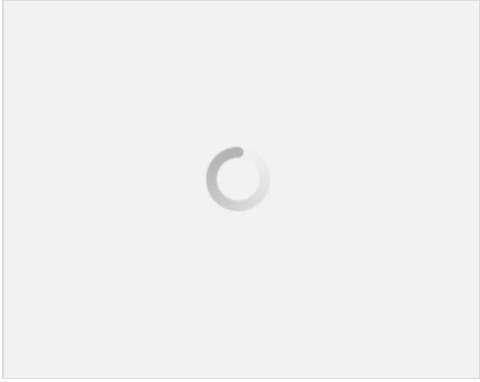
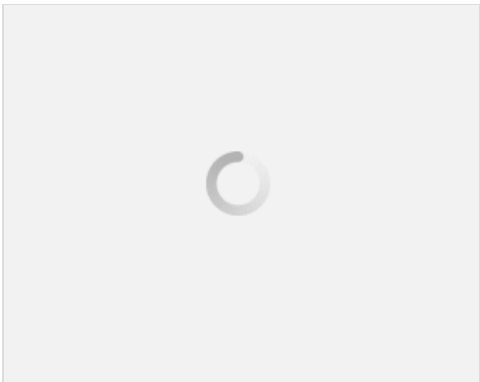
آموزش روش شناسایی کیلاگر : چگونه متوجه وجود Keylogger شویم؟ (نسخه PDF)

در مطلب گذشته که در مورد ویروس مخرب Keylogger بود با نحوه ی کار کردن آن و نرم افزار مشابه که Ilivid نام داشت آشنا شدیم و دانستیم که این بدافزار چه کارهایی را میتواند بر روی سیستم ما انجام دهد.امروز میخواهیم در مورد اینکه چگونه متوجه وجود این مخرب بر روی سیستم خود شویم صحبت کنیم و اینکه بعد از اطلاع یافتن از حضور این بدافزار چه اقداماتی را برای مقابله با آن باید انجام دهیم.



خب همانطور که گفته شد این بدافزار به صورت کاملا Hidden میباشد و به هیچ وجه اثری از خود نشان نمیدهد و همانند سایر ویروس ها نیست که براحتی توسط آنتی ویروس های نصب شده بر روی سیستم شناسایی گردد.کیلاگر از راه های مختلفی به سیستم وارد میگردد که میتواند به صورت سخت افزاری به سیستم شما متصل شده و در هارد دیسک شما قرار گیرد و اطلاعات را ثبت و ارسال کند و هم میتواند از طریق DVDهای آلوده بر روی فایل قرار گرفته و به سیستم شما نفوذ کند و یا اینکه چون کیلاگر نوعی تروجان میباشد قابلیت این را دارد که به فایل های مختلف اعم از PDF و یا فیلم و عکس متصل شده و به سیستمتان نفوذ کند و در گوشه ای برای خود جایی بگیرد بدون آنکه اثری از او قابل مشاهده باشد.البته این را در نظر داشته باشید که همه ی کیلاگر ها انقد حرفه ای نیستند به این معنی که همگی به صورت Hidden در سیستم نمیمانند و براحتی توسط آنتی ویروس هایی که وجود دارند قابل ردیابی میباشند.اما بحث ما در مورد کیلاگرهایی است که حرفه ای هستند و در سیستم ما بصورت مخفی درحال انجام فعالیت و ارسال دیتا به سازنده ی خود میباشند.

