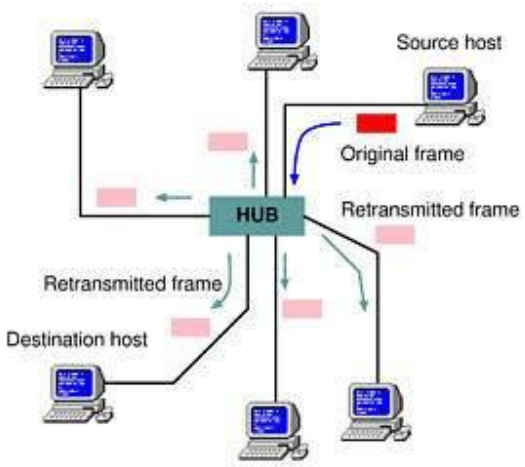
۱۲- شنود بسته های اطلاعات

یک برنامه شنود بسته های اطلاعاتی، برنامه ای است که دیتا را از اطلاعاتی که در حال انتقال در روی شبکه هستند، در اختیار می گیرد. این دیتا ممکن است شامل نام کاربران، کلمات عبور و هر اطلاعات اختصاصی دیگری باشد که روی شبکه و بدون اینکه رمز شده باشند، حرکت می کنند. با شاید صدها یا هزاران کلمات عبور گرفته شده توسط این برنامه، مزاحمین می توانند حملات گسترده ای را روی سیستمها پیاده کنند. نصب چنین برنامه ای لزوما به سطح دسترسی مدیر احتیاج ندارد.



نسبت به کاربران DSL و خطوط تلفن سنتی، کاربران مودمهای کابلی در معرض خطر بیشتری برای شنود قرار دارند، زیرا که تمام کاربران مودمهای کابلی همسایه بخشی از یک LAN هستند. یک برنامه شنود نصب شده روی کامپیوتر هر کاربر مودم کابلی ممکن است بتواند دیتا ارسال شده توسط هر مودم کابلی دیگر را در همان همسایگی دریافت کند.

از کوکی چه می‌دانید؟

کوکی چیست؟

«کوکی» بخش کوچکی از اطلاعات فرستاده شده توسط وب‌سرور برای ذخیره در مرورگر است تا بتواند بعدا از طریق آن مرورگر، دوباره خوانده شود. دیتای ذخیره شده برای اینکه وب‌سرور یک سایت، اطلاعات مشخصی را درباره بازدیدکننده آن وب‌سایت خاص بداند، مفید است. کوکی فرمت فایل متنی را دارد که در دایرکتوری مربوط به مرورگر ذخیره می‌شود و در هنگامی که مرورگر در حال اجراست در حافظه RAM قرار می‌گیرد. این اطلاعات می‌تواند هنگامی که کاربر از وب‌سایت خاصی خارج شد، در هارد درایو ذخیره شود. کوکی‌ها ابزار بسیار مهمی برای نگهداشتن state روی وب هستند. state به توانایی یک برنامه برای کار با کاربر بصورت محاوره‌ای اشاره دارد. برای مثال، شما برای استفاده از قطار یا اتوبوس بلیت رزرو می‌کنید. در روز سفر، هنگامی که بلیت را نشان می‌دهید، اجازه خواهید یافت که وارد قطار یا اتوبوس شوید، در غیراینصورت مسوول وسیله نقلیه نمی‌داند که آیا شما این اجازه را دارید یا خیر. در حقیقت در اینجا بلیت برای نگهداشتن state بین شما و مسوول قطار مهم است. HTTP یک پروتکل بدون قابلیت state است. به این معنی که هر بار مشاهده یک سایت توسط سرور بعنوان اولین مشاهده کاربر تلقی می‌شود. به این معنی که سرور همه چیز را بعد از هر درخواست فراموش می‌کند، مگر اینکه یک بازدیدکننده برای یادآوری آینده به سرور به طریقی مشخص گردد. کوکی‌ها این کار را انجام می‌دهند.

کوکی‌ها فقط می‌توانند به وب‌سرور بگویند که آیا شما قبلا هم از سایت دیدن کرده‌اید و اطلاعات کمی (مثلا یک شماره کاربر) در مرتبه بعد که از سایت دیدن می‌کنید از خود وب‌سرور به آن برگردانند. بیشتر کوکی‌ها هنگامی که از مرورگر خارج می‌شوید از بین می‌روند. نوع دیگری از کوکی‌ها بعنوان کوکی ماندگار وجود دارند که تاریخ انقضاء دارند و تا آن تاریخ روی هارددرایو شما باقی می‌مانند. کوکی ماندگار می‌تواند برای ردگیری عادات وبگردی یک کاربر با مشخص‌کردن وی هنگام مراجعه مجدد به یک سایت مورد استفاده قرار گیرد. اطلاعات در مورد اینکه اهل کجا هستید و به چه صفحات وبی سر می‌زنید در فایلهای لاگ یک وب‌سرور وجود دارد و می‌تواند برای ردگیری رفتار وبگردی کاربران مورد استفاده قرار گیرند، اما کوکی‌ها آن را آسانتر می‌کنند.

چگونه می‌توان از وجود کوکی‌های ماندگار روی سیستم مطلع شد؟

کوکی‌های ماندگار در مکانهای مختلفی روی سیستم شما بسته به مرورگر وب و نسخه‌ای از آن که استفاده می‌کنید، ذخیره می‌شوند. نت‌اسکیپ تمام کوکی‌های ماندگارش را در فایلی به نام cookies.txt روی کامپیوتر شما در دایرکتوری نت‌اسکیپ ذخیره می‌کند. می‌توانید این فایل را با یک ویرایشگر متن باز و ویرایش کنید و یا هر کوکی را که نمی‌خواهید نگهدارید، پاک کنید و چنانچه می‌خواهید از دست تمام کوکی‌ها خلاص شوید، فایل را پاک کنید. اینترنت‌اکسپلورر کوکی‌های ماندگار را در فایلهای جداگانه ذخیره می‌کند و توسط نام کاربر و نام دامنه سایتی که کوکی را فرستاده است، نامگذاری می‌کند. برای مثال john@wsiac.txt . این کوکی‌ها در دایرکتوری

/Windows/cookies یا /Windows/profiles/cookies ذخیره می‌شوند.

می‌توانید هرکدام از این کوکی‌ها را که نمی‌خواهید، پاک کنید. می‌توانید این فایلها را بازکنید تا ببینید از کجا آمده‌اند و چه اطلاعاتی دارند. برای مثال آنچه می‌بینید محتویات یک کوکی IE هستند.

WEBTRENDS_ID
61.1.129.58-1041789995.121030
www.bazwe.com/
1024
3872737152
30271763
3731731632
29537508

این فایل کوکی abishek@www.birt.txt (abishek شناسه فرد وارد شونده به سایت است) نامیده شده است. کوکی‌ها ممکن است اطلاعات مختلفی را دربرداشته باشند که بسته به کوکی متفاوت است. در این کوکی IP فرد نیز(61.1.129.58) ذخیره شده است. در اینجا قصد وارد شدن به جزئیات را نداریم.

Cookie:administrator@4icards	Cookie:administrator@4icards.c...	Text Document	1 KB	1/1/2005 8:30 AM
Cookie:administrator@atdmt	Cookie:administrator@atdmt.com/	Text Document	1 KB	6/28/2009 3:30 AM
Cookie:administrator@baazee	Cookie:administrator@baazee.c...	Text Document	1 KB	7/5/2005 6:38 PM
Cookie:administrator@babylon	Cookie:administrator@babylon.c...	Text Document	1 KB	1/1/2100 3:30 AM
Cookie:administrator@bonzi	Cookie:administrator@bonzi.com/	Text Document	1 KB	7/5/2004 6:07 PM
Cookie:administrator@dp.information	Cookie:administrator@dp.inform...	Text Document	1 KB	7/6/2004 1:42 PM
Cookie:administrator@fastclick	Cookie:administrator@fastclick....	Text Document	1 KB	6/24/2006 5:59 PM
Cookie:administrator@google	Cookie:administrator@google.com/	Text Document	1 KB	1/17/2038 10:44 ...
Cookie:administrator@ittoolbox	Cookie:administrator@ittoolbox....	Text Document	1 KB	7/5/2008 7:30 AM
Cookie:administrator@microsoft	Cookie:administrator@microsoft...	Text Document	1 KB	10/3/2006 10:30 ...
Cookie:administrator@passport	Cookie:administrator@passport....	Text Document	1 KB	12/30/2037 7:30 ...
Cookie:administrator@revenue	Cookie:administrator@revenue....	Text Document	1 KB	6/10/2022 8:35 AM
Cookie:administrator@search.domainsponsor	Cookie:administrator@search.d...	Text Document	1 KB	7/6/2004 1:43 PM
Cookie:administrator@search.information	Cookie:administrator@search.in...	Text Document	1 KB	7/6/2004 1:42 PM
Cookie:administrator@securitydocs	Cookie:administrator@securityd...	Text Document	1 KB	1/18/2038 3:30 AM
Cookie:administrator@securityfocus	Cookie:administrator@securityf...	Text Document	1 KB	1/1/2011 3:30 AM
Cookie:administrator@www.baazee	Cookie:administrator@www.baa...	Text Document	1 KB	7/3/2014 5:39 PM
Cookie:administrator@www.google	Cookie:administrator@www.goo...	Text Document	1 KB	6/29/2005 12:39 ...
Cookie:administrator@www.securityfocus	Cookie:administrator@www.sec...	Text Document	1 KB	7/3/2014 2:46 PM
Cookie:administrator@yahoo	Cookie:administrator@yahoo.com/	Text Document	1 KB	1/1/2038 3:30 AM
Cookie:administrator@z1.adserver	Cookie:administrator@z1.adser...	Text Document	1 KB	7/5/2005 3:29 PM

