شیوه‌های گوناگون سرقت رایانه‌ای

نوشته: بهنام صبحی شیشوان

هدف از نگارش این مکتوب نه آموزش بزه الکترونی بلکه آشنائی اساتید محترم و وکلای فرهیخته کانون با این پدیده بس مفید در عین واحد خطرناک می‌باشد.

امروزه استفاده از رایانه به عنوان وسیله کمکی بلکه به عنوان یک لزوم در انجام امورات روزانه درآمده و علم کاربردی این وسیله بطور اعجاب انگیزی در حال پیشرفت صعودی می‌باشد و خوشبختانه هر روز شاهد آن هستیم که در کشور ما بر تعداد کاربران اینترنت افزوده شده و این تکنولوژی جدید قرن بیستم میرود جای خود را در میان ایرانیان باز کند. اگر چه با ظهور اینترنت خدمات بی‌شائبه‌ای به مردم سراسرگیتی از قابلیت های سحر انگیز این شبکه جهانی به عرصه ظهور رسیده ولی بستر ساز نمود جرایم بیشماری نیز می‌باشد.

حال با عنایت به تعریف حقوق جزا اختصاصی..... که شامل تعریف انواع جرمها و تشریح شرایط و ارکان قانونی و مجازات خاصه..... و عطف به ماده ۲ قانون مجازات اسلامی در تعریف جرم... (هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده باشد جرم محسوب میشود....) وجوب امعان نظری جدی بر این مهم لازم میگردد.

در بیان این مهم آشنایی وکلا فرهیخته با بعضی از مسائل این پدیده به عنوان واجب قهرائی درآمده و این انگیزه گشت بر لزوم نگارش این مقاله.

در پهنه این مهم تنها با استفاده از پست الکترونیکی یا E-MAIL می‌پردازم.

برای آشنایی و تصور و درک وسعت و پهنه این علم، پاسخگوئی شما به سوالات زیر می‌تواند راهگشائی مناسب باشد.

آیا می‌دانید یک هکر(سارق کامپیوتری) توانائی ضبط صدای محیط اطراف رایانه را دارد.

آیا می‌دانید یک هکر (سارق کامپیوتری)توانایی کنترل دستگاه رایانه شما را دارد؟

آیا می‌دانید یک هکر (سارق کامپیوتری) توانایی روشن نمودن دستگاه شما و ضبط تصاویر دفتر یا منزل شما را دارد؟

آیا می دانید یک هکر (سارق کامپیوتری) توانایی دستکاری ، ارسال و دریافت کلیه اطلاعات تصاویر و هر فایلی را از دستگاه شما دارد؟

آیا می دانید یک هکر می‌تواند با نام شما و با استفاده از رایانه شما اقدام به هک کردن دیگران نماید؟

به یاد داشته باشید یک HACKER جزء نخبگان علمی جامعه می‌باشد و با یک بزهکار خیابانی تفاوت بسیار دارد. آیا می‌دانید برای هکر (سارق کامپیوتری) تنها ۱۵ دقیقه وقت و انگیزه و مجهز بودن قربانیش به یک دستگاه رایانه و تنها یکبار استفاده‌اش از اینترنت یا پست الکترونیکی برای او کافیست؟

شاید بگویید دستگاه رایانه من معمولاً خاموش است.

شاید بگویید من حتی رایانه خود را از برق هم جدا میسازم و فیوز و کلید را قطع میکنم.

شاید بگویید من تنها گهگاهی آنهم فقط نامه های الکترونیکی E-mail خود را چک می‌کنم.

شاید بگویید من حتی ارتباط رابط خط تلفنی را هم قطع میسازم.

شاید بگویید من از فیلترها firewall های ویژه استفاده میکنم.

در همه موارد پاسخ‌ها یکی است شما یک victim هستید.(به هدف یک هکر victim یا قربانی میگویند).

