آغاز سند
آخرین نکارش 18 جولای 2009

روشهای مقابله با شناسایی شدن در فضای اینترنت

هم میهنان گرامی ،

همانطور که میدانید مزدوران رژیم اسلامی اعم از سپاه پاسداران ، وزارت اطلاعات ، قوه قضاییه و نیروی انتظامی ، طی سالهای اخیر اقدام به ایجاد فضای رعب و وحشت در دنیای مجازی اینترنت نموده و علاوه بر فیلتر کردن بسیاری از سایت ها و وبلاگ ها، اقدام به ردیابی ، شناسایی و دستگیری مسئولین ،نویسندگان و حتی کاربران و بازدیدکنندگان سایت ها و وبلاگ های سیاسی و اجتماعی در ایران میکنند.

امید است با مطالعه آموزش های زیر ، بتوانید هر چه بیشتر و بهتر امنیت خود در اینترنت را تضمین کنید تا مزدوران رژیم اسلامی قادر به رهگیری و شناسایی شما نباشند و تیرشان به سنگ بخورد !

مزدوران رژیم اسلامی بطور کلی از 2 طریق قادر به شناسایی کاربران اینترنتی هستند :

1- ردیابی آی پی (IP) کاربران
2- مهندسی اجتماعی (تکنیک های ویژه جاسوسی و نفوذ به شیوه روان شناسی)

1- ردیابی آی پی :

آی پی چیست ؟

وقتی کامپیوتر شما به اینترنت وصل میشود ، شماره ای به آن اختصاص می یابد و بوسیله آن کامپیوتر شما در اینترنت با آدرسی منحصر به فرد شناخته می شود . همانند یک شناسنامه یا یک آدرس پستی. این آدرس در واقع آدرس کامپیوتر شما درشبکه است و از طریق آن ، دیگر کامپیوتر ها می توانند با کامپیوتر شما ارتباط برقرار کنند.
این شماره یا شناسه ، آی پی (IP) نام دارد و با این فرمت نوشته میشود : xxx.xxx.xxx.xxx که منظور از xxx عددی بین 0 تا 255 است. مثلا ممکن است آدرس شما به صورت 195.123.83.79 باشد.

برای دانستن آی پی حقیقی خود در زمان اتصال به اینترنت ، میتوانید در ویندوز به منوی Start رفته و بعد در قسمت Run ، تایپ کنید cmd و اینتر کنید . پنجره محیط داس باز میشود که در آنجا تایپ کنید ipconfig و اینتر کنید . مشاهده میکنید که آی پی شما در قسمت IP Address نمایش داده میشود. همراه با مشخصات و شماره های دیگر که در اینجا از توضیح آنها صرفنظر میکنیم.

IP یک الزام فنی محسوب می شود و هرگز با این سیاست در شبکه تدوین و تعریف نشده است که کاربر را افشا کند، اما به هر حال ممکن است مشکل ساز شود. با لو رفتن آی پی حقیقی شما ، مزدوران رژیم قادر به ردیابی شماره تلفن و محل جغرافیایی شما (منزل ، محل کار ، ..) خواهند بود و در مدت کوتاهی میتوانند شما را دستگیر کنند. بنابر این نهایت تلاش شما باید این باشد که آی پی حقیقی شما پنهان بماند و از یک آدرس آی پی دیگری به جای آی پی حقیقی استفاده شود تا در صورت لو رفتن خطری نداشته باشد. به عبارت دیگر برای امنیت بیشتر ، باید آی پی خود را به آی پی دیگری تغییر دهید.

- بهترین روش برای اینمنظور ، عدم استفاده از اینترنت منزل یا محل کار ، و به جای آن ، استفاده از کافی نت ها و همان سالن های اینترنت عمومی میباشد. (البته باید دقت کنید که سیستم های موجود در این مکان ها ، خود آلوده به تروجان یا نرم افزارهای جاسوسی نباشد. در ادامه به این موضوع خواهیم پرداخت)

- روش دیگر استفاده از پروکسی ها (Proxy) ها یا فیلترشکن ها برای تغییر آی پی است . (به سند آموزشی عبور از فیلترینگ توجه کنید). برنامه های فیلترشکن مثل : Ultra surf ، Free gate برای اینمنظور خوب است. این نرم افزارها علاوه بر اینکه شما را از سد فیلترینگ عبور میدهند ، آی پی شما را به یک آی پی دیگری تغییر میدهند. البته این روش فقط برای وبگردی و ایمیل تحت مرورگرهای وب (مثل Internet Explorer یا Firefox) مفید است و مثلا آی پی شما در مسنجرهای چت (مثل Skype یا Yahoo) تغییر نخواهد کرد.

چه وقت IP شما مشکل ساز شده و باعث شناسایی شما میشود؟

1- وقتی کامپیوتر شما هک میشود :

یک هکر(مهاجمی که به کامپیوتر دیگران نفوذ میکند) با دانستن IP شما در زمان اتصال شما به اینترنت می تواند وارد کامپیوتر شما شده و کنترل تمام کامپیوتر شما را در دست بگیرد و یا کارهایی که انجام میدهید را مشاهده یا ضبط کند و یا حداقل مشخصات کاربری و سیستم شما را مشاهده کند (که البته این خود نیازمند بکاربردن تکنیک های خاص و آلوده کردن کامپیوتر شما به تروجان و نرم افزارهای جاسوسی است) .

