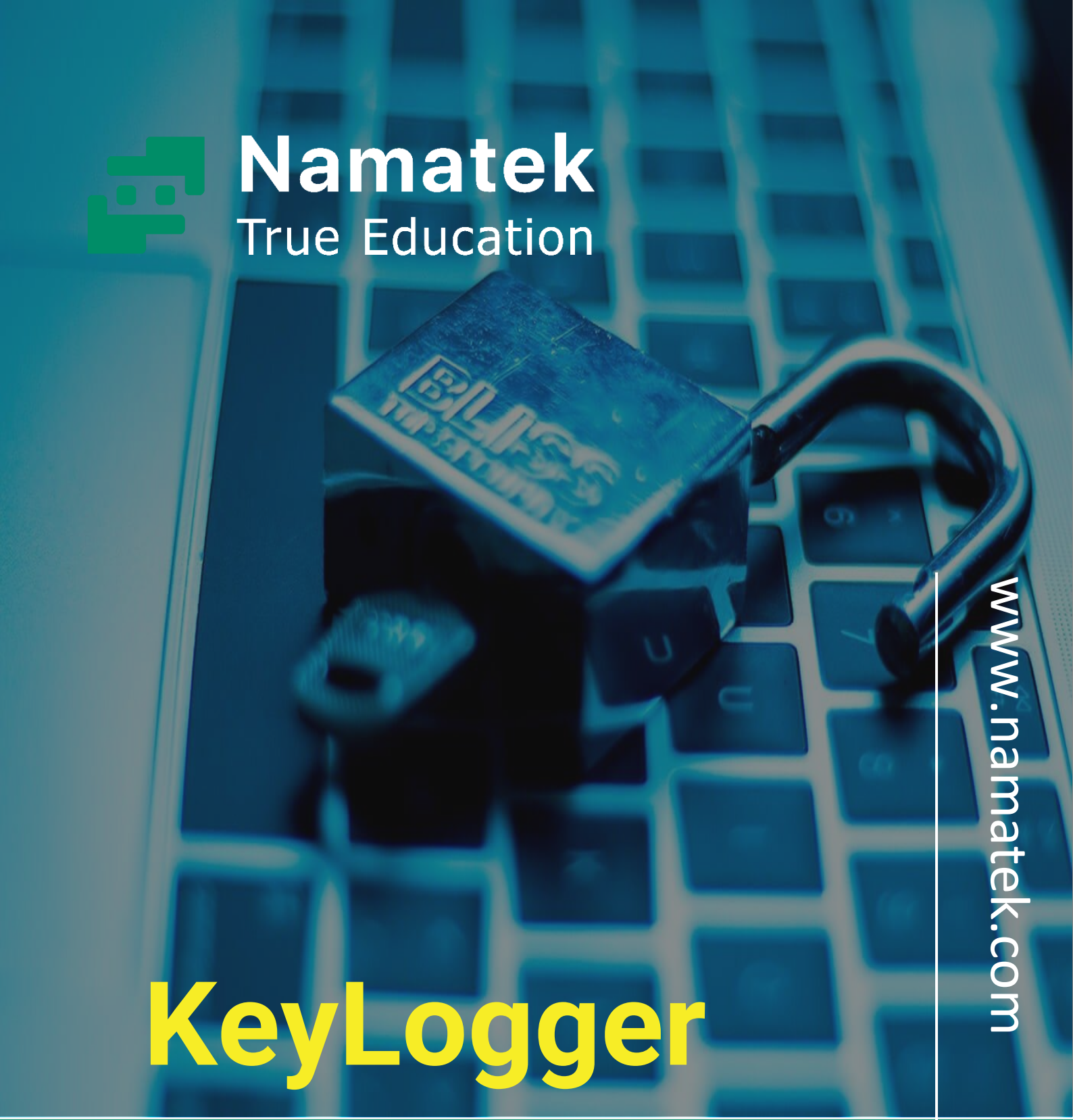


Namatek
True Education

www.namatek.com

KeyLogger

KeyLogger چیست؟

فهرست مطالب

شاید این طور به نظر برسد که برخی از تهدیدهای سایبری برای دسترسی به اطلاعات شما برگرفته از فیلم های علمی تخیلی باشند؛ اما این تهدیدها به همان اندازه واقعی هستند که رایانه های شما واقعی هستند، آیا می دانید KeyLogger چیست؟

در این مقاله به شما می گوییم که یکی از این تهدیدها استفاده از KeyLogger ها است که در آن مهاجمان از عدم آگاهی و آسیب پذیری دستگاه ها برای سرقت اطلاعات استفاده می کنند. برای دریافت اطلاعات بیشتر در این زمینه تا انتهای مقاله با ما همراه باشید.

