نقد و بررسی آنتی ویروس پادویش ایرانی قسمت ۶ (نسخه PDF)

نقد و بررسی آنتی ویروس پادویش ایرانی قسمت ۶ (نسخه چاپی)

اضافه کردن قسمت SIV برای جلوگیری از Rootkit

یکی دیگر از انتقادات و البته بحث و جدل هایی که در خصوص پادویش به مراتب بیشتر در تالارهای گفتمان مطرح بود ، مکانیزم جلوگیری ، شناسایی و البته پاکسازی Rootkit ها از سیستم عامل ها بود ، خوب در این خصوص بحث های زیادی انجام شده است اما نکته اینجاست که هنوز برخی دوستان تفاوت انواع بدافزار را درک نمی کنند و در همان ابتدای کار به سراغ Rootkit ها می روند !! محض اطلاع دوستان Rootkit می تواند کابوس شما در شبکه و سرورها باشد و از نظر من یکی از خطرناکترین نوع بدافزار در دنیا است که شناسایی و از بین بردن آن اصلا کار ساده ای نیست اما در پادویش با توجه با اینکه مکانیزم برنامه نویسی لایه پایین استفاده شده است و Rootkit ها نیز در پایین ترین لایه اکثرا فعالیت می کنند در خصوص شناسایی Rootkit های Wellknown عملکرد مناسبی دارد اما دقت کنید که هیچکس نمی تواند در دنیا تضمین کند که همه Rootkit ها را شناسایی می کند و آنها را پاکسازی می کند !! این کاملا غیرمنطقی است .

ما قطعا در حال حاضر Rootkit هایی داریم که در اصطلاح فنی Zero Day هستند و اصلا بعید است آنتی ویروس های بزرگ دنیا هم آنها را شناسایی و پاکسازی کنند ، پس منطقی باشیم و بحث و جدل بیهوده در این خصوص نکنیم . اگر قبول داریم محصولی کاملا بومی است باید قبول کنیم که حمایتش کنیم . اما در این خصوص نقد دارم ، به نظرم بایستی در پادویش مخصوصا نسخه های سرور (من نسخه سرور را تست نکرده ام) مکانیزم SIV برای پیشگیری از فعالیت Rootkit ها پیاده سازی شود و با بررسی کردن Integrity فایل های حساس سیستمی بتوان بعضا حتی zero day ها را نیز کشف و از ادامه فعالیت آنها جلوگیری کرد ، این از نظر امنیتی منطقی ترین راهکار پیشگیری از آلودگی به Rootkit ها است اما خوب بحث پاکسازی جدای این موضوع است . پیشنهاد می کنم نگاهی به پروژه AFICK بیندازید ، البته بنده برنامه نویس زیاد لایه پایینی نیستم و شما متخصصین قطعا دانش بیشتری به این موضوع دارید اما وجود چنین مکانیزمی واقعا می تواند اطمینان خاطر بدهد که سیستمی آلوده شده است و اگر آلوده شده است کجا و چه فایل هایی دقیقا باید تعمیر و بازسازی شوند.

امکان تعریف عمق اسکن فایل های فشرده

البته می دانم این یک مقدار ایراد بنی اسرائیلی است اما نقدی است که کاربران داشته اند و ما هم دیده ایم و امیدواریم امکانی برای پادویش نسخه جدید اضافه شود تا بتوانیم عمق اسکن فایل های فشرده را مشخص کنیم. برای مثال بصورت پیشفرض به نظر می رسد که پادویش فایل های فشرده سازی شده را اسکن نمی کند اما در نتایج جستجو نام فایل های فشرده سازی شده وجود داشت اما نمی توانیم فعلا درجه های فشرده سازی را در اسکن تعریف کنیم ، این طبیعی است که اینکار به شدت باعث سنگین شدن فرآیند اسکن می شود و می تواند به عنوان یک Option برای کاربران حرفه ای تر در نظر گرفته شد.