بنابر این :
- از بازکردن ایمیل های ناشناس ، بخصوص فایل های ضمیمه پرهیز کنید.
- همیشه ویندوز یا سیستم عامل دیگر خود را آپدیت (به روز رسانی) کنید. یک آنتی ویروس قوی روی سیستم خود نصب کنید و مرتبا آنرا آپدیت کنید. همچنین یک فایروال قوی یا همان نرم افزاری که جلوی نفوذ هکرها را سد میکند ، روی کامپیوتر خود نصب کنید و مرتبا آنرا آپدیت کنید.
- از رد و بدل کردن فایل با افراد ناشناس بخصوص در چت و مسنجرها ، پرهیز کنید.
- از کلیک کردن روی لینک های مشکوک با عناوین فریبنده خودداری کنید.

2- وقتی آی پی شما در سایت ها و وبلاگ هایی که بازدید میکنید ثبت میشود :

بسیاری از کاربران اینترنتی در ایران برای درج خاطرات روزانه یا بیان عقاید سیاسی و اجتماعی خود ، اقدام به تاسیس وبلاگ شخصی و یا درج نظرات خود در وبلاگ دیگران میکنند. بسیاری از سایت ها و وبلاگ ها ، توانایی ثبت اتوماتیک آی پی شما را دارند. اگر سرویس دهنده (سرور) اینگونه وبلاگ ها یا سایت ها ، غیرایرانی باشد مشکلی نخواهد بود مثل : بلاگر ، وردپرس ، ... ولی اگر ایرانی باشد مثل : پرشین بلاگ ، بلاگفا ، بلاگ اسکای ، میهن بلاگ و غیره ..... مشکل ساز خواهد بود بدان معنا که آی پی های ثبت شده در آنها میتواند به راحتی در دسترس وزارت اطلاعات و سایر مزدوران رژیم قرار گیرد، به همین دلیل است که این سرورها اعلام کرده اند که در محدوده قوانین جمهوری اسلامی فعالیت می کنند.

برای مثال ، امیدرضا میرصیافی ، وبلاگ نویس ایرانی به همین طریق به دام وزارت اطلاعات افتاد و دستگیر شد و در نهایت در زندان اوین در روزهای پایانی اسفند 87 به قتل رسید.

بنابراین اگر شما یک فعال اجتماعی یا سیاسی هستید هرگز از سایت هایی که در بالا ذکر شد استفاده نکنید و از درج پیام در آنها هم خودداری کنید ! استفاده از آنها بمانند دعوت از پلیس و وزارت اطلاعات برای دستگیری شماست!

بنابراین :
- برای تاسیس وبلاگ خود ، از خدمات سرورهای غیرایرانی مثل بلاگر یا وردپرس استفاده کنید.
- برای درج نظرات خود در وبلاگ دیگران ، از یک نرم افزار پروکسی یا فیلترشکن استفاده کنید ، در اینصورت آی پی شما تغییر خواهد کرد . برنامه های فیلترشکن مثل : Ultra surf ، Free gate برای اینمنظور خوب است. (به سند آموزشی "عبور از فیلترینگ" توجه کنید)

- همانطور که قبلا اشاره شد ، یک روش مفید هم این است که به جای استفاده از اینترنت در منزل یا محل کار خود ، در کافی نت ها و سالن های عمومی به اینترنت وصل شوید.

3- وقتی با شخص ناشناسی چت میکنید:

هنگامی که با کسی در یک مسنجر مثل یاهو یا اسکایپ یا ... چت می کنید ، مسنجر خود را بین شما و فرد مقابل قرار میدهد به اینصورت که شما و آن شخص به سرور مسنجر متصل می شوید و همه پیامها از آن سرور عبور می کنند. این بدین معنا است که پیام شما در ابتدا وارد سرور مسنجر می شود و سپس از طریق سرور مسنجر به فرد مقابلتان میرسد و بالعکس. خوب تا اینجا مشکلی نیست و آی پی شما شناسایی نخواهد شد ، ولی اگر شما و شخص در یک بازی مسنجری شرکت کنید یا فایلی را برای همدیگر ارسال کنید ، دو کامپیوتر به طور مستقیم به هم متصل می شوند ! در اینصورت آی پی شما را برای شخص مقابل ، قابل شناسایی است. همانطور که اشاره شد با روش های معمول از جمله استفاده از فیلترشکن ها ، نمیتوان آی پی را برای استفاده در مسنجرهای چت تغییر دهید و همان آی پی حقیقی شما

بنابر این :
- از چت کردن و ردوبدل کردن فایل در مسنجر با اشخاصی که نمی شناسید خودداری کنید .
- به جای مسنجرهای یاهو و ام.اس.ان که امنیت ضعیفی دارند و مکالمات در آنها توسط سیستم های جاسوسی قابل شنود و رهگیری است ، از مسنجر اسکایپ (Skype) استفاده کنید چون از پروتکل رمزنگاری استفاده میکند و قابل شنود و رهگیری نیست و امنیت بیشتری دارد.