کوکی‌ها برای چه استفاده می‌شوند؟

یک استفاده از کوکی‌ها برای ذخیره کلمات عبور و شناسه‌های برای وب‌سایتهای خاص است. همچنین برای ذخیره اولویتهای کاربران در صفحات آغازین نیز استفاده می‌شوند. در این حالت مقداری از هارد کامپیوتر شما برای ذخیره این اطلاعات از مرورگرتان تقاضا می‌شود. بدین طریق، هر زمان که به آن وب‌سایت وارد می‌شوید مرورگر شما بررسی می‌کند که ببیند آیا الویتهای از پیش تعیین‌شده (کوکی) برای آن سرور مشخص دارید یا خیر. اگر اینطور باشد، مرورگر کوکی را همراه با تقاضای شما برای صفحه وب، به وب‌سرور ارسال خواهد کرد. مایکروسافت و نت‌اسکیپ از کوکی‌هایی برای ایجاد صفحات آغازین شخصی روی وب‌سایتهایشان استفاده می‌کنند. استفاده‌های معمول که

شرکتها بخاطر آنها از کوکی استفاده می‌کنند شامل سیستمهای سفارش آنلاین، شخصی‌سازی سایتها و ردگیری وب‌سایتها می‌شود. کوکی‌ها منافعی دارند. شخصی‌سازی سایت یکی از مفیدترین استفاده‌های کوکی‌ها است. برای مثال، فردی وارد سایت CNN (یا حتی MyYahoo) می‌شود اما نمی‌خواهد اخبار تجاری را ببیند. این سایت به فرد اجازه این انتخاب را می‌دهد. از این به بعد (یا تا زمانیکه کوکی منقضی می‌شود) این شخص اخبار تجاری را وقتی به سایت CNN متصل می‌شود، نمی‌بیند. حتما تا حالا دیده‌اید که در بعضی وب‌سایتها هنگامی که با استفاده از شناسه و گذرواژه وارد می‌شوید، انتخابی تحت عنوان «مرا دفعه بعد بخاطر داشته باش» وجود دارد. این امر با ذخیره شدن شناسه و کلمه عبور شما در یک کوکی روی کامپیوترتان، میسر می‌شود. بعضی بازدیدکنندگان آن را بعنوان تعرض به حریم خصوصی می‌پندارند برای وب‌سایتهایی که روند فعالیتشان روی یک سایت را ردگیری می‌کنند. این کمک می‌کند که اطلاعات و سرویس‌های مورد جستجو را بسرعت بیابید و بدون تاخیر به سر کار اصلی خودتان برگردید. آمار برای طراحی مجدد سایت بسیار مهم هستند. گاهی مدیر سایت نیاز دارد بداند آیا ۱۰۰ نفر مختلف از سایتش بازدید کرده‌اند یا فقط یک فرد (یا روبات) بطور پیوسته ۱۰۰ مرتبه دکمه reload (یا refresh) را انتخاب کرده است. کوکی‌ها کاربردهای دیگری نیز دارند و یکی از آنها امکان ردگیری فعالیت کاربران است. اجازه دهید که یک مثال را ببینیم. DoubleClickNetwork سیستمی است که توسط DoubleClickCorporation ایجاد شده است تا پروفایل افرادی را

که از وب استفاده می‌کنند ایجاد کند و آگهی‌های تجاری متناسب با علاقه‌شان را به آنها ارائه کند. مشتری‌های DoubleClick وب‌سایتهایی هستند که قصد تبلیغ خدماتشان را دارند. هر عضو این شبکه میزبانی برای تبلیغ سایر اعضاء می‌شود. هر وب‌سایت که عضو می‌شود تبلیغ خود را ایجاد و در اختیار سرور DoubleClick قرار می‌دهد. هنگامی که یک کاربر به یکی از این سایتها می‌رود، یک آگهی از سایر سایتها نیز در HTML ارائه شده به کاربر وجود دارد. با هربار بارگذاری مجدد صفحه، آگهی متفاتی به کاربر ارائه می‌شود. از نظر کاربران این تبلیغات با سایر تبلیغات تفاوتی ندارند، در حالیکه اینطور نیست. هنگامی که کاربری برای اولین بار به سرور DoubleClick متصل می‌شود، سرور یک کوکی برای آن مرورگر ایجاد می‌کند که یک شماره مشخصه یکتا در بردارد. از آن به بعد هر زمان که کاربر به یکی از وب‌سایتهای عضو DoubleClick متصل می‌شود، شماره مذکور به سرور ارسال می‌شود و کاربر تشخیص داده می‌شود. با گذشت زمان و داشتن اطلاع از سایتهایی که کاربر بازدید کرده است، پروفایلی از علائق کاربر در اختیار سرور قرار می‌گیرد. با داشتن این پروفایل، سرور DoubleClick می‌تواند تبلیغاتی را که بیشتر مورد نظر کاربر است انتخاب کند. بعلاوه می‌تواند از این اطلاعات برای دادن بازخورد مناسب به اعضا مانند پروفایل کاربران و میزان تاثیر تبلیغاتشان استفاده کند. برای اینکه بفهمید آیا توسط DoubleClick ردگیری شده‌اید یا نه، کوکی‌های مرورگر خود را امتحان کنید و ببینید آیا چیزی شبیه به این: ad.doubleclick.net FALSE / FALSE 942195440 IAA d2bbd5 در کوکی‌ها وجود دارد یا خیر.

کوکی‌ها و مسائل امنیتی

بررسی انواع کوکی

علاوه بر کوکی‌های **موقت** و **ماندگار** که در مقاله قبل در مورد آن صحبت شد، کوکی‌ها دسته‌بندی دیگری نیز دارند:

کوکی‌های **شخص‌اول!** در مقابل کوکی‌های **شخص‌ثالث**: یک کوکی شخص‌اول از وب‌سایتی نشات می‌گیرد یا به آن فرستاده می‌شود که در آن زمان در حال مشاهده آن هستید. این کوکی‌ها معمولا برای ذخیره اطلاعات مانند اولویتهای شما استفاده می‌شوند. یک کوکی شخص ثالث از وب‌سایت متفاوت با آنچه در حال مشاهده آن هستید نشات می‌گیرد یا به آن فرستاده می‌شود. وب‌سایتهای شخص‌ثالث معمولا محتویاتی روی وب‌سایتی که در حال مشاهده هستید، ارائه می‌کنند. برای مثال، بسیاری سایتها از تبلیغات وب‌سایتهای شخص‌ثالث استفاده می‌کنند و آن وب‌سایتها ممکن است از کوکی استفاده

کنند. یک استفاده معمول برای این نوع از کوکی ردیابی استفاده از صفحه‌وب شما برای تبلیغات یا سایر مقاصد بازاریابی است. این نوع کوکی‌ها می‌توانند موقت یا ماندگار باشند.

نوعی از کوکی‌ها هستند که بعنوان کوکی‌های **ناخوشایند** نامیده می‌شوند. کوکی‌هایی هستند که ممکن است اجازه دسترسی به اطلاعات شخصا قابل‌شناسایی شما را برای اهداف ثانویه بدون اجازه شما، فراهم کنند.

مزایا و معایب کوکی‌ها از دید کاربران اینترنت

اگرچه خیلی‌ها از کوکی‌ها تصورات بدی دارند، اما اکنون می‌دانید که کابردهای خوبی نیز دارند. بسیاری از افراد کوکی‌ها را دوست ندارند زیرا آنها را ابزار "بردار بزرگ" (کسی که همواره ناظر بر اعمال و رفتار آنهاست) می‌دانند. بعبارتی بعلت ردیابی شدن توسط کوکی‌ها، به آنها سوءظن دارند. این افراد باید بدانند که این نوع ردگیری می‌تواند توسط تکنیک‌های دیگر نیز انجام گیرد، اما از کوکی‌ها بدلیل ثبات بیشتر آنها نسبت به سایر روش‌ها استفاده می‌شود. برای آنان که دوست ندارند دیگران بدانند در اینترنت چه می‌کنند یا به کدام سایتها سر می‌زنند، این امر مساله ساز است.