#۱ KeyLogger چیست؟

درواقع KeyLogger به عنوان یک روش برای نظارت و ثبت مخفیانه تمام کلیدهای فشرده شده طراحی شده است. کی لاگرها مانند سایر نرم

افزارهای قانونی که به مدیران امکان می دهند آنچه کارمندان در طول روز انجام می دهند را ردیابی کنند، عمل می کنند. کاربران سیستم ها نیز می توانند با استفاده از آن فعالیت اشخاص ثالث را در رایانه های خود ردیابی کنند. به همین دلیل بیشتر KeyLogger های مدرن نرم افزاری یا سخت افزاری قانونی محسوب می شوند و در بازار آزاد فروخته می شوند.

توسعه دهندگان و فروشندگان موارد مختلفی را برای استفاده قانونی از KeyLogger ارائه می دهند؛ از جمله:

- کنترل فرزندان توسط والدین: والدین می توانند کاری را که فرزندانشان در اینترنت انجام می دهند ردیابی کنند؛ اما مزیت این روش استفاده از KeyLogger چیست؟ با استفاده از این روش درصورت تلاش فرزندان برای دسترسی به وب سایت های حاوی محتوای بزرگسالان یا مطالب نامناسب، می توان تدابیر لازم را در نظر گرفت.
- امنیت شرکت: استفاده از KeyLogger برای ردیابی ورودی کلمات و عبارات کلیدی مرتبط با اطلاعات تجاری که در صورت افشای آن می تواند به شرکت آسیب برساند.
- امنیت در حوزه های دیگر (به عنوان مثال اجرای قانون): استفاده از سوابق KeyLogger برای تجزیه و تحلیل و ردیابی حوادث مرتبط با استفاده از رایانه های شخصی می تواند بسیار کمک کننده باشد.

با این حال، توجیهات ذکر شده در بالا بیشتر ذهنی است تا عینی؛ چرا که بدون استفاده از کی لاگرها نیز می توان شرایط را حل کرد. علاوه بر این،

هر برنامه قانونی از KeyLogger ها می تواند برای هک و دزدی اطلاعات نیز استفاده شود. امروزه از KeyLogger ها به طور عمده برای سرقت داده های کاربران در سیستم های مختلف پرداخت آنلاین استفاده می شود و ویروس نویسان دائما در حال نوشتن Trojan های جدید برای KeyLogger ها هستند.

#۲ KeyLogger چطور کار می کند؟

روش عملکرد نرم افزار و سخت افزار های KeyLogger چیست؟ در یک جمله می توان گفت، ورود و دستیابی به سیستم از طریق ثبت کلیدهای فشرده شده توسط کاربر. در حقیقت فشردن کلید نحوه صحبت کردن شما با رایانه است. هر ضربه کلید سیگنالی را منتقل می کند که به برنامه های رایانه شما می گوید شما می خواهید چه کاری انجام دهند. زمانی که شما وارد سیستم می شوید، تمام این اطلاعات (فشردن کلیدها در زمان های مختلف، مانند نگه داشتن دکمه Alt و پس از مدتی فشردن کلید Shift برای تغییر زبان) مانند گوش دادن به مکالمه خصوصی شما است.

در حمله KeyLogger وقتی شما بر این باورید که فقط با سیستم خود در حال تبادل اطلاعات هستید، شخص دیگری در حال گوش دادن و نوشتن چیزهایی است که گفته اید.

این در حالی است که با توجه به زندگی دیجیتالی امروزی، ما اطلاعات حساس زیادی را در رایانه های خود ذخیره کرده و یا آن ها را به مقصدی معین ارسال می کنیم. به عنوان مثال اتصال به درگاه بانکی از طریق سیستم های کامپیوتری. به همین جهت، رفتار کاربر و داده های خصوصی او را می توان به راحتی از طریق کلیدهای فشرده شده توسط او در شبکه های مختلف جمع آوری کرد.