2- مهندسی اجتماعی (تکنیک های جاسوسی و نفوذ به شیوه روان شناسی)

یک هکر یا مهاجم با برقراری ارتباط با شما و استفاده از تکنیک های خاص اجتماعی مثل : جلب اعتماد ، جلب توجه ، ریختن طرح دوستی با شما ، هم عقیده نشان دادن خود با شما ، جعل هویت یکی از دوستان شما و ...، سعی میکند به اطلاعات حساس موجود در کامپیوتر شما دست یابد و یا با شما قرار ملاقات بگذارد .

برای مثال : آقای "مظاهر" وبلاگ نویسی که در زمینه مسیحیت فعالیت داشت با آغاز دوستی و ارتباط با یکی از کاربران خود به نام "کشیش رضا" از طریق چت قرار ملاقات میگذارد. کشیش رضا در حقیقت یکی از ماموران اطلاعاتی رژیم بوده. با قبول این ملاقات ، مظاهر و خواهرش به محل ملاقات رفته و پس از درخواست کشیش رضا به مکانی دیگر میروند و در آنجا ناگهان با هجوم چند لباس شخصی و مزدور رژیم مواجه شده و سپس به بازداشتگاه نامعلومی منتقل میشوند.از سرنوشت آنها هنوز خبری در دست نیست.

مثال دیگر : مدیران سایتهای ایرانی پورنوگرافی (آویزون و ...) هم که چندی پیش دستگیر شدند ، در اروپا و کانادا اقامت داشته اند و از طریق مهندسی اجتماعی به ایران کشیده شده و دستگیر شدند.

سپاه پاسداران در قالب گروهی موسوم به "گرداب" یا بهتر است بگوییم " گندآب" ، مایل است که دستگیری این افراد را بعنوان درجه بالای علمی و فنی خود در علوم ردیابی کامپیوتری (نیروهای سایبری) نشان دهد اما واقعیت این است که مدیران سایت ها و وبلاگ ها بیشتر از طریق مهندسی اجتماعی به ایران کشانده شده و زیر شکنجه نام کاربری و پسورد سایت های خود را در اختیار مزدوران سپاه قرار میدهند .

استفاده از مهندسی اجتماعی توسط سازمانهای جاسوسی یکی از قدیمی ترین شیوه ها برای دستیابی به اطلاعات می باشد.

مثال دیگر :استفاده موساد از روابط جنسی یکی از جاسوسان خود با یکی از دانشمندان عراقی برای دستیابی به اطلاعات لازم درباره نیروگاه اتمی عراق . اسرائیل با استفاده از همین اطلاعات نیروگاه اتمی عراق را بمباران کرد.

بنابراین :
- به تلفن ها ، ایمیل ها و درخواست ملاقات هایی که عموما ناخواسته هستند ، مشکوک بوده و با دیده سوء ظن به آنان نگاه کنید . در صورتی که یک فرد ناشناس ادعا میکند که از یک سازمان معتبر است ، سعی نمائید با سازمان مورد ادعای وی تماس گرفته و نسبت به هویت وی کسب اطلاع کنید. (استعلام هویت)
- هرگز اطلاعات سایت خود را (مثل یوزر و پسورد) را در اختیار دیگران قرار ندهید و در جایی هم ننویسد و سعی کنید فقط از برکنید.
- هرگز اطلاعات حساس و مهم شخصی خود را بر روی اینترنت ارسال نکنید. در صورت ضروری بودن ارسال اطلاعات ، حتما از "شیوه رمزنگاری و ارسال محرمانه" استفاده نمایید . اطلاعات بیشتر در اینجا.
- مواظب روابط شخصی خود باشید و از دیدار با افراد ناشناس که صرفا در اینترنت با آنها تماس داشته اید خودداری کنید. از دادن شماره تلفن یا موبایل خود به آنان نیز خودداری کنید.

نکات امنیتی دیگر :

1- برای ایجاد اکانت ایمیل خود ، هرگز از سرورهای ایرانی استفاده نکنید چون امنیت پایینی دارند و همینطور میتوانند تمام نامه هایی که ارسال یا دریافت میکنید را در منابع خود ذخیره کنند ، که با توجه به دسترسی وزارت اطلاعات به آنها ، مشکل ساز خواهد شد. پس فقط از سرورهای خارجی مثل Gmail یا Yahoo یا Hotmail استفاده کنید چون امنیت بیشتری دارند و مزدوران رژیم هم قادر به کنترل آنها نیستند. از بین این سرورها ، سرویس Gmail امنیت بیشتری دارد ، چون هنگامی که ایمیلی ارسال میکنید ، آی پی شما را مخفی میکند و همچنین از رمزنگاری و پروتکل امن HTTPS استفاده میکند.

2- برای استفاده از ایمیل خود و دریافت و ارسال نامه ها، هرگز از برنامه های کنسولی مثل outlook express یا Microsoft outlook که روی کامپیوتر نصب میشوند استفاده نکنید. چون

این برنامه ها تمام نامه های ارسالی و دریافتی شما را روی کامپیوتر ذخیره می کنند ، و اگر کامپیوتر شما به سرقت رود یا هکری به آن نفوذ کند ، مشکل ساز خواهد شد و تمام نامه ها لو میرود .پس فقط از سرورهای خارجی که در بالا ذکر کردیم ، بطور آنلاین و با استفاده از مرورگر خود مثل Internet Explorer یا Firefox استفاده کنید. در اینصورت نامه ها روی کامپیوتر شما ذخیره نخواهد شد و از نظر امنیتی بهتر خواهد بود. برای خروج از محیط ایمیل خود هم همیشه Log off یا Sing off کنید تا اثری از آنچه در ایمیل انجام داده اید روی کامپیوتر شما باقی نماند.