مردم همچنان کوکی‌ها دوست ندارند، زیرا آنها را موجوداتی "آب‌زیرکاه" می‌دانند. مگر اینکه نسخه‌های جدید مرورگرها را داشته باشید تا بتوانید با تنظیماتی که انجام می‌دهید از

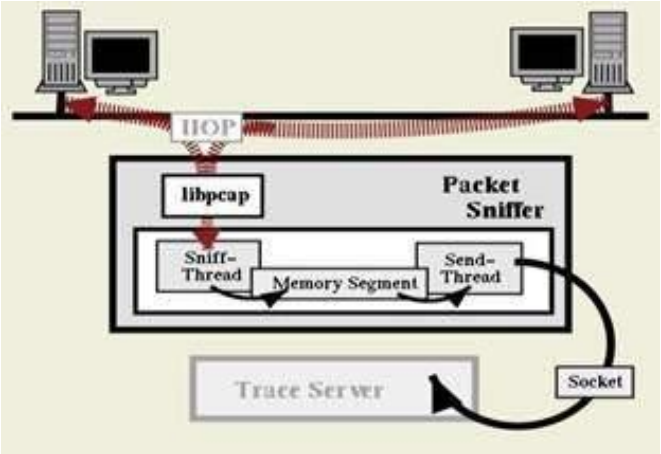
ورود آنها مطلع شوید، در غیر اینصورت آنها بدون هیچ نشانی وارد هارد شما می‌شوند. سیس می‌توانند بدون اطلاع کاربر کارهای خاصی انجام دهند (شاید هدف قرار دادنتان برای اعمال تبلیغاتی).

بهرحال فکر کردن به این موضوع خوشایند نیست که در آینده نزدیک علائق خصوصی ما ممکن است برای کسانی که دوست نداریم، فاش شود. این نگرانی و عیب اصلی کوکی‌هاست. تقریبا قرار دادن ویروس از طریق کوکی فعلا ممکن نیست و جای نگرانی

ندارد. همچنین کوکی‌ها نمی‌توانند به هارد شما صدمه وارد کنند، یا از آنچه روی هارد خود دارید، تصویری تهیه کنند یا هر کار دیگری شبیه اینها. **کوکی‌ها فقط آنچه را شما به آنها می‌گویید، میدانند**. بهرحال اگر شما اطلاعاتی را در وب‌سایتی وارد کنید، مطمئنا در جایی در یک کوکی قرار خواهد گرفت. جایگزینهای آینده بجای کوکی‌ها باید با آغوش باز پذیرفته شود و اگرچه ممکن است همه چیز را حل نکنند، اما بعضی از نگرانیها را از بین خواهند برد.

مسائل امنیتی مربوط به کوکی‌ها

کوکی‌ها باعث بعضی خطرات امنیتی می‌شوند. می‌توانند توسط افرادی که بسته‌های اطلاعاتی را شنود می‌کنند برای اهداف غیراخلاقی استفاده شوند و باعث دسترسی غیرمجاز به وب‌سایت‌ها یا تراکنش‌های غیرمجاز شوند. (یک سیستم شنود، کامپیوتری است که نرم‌افزارهایی را اجرا می‌کند تا تمام بسته‌های TCP/IP وارد و خارج‌شونده را بررسی کند)



ایجادکنندگان وب‌سایتها کوکی‌ها را می‌سازند تا امکان دسترسی بهتر به سایتشان را فراهم کنند، یا در انواع دیگر تراکنش با سرورشان استفاده می‌شوند. آنها باید از امکان وقوع این امر مطلع باشند و سیستم را طوری طراحی کنند تا خطر را به حداقل ممکن برسانند.

چند مورد وجود دارد که ایجادکننده وب‌سایت می‌تواند انجام دهد:

- مطمئن شود که کوکی‌ها کمترین اطلاعات خصوصی را دربردارند.
- مطمئن شود که اطلاعات حساس قرارگرفته در کوکی‌ها همیشه رمزنگاری می‌شود. (هرگز و هرگز شناسه‌ها و کلمات عبور نباید بصورت متن رمزنشده استفاده و ذخیره شوند)• کل کوکی را رمز کند.

کوکی‌ها باید اطلاعات کافی را برای تایید اینکه فرد استفاده کننده از کوکی، مجاز به استفاده از آن است، دارا باشند. بیشتر سایتهای استفاده‌کننده از کوکی، اطلاعات زیر را نیز لحاظ می‌کنند:

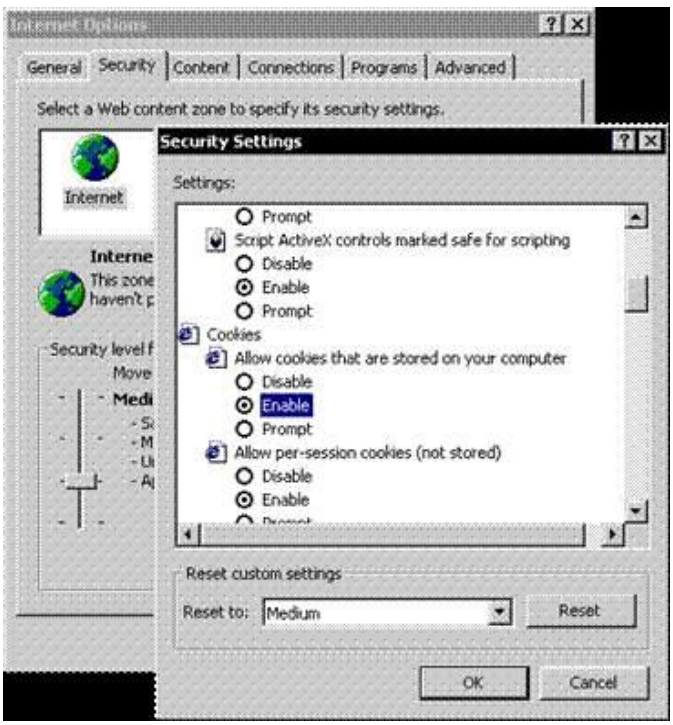
- اطلاعات لازم برای دادن اجازه به فرد
- ساعت و تاریخ
- آدرس IP استفاده کننده وب
- تاریخ انقضاء
- کد MAC (Message Authenticity Check)

قراردادن آدرس IP به این منظور است که کوکی تنها در صورتی تایید شود که آدرس IP ذخیره‌شده در سرور با آدرس IP مرورگر فرستنده کوکی یکسان باشد. تاریخ انقضاء مدت زمان استفاده از یک کوکی را محدود می‌کند و MAC تضمین می‌کند که کوکی دچار تغییر نشده است.

کد MAC شامل یک رشته ادغامی از فیلدهای داده در کوکی و یک رشته مخفی است که به آن اضافه می‌شود. اطلاعات کد می‌شود سپس مجددا ادغام می‌شود و دوباره کد می‌شود. نتیجه نهایی در داده کوکی قرار می‌گیرد. هنگامی که کوکی به سرور برمی‌گردد، سرور خود، MAC را تولید می‌کند و با MAC موجود در کوکی مقایسه می‌کند. در صورت یکسان بودن، نشانه عدم تغییر کوکی است.

کار با کوکی‌ها

مرورگرهای جدید اجازه نحوه کار با کوکی‌ها را به شما می‌دهند؛ می‌توانید تنظیمات مرورگر خود را طوری انجام دهید که به شما قبل از قراردادن کوکی روی کامپیوترتان خبر داده شود. (این کار به شما این امکان را می‌دهد که اجازه قراردادن کوکی را بدهید یا خیر)؛ همچنین می‌توانید توسط مرورگر خود جلوی ورود تمام کوکی‌ها را بگیرید.



بعنوان مثال در اینترنت اکسپلورر امکان تنظیم نحوه برخورد با کوکی‌ها از سایتهای مشخص گرفته تا کل سایتها وجود دارد. برای اطلاع یافتن بیشتر از نحوه کار با کوکی‌ها راهنمای مرورگر خود را مطالعه کنید.

محتویات فعال و کوکی

هر یک از ما در مدت زمان اتصال به اینترنت از وب سایت ها و یا وبلاگ های متعددی دیدن می نمائیم. طراحان و پیاده کنندگان وب سایت ها و وبلاگ ها به منظور ارائه خدمات مورد نظر خود از امکانات و یا بهتر بگوئیم تکنولوژی های متفاوتی استفاه می نمایند . اغلب ملاقات کننده گان، احساس خاصی نسبت به این تکنولوژی ها نداشته و صرفا" برای آنان نوع سرویس ها و خدمات ارائه شده دارای اهمیت است.

برخی از تکنولوژی های استفاده شده علیرغم داشتن جنبه های مثبت و مهم به ابزارهائی برای برنامه ریزی برخی حملات تبدیل شده و حریـــم خصوصی کاربران را به مخاطره می اندازد. محتویات فعال (Active contents) و کوکی ها (Cookies) از جمله موارد فوق، می باشند.

محتویات فعال چیست ؟

در اغلب وب سایت ها به منظور افزایش پتانسیل های قابل ارائه به کاربران و یا تزئین سایت از اسکریپت هائی که باعث اجرای برنامه ها بر روی مرورگر وب می شود، استفاده می گردد. ایجاد منوهای Drop-down و یا انجام افکت های گرافیکی متفاوت در یک صفحه وب، نمونه هائی در این زمینه می باشند. این نوع اسکریپت ها که به "محتویات فعال"معروف شده اند، اغلب به روشی برای انواع حملات نظیر سرقت اطلاعات و یا اجرای کدهای مخرب بر روی کامپیوتر کاربران، تبدیل شده اند.

