به نام خدا

مقاله ای کوتاه در مورد :

روش های هک آی دی یاهو

و

نکاتی در مورد جلوگیری از هک شدن

با تشکر از استاد ارجمند جناب آقای پورشمسی

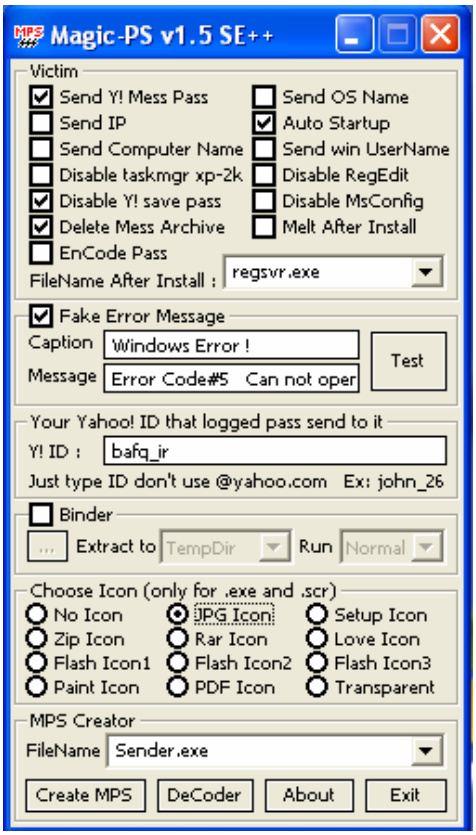
نویسنده : سید منصور میرهدایی

چند روش از روش های بدست آوردن پسورد آی دی های یاهو

۱) استفاده از تروجان :

کار اصلی تروجان ها فرستادن اطلاعات از کامپیوتر قربانی به سازنده خود است هکر ها نرم افزار هایی را طراحی کرده اند که با تنظیماتی که بروی آن ها انجام میدهیم یک فایل بسیار کم حجم را برای ما میسازد که وقتی این فایل بروی سیستم قربانی اجرا شد آن سیستم به تروجان آلوده شود و هردفه به اینترنت وصل شد اطلاعات مشخص شده فرستاده شود . این اطلاعات به تنظیمات و قدرت برنامه ساخت تروجان بستگی دارد .

برای مثال به معرفی یک سازنده تروجان می پردازیم : (MAGIC-PS)



قسمت victim : اطلاعات مورد نیاز که می خواهیم برایمان فرستاده شود (آی دی و پسورد یاهو مسنجر ، آدرس اینترنتی کامپیوتر ، نام کامپیوتر و ...)

قسمت Fake Error messege : طراحی یک پیام نمایشی بعد از اجرای تروجان

قسمت your yahoo id : در این قسمت باید آی دی خود را وارد کنید تا اطلاعات به آن فرستاده شود

قسمت binnder :این قسمت به شما اجازه میدهد تا فایلی را انتخاب کنید تا بعد از اجرای آن تروجان آن فایل اجرا شود

قسمت choose icon : برای انتخاب یک شکلک برای فایل تروجان تان .

قسمت mps : دراین قسمت نامی را برای تروجان انتخاب میکنید .

و در آخر بروی کلید create mps کلیک می کنید.

نکته ۱ : هیچ موقع بروی کامپیوتر خود اجرا نکنید .

نکته ۲ : بدلیل قدیمی بودن این تروجان برای تعدادی از ویروس کش ها قابل شناسایی می باشد شما میتوانید با تغیرات در ساختار فایل از شناسایی آن جلوگیری کنید یا از تروجان های جدید استفاده کنید .

نکته ۳ : این تروجان برای همه ورژن های یاهو مسنجر جواب میدهد.

نکته ٤ : سازنده این تروجان را می توانید از آدرس **http://bafq.ir/mps.exe** دریافت کنید .

۲) استفاده از نرم افزار های جاسوسی

یکی دیگر از روشهای بدست آوردن پسوردها و مانیتور کردن سیستم قربانی استفاده از نرم افزار های جاسوسی می باشد این نرم افزار ها بعد از نصب بروی کامپیوتر قربانی فعال شده و تمامی فعالیت هایی را که در آن کامپیوتر انجام میشود (کلید های زده شده ، پسورد های وارد شده ، تصاویر دیده شده ، آدرس فایل های اجرا شده ، آدرس سایت های دیده شده ، زمان روشن و خاموش شدن کامپیوتر و...) را برای ایمیل مشخص شده می فرستد این نرم افزارها دارای قدرت بسیار زیادی هستند و عملیات خود را بروی وقفه ها و ثبات ها و رجیستر ویندوز انجام میدهند .(نام بعضی از این نرم افزارها عبارت است از : keyloger 2 ، Star ، PC Agent 4.0 و ...) خوشبختانه بهترین و قدرتمند ترین نرم افزارهای جاسوسی بسیار گران هستند و یا دارای قفل های قوی هستند که کرک کردن آن ها کار بسیار دشواری است . انشا ا... در مقاله دیگر به کرک کردن نرم افزارها می پردازیم .