3- تا جای امکان ، از ذخیره سازی اسناد شخصی روی هارد کامپیوتر خود ، مثل عکس یا فیلم یا فایل های صوتی یا متنی یا هر فایلی که منجر به افشا شدن هویت شما یا بستگان یا دوستان شما میشود ، خودداری کنید. در اینصورت اگر هم هکر به کامپیوتر شما نفوذ کند ، چیزی نصیبش نخواهد شد و قادر به شناسایی شما نخواهد بود. همچنین میتوانید برای ردگم کردن ، عکس های متفرقه دیگران را از اینترنت دانلود کنید و در کامپیوتر خود ذخیره کنید !

4- هرگز از نام حقیقی خود برای ایجاد اکانت ایمیل ، وبلاگ و ... استفاده نکنید ، بلکه از نام های مستعار استفاده کنید و سعی کنید فقط از یک نام مستعار هم استفاده نکنید و چند نام مستعار برای خود انتخاب کنید.

5- در هنگام نصب ویندوز ، Computer Name خود را هرگز نام حقیقی خود یا نامی مرتبط با خود انتخاب نکنید.

نام های عمومی مثل HOME یا USER که معمولا بعنوان پیش فرض قرار میگیرند ، میتوانند بسیار خوب باشند.

6- نرم افزارهایی مثل آفیس ورد ، اکسل ، فتوشاپ ، و ... را که قرار است با آنها فایل هایی را ایجاد و ویرایش کنید به هیچ وجه با نام حقیقی خود رجیستر نکنید. چرا که اینگونه فایل ها ممکن است برای قراردادن بر روی وب استفاده شوند. این فایل ها با خود اطلاعات سازنده یا نویسنده فایل (Author) را نگهداری می کنند و بعد از چندین بار دست به دست شدن هم باز نام نویسنده اصلی فایل بر روی آنها باقی می ماند. بنابراین به هیچ وجه موقع نصب اینگونه برنامه ها ، نام حقیقی خودتان را برای رجیستر کردن استفاده نکنید.

7- از هر فیلتر شکن یا VPN ای استفاده نکنید. هر کس میتواند به سادگی و با داشتن مقداری فضا در اینترنت که به عنوان مثال PHP را پشتیبانی کند، یک فیلترشکن راه بیندازد ، از

اینرو هر فیلترشکنی لزوما امن نیست ، چرا که تمامی فعالیت هایی که یک کاربر با استفاده از آن انجام میدهد ، در Log آن فیلترشکن یا VPN قابل ذخیره شدن هستند. از اینرو به تازگی وزارت اطلاعات ، تعدادی فیلترشکن و VPN قلابی را در اینترنت در سایت های مختلف با نام های فریبنده تبلیغ و بطور رایگان عرضه میکند که در حقیقت همگی ابزارهای جاسوسی خود وزارت اطلاعات و سپاه هستند. پس تنها از فیلترشکن های معتبر مثل UltraSurf یا Free Gate استفاده کنید. و از اعتماد به افرادی که مدعی ارائه فیلترشکن یا VPN هستند ، خودداری کنید.

8- اگر مدیر یک وبلاگ یا وب سایت سیاسی یا اجتماعی هستید ، از کونترهای ایرانی مثل وبگذر یا ... استفاده نکنید. استفاده از کونترهای غیرایرانی امنیت بیشتری دارد و معقول تر به نظر میرسد. برای اینمنظور statcounter که یک کونتر ایمن و رایگان میباشد را توصیه میکنیم.

همچنین برای ثبت دامین یا فضای سایت خود ، از شرکت های ایرانی استفاده نکنید. استفاد از شرکت های کانادایی ، امریکایی و اروپایی مطمئن تر و معقول تر میباشد.

9 - انتخاب پسورد پیچیده : همیشه یک پسورد (رمز عبور) قوی و پیچیده برای اکانت های خود (ایمیل ، وبلاگ ،....) انتخاب کنید تا شانس هک شدن آنها به حداقل برسد. برای اینمنظور موارد زیر را حین انتخاب پسورد در نظر داشته باشید :

- طول پسورد حداقل 8 کاراکتر (حرف) باشد.

-پسورد را مخلوطی از حروف بزرگ و کوچک و اعداد تصادفی و کاملا بی‌معنی انتخاب کنید.

-حتما یک حرف غیر الفبایی مثل _ یا $ یا @ یا ... در لابلای حروف و اعداد قرار دهید.

- هرگز کلمات مشهور یا معناداری از اعداد و حروف انگلیسی یا فارسی را در پسورد قرار ندهید ! چون هکرها معمولا دارای برنامه های حاوی لغت نامه های زبانهای مشهور هستند و با روش "بروت فورس" ابتدا به سراغ مطابقت پسورد با آن کلمات میروند. مثلا پسوردی مثل Hossein95 یا Ali478 به راحتی هک میشود !