- **جاوا اسکریپت** : جاوا اسکریپت یکی از متداولترین زبان های اسکریپت نویسی در وب است که در اکثر وب سایت ها از آن استفاده می گردد.

- (VBscript,ECMAScript و Jscript نمونه هائی دیگر در این زمینه می باشند). تامین طیف وسیعی از خواسته ها، عملکرد مناسب، سادگی در استفاده و ترکیب آسان با سایر نرم افزارها از جمله دلایل گسترش استفاده از زبان های اسکریپت نویسی در وب می باشد.مهاجمان نیز از پتانسیل های ارائه شده توسط زبان های اسکریپت نویسی به منظور نیل به اهداف مخرب خود استفاده می نمایند . مثلا" یکی از حملات متداول که با محوریت جاوا اسکریپت صورت می پذیرد، هدایت کاربران از یک وب سایت مطمئن به یک وب سایت مخرب است که در آن اقدام به download ویروس ها و یا جمع آوری اطلاعات شخصی کاربران می گردد.
- **اپلت های جاوا و کنترل های اکتیوایکس**: اپلت های جاوا و کنترل های اکتیوایکس برنامه هائی می باشند که بر روی کامپیوتر شما مستقر شده و یا از طریق شبکه بر روی مرورگر شما download می گردند. در صورتی که اینگونه برنامه ها (خصوصا" کنترل های اکتیوایکس) توسط مهاجمان مدیریت و هدایت گردند، امکان انجام هر گونه عملیاتی بر روی کامپیوتر شما وجود خواهد داشت. اپلت های جاوا معمولا" دریک محیط محدودتر اجراء می گردند. این نوع از برنامه ها در صورت عدم ایمنی مناسب محیط ایجاد شده، فرصت های مناسبی به منظور انواع حملات را برای مهاجمان فراهم می نمایند.

استفاده از جاوا اسکریپت، اپلت های جاوا و کنترل های اکتیوایکس، همواره خطرناک نمی باشد. ولی می بایست به این موضوع دقت شود که امکانات فوق به ابزارهائی برای انواع حملات توسط مهاجمان، تبدیل شده اند. به منظور پیشگیری در خصوص محتویات فعال ، امکانات متعددی در اکثر مرورگرها پیش بینی شده است که با استفاده از آنان و تنظیم بهینه پارامترهای موجود می توان یک سطح ایمنی مناسب را ایجاد نمود. بموازات افزایش ضریب ایمنی مرورگر خود به منظور برخوردبا محتویات فعال، ممکن است محدودیت های خاصی در خصوص برخی ویژگی های ارائه شده توسط برخی

سایت ها، ایجاد گردد. در صورتی که از یک وب سایت دیدن می نمائید که نسبت به آن شناخت کافی وجود ندارد، می بایست پیشگیری لازم در خصوص غیر فعال نمودن محتویات فعال را انجام داد. تهدیدات مشابهی نیز می تواند متوجه برنامه های پست الکترونیکی باشد. تعداد زیادی از برنامه های پست الکترونیکی از برنامه های مشابه مرورگرها به منظور نمایش HTML استفاده می نمایند . بنابراین امکان تهدید محتویات فعال در خصوص نامه های الکترونیکی نیز می تواند وجود داشته باشد. به منظور پیشگیری لازم در خصوص این نوع تهدیدات می توان پیام ها را به صورت متن معمولی، مشاهده نمود.

در زمان استفاده از اینترنت، امکان جمع آوری و ذخیره اطلاعات شما وجود خواهد داشت . اطلاعات فوق ممکن است اطلاعاتی عمومی در خصوص کامپیوتر شما نظیر آدرس IP ، نام Domain استفاده شده به منظور ارتباط با اینترنت، نوع مرورگر و سیستم عامل، باشد. اطلاعات جمع آوری شده می تواند شامل موارد خاصی نظیر آخرین مرتبه ای که یک وب سایت را ملاقات نموده اید و یا اطلاعات شخصی شما در زمان استفاده از یک وب سایت خاص نظیر آدرس پست الکترونیکی باشد.

- **Session cookie** . این نوع کوکی ها صرفا" و تا زمانی که از مرورگر استفاده می گردد، اطلاعاتی را ذخیره نموده و پس از بستن مرورگر اطلاعات از بین می رود. هدف از بکارگیری این نوع کوکی ها، ارائه تسهیلات لازم در خصوص حرکت بین صفحات متعدد است. مثلا" تشخیص مشاهده یک صفحه خاص و یا نگهداری اطلاعاتی در خصوص داده های مرتبط با یک صفحه.
- **cookie Presistent** : این نوع کوکی ها اطلاعاتی را بر روی کامپیوتر شما ذخیره می نمایند. بدین ترتیب امکان نگهداری اطلاعات شخصی مرتبط با شما فراهم می گردد . در اکثر مرورگرها برای این نوع از کوکی ها می توان یک مدت

-
- زمان خاص را مشخص نمود(عمر مفید). در صورتی که یک مهاجم امکان دستیابی به کامپیوتر شما را پیدا نماید، می تواند با مشاهده محتویات فایل های فوق به اطلاعات شخصی شما دسترسی نماید.

به منظور افزایش سطح ایمنی خود، می بایست تنظیمات امنیتی لازم در خصوص اعمال محدودیت و یا بلاک نمودن کوکی ها را در جهت حفظ حریم خصوصی، انجام داد. در صورتی که از یک کامپیوتر عمومی استفاده می نمائید، می بایست کوکی ها را غیر فعال نموده تا پیشگیری لازم در خصوص دستیابی سایرین به اطلاعات شخصی شما ، صورت پذیرد .

داده های حساس

فرض کنید هارددیسک کامپیوتر شما در اختیار فرد و یا افرادی دیگر قرار بگیرد، آیا آنان می توانند با بررسی آن اطلاعات خاصی در خصوص شما و نوع فعالیت هائی که انجام می دهید را کسب نمایند؟ در پاسخ می بایست با صراحت گفت که چنین امری میسر است و شاید بیش از آنچیزی که احتمال آن را می دهید. در این مطلب قصد داریم به بررسی این موضوع بپردازیم که چگونه یک کارشناس کالبد شکافی اطلاعات کامپیوتر قادر است داده هائی را که به نظر شما مدت ها است از روی کامپیوتر حذف و ظاهرا" اثری از آنان مشاهده نمی گردد را جان دوباره داده و از آنان استفاده نماید. بررسی این موضوع از دو زاویه می تواند مفید باشد: اول برای افرادی که قصد بازیافت اطلاعات(recovery) خود را دارند و دوم برای افرادی که می خواهند مقاومت سیستم خود را در مقابل بازبینی های غیرمجاز، افزایش دهند.

به منظور ایمن سازی کامپیوتر خود و حفاظت از اطلاعات حساس موجود بر روی آن لازم نیست که حتما" یک کارشناس حرفه ای کامپیوتر باشیم، با اندک دانشی نسبت به نحوه عملکرد سیستم عامل نصب شده بر روی کامپیوتر نظیر ویندوز، می توان اقدامات لازم در این خصوص را انجام داد. افشای اطلاعات حساس موجود بر روی هارددیسک، آگاهی از وب سایت های مشاهده شده و فایل هائی که از طریق اینترنت download شده اند و بازیابی فایل های حذف شده، از جمله مواردی می باشند که می تواند توسط هر فردی که به سیستم شما دستیابی پیدا می نماید و دارای دانش مختصری در رابطه با نحوه بازیافت اطلاعات است، مورد سوء استفاده قرار گیرد. افراد فوق با در اختیار گرفتن مجموعه ای از ابزارهای موجود که بدین منظور و گاها" با اهداف خیرخواهانه طراحی شده اند، می توانند حتی اقدام به بازیابی داده هائی نمایند که شما قبلا" آنان را حذف نموده اید.

آنان در این رابطه اقدام به بازیابی مجموعه ای از بیت ها و بایت ها نموده و در ادامه با قرار دادن آنان در کنار یکدیگر، قادر به دستیابی و مشاهده اطلاعات حذف شده خواهند بود.

داده های مخفی و نحوه یافتن آنان

کامپیوترهای موجود در منازل و یا سازمان ها مملو از داده هائی است که کاربران از وجود آنان بر روی سیستم خود بی اطلاع می باشند. حتی تعداد زیادی از کارشناسان حرفه ای فن آوری اطلاعات نیز در این رابطه اطلاعات و یا شناخت مناسبی را ندارند. بر روی کامپیوتر مکان های دنج و خلوتی وجود دارد که داده ها در آنجا مخفی شده و با شناخت مناسب نسبت به محل اختفای آنان، احتمال بازیابی و سوء استفاده از آنان وجود خواهد داشت. با بازرسی مکان های فوق و بررسی ردپای داده های به جا مانده بر روی سیستم، می توان اطلاعات زیادی در خصوص استفاده کننده کامپیوتر و نوع فعالیت های وی را کسب نمود و حتی متوجه شد که وی با چه سرویس دهندگانی ارتباط داشته است. در ادامه به بررسی متداولترین موارد در این خصوص خواهیم پرداخت.