حال چه باید کرد؟ ترسید و رایانه خود را در چاله‌ای اطراف تهران خاک کرد و یا آرزو کنیم که خدای ناکرده خیال و هوس و انتخاب ما به عنوان victim را ننماید؟

من در این مجموعه آموزش سرقت را به عنوان بهترین و کاربردی ترین روش جلوگیری از این پدیده و آشنایی و درک فاجعه ای بزرگتر و شناخت اساتید محترم با شیوه‌های جدید بزه را برگزیده و سعی در آشنائی شما می‌نمائم. باشد تا مقبول افتد.

پیشدرامد و جرقه ساخت و ابزار این گونه سرقت‌ها و ساخت ابزار HACK بسیار شنیدنی و جالب و البته برای من به عنوان یک ایرانی با دارا بودن تمدنی ۲۵۰۰ ساله البته دل ازآرو موجب افسردگی و دریغ و باز هم افسوس است و بیادآورنده جام جم. جامی که در دست داریم و ز بیگانه تمنا میکنیم.

اجازه می‌خواهم برای شما افسانه‌ای تعریف کنم که قطعاً به شما در درک بهتر مسئله کمک خواهد کرد.

افسانه از اینجا آغاز می‌گردد که در ۱۲ قرن پیش از میلاد دو قبیله با نامهای troy و greeks به مدت ۱۰ سال با هم می‌جنگیدند ولی هیچکس موفق به غلبه بر دیگری نمی‌شدند .greeks دارای سپاهیان بسیار در عین حال ورزیده و باهوش بودند و troy دارای قلعه‌ای محکم که به شکست ناپذیر ملقب شده بود. سرانجام greeks با بکار بردن ترفندی به قلعه troy ها نفوذ کرده و بر آنها پیروز و مسلط شدند greeks ها تندیس فوق العاده بزرگی از چوب به شکل یک اسب ساختند و گروهی از سربازانشان را در آن قرار دادند. سپس این مجسمه غول پیکر را به کمک چرخهایی که در زیر آب تعبیه کرده بودند تا نزدیکی دربهای قلعه troy ها آورده و بعد از آنجا گریختند. tory های ساده لوح به گمان اینکه این یک هدیه از طرف greeks ها است پس از فرار از آنان مجسمه بزرگ را به عنوان نماد پیروزی داخل قلعه خود کرده و مشغول برگزاری جشن و شادمانی شدند. غافل از اینکه شب هنگام زبده ترین سربازان greeks از داخل آن بیرون آمده و درهای قلعه را برای ورود بقیه سربازان باز خواهند کرد. دقیقاً همین مسأله بر روی کامپیوتر قربانی اتفاق خواهد افتاد. بدین ترتیب که هکر(نفوذگر) فایلی را برای فرد قربانی(همان اسب چوبی غول پیکر) می‌فرستد. و قربانی به گمان آنکه این فایل مثلاً تصویری یا فاکسی یا متنی یا موزیکی دلنشین است آنرا اجرا می‌کند (یعنی همان اسب چوبی غول پیکر را به قلعه خود داخل می‌کند) که در این صورت از این لحظه به بعد هر زمان به محض ورود مجدد کامپیوتر قربانی به اینترنت دربهای کامپیوتر وی (همچون درب قلعه troy ها) بر روی هکر باز خواهد شد و این امکان را پیدا خواهد کرد تا هر بلایی که مایل است بر سر فرد قربانی و کامپیوترش بیاورد.

یک سارق کامپیوتری جزء نخبگان علمی جامعه است و با یک بزهکار خیابانی تفاوت بسیاری دارد

این افسانه دستاویزی گشت برای نگارش نرم افزارهائی برای نفوذ که این نرم افزارها TROJAN نام گرفتند. HACKER باید مانند اسب تروا ابتدا بسته ای همانند اسب چوبی حاوی سربازان وارد رایانه شما نماید و بعد از آن بنشیند و پیروزی خود را جشن بگیرد.

از جمله نرم افزارهای معروف netbus و یا subv و یا back orifice می‌باشد.

تمام این نرم افزارها شامل ۳ بخش می‌باشند.

۱- SERVER که باید با یک ترفندی برای قربانی ارسال شود

۲- CLIENT بهترین و جالب ترین قسمت است و در رایانه خودش نصب میشود

۳- EDIT SERVER در این بخش شما می‌توانید SERVER خود را ویرایش نمائید.