-استفاده از کلید Space هم در بین حروف و اعداد مفید است.

- هرچند وقت یکبار ، پسوردهای خود را عوض کنید. (مثلا هر دو ماه یکبار)

- بعضی ها به دلایل زیادی مثلا مشکل در به خاطرسپاری پسوردها، وقتی میخواهند پسوردشان را عوض کنند ، آن را با کمی تغییر به پسوردی که قبلا داشته اند تغییر میدهند، مثلا پسورد اولی ToK_tomبوده و حالا به ToK_tom2و یا ToK_tom3 تغییر میده ند. یعنی در حقیقت یک شماره سریال به آخر پسورد قبلی اضافه میکنند. این مورد هم از نظر امنیتی مناسب نیست و بهتر است یک پسورد کاملا متفاوت با پسورد قبلی انتخاب کنید.

- هرگز پسورد خودرا در جایی ننویسید ! و فقط سعی کنید آنرا به حافظه خود بسپارید.

- در حین انتخاب پسورد ، از بکاربردن حروف یا اعدادی که سایرین با افشای هویت شما قادر به حدث آن باشند مثل تاریخ تولد ، شماره شناسنامه ، نام یا نام خانوادگی و از این قبیل خودداری کنید.

- برای اکانت های مختلف مثل یاهو ، هات میل ، جی میل ، پسورد ورودی ویندوز ، ...
پسوردهای مختلف انتخاب کنید تا اگر یکی از آنها هک شد ، بقیه لو نروند و در امان باشند.

با توجه به فاکتور های بالا ، مثلا یک پسورد خوب چیزی شبیه به این خواهد بود :

$ToKt@m_89-573$

آیا کسی به غیر از خود شما به اکانت جی میل (Gmail) شما دسترسی داره یا خیر؟ به عبارت دیگه آیا کسی جی میل شما رو هک کرده یا خیر؟ و اگر جواب مثبته ، از کجاها وارد اکانت شما میشه ؟

همانطور که میدانید بعد از وارد شدن به اکانت جی میل خود از طریق یک کامپیوتر، یک نشست (Session) ایجاد و ثبت میشود. تا زمانیکه از اکانت خارج نشوید ، این نشست روی آن کامپیوتر باقی میماند و نفر بعدی که با آن کامپیوتر کار کند قادر خواهد بود بدون دانستن پسوورد شما، وارد اکانت شما شده و ایمیل های شما را بخواند. برای همین توصیه میشود که همیشه در کافی نت ها و سالن های عمومی اینترنت ، بعد از مطالعه یا ارسال ایمیل ها ، اول از اکانت خود خارج شوید (Log offیا Sign off کنید) و سپس مرورگر را ببندید.

حالا فرض کنید در اثر رعایت نکردن این نکته امنیتی یا به هر دلیل دیگری ، پسورد جی میل شما هک شده باشه ، حالا باید چه کار کنید؟

ابتدا از امکان جدید جی میل ، بنام "رهگیری نشست ها " استفاده کنید تا ببنید آیا واقعا شخص یا اشخاص دیگری غیر از شما وارد اکانت ایمیل شما میشوند یا خیر. در صورتیکه مطمئن شدید که اکانت شما هک شده ، پسورد خود را بلافاصله عوض کنید.

البته باید از مرورگر IE 7 یا FireFox 3 استفاده کنید.و ورژن جی میل هم باید به روز باشد.

سپس به ترتیب زیر عمل کنید:

مطابق معمول ، با وارد کردن یوزر و پسورد وارد اکانت خود شوید. پاورقی جی میل ، وقتی که وارد Inbox میشوید به صورت زیر خواهد بود:

Select: All, None, Read, Unread, Starred, Unstarred

Archive | Report spam | Delete | Move to ▾ | Labels ▾ | More actions ▾ | Refresh | 1 - 1 of 1

Get your mail **on your mobile phone** at http://mail.google.com/a/tondar.org/ using your phone's web browser.

You are currently using 0 MB (0%) of your 7317 MB. اینجا را کلیک کنید

Last account activity: 1.5 hours ago at this IP ( ). Details

tondar.org Mail view: standard | turn off chat | basic HTML Learn more

©2009 Google - Terms of Service - Privacy Policy - Program Policies - Google Home

Powered by Google

که مطابق شکل بالا ، روی Details کلیک میکنید تا جدول زیر نمایش داده شود.

Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. Learn more

This account is open in one other location.
(*Location* may refer to a different session on the same computer.)

Concurrent session information:

Access Type [?] (Browser, mobile, etc.)	IP address [?]
Browser	228.58.8.6

Sign out all other sessions

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	IP address [?]	Date/Time (Displayed in your time zone)
Browser	127.1.25.30	5:02 pm (0 minutes ago)
Mobile	230.10.10.2	11:17 am (5 hours ago)
Browser	228.58.8.6	9:42 am (7 hours ago)
POP3	230.9.19.17	6:30 am (10 hours ago)
Browser	228.58.8.6	Jun 29 (18 hours ago)

* indicates activity from the current session.

This computer is using IP address 127.1.25.30.

مشاهده میکنید که جدولی باز میشود بنام Activity on this account(فعالیت های این اکانت) ، که مشخصات تمام نشست ها یا همان دسترسی ها به اکانت شما را نشان میدهد.
مشخصاتی از قبیل : IP هایی که با آنها وارد اکانت شدید/شدند ، نوع دسترسی ، تاریخ و زمان.