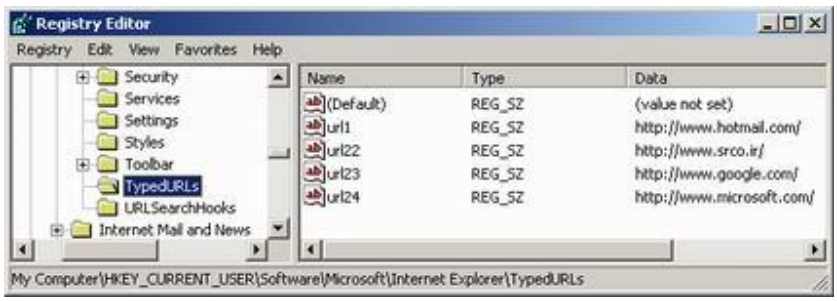
آگاهی از وب سایت های مشاهده شده

جملگی می دانیم که با بررسی history مرورگر و فایل های موقت اینترنت (Cache)، می توان آگاهی لازم در خصوص وب سایت های مشاهده شده توسط کاربر یک کامپیوتر را پیدا نمود. در صورتی که نمی خواهیم ردپای استفاده از وب بر روی سیستم برجای بماند، می بایست این نوع فایل ها را حذف نمود.(فرآیندی ساده در اکثر مرورگرها). کلیک بر روی یک دکمه به منظور حذف یک فولدر به تنهائی کافی نبوده و همچنان احتمال بازیابی آنان وجود خواهد داشت. حتی در مواردی که اقدام به پاک نمودن history مرورگر می شود، تمامی فایل ها حذف نخواهند شد!

سرنخ وب سایت های مشاهده شده در مکان هائی دیگر مخفی شده و همچنان باقی خواهند ماند. با بررسی فولدرهای Favorites و یا Bookmarks نیز می توان اطلاعات زیادی در خصوص سایت هائی که توسط یک کاربر به تناوب استفاده می گردد

را پیدا نمود. بررسی فولدر کوکی (Cookies) نیز می تواند نشان دهنده سایت های مشاهده شده توسط یک کاربر باشد. نظر شما در رابطه با آدرس هائی که در بخش آدرس مرورگر تایپ می گردد و ادامه آن به صورت اتوماتیک توسط برنامه مرورگر درج می گردد، چیست؟ یک فرد آشنا به کامپیوتر می تواند با تایپ تصادفی حروف، متوجه شود که شما قبلاً" چه آدرس هائی را در این بخش مستقیما" تایپ نموده اید. آدرس وب سایت هائی را که شما مستقیما" در بخش آدرس یک مرورگر تایپ می نمائید(منظور کلیک بر روی لینک های pop up نمی باشد) در کلید ریجستری زیر ذخیره می گردند:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs



حذف history در مرورگر IE باعث حذف URLs تایپ شده می گردد. در صورت تمایل، می توان این عملیات را مستقیما" و با اجرای برنامه regedit انجام داد. در چنین مواردی می توان یک و یا چندین URLs را مستقیما" حذف نمود(یافتن کلید ریجستری اشاره شده، انتخاب یک و یا چندین URLs، کلیک سمت راست و فعال نمودن دکمه Delete). بررسی فولدرهای Download My و دایرکتوری های temp نیز می تواند مشخص کننده فایل های Downlaod شده توسط شما باشد. با استفاده از نرم افزارهائی که بدین منظور طراحی شده است، می توان به سادگی تمامی "نشانه های وب " را از روی سیستم پاک نمود. Web Cache Illuminator ، یک نمونه در این رابطه است.

در صورتی که شما از طریق یک فایروال از اینترنت استفاده می نمائید، در اغلب موارد فایروال مربوطه و یا سرویس دهنده پروکسی لیستی از وب سایت های مشاهده شده توسط کاربران و یا کامپیوترهای موجود در شبکه را ثبت می نماید.

سایر مکان های داده های مخفی

علاوه بر موارد اشاره شده در خصوص محل اختفای داده ها خصوصا" وب سایت های مشاهده شده، مکان های دیگری نیز وجود دارد که احتمال ذخیره سازی داده ها و بالطبع بازیابی(بازیافت) آنان توسط افراد غیر مجاز وجود خواهد داشت :

- **برنامه های واژه پرداز و سایر برنامه هائی که فایل های موقتی را ایجاد می نمایند**. این فایل ها معمولا" به صورت اتوماتیک و پس از خروج از برنامه و یا حتی راه اندازی کامپیوتر، حذف نمی گردند. فایل های فوق ممکن است در فولدری مشابه با محل نصب برنامه و یا فولدرهای موقتی که بدین منظور توسط برنامه ایجاد می گردد، ذخیره شوند.

- **Clipboard مربوط به ویندوز و یا آفیس**، می تواند داده هائی را که اخیرا" توسط سند مربوطه Cut و Copy شده اند، افشاء نماید. (حتی در صورتی که سند مورد نظر حذف گردد). Clipboard آفیس، می تواند شامل چندین آیتمی باشد که در طی مراحل قبل Cut و Copy شده اند (صرفا" شامل آخرین آیتم نمی باشد).

- **برنامه های IM یا Instant Messenger** ممکن است بگونه ای پیکربندی شده باشند که ماحصل مکالمه و یا محاوره انجام شده را در یک فایل و بر روی هارد دیسک ذخیره نمایند.

- سیستم های IM سرویس گیرنده – سرویس دهنده که از طریق یک سرویس دهنده IM مرکزی امکان ارتباط را فراهم می نمایند، ممکن است ماحصل مکالمه و یا گفتگوی انجام شده را بر روی سرویس دهنده ذخیره نمایند. لیست تماس و یا buddy موجود در این نوع نرم افزارها نیز نشاندهنده افرادی است که شما عموما" با آنان ارتباط برقرار می نمائید (مثلا" چت).
- **نرم افزار پست الکترونیکی و یا برنامه مربوط به نگهداری لیست تماس شما،** ممکن است باعث افشای اطلاعات موجود در آن نظیر آدرس پست الکترونیکی، آدرس فیزیکی و شماره تلفن افرادی گردد که شما با آنان در ارتباط هستید. همچنین تقویم و لیست فعالیت های روزمره نیز می تواند برخی اطلاعات شما را افشاء نماید.
- **فولدرMy Documents نیزمیتواند اسنادی را که اخیرا" با آنان کار نموده اید را مشخص نماید.** playlist مربوط به نرم افزارهای Media Player و بخش history آنان نیز می تواند نشان دهنده فایل های تصویری و صوتی باشد که آنان را مشاهده و یا گوش داده اید.
- **درایوهای مربوط به tape، سی دی، فلاپی و حافظه های فلش** نیز ممکن است همچنان دارای نسخه هائی از اسناد و فایل هائی باشند که شما آنان را از روی کامپیوتر حذف نموده اید.
- **اطلاعاتی که اخیرا" شما اقدام به حذف آنان نموده اید،** ممکن است همچنان و تا زمان Shut down نمودن کامپیوتر در حافظه و یا حافظه مجازی (فایل های swap) موجود باشند.

فایل های حذف شده

با حذف یک فایل آن فایل از روی کامپیوتر شما پاک نمی گردد. مثلا" زمانی که شما یک نامه الکترونیکی را حذف می نمائید، پیام حذف شده صرفا" به یک فولدر دیگر

(Deleted Items)، منتقل می گردد. زمانی که فولدر فوق خالی می گردد (دستی و یا بر اساس برنامه زمانبندی پست الکترونیکی)، تمامی آیتم های موجود به صورت پیش فرض به Recycle Bin منتقل می گردند. حتی در صورت تخلیه Recycle Bin ماجرا خاتمه نیافته و فایل های حذف شده توسط سیستم عامل از روی دیسک حذف نخواهند شد. در حقیقت پس از حذف یک فایل و یا مجموعه ای از فایل ها، صرفا" اشاره گرهائی که به فایل های فوق اشاره می کنند از جدول سیستم فایل حذف شده و فضای استفاده شده توسط فایل های حذف شده بر روی دیسک، علامت " قابل استفاده مجدد " درج می شود. صفرها و یک هائی که داده های موجود در یک فایل را تشکیل می دهند، همچنان در مکان های مورد نظر خود موجود بوده و احتمال بازیابی تمام و یا بخش هائی از آنان وجود خواهد داشت. حتی با فرمت کردن هارد دیسک، فایل های حذف شده موجود بر روی آن، دور انداخته نخواهند شد. حتما" این سوال برای شما مطرح شده است که وجود این نوع اطلاعات حذف شده بر روی کامپیوتر چه تهدیدات امنیتی را ایجاد خواهد کرد و یا چگونه و با استفاده از چه روش و یا روش هائی امکان بازیافت مجدد آنان وجود خواهد داشت؟

مهاجمان و یا بهتر بگوئیم افراد غیر مجاز با استفاده از نرم افزارهای خاصی قادر به برگرداندن داده هائی می باشند که عملا" و از دید کاربر حذف شده ولی همچنان بر روی محیط ذخیره سازی نظیر هارددیسک موجود می باشند. معمولا" فرآیند بازیافت و ریکاوری اطلاعات عملیاتی پیچیده و در عین حال طولانی است. بدیهی است نرم افزارهائی که قادر به انجام اینچنین عملیاتی می باشند، بسیار گرانقیمت باشند:

- File Scavenger
- GetDataBack
- Back2Life

به منظور بازیابی اطلاعات حذف شده می توان از برخی نرم افزارهای ارزان قیمت و یا رایگان موجود نیز استفاده نمود. برخی از نرم افزارهای فوق را می توان با مراجعه به آدرس:http://free-backup-software.net/data-recovery.htm دریافت نمود.