مثل همه ی وسایل و نرم افزار های مختلف که هم مخرب هستند و تحت شرایطی هم مفید هستند کیلاگر نیز همیشه مضر نیست بلکه در برخی از سازمان های امنیتی و مهم از این بدافزار در راه درست استفاده میکنند مثلا مدیر میخواهد بداند که وقتی از شرکت خود خارج میگردد چه کسی به سراغ کامپیوتر وی میرود و کارهایی که بر روی آن انجام میدهند چیست در این صورت وی بر روی سیستم خود کیلاگر را نصب میکند و وقتی که از محل کار خارج شد میتواند در ایمیل خود ببیند که چه اتفاقی بر روی سیستم وی در حال انجام است.حال فرض کنید که ما یک سیستمی داریم که بر روی آن بدست یک شخص محترم هکر آلوده به کیلاگر شده است و ما باید جلوی این ویروس مخرب را بگیریم اما چگونه؟چون ما که نمیتوانیم این بدافزار را ببینیم و سیستم آنتی ویروسی ما نیز اونقدر قدرت ندارد که بتواند این بدافزار را تشخیص دهد.البته در ایران که اکثرا به اخطارهای آنتی ویروس توجهی نمیکنیم و هرچی پیغام میدهد در نظر نمیگیریم و بعضا اون رو غیر فعال میکنیم پس دیگه براحتی تمام طعمه ی این بدافزار و هکر محترم خواهیم بود.



راه های تشخیص وجود کیلاگر بسیار زیاد میباشند که ما به مهمترین و واضح ترین آن ها میپردازیم.یکی از نشانه های وجود کیلاگر بر روی سیستم ما کندی بیش از حد سیستم میباشد.اگر میبینید که سیستم شما به شدت کند شده است همیشه این فکر که بخاطر نرم

افزارهایی است که بر روی آن نصب کرده ام کنـد شـده درست نمیباشد بلکه ممکن است یک کیلاگر در حال فعالیت بر روی سیسـتم شـما هست و اطلاعات شما را در قالب یک فایل Text رمزنگاری شده به مقصد خود ارسال میکند چون در حافظه اصلی قرار دارد در نتیجه باعث کاهش سـرعت رم و کندی سیسـتم شـما میگردد.یکی از راه های پیدا کردن ویروس دیدن سـری پروسه هایی است که در سیستم شما در Taskmanager درحال نشان دادن میباشد وو وقتی میبینید که این سـرویس برای شـما نا آشنا است پس بهتر است که آن را حذف کنید و یا در قسمت Startup سیستم فایل هایی وجود دارند که سازنده ی آن را به صورت UNKNOWN نوشته است که اگر شما با این فایل آشنایی ندارید باید آن را پاک کنید تا در سیستمتان فعالیت نکند.

اما از آنجا که کیلاگر جوری برنامه ریزی شده است که قادر به ردیابی و شـناسایی در Startup ویا Taskmanager نباشد شما نمیتوانید که از روی پروسه های در حال انجام آن را تشـخیص دهید.در اینجا شـما باید برای اینکه ببینید آیا بر روی سیسـتم شـما کیلاگری وجود دارد یا خیر باید به قسمت History مرورگرهای خود برویـد چرا که این بدافزار همواره با هر حرکت شـما اطلاعات را ارسال میکند پس در History مرورگر شما رد پایی از آن وجود دارد و میتوان آن را دید و برای جلوگیری از آن اقدامات لازم را انجام داد.

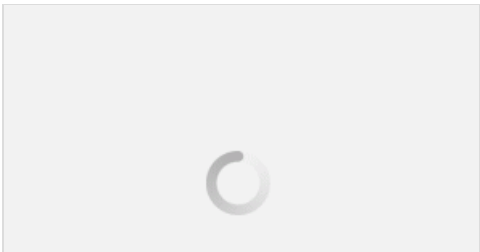
البته کیلاگر در مرورگر بطور کامل قابل تشـخیص نیست اما اگر شـما آمار دقیق تاریخچه ی مرورگر خود را داشـته باشید براحتی کوچکترین تغییر در آن شـما را متوجه وجود کیلاگر در سیسـتمتان میکنـد و در اینجا بایـد شـروع به جلوگیری از این بـد افزار بکنیـد.یکی از راه های جلوگیری از کیلاگر اسـتفاده از آنتی ویروس های قوی و آپدیت است که به صورت دوره ای سیسـتم شـما را اسـکن میکند و بروز بودن نرم افزارهای موجود بر روی سیسـتم شما نیز اهمیت زیادی برای کشف بدافزار ها و مقابله با آن دارد.برخی برنامه های Antispyware که کار آن ها جلوگیری از ورود و نصب کیلاگر میباشـد مثل Spyware blaster میتواند کمک زیادی برای افزایش امنیت شـما در سیسـتمتان بکند که این ها بصورت دوره ای که برایش تعریف میکنیـد سیسـتم شـما را اسـکن کرده و اگر کیلاگری را پیدا کند درجا شـما را از شـر آن خلاص میکند.