همینطور قسمتی با عبارت زیر نمایش داده میشود :

This computer is using IP address :xxx.xxx.xxx.xxx

که در حقیقت آدرس IP شما را مشخص میکند و میتوانید آنرا با سایرIP های جدول مقایسه کنید تا مطمئن شوید که آیا شخص دیگری هم به اکانت شما دسترسی داشته یا نه.

اگر مطمئن شدید که اکانت شما هک شده ، روی قسمت sign out all other sessions کلیک کنید تا تمام نشست ها بسته شود و بلافاصله به سراغ تعویض پسورد اکانت خود بروید.

البته ممکن است ابتدا با دیدن IP های مختلف ، نگران شوید و فکر کنید که اکانت شما توسط شخص دیگری هک شده . خیلی از این نگرانی ها ممکن است بی مورد باشد و در حقیقت آن IP های دیگر خود شما باشید !!! مثلا اگر :

1- اگر از اینترنت Dial Up استفاده می کنید ، به ازای هر بار که به اینترنت وصل می شوید، یک IP جدید به شما اختصاص داده میشود. و در حقیقت IP های مختلفی که همگی متعلق به خود شماست در این جدول نشان داده خواهد شد. پس اگر از دایل آپ استفاده میکنید ، فقط به زمان ها و ساعت هایی که وارد اکانت خود میشوید توجه کنید. میتوانید آنها را در جایی برای خود یادداشت کنید و هرچندوقت یکبار با مشخصات جدول مقایسه کنید.

2- اگر از اینترنت ADSL استفاده میکنید، در صورتیکه شبکه به شما یک IP استاتیک اختصاص نداده باشد، IP شما دینامیک است و در اینصورت بازهم سناریوی بالا تکرار میشود چون IP دینامیک هم مدام تغییر میکند. پس باز هم مثل بالا ، فقط به زمان ها توجه کنید..

3- اگر از جاهای مختلفی وارد اکانت خود شده باشید، مثلا کافی نت ها و سالن های اینترنت عمومی در دانشگاه ها و .... ، باز هم سناریوی بالا تکرار میشود چون هر جایی IP جداگانه ای دارد. پس باز هم مثل بالا ، فقط به زمان ها توجه کنید.

برای ردیابی IP ها و اینکه ببینید از کجا به اکانت شما وارد شده اند/شده اید میتوانید از یک سایت ردیاب آی پی (Whois IP) استفاده کنید. کافیست در جستجوگر گوگل آنرا جستجو کنید و یا به سایت زیر بروید :

http://www.ripe.net

پاک کردن سیستم از فایل های جاسوسی و مخرب:

Key Logger چیست؟

Log به معنای رویدادنگاری و یا واقعه نگاری هست. به زبانی ساده تر یعنی ثبت و ضبط کردن فعالیت ها. بنابراین Key Logger یعنی ثبت کننده کلید. پس فایل های "کی لگر" میتوانند در

صورتیکه روی سیستم شما نصب شده باشند ، تمامی کلیدهایی که شما هنگام کار با کامپیوتر می فشارید رو ثبت کنند ، در یک فایل ذخیره کنند و به یک شخص دیگر (هکر) بفرستند. نظیر نام کاربری، پسورد، متن ایمیلهایی که تایپ می کنید، متن چت ها، ، آدرس سایت هایی که بازدید میکنید و هر فعالیت دیگری از این قبیل . در حالت پیشرفته تر، حتی قادرند از کلیه کارهایی که در ویندوز انجام میدهید(تماشای فیلم ، عکس ،....) عکس بگیرند و برای هکر ارسال کنند !!!

پس کی لاگرها در زمره نرم افزارهای جاسوسی (تروجان ها) قرار میگیرند.

تروجان چیست ؟

تروجان ها، فایل های جاسوسی هستند که در قالب یک فایل به اصطلاح بی آزار وارد سیستم میشوند (از طریق ضمیمه ایمیل های آلوده یا لینک های آلوده) و سپس کامپیوتر رو آلوده می کنند و مثل یک جاسوس ، اطلاعات مختلف که در بالا اشاره شد را از کامپیوتر قربانی به کامپیوتر هکر میفرستند.

چگونه فایل های جاسوسی و مخرب را تشخیص دهیم و از بین ببریم ؟

بیشتر آنتی ویروس ها مثل Kaspersky یا Nod32 یا Norton علاوه بر تشخیص و از بین بردن ویروس ها ، قادر به تشخیص و از بین بردن بیشتر تروجان ها هم هستند. با اینحال همیشه تروجان های جدید در اینترنت پخش میشوند ، پس سعی کنید یک آنتی ویروس قوی روی سیستم خود نصب کنید و آنرا مرتبا به روزرسانی (آپدیت) کنید.

این هم ویروس یاب آنلاین Norton که نیاز به نصب ندارد و بطور آنلاین میتواند سیستم شما را اسکن کند. البته این امکان آنلاین ، قادر به پاک کردن ویروس نیست و باید بعد از شناسایی ویروس ، خودتان ویروس را حذف کنید و یا به سراغ آنتی ویروس دیگری بروید.