اکثر نرم افزارهای فوق با این هدف طراحی شده اند که اگر شما به صورت تصادفی فایل و یا فایل هائی را حذف کرده باشید، امکان بازیابی مجدد آنان را در اختیار شما قرار دهند. متاسفانه مهاجمان و سایر افراد غیرمجاز نیز می توانند با استفاده از نرم افزارهای فوق به برخی از اطلاعات موجود بر روی سیستم شما دستیابی پیدا نمایند.

مهاجمان و افراد غیر مجاز دارای آگاهی لازم در خصوص مکان هائی که ممکن است داده ها در آنجا مخفی شده اند نیز می باشند. برخی از کاربران به منظور مخفی نمودن فایل های مورد نظر خود، آنان را در یک مکان غیرمتداول و در یک دایرکتوری خاص نظیر دایرکتوری های سیستم ذخیره می نمایند. یک جستجوی ساده برای نوع های خاصی از فایل (نظیرjpeg و یا gif) و یا فایل هائی با ظرفیت بالا که تعمدا" مخفی شده اند، باعث افشای آنان می گردد. مهاجمان و افراد غیرمجازی که اقدام به کنکاش در یک سیستم می نمایند، سعی می نمایند که پس از اتمام عملیات خود وضعیت هارددیسک را به حالت اولیه برگردانند. با توجه به این که هر گونه تلاش در جهت بازیافت اطلاعات ممکن است تغییر داده و ساختار اطلاعاتی موجود بر روی یک هارد دیسک را بدنبال داشته باشد،

مهاجمان در ابتدا اقدام به ایجاد نسخه های ثانویه از اطلاعات موجود بر روی یک هارددیسک نموده و در ادامه عملیات مورد نظر خود را بر روی آنان انجام می دهند (نسخه های ثانویه در سطح بیت ایجاد می گردد). در برخی موارد مهاجمان و افراد غیر

مجاز اقدام به نصب Spyware (برنامه های جاسوسی) و یا سخت افزار خاصی بر روی سیستم نموده تا به سادگی اقدام به جمع آوری و ارسال اطلاعات به یک آدرس مشخص شده را بنمایند. در اینجا لازم است به نقش خطرناک نرم افزارهای موسوم به لاگرها(loggers) نیز اشاره گردد که به صورت سخت افزاری و یا نرم افزاری ارائه می شوند. لاگرها، قادر به انجام عملیات متفاوت و در ابعاد گسترده ای می باشند. ثبت تمامی اطلاعات تایپ شده توسط صفحه کلید، مانیتور نمودن صفحه نمایشگر و گرفتن تصاویر لازم از اطلاعات موجود بر روی نمایشگر، تکثیر پیام های پست الکترونیکی و ذخیره آنان در یک فولدر خاص و یا حتی ارسال آنان به افراد و یا مراکزی خاص بر روی اینترنت بدون آگاهی کاربران، نمونه هائی از عملکرد مخرب لاگرها می باشد.

نحوه حفاظت و ایمن سازی سیستم

در این رابطه می توان اقدامات زیر را انجام داد:

- حصول اطمینان از خالی بودن فولدر Deleted Items برنامه پست الکترونیکی، حذف history مرورگر و Cache مربوط به نگهداری موقت فایل های اینترنت و تمامی فایل های temp در زمان Sign on
- حساسیت لازم در خصوص فایل های موجود در فولدر Downloads ، لاگ مربوط به برنامه ها(نظیر برنامه IM)، و history lists برنامه های متفاوت
- پیکربندی سیستم به منظور عدم نگهداری لیستی از اسنادی که اخیرا" با آنان کار شده است
- رمزنگاری اسناد و فایل های حاوی اطلاعات حساس
- استفاده از رمزهای عبور مناسب در رابطه با account مربوط به Email و سایر نرم افزارهای حفاظت شده
- خاموش نمودن کامپیوتر به منظور پاک نمودن حافظه اصلی

-
- حذف فایل های page و یا swap مربوط به حافظه مجازی قبل از خاموش نمودن سیستم (فایل های فوق پس از راه اندازی مجدد کامپیوتر ایجاد خواهند شد). در صورتی که قصد فروش و یا ارتقای سیستم خود را دارید و نگران اطلاعات موجود بر روی هارد دیسک آن می باشید، فرمت کردن آن به تنهائی کفایت نخواهد کرد. در چنین مواردی لازم است از یک برنامه overwriting به منظور بازنویسی اطلاعات بر روی دیسک و آنهم چندین مرتبه، استفاده گردد. برنامه های زیر نمونه هائی در این زمینه می باشند.

- Cyber scrub
- Wipe Drive
- Data Gone

داده ها و یا اطلاعات دارای نقشی اساسی در عصر حاضر می باشند. اهمیت این موضوع به حدی است که عصر حاضر را عصر اطلاعات نامیده اند. کامپیوتر نیز در این هنگامه توانسته است با توجه به توان بالای پردازش، سرعت مطلوب در امر ذخیره و بازیابی اطلاعات نقشی محوری و تعیین کننده را برعهده بگیرد. صیانت از اطلاعات حساس موجود بر روی هر کامپیوتر وظیفه ای مهم برای هر کاربر کامپیوتر است. برخی از داده های حساس در مکان های خاصی بر روی کامپیوتر ذخیره و بنوعی مخفی نگاه داشته می شوند. مهاجمان و یا افراد غیر مجاز که تمایل و علاقه به وارسی و کنکاش در سیستم های کامپیوتری را دارند، می توانند با مراجعه به محل اختفای داده ها و بازیابی آنان، اطلاعات زیادی را در خصوص استفاده کننده کامپیوتر کسب نمایند. با کمی صبر و حوصله و دانش اندکی نسبت به کامپیوتر می توان تمهیدات امنیتی لازم در این خصوص را اندیشید و پیشگیری لازم را انجام داد. دستیابی و استفاده از داده های حساس توسط افراد غیرمجاز مهمترین تهدید امنیتی در حال حاضر است که می بایست همواره نسبت به آن حساسیت خاصی را داشت.

Spam

Spam یکی از متداولترین و در عین حال منفی ترین جنبه های دارا بودن یک آدرس Email است. با این که در حال حاضر و با توجه به تکنولوژی های موجود امکان حذف کامل این نوع از نامه های الکترونیکی ناخواسته وجود ندارد، ولی می توان با استفاده از برخی روش های موجود تعداد آنان را کاهش داد.

Spam چیست ؟

Spam ، نسخه الکترونیکی از " نامه های بدرد نخور " است. واژه Spam به پیام های الکترونیکی ناخواسته، اطلاق می گردد. این نوع از نامه های الکترونیکی ارتباط مستقیمی با ویروس نداشته و حتی ممکن است پیام هائی که از منابع معتبر ارسال شده اند نیز در زمره این گروه قرار گیرند.

چگونه می توان میزان Spam را کاهش داد ؟

با رعایت برخی نکات، می توان میزان Spam دریافتی را بطرز محسوسی کاهش داد:

- **آدرس Email خود را بدون دلیل در اختیار دیگران قرار ندهید** . آدرس های پست الکترونیکی به اندازه ای متداول شده اند که شما می توانید بر روی هر فرمی که به منظور کسب اطلاعات شما در نظر گرفته می شود، وجود فیلد خاصی به منظور دریافت آدرس Email را مشاهد نمائید. تعدادی زیادی از مردم بدون درنظر گرفتن مسائل جانبی، آدرس Email خود را در هر محلی و یا هر فرمی درج می نمایند. مثلا" شرکت ها، اغلب آدرس ها را در یک بانک اطلاعاتی ثبت تا بتوانند وضعیت مشتریان خود را در آینده دنبال نمایند. برخی اوقات، اطلاعات فوق به سایر شرکت ها فروخته شده و یا امکان استفاده مشترک برای آنان، فراهم می گردد. بدیهی است در چنین مواردی ممکن است برای شما یک Email و از طرف شرکتی ارسال شود که نه توقع آن را داشته اید و نه از آنان درخواستی مبنی بر ارائه اطلاعات خاصی را داشته اید.