در این لینک تعدادی نرم افزار برای جلوگیری از کیلاگر موجود میباشد.

Keylogger Detector

راه دیگر تحلیل پردازش هایی است که در سیسـتم عامل رخ میدهـد که این کار بصورت تخصصـی و توسط نرم افزارهای مختص آن انجام میگیرد که آنان تمامی پردازش های شـما را تحت نظر دارند و کوچکترین پردازشـی که تشخیص دهند مخرب است را گزارش کرده و پاک میکنند.بعـد از پاک شدن پردازش کیلاگر از بین نمیرود بلکه شـما باید توسط آنتی ویروس قوی آن را از بین ببرید در غیر این صورت پس از ریست شدن سیستم و بالا آمدن آن دوباره کیلاگر پیدا شده و شروع به کار کردن میکند و دوباره روز از نو روزی از نو.

روش دیگر از بین بردن و جلوگیری از ورود و کار کردن کیلاگر فرمت کردن سیسـتم به صورت دوره ای میباشـد.به این صورت که شـما یک Backup از سیستمتان میگیرید و توسط CD Windows آن را فرمت میکنید که اگر کیلاگر یا هر بدافزار دیگه ای وجود داشته باشد را از بین ببرد.اینها روش های از بین بردن کیلاگر نرم افزاری بود.برای از بین بردن کیلاگر سـخت افزاری شما باید اتصال سخت افزار مورد نظرتان را که حالا چه به صورت کولدیسک و یا به صورت CD باشد را جدا کنید.



امیدوارم این مطلب برای شما مفید باشد و بهره ی لازم را از آن ببرید تا در دام هکرهای محترم نیفتید.موفق و سربلند و ITPRO باشید.

نویسنده:امیرمحمد رسول خمینی

منبع: جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو

وحید معصومی اصل

با تشکر از آقای رسول خمینی بابت این مقاله خوبتان

شما فرمودید که یکی از راههای از بین بردن Keylogger ها فرمت سیستم می باشد که در اینصورت باید اول از سیستم بکاپ بگیریم و سپس اقدام به فرمت کنیم، حال سوالم این هست که ما داریم از یک سیستمی بکاپ می گیریم که آلوده به ویروس هست و محتویات بکاپ نیز آلوده خواهد بود که در اینصورت اگر بعد از فرمت سیستم اطلاعات مربوط به بکاپ رو restor کنیم سیستم باز هم آلوده خواهد شد.!

امیر محمد رسول خمینی

سلام دوست عزیز

خیر ساختار کیلاگر اینجوریه که بعد از ورود به سیستم روی هارد قرار میگیره و به اطلاعات کاری ندارد یعنی مثل ویروس های دیگه نیست که به تمامی فایل ها متصل شود در نتیجه اطلاعات شما پاکه ولی هارد شما کیلاگر رو داره و نشونش نمیده.شما اطلاعات رو بکاپ بگیرید و هارد رو فرمت کنید تا کیلاگر از روی هارد پاک شود.موفق باشید

امیر شاه حسینی

key loger رو میشه از اینترنت دانلود کرد؟

امیر محمد رسول خمینی

بله میشه دانلود کرد اما ورژن های خاصش که دیگه حرفه ای عمل میکنه و ایمیل میزنه پولی هست و ۵۰دلار هستش

امیر شاه حسینی

ایمیل نزنه که به درد نمیخوره

امیر محمد رسول خمینی

گفتم که ورژن حرفه ایش هست که پولیه ایمیل هم میزنه

مطلب اصلی