۳) استفاده از صفحات لوگین

همانطور که مطلع هستید یک هکر بجزء قدرت برنامه نویسی به زبان های مختلف بخصوص شبکه و آشنایی کامل با سیستم عامل و سخت افزار باید دارای روانشناسی بالایی باشد تا بتواند با زمینه سازی یک حقه طرف مقابل خود را به سادگی فریب دهد . بعضی از هکر ها صفحه ای همانند صفحه ورود به ایمیل یاهو طراحی کرده ودر سایت خود آپلود میکنند وآدرس آن صفحه را با کلک های متفاوتی برای قربانی میفرستند و قربانی غافل از جریان ایمیل و رمز خود را توسط این صفحه برای هکر میفرستد . یکی از روشهایی که طرف مقابل فریب میخورد این است که یک ایمیل به او بزنیم و در آن ایمیل از یک اسکریپت لینک دهنده به آدرس آن صفحه استفاده کنید .طرف مقابل با چک کردن ایمیل به صورت اتوماتیک از ایمیلش خارج شده و به آن صفحه میرود و او برای ورود مجدد دوباره رمز خود را میزند واصلا متوجه نمی شود هک شده است

٤) استفاده از اطلاعات شخصی افراد

بسیاری از افراد رمز های خود را بر حسب اطلاعات شخصی خود قرار میدهند بعضی ها شماره موبایل خود را می گذارند بعضی ها هم نام ، نام خوانوادگی و . . . بعضی از افراد هم برای رمز خود قانون می سازند ویا از ۱۲۳۴۵۶ استفاده میکنند خلاصه مطلب اینکه میتوان رمز آنها را به راحتی حدس زد تنها باید بتوانیم ذهن و فکر طرف مقابلمان را بخوانیم . ضمناً نرم افزار هایی وجود دارند که بانک رمز خود را به صورت تصادفی برای ایمیل مشخص شده امتحان میکنند اما این نرم افزار ها دیگر برای یاهو کاربرد ندارند چون سیستم یاهو به گونه ای است که وقتی برای چند بار رمز را اشتباه وارد کنیم از ما یک کد امنیتی میخواهد تا ربات ها نتوانند رمز ها را پیدا کنند.

۵) بدست آوردن اشتراک های دیگر

اکثر افراد تمامی رمز های خود را یکی انتخاب می کنند تا از خطر فراموش کردن آن جلوگیری شود پس ما میتوانیم بدلیل امنیت بالای یاهو از هک کردن ایمیل یاهو به صورت مستقیم دست برداریم و با بدست آوردن شناسه او در سایت های دیگر آن شناسه را هک کنیم که در واقع با پیدا کردن آن پسورد ، رمز اصلی آن لو رفته است هک کردن شناسه سایت ها open source کار بسیار دشواری نیست ولی خارج از بحث ما می باشد

٦) استفاده از فرمان های رجیستر و ساختار سیستم عامل

ما میتوانیم با بهره گیری از فرمان های رجیستری ویندوز آی دی ها و رمز های وارد شده در این سیستم را بدست آوریم مثلا اگر خصوصیت HKEY_CURRENT_USER\Software\yahoo\pager\Save Password را ۱ قرار دهیم آی دی و رمز آخرین نفری را که وارد یاهو مسنجر شده را بروی یاهو مسنجر به حالت ثبت شده در می آورد و ما با زدن دکمه Sing in ما وارد ای دی طرف میشویم . ضمناً همانطور که میدانید تمامی فعالیت هایی که ما با کامپیوتر انجام میدهیم ثبت میشود تنها ما با Decode کردن آن اطلاعات ثبت شده می توانیم به رمز های کاربران دست یابیم فایل هایی که اطلاعات در آن ها ثبت می شود عبارتند از (User.dat ، System.dat و ...)