به یاد دارم دوست ارجمند و همکار دانشمندم را در امری همراهی میکردم. در بین راه علت نگرانی و دغدغه‌اش را جویا شدم . که نقل آن برای شما خالی از لطف نیست.

این عزیز فرمودند موکلی دارم که پرونده اش زندگی ام را متحول کرده. با توجه به شناخت چندین ساله از وی برایم جالب بود. بیشتراصرار کردم. پس از فرارهای بسیار از پاسخ بالاخره تسلیم شد و داستان را نقل کرد.

از جانب آقای م با خانم ا-ن آشنا شدم. آقای م که خواستگار این بانو بسیار ثروتمند بوده با توسل به رمالها ، فالگیرهای شهرهای مختلف درصدد دفع ارواح خبیس برآمده ولی با تقبل یازده میلیون تومان کماکان مغلوب این ارواح است. تازه کار را به تهدید اینجانب نیز رسانده اند و اخطار داده اند. داستان برایم جالب شده بود و اعتراف می‌کنم اشتیاق کنجکاوی در اوج خود. نکته جالب تر این بود که دوست من اصلاً به این گونه موارد اعتقاد نداشت، حال چه مهمی پیش آمده که او را این چنین هراسان کرده جالب بود .

خانم م پس از مراجعه از سفر خارج خود که به قصد تجدید دیدار از خانواده بـه منزل مراجعه مینماید کاغذهای در اطاق خود روی زمین توجهش را جلب میکند که با فحاشی بسیار او را به عالم دیگر فرا می‌خوانند.
نکته در این بود که ارواح حتی از آشنائی پنهانی وی در این سفر با شخصی در ایتالیا نیز خبر داشت. و اخبـاری میداد که حاکی از حداقل آشنائی مستقیم داشت. رنگ چشم . گروه خونی قد سن تلفن و... داسـتان از اینجا شـروع می‌شـود که بـا توجه به زندگی مجردانه تمام شک‌ها متوجه موکل(آقای م) از همه جا بی‌خبر می‌شود که حتماً مرا تعقیب کرده ، برایم بپا گذاشته و تا ایتالیا مرا تعقیب کرده، و شک و تصور خود را به یقین تبدیل کرده و گوشی را برداشته و بـار گناهان و ترس خود را سر موکل من پیاده میکند. و خواستار قطع رابطه از چنین فرد فضول و ترسوئی میشود که حتی جرات اعتراف هم ندارد. در انتها از روی لجبازی اقرار به آشنائی با فرد جدید میکند و بیان میکند از آدمهای مرد نما و غیرتی بیزار اسـت . . . میتونستم قیافه بـهت زده‌اش را تجسـم کنم. ولی داسـتان در نیمه شـب بـا روشـن شـدن ناگهانی کامپیوتر و چاپ همان نوشته‌ها به همراه صداهای ترسناک و با صدای بسیار بلند به مرحله جدیدی رسید. ظاهر شدن نوشته‌هائی روی رایانه و معرفی خود بـه روح سرگردان و دادن اطلاعاتی از خانواده پدر مادر آهنگ های مورد علاقـه مهمانی هائی که سـالها پیش رفته حـتی لباسـی که در حـال حـاضر پوشـیده و یا بـه پخش صدای خودش که ۳ سـاعت پیش بـا تلفن حـرف زده دخترک را تسلیم بی چون و چرا و خلع سلاح مطلق نمود. اما نکته‌ای که دوست عزیزم هم به آن توجه ننمود بود این بـود که گفت : جالبه ارواح به اشیاء عتیقه علاقمندند. دخترک را به بـهانه آرامش ارواح خانوادگی روح مهاجم مجبـور بـه خرید عتیقه‌ای از مغازه‌های در خیابان فرشته نموده و امر کرده به بیابان اطراف اندیشه برود و در محلی که عنوان کرده محل کشف این اجناس بوده دوباره دفع نماید.
. . . وکیل محترم توجه نکرده بود بـه فرض هم که ارواح دنبـال اشـیاء عتیقـه بـرای آرامش خود باشـند دیگر چرا دنبـال مغازه‌های خیابان فرشته هستند. لابد روح از خانواده اصیل قاجاری بوده. . . .
میبینید عدم آشنایی با این بزه و عدم اطلاع از علوم رایانه جای عقل و خرد با خرافات پر میشود.