در ضمن به همراه یکی از آنتی ویروس های بالا ، یک برنامه آنتی تروجان مثل Trojan Remover هم روی سیستم خود نصب کنید.

همینطور یک فایروال قوی مثل Comodo یا ZoneAlarm هم روی سیستم خود نصب کنید. فایروال خود ویندوز xp را هم فعال کنید.

نصب برنامه های فوق ممکن است باعث کاهش سرعت پردازش سیستم شما شود ، ولی با توجه به اهمیت امنیتی آنها ، اجتناب ناپذیر هستند. پس اگر با کاعش سرعت سیستم مواجه شدید ، سیستم خود را ارتقا دهید. (CPU و RAM خود را با مدل های بهتر و پرسرعت تر تعویض کنید)

برای تشخیص اینکه آیا روی سیستم شما کی لاگری نصب شده یا نه؟

میتوانید از فایل Gernova Keylock استفاده کنید که به زبان آلمانی هست. بعد از آنزیپ و نصب کردن، اجراش کنید و روی Suchlauf Starten (آغاز جستجو) کلیک کنید تا یک اسکن طولانی شروع شود. اگر با پیغام Restart روبرو شدید آنرا تایید کنید.

نکته : موقع اجرا شدن این فایل ، نشانگر موس شما برای مدت کوتاهی ممکن است مدام به اطراف حرکت کند. این کار توسط خود برنامه برای کنترل و تست رفتارهای موس میباشد پس نگران نباشید !

نکته : در حین اجرا شدن ، برنامه 3 بار از شما میخواهد که حروف یا اعدادی را به عنوان داده ، به دلخواه خود وارد کنید. این هم مربوط به تست های برنامه است که در برابر کی لاگر های احتمالی و کنترل واکنش اون ها انجام میشود.

در پایان هم، برنامه هایی که به صورت بالقوه خطرناک هستند ، لیست میشوند. البته همه آنها الزاما خطرناک نیستند پس در پاک کردن آنها مراقب باشید تا به سیستم عامل صدمه نخورد.

امن سازی کیبرد در مرورگرهای Internet Explorer و FireFox :

Keyscrambler نرم افزاری است که حروفی که در مرورگر اینترنتی خود تایپ میکنید را رمزنگاری میکند تا اگر کی لاگری روی سیستم شما نصب شده باشد و حتی آنتی ویروس هم قادر به تشخیص آن نباشد، خنثی شده و کلیدهایی رو دریافت کند که رمزشده هستند و بنابراین هکر نخواهد توانست حروف اصلی تایپ شده را مشاهده کند.

مقابله با حملات Exploit ، Phishing و Fake Login :

روش های حمله دیگری که هکرها برای نفوذ به کامپیوتر سایرین استفاده میکنند عبارتند از : ارسال لینک های صفحات آلوده به اسکریپ های مخرب (Phishing یا Exploit) و صفحات لوگین تقلبی (Fake Login) .

به اینصورت که مثلا یک هکر می آید و لینک یک صفحه را به شما از طریق ایمیل یا در چت میفرستد ، و هنگامیکه شما روی آن لینک کلیک میکنید با صفحه ای مواجه میشود که همانند صفحه لوگین یاهو یا جی میل یا پی پل و ....طراحی شده و دارای کادرهایی برای واردکردن یوزر و پسورد است. طبیعی است که خیلی ها فریب این صفحات تقلبی را میخورند و بلافاصله یوزر و پسورد خود را وارد میکنند ، غافل از اینکه این مشخصات بلافاصله به هکر ارسال میشوند و هکر قادر خواهد بود به اکانت های قربانی دسترسی پیدا کند !

روش فیشینگ و اکسپلویت هم به اینصورت است که شما روی لینک آلوده کلیک میکنید و وارد صفحه ای میشوید که دارای کدها و اسکریپ های آلوده است و میتواند از طریق کوکی ها و یا با

تکنیک های دیگر ، اطلاعات مهم کامپیوتر شما مثل یوزرها و پسوردها و.... را سرقت کند و به هکر بفرستد و یا راه را برای ارسال و نصب ناخواسته تروجان ها روی کامپیوتر شما بازکند بطوریکه آنتی ویروس شما قادر به تشخیص آنها نباشد. و کلی تکنیک های عجیب و قریب دیگر !!!

راه های مقابله :

1- هرگز به لینک های مشکوک که در چت یا ایمیل به شما فرستاده میشود اعتماد نکنید و روی آن کلیک نکنید. یک کلیک میتواند سیستم شما را آلوده کند. خیلی از این لینک ها با عناوین فریب دهنده طراحی میشوند تا بتوانند کاربر را گول بزند و وی را وادار به کلیک کردن کنند. مثلا عناوین تحریک کننده سکسی ، و یا اخبار جعلی مثل " جورج بوش ترور شد!" و از این قبیل . که معمولا با بهره گیری از تکنیک های خاص روانی برای جلب توجه خواننده طراحی میشوند.

2- هرگز فایل ها یا نرم افزارهای ناشناس را از سایت هایی که نمی شناسید دانلود نکنید. همینطور از دریافت فایل از افراد ناشناس در چت خودداری کنید. بسیاری از این فایل ها در نگاه اول بعنوان عکس یا موزیک هستند ولی در حقیقت فایل های آلوده به ویروس و تروجان هستند که در صورت دانلود و اجرا شدن ، امنیت سیستم شما را تهدید خواهند کرد.

