فرایند دانلود آن از اینترنت است که از نمونه های آن می توان به انتقال آن از طریق ایمیل اشاره نمود. معمولا در این روش ایمیل دریافتی با مضمونی معقول و قانونی می باشد اما زمانی که کاربر روی لینک درون ایمیل کلیک میکند تنها یک بد افزار دانلود و اجرا می شود.

در برخی موارد بد افزار ها فقط اقدام به تحویل نمی کنند بلکه میتوانند عملکرد سیستم را تحت تاثیر خود قرار دهند و بار اضافی به سیستم تحمیل کنند.

در موارد جاسوسی بد افزار ها خود را پنهان می کنند بطوریکه حتی آنتی ویروس ها نیز قادر به تشخیص آن ها نیستند. بد افزار ها اطلاعات ارزشمند و حیاتی از قربانی خود را به مبدأ ارسال می کنند.

نحوه تاثیر بد افزار ها :

نحوه تاثیر گذاری آن ها روی هر یک از سیستم عامل ها مانند اندروید ، مک، ویندوز، لینوکس ، به دلیل متمایز بودن سطح و قدرت ومکانیزم های امنیتی آن ها متفاوت است.

انتشتار آلوده سازی فایل ها وابستگی کامل به سیستم عامل دارد به عنوان مثال بد افزاری که روی سیستم فایل مکینتاش کار می کند ممکن است روی ویندوز کار نکند ،از این رو توسعه دهندگان کدهای مخرب با روش های جدید برنامه هایی تولید کرده اند که بتوانند روی چندین سیستم عامل کار کنند ؛ اما ممکن است روی تمام این سیستم عامل ها نتواند کارایی مشابهی داشته باشد.

گروه های اصلی بد افزار ها شامل:

۱- Virus (ویروس رایانه ای)
۲- Worm (کرم رایانه ای)
۳- Spywore (جاسوس افزار)
٤- Adwore (ابزار های تبلیغاتی مزاحم)
٥- Trojon (تروجان)
٦- Botnet (بات نت)
۷- Web bot (وب بات)

ویروس رایانه ای:

برنامه ای که قادر به تخریب و همانند سازی برای آلوده سازی میزبان خود است. ویروس ها به یک برنامه یا فایل و لینک اضافه می شوند.

کرم رایانه ای:

یک نوع از برنامه های مخرب هستند که خود را بطور پنهان در یک شبکه انتشار داده و منتقل می شوند.اثر گذاری کرم ها متفاوت از ویروس ها است، زیرا ویروس ها برای جابجایی خود به یک فایل کمکی نیاز دارند در حالی که کرم ها با استفاده از شبکه و یا ارسال از طریق ایمیلِ ناخواستهِ آلوده ،خود را پخش می کنند ؛ برای نمونه ای از کرم ها میتوان به confikcer که با نام Downadup نیز شناخته می شود اشاره کرد.

جاسوس افزار:

عملکرد این نرم افزار ها جمع آوری اطلاعات حساس از رایانه مانند رمز عبور، شماره های حساب، و هر اطلاعات ارزشمند دیگر است که انتشار آن ها می تواند به افراد ، شرکت ها و سازمان ها صدمات جبران ناپذیری وارد کند.

ابزار های تبلیغاتی مزاحم:

زمانی که کاربر پیام های تبلیغاتی را مشاهده می کند کدهای جاسازی شده در آن روی رایانه نصب می شوند.

این بد افزارها غالباً قصد دارند که فعالیت های کاربر را در هنگام فعالیت در اینترنت جمع آوری و برای اهداف تبلیغاتی خود و یا هدف هایی برای سوء استفاده از اطلاعات استفاده نمایند.

تروجان:

تروجان ها سعی می کنند در ابتدا اطلاعات حساسی مانند پسورد ها را به سرقت برده و فعالیت کاربر را مشاهده کنند و در مراحل بعدی حتی فایل های سیستمی رایانه را تخریب نمایند.

این دسته از بد افزار ها قادر به دستیابی اطلاعات حساس و جاسوسی از راه دور به رایانه کاربر هستند.

بات نت:

این بد افزار ها کنترل یک سیستم را از راه دور در اختیار میگیرند و از آنجا جاسوس افزار را به دیگر قربانیان ارسال می کند. بیشتر بات نت ها بصورت قربانی در اختیار هکر بوده و منتظر فرمان برای انجام اقدامات خود از سوی هکر هستند.

وب بات:

دسته ای از بات نت ها هستند که اخیراً در اینترنت بسیار رایج شده اند. هدف وب بات ها خزیدن در محتوای وب است.

با یک دید مثبت بات نت ها برای تست ارتباطات و اتصالات و ایجاد محتوای سودمند، مفید هستند. اما در دیدی دیگر وب بات ها ابزاری برای جاسوسی، انتشار بد افزار های دیگر، سرقت دارایی های معنوی، کشف نقاط آسیب پذیر سایت ها و... هستند.

چگونه با بد افزار ها مقابله کنیم؟

با رعایت نکات ایمنی مثل دانلود نکردن نرم افزارهای رایگان و یا مدت دار از سایت های نامعتبر که باعث مجهز شدن رایانه به جاسوس افزار می شود، دانلود نکردن بازی های رایگان یا صفحات تبلیغاتی در وب سایت ها که رایانه را به ابزار های تبلیغاتی مزاحم آلود می کند، به روز نگه داشتن سیستم عامل، استفاده از آنتی ویروس و یا نرم افزار های امنیتی و دیوار آتش سیستم رایانه ای آپدیت شده، همه این ها میتوانند برای مقابله با بد افزار ها مفید باشند.

دو هفته نامه انجمن علمی مهندسی کامپیوتر
زیر نظر معاونت فرهنگی دانشجویی موسسه آموزش عالی ارشاد دماوند

نویسندگان :

مهشید احمدی

محیا کریمی

تهیه کنندگان :

لیلا نوری (سردبیر نشریه)

زینب حیدری

محمدرضا سرائی

اگر میدانستید که افکارتان چقدر قدرتمند هستند، حتی برای یک لحظه ی دیگر هم منفی فکر نمی کردید ...

شماره پنجم مگیت

دی ماه ۱۳۹۸