به عنوان مثال:

- شبکه های اجتماعی

- ایمیل
- وب سایت های بازدید شده
- پیام های متنی ارسال شده

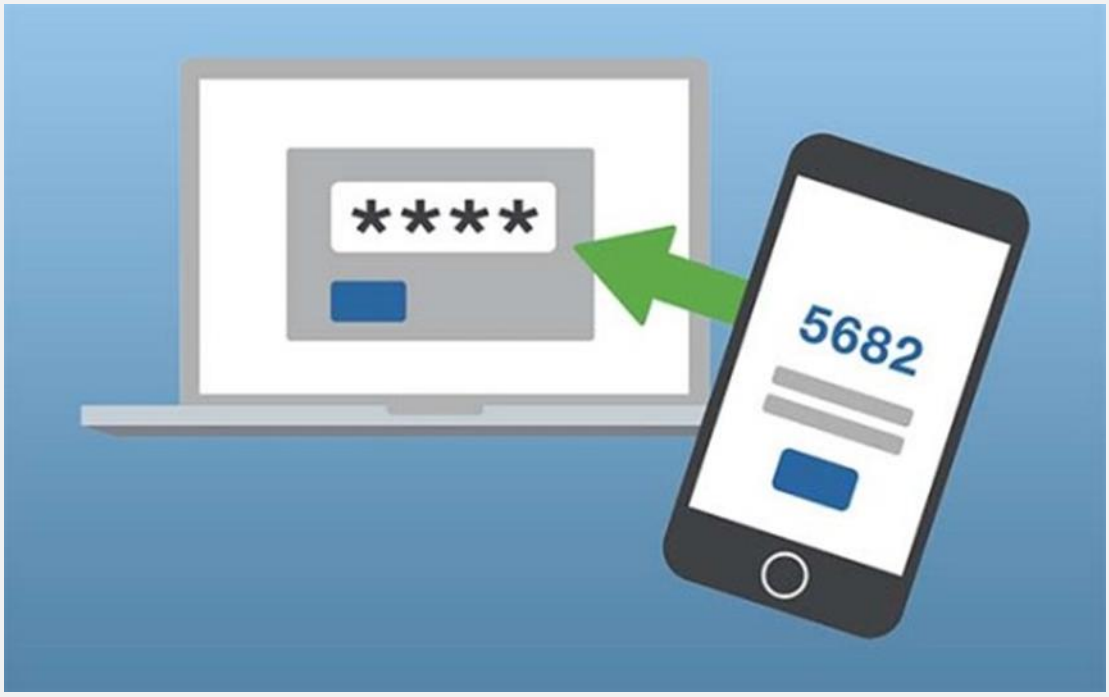
#۳ جلوگیری از سرقت اطلاعات توسط کی لاگر ها

اکثر شرکت های آنتی ویروس قبلا KeyLogger های شناخته شده را به پایگاه داده خود اضافه کرده اند تا از سیستم ها در برابر KeyLogger محافظت کنند. البته می بایست پایگاه داده آن ها را به طور منظم به روز کنید تا موارد جدید نیز به پایگاه داده آنتی ویروس شما اضافه شوند. اما از آن جا که هدف اصلی KeyLogger به دست آوردن اطلاعات محرمانه

(شماره کارت بانکی، گذرواژه و غیره) است، منطقی ترین راه های محافظت در برابر KeyLogger های ناشناخته به شرح زیر است:

#۳-۱ استفاده از رمزهای عبور یک بار مصرف یا احراز هویت دو مرحله ای

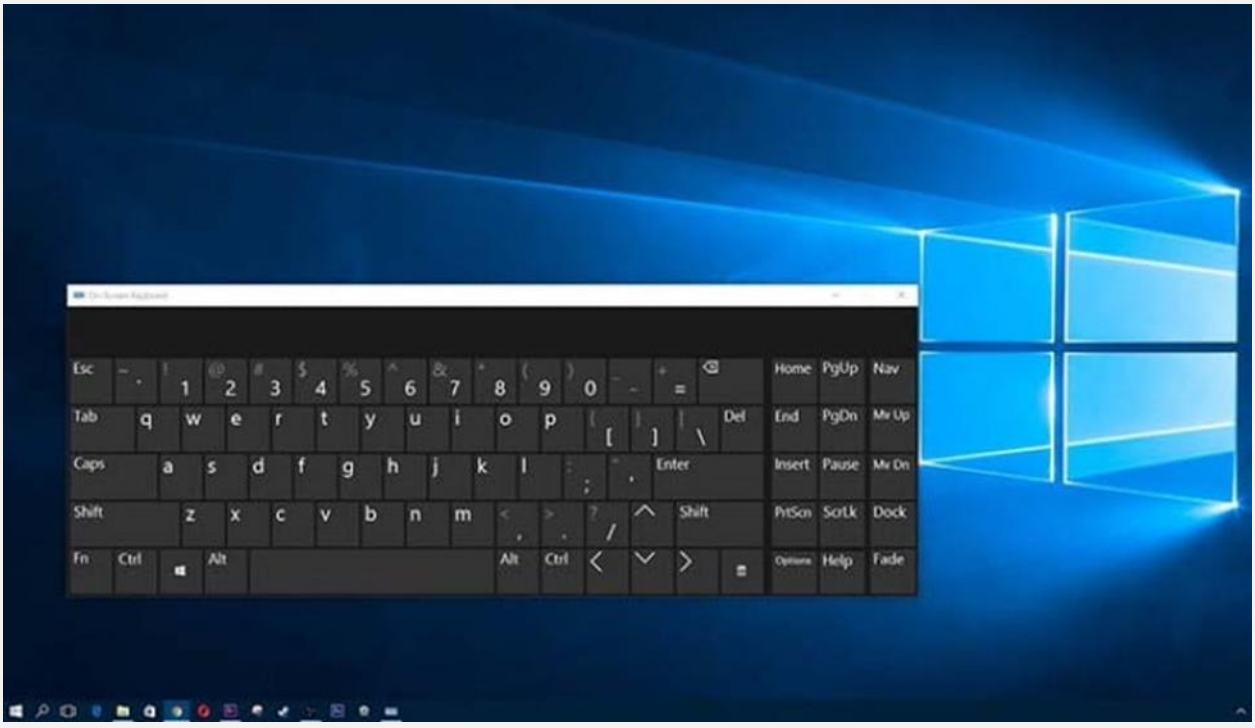
استفاده از رمز یک بار مصرف می تواند میزان ضرر و زیان را به حداقل برساند؛ زیرا رمز ورود ایجاد شده فقط یک بار قابل استفاده بوده و مدت زمان استفاده از آن محدود است.



حتی در صورت دسترسی مهاجم به رمز عبور یک بار مصرف، نمی تواند از آن برای دستیابی به اطلاعات محرمانه استفاده کند.

#۲-۳ استفاده از صفحه کلید مجازی

روش دیگری که می تواند برای محافظت در برابر نرم افزار ها و سخت افزار های کی لاگر مورد استفاده قرار گیرد، استفاده از صفحه کلید مجازی است. صفحه کلید مجازی برنامه ای است که صفحه کلید را روی صفحه مانیتور نشان می دهد و با استفاده از کلیک ماوس می توان کلیدها را فشار داد. قطعا در خریدهای آنلاین خود مشاهده کرده اید که برخی از درگاه های پرداخت شما را ملزم به ورود اطلاعات از طریق صفحه کلید مجازی می کنند.



در موارد حساس شما نیز می توانید از صفحه کلید مجازی سیستم خود برای وارد کردن اطلاعات خود استفاده کنید. البته ایده صفحه کلید مجازی چیز جدیدی نیست. به عنوان مثال سیستم عامل ویندوز دارای صفحه کلید مجازی است. اگرچه به طور کلی این ابزار برای محافظت در برابر

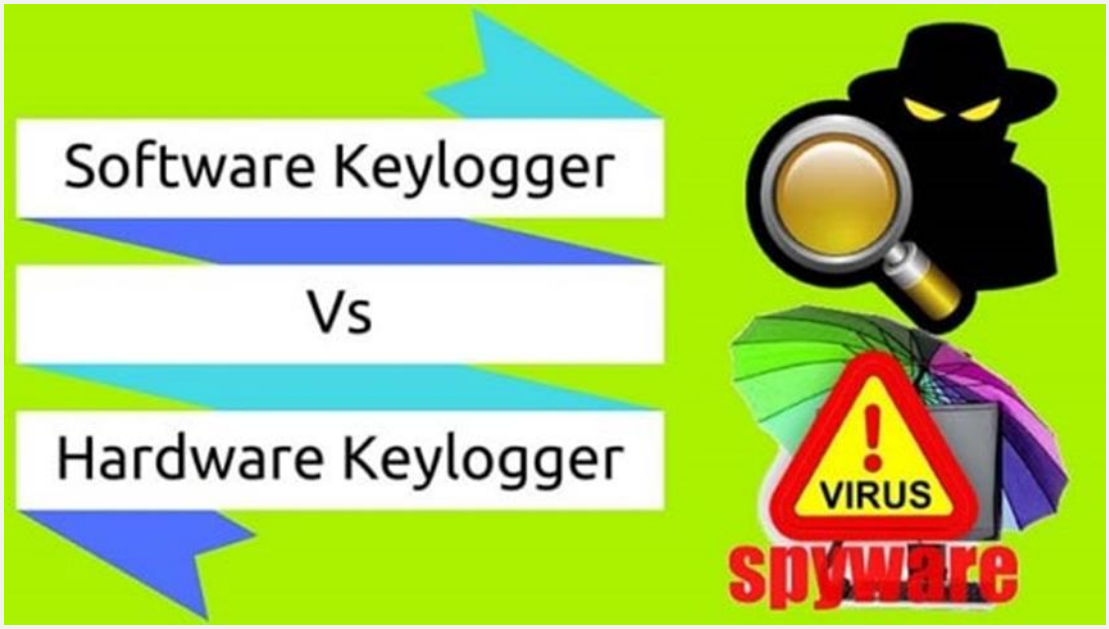
تهدیدات سایبری طراحی نشده و به عنوان ابزاری برای دسترسی کاربران معلول طراحی شده است؛ اما در برخی از موارد می تواند موثر باشد. توجه داشته باشید که اطلاعات وارد شده با استفاده از صفحه کلید مجازی نیز کاملا امن نیست و می تواند با استفاده از روش هایی توسط یک برنامه مخرب شنود شود. به همین دلیل برای محافظت در برابر KeyLogger ها، صفحه کلید های مجازی باید به طور خاص طراحی شوند تا اطمینان حاصل شود که اطلاعات وارد شده از طریق آن ها قابل رهگیری نیستند.