- **بررسی سیاست های محرمانگی**. قبل از ارسال آدرس Email خود به صورت online، بدنبال Privacy سایت مورد نظر بگردید. تعداد بسیار زیادی از سایت های شناخته شده و خوشنام دارای یک لینک خاص بر روی سایت خود به منظور آشنائی کاربران با سیاست های آن سایت در خصوص نحوه برخورد با اطلاعات ارسالی شما می باشند. (همواره این پرسش را برای خود مطرح نمائید که آیا ما آدرسEmail خود را در سایت هائی درج می نمائیم که نسبت به آنان شناخت کافی داریم ؟). شما می بایست قبل از ارسال آدرس Email خود و یا سایر اطلاعات شخصی، سیاست های اعلام شده توسط سایت مورد نظر را مطالعه نموده و از این موضوع آگاه شوید که مالکین و یا مسئولین سایت قصد انجام چه کاری را با اطلاعات ارسالی شما دارند.
- **دقت لازم در خصوص گزینه هائی که به صورت پیش فرض فعال شده اند.** زمانی که شما برای دریافت خدمات و یا Account جدید عملیات sign in را انجام می دهید، ممکن است بخشی وجود داشته باشد که به شما مجموعه ای از گزینه ها را در خصوص دریافت email در خصوص محصولات و یا سرویس های جدید، ارائه نماید. در برخی مواقع، گزینه ها به صورت پیش فرض انتخاب شده اند، بنابراین در صورتی که شما آنان را به همان وضعیت باقی بگذارید، در آینده نه چندان دور برای شما حجم زیادی از نامه های الکترونیکی که شاید انتظار آنان را نداشته باشد، ارسال گردد.
- **استفاده از فیلترها**: تعدادی زیادی از برنامه های پست الکترونیکی امکان فیلترینگ را ارائه می نمایند. پتانسیل فوق به شما این اجازه را خواهد داد که آدرس های خاصی را بلاک نموده و یا امکان دریافت نامه را صرفا" از طریق لیست تماس موجود بر روی کامپیوتر خود، داشته باشید. برخی مراکز ارائه دهنده خدمات اینترنت(ISP) نیز سرویس فیلترینگ و علامت گذاری مربوط به مقابله با Spam

- را ارائه می نمایند. در چنین مواردی ممکن است پیام های معتبری که بدرستی طبقه بندی نشده باشند به عنوان spam درنظر گرفته شده و هرگز به صندوق پستی شما ارسال نگردند.
- **هرگز برروی لینک های موجود در یک Spam ، کلیک ننمائید** . برخی از منابع ارسال کننده Spam با ارسال آدرس هـــــای Email متغیـــر در یک Domain خاص، سعی در تشخیص معتبر بودن یک آدرس Email می نمایند. (مثلا" تشخیص آدرس های Email معتبر موجود بر روی hotmail و یا yahoo). در صورتی که شما بر روی یک لینک ارسالی توسط یک Spam کلیک نمائید، صرفا" معتبر بودن آدرس Email خود را به اطلاع آنان رسانده اید. پیام های ناخواسته ای که یک گزینه "عدم عضویت " وسوسه انگیز را در اختیار شما قرارمی دهند، اغلب به عنوان روشی به منظور جمع آوری آدرس های Email معتبر مورد استفاده قرار گرفته که در آینده از آنان به منظور ارسال Spam استفاده گردد.
- **غیرفعال نمودن گزینه دریافت اتوماتیک گرافیک در نامه های الکترونیکی با فرمت HTML** . تعداد زیادی از شرکت ها، نامه های الکترونیکی را با فرمت HTML و همراه با یک فایل گرافیکی لینک شده ارسال نموده که در ادامه از آن به منظور ردیابی فردی که پیام الکترونیکی را باز نموده است، استفاده می نمایند. زمانی که برنامه سرویس گیرنده پست الکترونیکی شما، اقدام به download گرافیک از سرویس دهنده آنان می نماید، آنان می دانند که شما پیام الکترونیکی را باز نموده اید. با غیر فعال نمودن HTML mail و مشاهده پیام ها با فرمت صرفا" متن، می توان پیشگیری لازم در خصوص این مسئله را انجام داد.
- **ایجاد و یا باز نمودن Account های جدید اضافی**: تعداد زیادی از سایت ها، اقدام به عرضه آدرس پست الکترونیکی به صورت رایگان می نمایند.

- در صورتی که شما بطور مداوم اقدام به ارسال آدرس Email خود می نمائید (برای خرید online ، دریافت سرویس و ...)، ممکن است مجبور به ایجاد یک account دیگر به منظور حفاظت آدرس account اولیه خود در مقابل spam شوید. شما همچنین می بایست از یک account دیگر در زمانی که اطلاعاتی را بر روی بولتن های خبری online، اطاق های چت، لیست های عمومی Mailing و یا USENET ارسال می نمائید، استفاده نمائید. بدین ترتیب می توان یک سطح حفاظتی مناسب در خصوص دریافت spam به آدرس Email اولیه خود را ایجاد کرد.
- **برای سایرین Spam ارسال ننمائید.** یک کاربر متعهد و دلسوز باشید. در خصوص پیام هائی که قصد فوروارد نمودن آنان را دارید، سختگیرانه عمل کنید. هرگز هرگونه پیامی را برای هر شخص موجود در لیست دفترچه آدرس خود فوروارد نکرده و اگر فردی از شما بخواهد که پیامی را برای وی فوروارد ننمائید، به درخواست وی احترام بگذارید.

Spyware

اینترنت با سرعتی باورنکردنی همچنان به رشد خود ادامه می دهد و این پدیده نسبتا" جدید بشریت مورد توجه تمامی افراد و سازمان ها با اهداف مثبت و منفی قرار گرفته است. استفاده از اینترنت برای آگهی های تجاری و بازرگانی از جمله موارد فوق است. در صورتی که فرآیند پخش آگهی های تجاری با آگاهی و رضایت استفاده کننده اینترنت باشد، نمی توان چندان بر آن خرده گرفت ولی در صورتی که فرآیند فوق بدون آگاهی و یا کسب مجوز کاربران انجام شده و با نصب یک برنامه ناخواسته از سیستم های آنان برای ارسال آگهی های تجاری استفاده شود، حریم خصوصی کاربران در معرض تهدید قرار گرفته و این موضوع می تواند پیامدهای بمراتب خطرناکتری را بدنبال داشته باشد و آن زمانی است که اینگونه نرم افزارها از محدوده وظایف خود تعدی نموده و اقدام به جمع آوری و ارسال اطلاعات شخصی کاربران، بدون آگاهی و رضایت آنان می نمایند. ما امروزه شاهد تولد نسل جدیدی از نرم افزارهای جاسوسی می باشیم که از آنان با نام Spyware یاد می گردد. نصب اینگونه نرم افزارهای ناخواسته، مسائل متعددی را برای کاربران بدنبال خواهد داشت.

SpyWare چیست ؟

Spyware ، نرم افزاری است که اقدام به جمع آوری اطلاعات شخصی بدون آگاهی و یا اجازه کاربران می نماید. اطلاعات جمع آوری شده می تواند شامل لیست سایت های مشاهده شده توسط کاربر و یا اطلاعات بمراتب حساس تری نظیر نام و رمز عبور باشد. به این نوع برنامه ها adware نیز گفته می شود. نرم افزارهای فوق پس از نصب بر روی کامپیوتر، قادر به ارسال آگهی های تجاری pop-up ، هدایت مرورگر به

وب سایت هائی خاص، ارسال لیست سایت های مشاهده شده توسط کاربر و یا مانیتورینگ عملکرد کاربران در زمان اتصال به اینترنت می باشند. برخی از برنامه های Spyware ، قادر به ردیابی و تشخیص اطلاعات تایپ شده از طریق صفحه کلید نیز می باشند. با توجه به انجام پردازش های اضافی توسط اینگونه نرم افزارها، سیستم های کاربران کند و کارآئی آنان بطرز محسوسی کاهش خواهد یافت. در صورت دریافت موزیک از طریق برنامه های اشتراک فایل، بازی های رایگان از سایت های ناامن و یا سایر نرم افزارها از منابع ناشناخته، شرایط لازم به منظور نصب اینگونه نرم افزارها و در نهایت آلودگی سیستم فراهم می گردد.

نحوه تشخیص Spyware

علائم زیر می تواند نشاندهنده نصب Spyware بر روی یک کامپیوتر باشد:

- نمایش مستمر پنجره های pop-up آگهی
- هدایت ناخواسته کاربران به وب سایت هائی که هرگز نام آنان در مرورگر تایپ نشده است.
- نصب Toolbars جدید و ناخواسته در مرورگر وب
- تغییر ناگهانی و غیرمنتظره صفحه اصلی مرورگر(home page)
- تغییر موتور جستجوی مرتبط با مرورگر پس از کلیک بر روی دکمه Search همراه مرورگر
- عدم عملکرد صحیح برخی کلیدها در مرورگر (نظیر کلید Tab زمانی که بر روی فیلدهای یک فرم حرکت می شود)
- نمایش تصادفی پیام های خطاء
- کاهش ملموس سرعت کامپیوتر در زمان فعال نمودن برنامه ها و یا انجام عملیاتی خاص (ذخیره فایل ها و ...)