۷) استفاده از امکانات یاهو برای فراموشی رمز

ما میتوانیم خودمان را جای طرف مقابلمان قرار دهیم و فکر کنیم رمزمان را فراموش کرده ایم البته باید با اطلاعات شخصی آن طرف آشنا باشیم و قربانی را کاملا بشناسیم

۸) استفاده از قابلیت های جدید کنترل پنل های جدید وب

برای راحتی و مخفی ماندن روش هک بعضی از هکر ها فایل های تروجان خود را بروی سرورهای وب قرار داده که قابلیت ها و امکانات جدیدی دارند . بعضی از سرور ها توانایی اجرای فایل های exe را دارند و تنها نیاز است آدرس آن فایل را طوری در صفحه وب قرار دهیم که خود به خود فرا خوانی شود و سیستم قربانی را آلوده کند .برای فراخوانی می توانیم از زبانهای cgi ، php و زبان های دینامیک دیگر استفاده کرد .این روش در اکثر مواقع جواب میدهد ولی برای افرادی که بروی کامپیوترشان یکی از برنامه های مدیریت دانلود نصب است اجازه دانلود میگیرد که باعث لو رفتن کار میشود

۹) دست یافتن به دیتابیس یاهو

عده ای گاهی به این فکر می افتند که به سرور یاهو وارد شوند . سرور یاهو دارای امنیت بسیار بالایی است و تمامی راه های نفوذی آن بسته است البته هنوز هم می توان آن را هک کرد ولی تنها برای چند ثانیه چون سیستم مانیتورینگ یاهو به سرعت به آن شرکت اخطار میدهد و به سرعت شما شناسایی می شوید و خدمات یاهو از شما گرفته میشود پس شما برای این کار باید از سرعت ارتباطی بالایی با اینترنت برخودار باشید تمامی مسیر های یاهو را بدانید هدف را مشخص کنید به زبانهای برنامه نویسی تحت وب تسلط داشته باشید با ساختار یاهو آشنا باشید از باگ های یاهو مطلع باشید با از دست دادن خدمات یاهو ناراحت نشوید

با دانستن این نکات دیگر هک نمی شوید

۱- در انتخاب رمز دقت کنید.

۲- قرار دادن کلمه :YMSGR در رمز خود باعث جلوگیری از فرستادن رمز توسط تروجان میشود البته اگر میخواهید در وسط رمز این کلمه را استفاده کنید باید قبل از آن یک فضای خالی یا همان space قرار گیرد .

۳-قرار دادن کارکتر & و در ادامه تعدادی فاصله یا همان space در پایان رمز باعث میشود اگر رمز به وسیله برنامه های جاسوسی فرستاده شد قابل خواندن نباشد .

۴-در انتخاب یک ویروس کش خوب دقت کنید و از ویروس کش هایی استفاده کنید که ضد جاسوسی (spyware) هم باشند .

۵- از دریافت فایل های ناشناس جدداً خودداری کنید.

۶- چنانچه فایلی دریافت کردید قبل از اجرا، راست کلیک کرده و با مطالعه properties از نوع فایل مطمئن باشید فایل اجرایی نمی باشد.(... Application)

۷- عکس های غالباً با پسوند jpg. و gif. می باشد. در صورتی که پسوند های مشکوک و یا اجرایی مانند exe. داشت با shift+delete آن را پاک کنید.

۸- از voice chat بپرهیزید.

۹- چنانچه به شخصی مشکوک هستید یا ایجاد مزاحمت می نماید id شخص را به هیچ وجه add نکرده و در صورت add بودن delete کنید و سپس ignore نمایید.

۱۰- آی دی و پسورد خود را بروی هر کامپیوتری وارد نکنید .

۱۱- بعد از اتمام کار با یک آی دی فرضی وارد شوید .

۱۲- در پایان کار با ایمیل ،ایمیل خود را log of یا sing out کنید .

۱۳- در سایت های غیر رسمی عضو نشوید یا اینکه یک رمز دیگر را برای آن عضویت قرار دهید .

۱۴- هر موقع می خواهید وارد ایمیل شوید از صحیح بودن آدرس صفحه لوگین اطمینان حاصل کنید .

۱۵-هر چند مدت یکبار از طریق msconfig ، start up سیستم خود را چک کنید تا نرم افزار های مشکوک در حال اجرا نباشند .

۱۶- بیننده سایت های مشکوک نباشید .

۱۷- هر چند مدت یکبار کوکی های کامپیوتر های خود را پاک کنید .

((این مقاله بصورت فی البداع وذهنی تایپ شده است احتمالا دارای اشکالات زیادی باشد .

امیدوارم به بزرگواری خودتان ببخشید))