#۴ شناسایی و حذف KeyLogger پس از حمله

روش های مختلفی برای شناسایی KeyLogger وجود دارد. اگر چه انجام همه این موارد ضروری نیستند؛ اما اگر حدس می زنید که کامپیوترتان دارای KeyLogger است، بهتر است این روش ها را امتحان کنید:

- با اجرای آنتی ویروس شروع کنید؛ چرا که آنتی ویروس ها اغلب می توانند یک KeyLogger را در سیستم شما شناسایی کند.
- لیست برنامه های فعال خود را با فشار دادن Ctrl+Alt+Del در ویندوز بررسی کنید. با این کار می توانید از اجرای برنامه های ناشناس آگاه شوید. همچنین می توانید برخی از برنامه هایی که در لیست نمایش داده شده را در موتور جستجو سرچ کرده و با کاربرد آن ها آشنا شوید.
- برنامه ای مانند Spybot Search and Destroy یا MalwareBytes را برای بررسی نوع خاصی از KeyLogger ها اجرا کنید.
- هارد دیسک خود را برای جدیدترین پرونده های ذخیره شده اسکن کنید. به محتویات فایل های ناشناسی که اغلب به روز می شوند نگاه کنید؛ زیرا ممکن است اطلاعات ذخیره شده توسط KeyLogger ها در آن ها باشد.
- اما کاربردی ترین روش برای شناسایی KeyLogger چیست؟ کاربردی ترین روش، مشاهده برنامه هایی است که در هنگام راه اندازی رایانه بارگیری می شوند (یعنی برنامه های موجود در Startup.) برای مشاهده لیست این برنامه ها دستور msconfig را در پنجره Run یا کادر جستجوی بخش Start تایپ کرده و با فشردن دکمه Enter اجرا کنید.

#۵ انواع KeyLogger



۱. نرم افزار KeyLogger

نوع نرم افزاری KeyLogger چیست؟ این نوع از کی لاگرها استفاده بیشتری از نوع سخت افزاری دارند. برخی از این KeyLogger ها می توانند تبادل اطلاعات سیستم شما را در فواصل تصادفی ضبط کنند. نرم افزار KeyLogger ضربات کلید شما را به طور معمول در یک فایل کوچک ذخیره می کند که بعدا قابل دسترسی است یا به طور خودکار برای شخصی که اقدامات شما را کنترل می کند از طریق ایمیل ارسال می شود.

۲. سخت افزار KeyLogger

نوع سخت افزاری KeyLogger چیست؟

KeyLogger های مبتنی بر سخت افزار می توانند فعالیت های شما را کنترل کنند؛ بدون این که هیچ گونه نرم افزاری روی سیستم شما نصب شود.

نمونه هایی از این موارد عبارتند از:

- سخت افزار صفحه کلید:

این دستگاه به شکل یک قطعه سخت افزاری در جایی بین صفحه کلید و رایانه قرار می گیرد. این نوع از KeyLogger ها برای مهاجمان بسیار سودمند است؛ زیرا به هیچ نرم افزاری وابسته نیست و توسط هیچ نرم افزاری قابل تشخیص نیست.

- شنود صفحه کلید بی سیم:

این امکان وجود دارد که سیگنال های فرستاده شده از صفحه کلید بی سیم به گیرنده آن، توسط یک سخت افزار شنود بی سیم شنود شود.