3- فایل های Temporary Internet Files یا همان Cash مرورگر خود (که حاوی کوکی هستند) را به طور مرتب پاک کنید.

4- تنظیمات مرورگر خود را طوری تنظیم کنید تا پنجره های pop-up (که بطور ناخواسته همراه با صفحات دیگر باز میشوند) را بلوک کند تا باز نشوند.

5- اگر از مرورگر اینترنت اکسپلورر استفاده میکنید ، سطح امنیتی آنرا در متوسط یا بالای متوسط قرار دهید. برای اینمنظور به منوی Tools سپس Internet options رفته و به زبانه security بروید و در آنجا سطح امنیتی را روی وضعیت Medium High قرار دهید. با این کار جلوی نصب و اجرای خودبخود اکتیوایکس ها و جاوااسکریپت ها و کوکی های خطرناک (امکاناتی که هکرها با سوءاستفاده از آنها به سیستم شما نفوذ میکنند) گرفته خواهد شد و مرورگر شما امنیت بیشتری خواهد داشت.

6- اگر از مرورگر فایرفاکس استفاده میکنید ، افزونه امنیتی NoScript را دانلود و نصب کنید. با این کار جلوی نصب و اجرای خودبخود اکتیوایکس ها و جاوااسکریپت ها و کوکی های خطرناک (امکاناتی که هکرها با سوءاستفاده از آنها به سیستم شما نفوذ میکنند) گرفته خواهد شد و مرورگر شما امنیت بیشتری خواهد داشت.

7- ایمیل های ناشناس و ناخواسته با عناوین یا محتویات عجیب و قریب را هرگز باز نکنید ، بخصوص ضمیمه های آنها (فایل هایی که همراه آنها فرستاده میشوند) میتوانند بسیار خطرناک باشند. اینگونه ایمیل ها را هرگز باز نکنید و به عنوان Spam یا Phishing گزارش و بلوک کنید.

8- سعی کنید یوزرنیم و پسوردهای خود را در مرورگرهای خود ذخیره نکنید .هینطور قابلیت های Auto Complete و Auto Save را از تنظیمات مرورگرهای خود غیرفعال کنید. برای ذخیره پسوردهای مختلف خود در مرورگرها و سهولت در بکاربردن آنها ، افزونه امنیتی Roboform را پیشنهاد میکنیم.

نکات امنیتی پیشرفته تر :

نکات زیر مربوط به محدودکردن شبکه (Networking) یک سیستم است. رعایت این نکات میتواند در امنیت بیشتر سیستم شما نقش به سزایی ایفا کند ، با اینحال نسبت به نکات قبلی ضروری نیستند. به خصوص اگر کامپیوتر شما با کامپیوترهای دیگر ، شبکه نشده باشد. در اینصورت نیازی به این تنظیمات نیست :

1- قابلیت Sharing Documents and Folders (به اشتراک گذاری فایل و پوشه ها در شبکه) را در سیستم خود غیرفعال کنید. برای این منظور میتوانید از برنامه TuneUp Utilities استفاده کنید.

روش دیگر برای اینمنظور ، مسیر زیر در رجیستری ویندوز (Regedit) است :

قدم اول : مسیر زیر را در رجیستری پیدا کنید :

Hkey-current-user> software> microsoft> windows> current-version> policies> explorer

بعد یک مقدار از نوع Dword ایجاد کنید با نام NoSharedDocuments و مقدار 0 .

قدم دوم : مسیر زیر را در رجیستری پیدا کنید :

Hkey-local-machine> software> microsoft> windows> current-version> policies> explorer

بعد یک مقدار از نوع Dword ایجاد کنید با نام NoSharedDocuments و مقدار 0 .

قدم سوم : مسیر زیر را در رجیستری پیدا کنید :

Hkey-local-machine> software> microsoft> windows> current-version> explorer> my computer> name sspace> delegate folders

بعد مقدار {.....-a47-3f72-44a7 } را پاک کنید.

قدم چهارم :

به My Computer بروید و وارد منوی Tools شده و به Folder Options بروید و از آنجا وارد زبانه View شوید ، در لیستی که باز میشود گزینه Use simple file sharing را پیدا کنید و تیک آنرا بردارید.

قدم پنجم :

روی My Computer راست کلیک کنید و به قسمت Manage رفته و لیستی که باز میشود وارد Shared Folders شوید. در آنجا در قسمت سمت راست وارد shares شوید و پوشه هایی که در آنجا قرار دارد را پاک کنید. همینطور اگر کسی (سیستمی) به منابع به اشتراک گذاشته شما دسترسی داشته باشد در قسمت sessions نمایش داده میشود که میتوانید آن دسترسی ها را قطع کنید.

2- قابلیت NetBIOS را در سیستم خود غیرفعال کنید. اطلاعات بیشتر در اینجا.

3- قابلیت Remote Desktop را در سیستم خود غیرفعال کنید. اطلاعات بیشتر در اینجا.

M.E

با همکاری روزبهان 7105

تکاوران تندر – انجمن پادشاهی ایران

www.takavaran-tondar.tk

پایان سند