یک پیشنهاد به پادویش دارم ، اگر ممکن است امکانی اضافه کنید که فایل هایی که دارای پسورد هستند یا رمزنگاری شده اند و یا به هر دلیلی توسط پادویش امکان اسکن شدن ندارند را در نسخه های بعدی به شما معرفی کنند ، برای مثال من در پوشه دانلود خودم یک فایل فشرده دارای پسورد حاوی هزاران نوع بدافزار داشتم اما هیچ گزارشی از وجود چنینی فایلی دریافت نکردم ، اگر گزارشی از این نوع فایل ها داشته باشم می توانم بصورت دستی حداقل آنها را بررسی کنم. این هم یک پیشنهاد است اما طبیعتا ابعاد مختلف و دلایل پیاده سازی نشدن آن هم قطعا قابل پذیرش است.

پشتیبانی از سیستم عامل های قدیمی

یکی از مشکلاتی که در پست های کاربران مطرح بود عدم پشتیبانی پادویش از سیستم عامل های قدیمی !! عدم پشتیبانی پادویش از سیستم عامل های جدید !! در طی زمان بود !! یعنی یکبار بحث اینجا بود که چرا از سیستم عامل هایی مثل XP و ۲۰۰۰ و ۲۰۰۳ پشتیبانی نمی کند و یکبار بحث اینجا بود که چرا از ویندوز ۱۰ پشتیبانی نمی کند !! امروز که در خصوص پادویش صحبت می کنیم از ویندوز ۱۰

پشتیبانی می کند قطعا اما قرار نیست به نظرم از ویندوز XP هم پشتیبانی کند !! اینکه استدلال کنیم که خیلی از سازمان های ما همچنان XP و ۲۰۰۰ دارند یا در شبکه بانکی و ATM ها ویندوز ۹۸ همچنان هست هیچ ربطی به قابلیت های پادویش ندارد !

وقتی سیستم عاملی بصورت رسمی از پشتیبانی شرکت سازنده خارج می شود حفره های امنیتی پیدا می کند که آنتی ویروس ها نیز بعضا از پوشش دادن آنها عاجز هستند و پشتیبانی از این نوع سیستم ها فقط باعث سنگین تر کردن کار پادویش و سایر آنتی ویروس ها می شود . مثل این است بگوییم که توسینسو چرا از Internet Explorer نسخه ۶ و ۷ پشتیبانی نمی کند ؟ خوب عزیز من اگر بخواهیم مبتنی بر این مرورگرها سرویس های به روز ارائه بدهیم وب سایت دیگر نمی تواند از برخی امکانات و قابلیت های روز دنیا استفاده کند ، کمی منطقی باشیم کسیکه حاضر نیست بعد از گذشت ۱۸ سال از عمر یک سیستم عامل آن را تغییر بدهد و به روز رسانی کند محکوم به آلودگی بدافزاری و هک شدن است ، دیگه دانشجوهای ساده کلاس Security+ من برای خنده XP سرویس پک ۳ و ۲۰۰۰۳ و حتی ۲۰۰۸ رو هک می کنند اون هم با داشتن آنتی ویروس چرا اصرار دارید یک چیز را عقب گرد کنید ! نمی دانم پادویش الان از XP پشتیبانی می کند یا خیر اما به نظر من پشتیبانی نکند خیلی منطقی تر است . الان دقیقا پادویش باید به ساز کدام Troll برقصد ؟ ...

ادامه دارد ...

نویسنده : محمد نصیری

منبع : جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو

هادی صارمی

سلام وقت بخیر مهندس

توضیحات شما کامل

اینکه از ویندوز XP و سرور ۲۰۰۸ پشتیبانی میکند که من خودم نصب کردم تحت شبکه پشتیبانی میکند و هیچ مشکلی ندارد.

در نسخه شبکه این آنتی ویروس چند ایراد کوچیک در خصوص تفکیک قسمت وجود داره که اجازه بدین با بررسی بیشتر در یک پست مطرح میکنم.

محاسن این آنتی ویروس خیلی خیلی بیشتر از معایبش هست، امیدوارم که توسعه این آنتی ویروس ادامه دار باشه.

محمد نصیری

قطعا در پست ها یا در ادامه تحلیل این موارد رو مطرح کنید ، ایرادها رو باید کمک کنیم برطرف بشه ، من فقط به دلیل اینکه میدونم رسیدگی می کنن به این موارد و دوست دارم پادویش بهتر از هر روز بشه این رو میگم.

مطلب اصلی