با hack کردن رایانه خانم و دیدن تمام اطلاعات ذخیره شده وی و حتی دیدن نامه الکترونیکی که از ایتالیا رسـیده بـود قبل از دستیابی (خانم ا- م) و پاک کردن آن و دیدن پروفایل ارسال کننده نامه و عکس وی و دیدن عکسـهایی که در رایانه بودند بانضمام روانشناسی ذکاوتمندانه دست به دست هم در جهت اغفال و انجام اعمال متقلبانه می‌گردد.
با تبدیل speaker بلندگوهای رایانه به میکروفون صدای خانه را ضبط میکرده و با روشن کردن webcam تصویر از اطاق وی هم داشـته و بـا روشـن کردن printer و چاپ نامه‌های مکرر تهدید آمیز نامه ها را در کف اتاق منظره قابـل توجهی را پدید آورده بود حال با آشنا شدن با این نرم افزارها و راههای hack کردن بهترین گزینه را بـرای جلوگیری از این اعمال می‌یابید
همانگونه که متذکر شـدم هر trojan شـامل ۳ بـخش است. بـخش نخسـت که در server نام دارد و همان اسـب تروا میباشد میبایست با ترفندی برای قربانی ارسال شود. ارسال این بسته بـه روانشناسـی شـخص قربـانی و ذکاوت شما بسـتگی دارد. بسـیار دیده شـده از طریق نامه انجام شـده. در قسـمت ۳ که مخصوص ویرایش server اسـت بـا انتخاب attach file میتوان این server را به هر فایلی چسبـاند. مثلا بـه نامه‌ای یا فکسـی یا قـطعه موزیکی یا عکسـی یا... در همین قسمت گزینه ای دارد که با انتخاب آن server بعد از ورود به رایانه قربـانی victim در ۰/۰۰۰۱ ثانیه نصب و خود بخود پاک و محو میشود.
قابل ذکر است server که به فایل attach شده پنهان hidden است و غیر قابل دید.
ساده‌ترین روش این است که به رایانه قربانی دستیابی داشته باشیم و در کمتر از ۱ دقیقه میتوان نرم افزار را نصب کرد.
یکی دیگر از روش‌ها این است برای قربانی نامه ای آلوده به server ارسال کنیم.
یکی دیگر از روشها است قربانی وارد به سایت آلوده به server شود.
یکی دیگر از روشها این است برای قربانی cd آلوده به server ارسال کنیم.
تصور فرمائید برای شما نامه‌ای ارسال شده باشد بـا اسـم موکلی یا از جانب سـازمانی یا شـخصی یا ارگانی همین که نامه را باز کنید در کمتر از ۰/۰۰۰۱ ثانیه نصب و محو می‌گردد و تنها چیزی که می‌بینید یک نامه ساده است . بعد از نصب server کار خودش را سریعاً و پنهانی شروع میکند. ابتدا تمام رمزهای رایانه به انضمام رمزهای اینترنتی که شما از آن استفاده کرده اید مشخصات دقیق دستگاه شـما و کلیه اطلاعات مورد نیاز را از طریق e-meil بـرای hacher ارسـال می‌نماید. حال حتی اگر قربانی دستگاه خود را خاموش نماید و رابط خط تلفن را هم قطع نماید، server به کار خود ادامه میدهد و منتظر می‌ماند در اولین باری که شما دوبـاره ONLINE شـوید تمام این ارتبـاط و اطلاعات را بـرای HACHER ارسال و وی را از ONLINE شدن قربانی با خبر می‌نماید.
در قسمت ۲ که در رایانه HACHER می‌باشد و از آن به شیرین ترین قسـمت نام می‌بریم و client نام دارد و ثمره کار است پنجره‌ای باز می‌شود که گزینه ها و توانائی های زیر را دارا می‌باشد:
۱- باز کردن درب CD-ROM رایانه قربانی
۲- روشن و خاموش کردن MONITOR رایانه قربانی ۳- دریافت اطلاعات از رایانه قربانی
٤- پاک کردن هر قسمت از رایانه قربانی

۵- روشن و خاموش کردن و چاپ هر نوشته‌ای بر PRINTER رایانه قربانی

۶- ظاهر کردن هر متنی بر روی دستگاه قربانی

۷- مشاهده صفحه روی کامپیوتر قربانی و مشاهده چیزی که قربانی بروی رایانه می‌بیند.

۸- از کار انداختن کلیدهای صفحه کلید به انتخاب و یا تعویض آنها با هم

۹- RESTART کردن رایانه قربانی و مشاهده چیزی که قربانی بروی رایانه می‌بیند

۱۰- به کار انداختن WEBCAM و ضبط و ارسال تصاویر گرفته شده

۱۱- به کار انداختن هر برنامه ای مثلاً اجراء موزیک یا صدای ارسالی از جانب HACKER

۱۲- از کار انداختن MOUSE رایانه قربانی

۱۳- SPIES فعال شدن قابلیت‌های جاسوسی

۱۴- دریافت گزارش از تمامی E-MEIL های ارسالی و دریافتی طی ماههای گذشته

۱۵- SPY MANAGER با این قابلیت میتوان کلمات عبور اشتراکهای (account) کاربری هریک از سرویسهای yahoo,msn.... را دریافت کرد و با حساب دیگران از رایانه استفاده نمود

۱۶- ..... و دهها قابلیت دیگر

حال سوالی مطرح میسازیم آیا شما از سیستم عامل ویندوز در رایانه خود استفاده مینمائید؟

قبل از اینکه به سوال مطروحه پاسخگو باشید به نکته ذیل توجه فرمائید.

نکته دیگر قابل تأمل(؟) برای آلوده کردن قربانی هائی که به رایانه آنها دسترسی داریم ساخت cd آلوده میباشد آنهم بصورت hidden و غیر قابل دید و تغییر نام شده rename کافی است در هنگام ضبط یک دیسک(write cd) ، server را در آن بگذاریم. حال خدا میداند چند درصد از cd های وارداتی به کشور آلوده بوده‌اند و چند درصد از رایانه‌های کشور ناآگاهانه پایگاه جاسوسی و ارسال اطلاعات به خارج واقع شده‌اند. نکته جالب تر و قابل تامل تر اینکه پولدار ترین شخص در دنیا که صاحب شرکت MICROSOFT میباشد طراح و فروشنده ویندوز و (سیستم عامل) رایانه ها می‌باشد که از دست روزگار در تمام دنیا و گیتی از همین سیستم عامل ویندوز استفاده میشود(؟).

برای درک بهتر فاجعه دعوت می‌کنیم که شما به آدرس اینترنتی شرکت MICROSOFT به نشانی زیر سری بزنید.

http://privacy.net/analyze

به محض ورود در آنجا شما اطلاعات رایانه خودتان را در کمال تعجب با نام خودتان خواهید یافت. چه مانیتوری با چه مارکی، از چه هاردی با چه ظرفیتی، چه مدل رایانه ای و مدل و قدرت CPU، از چه نوع سیستم عاملی استفاده می کنید، چه شرکت با چه نامی این سیستم را برای شما تدارک دیده، آدرس ip درجه وضوح صفحه نمایش و..... جای بس شگرف و بسیار اندوه که حتی واقف به عمق فاجعه نیز نمیباشیم و حتی حاضر به تامل در خصوص فاجعه. در بحث کلان ماجرا اگر لحظه‌ای بیشتر تامل کنیم در می‌یابید سرویسهای جاسوسی آمریکا بدون نیاز به ماهواره دارای حداقل ۱۰ میلیون جاسوس بی مواجب و بی‌ادعا، بدون بیمه و تعرفه قانون کار میباشند.

انتظار می‌رود با شناخت راههای نفوذ دیگر به سادگی فریب هکر ها را نخورده و زمام کامپیوتر خود را به دست آنها نسپارید و از باز کردن هر نامه ارسالی به صندوق پستی خود اجتناب نمائید.