- فعال شدن مرورگر و بدنبال آن وب سایت های آگهی بدون انجام عملیاتی خاص توسط کاربر
- عدم کارکرد صحیح لینک های همراه یک برنامه
- توقف ناگهانی و غیرمنتظره مرورگر وب
- عدم عملکرد صحیح برخی از عناصر سیستم عامل و یا سایر برنامه ها

نحوه پیشگیری از نصب Spyware

- **عدم کلیک بر روی لینک های موجود در پنجره های pop-up** . با توجه به این که پنجره های pop-up اغلب محصول و یا نوع خاصی از Spyware می باشند، کلیک بر روی آنان می تواند باعث نصب یک نرم افزار Spyware گردد. برای بستن این نوع پنجره ها از آیکون "X" در titlebar استفاده گردد(در مقابل لینک close همراه پنجره).
- **پاسخ منفی به سوالات ناخواسته**: در صورت برخورد با جعبه های محاوره ای که درخواست اجرای یک برنامه را نموده و یا قصد انجام عملیات خاص دیگری را دارند، همواره گزینه NO و یا Cancel انتخاب گردد. در موارد خاص می توان از آیکون "X" موجود در titlebar استفاده نمود.
- **دقت لازم در خصوص دریافت نرم افزارهای رایگان از اینترنت**: سایت های زیادی اقدام به ارائه Toolbar های سفارشی و یا ویژگی های خاص دیگری می نمایند. تا زمانی که نسبت به ایمن بودن این نوع سایت ها اطمینان حاصل نشده است، نمی بایست فایل و یا برنامه ای را از طریق آنان Download نمود.
- **عدم کلیک بر روی لینک های موجود در Email که ادعای ارائه یک نرم افزار Anti-Spyware را دارند**. نظیر ویروس های کامپیوتری،

لینک های موجود در نامه های الکترونیکی ممکن است اهداف سودمندی را دنبال ننموده و نصب Spyware بر روی سیستم شما را بدنبال داشته باشند.

علاوه بر موارد فوق و خصوصا" در مواردی که احساس می شود بر روی کامپیوتر Spyware نصب شده است و قصد داشته باشیم عملکرد آن را به حداقل مقدار خود برسانیم می توان عملیات زیر را انجام داد:

- **اعمال محدودیت در رابطه با پنجره های Pop-up و کوکی ازطریق تنظیمات برنامه مرورگر**: پنجره های pop-up توسط نوع خاصی از اسکریپت ها و یا محتویات فعال(اپلت های جاوا، کنترل های اکتیوایکس) ایجاد می گردند. با تنظیم مناسب پارامترهای برنامه مرورگر، می توان محدودیت لازم در اجرای اسکریپت ها، اپلت های جاوا، کنترل های اکتیو ایکس و تعداد پنجره های pop-up را اعمال نمود. عملکرد برخی از کوکی ها مشابه Spyware می باشند، چراکه از طریق آنان مشخص خواهد شد که شما چه وب سایت هائی را مشاهده نموده اید. با تنظیم پارامترهای برنامه مرورگر می توان محدودیت لازم در خصوص ایجاد کوکی ها را اعمال نمود.

نحوه حذف Spyware

- **اجرای یک برنامه ضد ویروس و پویش کامل کامپیوتر**: برخی از نرم افزارهای آنتی ویروس قادر به یافتن و حذف برنامه های Spyware می باشند.
- **اجرای یک برنامه معتبر که مختص حذف Spyware طراحی شده است.** تعداد زیادی از تولیدکنندگان محصولاتی را به منظور شناسائی وحذف برنامه های Spyware ، ارائه داده اند.

Adaware, Webroot's SpySweeper, PestPatrol, LavaSoft's Spybot Search and Destroy ، نمونه هائی در این زمینه می باشند.

نرم‌افزارهای جاسوسی و مقابله با آنها (۱)

نرم‌افزار جاسوسی چیست؟

حتما تاحالا برایتان پیش آمده است که در حال کار با اینترنت ناگهان پنجره‌های مختلف زیادی بدون میل شما باز می‌شوند که اصطلاحا popup windows نام دارند و وقت زیادی را باید برای بستن آنها صرف کنید. اگر در آن موقع کم‌حوصله باشید سریعا از کوره در میروید! این مطلب به شما کمک می‌کند که متوجه شوید این پنجره‌های مزاحم از کجا می‌آیند.

نرم‌افزار جاسوسی هر نوع فناوری یا برنامه روی کامپیوتر شماست که اطلاعات را بطور پنهانی جمع‌آوری می‌کند. این دیتا سپس به تبلیغ‌کنندگان یا به سایر گروه‌های علاقه‌مند

فروخته می‌شود. نوع اطلاعاتی که از کامپیوتر شما جمع‌آوری می‌شود متفاوت است. بعضی نرم‌افزارهای جاسوسی فقط اطلاعات سیستمی شما را ردیابی می‌کنند – مانند نوع اتصال شما به اینترنت و سیستم‌عامل کامپیوترتان. بقیه نرم‌افزارهای جاسوسی اطلاعات فردی را جمع‌آوری می‌کنند ـ مانند ردگیری عادات و علائق شما در هنگام کار با اینترنت و یا گاهی بدتر، با فایلهای شخصی شما سروکار دارند. نرم‌افزار جاسوسی بدون رضایت و اجازه کاربر نصب می‌گردد. (چنانچه به یک شرکت اجازه جمع‌آوری دیتا را بدهید، دیگر نام این عمل جاسوسی نیست، بنابراین همیشه قبل از اجازه دادن، موارد افشای دیتا بصورت آنلاین را با دقت بخوانید). بعضی افراد به جاسوسی عمومی که گرایشات اینترنتی و نرم‌افزاری را ردگیری می‌کند تا جاییکه اطلاعات مشخصه فردی را شامل نشود، اعتراضی ندارند. اما بقیه به هر نوع دیتایی که بدون اجازه از کامپیوترشان برداشته می‌شود، معترض هستند. بهرحال، نرم‌افزار یا ابزاری که این اطلاعات را جمع‌آوری می‌کند، نرم‌افزار جاسوسی نامیده می‌شود.

نصب نرم‌افزار جاسوسی روی کامپیوتر شما می‌تواند با مشاهده یک وب‌سایت، دیدن یک ایمیل به فرمت HTML یا با کلیک‌کردن یک پنجره بازشونده (pop-up) آغاز شود. روند دانلود به شما اطلاع داده نمی‌شود، بنابراین شما از اینکه کامپیوترتان پذیرای یک نرم‌افزار جاسوسی شده است، بی‌اطلاع خواهید ماند.

تولد نرم‌افزارهای جاسوسی

قبل از ظهور نرم‌افزارهای جاسوسی تبلیغ اینترنتی از طریق قرار دادن bannerهایی بود که در صفحات وب قابل مشاهده بود (البته هنوز هم وجود دارند)، و کاربران با کلیک

کردن روی آنها از اطلاعات یا خدمات ارائه‌شده به دلخواه آگاهی می‌یافتند. اما بتدریج کاربران از این نحو تبلیغ خسته شده‌بودند و به این ترتیب تبلیغ‌کنندگان در حال ورشکستگی بودند، زیرا میزان درآمد آنها متناسب با میزان کلیک از طرف بازدیدکنندگان بر روی تبلیغاتی بود که بر روی وب‌سایت خود قرار می‌دادند.

تبلیغ‌کنندگان دریافتند که اگر همچنان می‌خواهند از طریق اینترنت درآمد داشته باشند، مجبور به تغییر تاکتیکهایشان هستند. بسیاری از آنها دریافت خود را بر اساس میزان واقعی فروش قرار دادند. بقیه به راههای جدید تبلیغ فکر کردند. آنها به روشی تازه رسیدند که به آنها اجازه تبلیغ محصولات را بدون داشتن وب‌سایت یا سرویس‌دهنده می‌داد و به این ترتیب نرم‌افزارهای جاسوسی پدید آمدند.

در ابتدا نرم‌افزار جاسوسی در دل برنامه‌های رایگان قرار می‌گرفت، اما بعده‌ها به حقه‌های کثیف‌تری! رو آوردند و آن استفاده از سوءاستفاده‌های هکری برای نصب نرم‌افزار جاسوسی روی کامپیوترهاست. اگر از سیستم‌های عامل رایج استفاده می‌کنید شانس شما برای داشتن نرم‌افزار جاسوسی روی سیستم‌تان بیشتر است. براحتی می‌توان ادعا کرد که بسیاری از کاربران خانگی بر روی کامپیوتر خود جاسوس! دارند.

انواع نرم افزارهای جاسوسی

همانطور که گفته شد، نرم افزار جاسوسی هر نوع نرم افزاری است که اطلاعات را از یک کامپیوتر بدون آگاهی کاربر بدست میاورد. انواع زیادی از این نوع نرم افزارها در اینترنت فعال هستند اما میتوان آنها را به دو گروه عمده تقسیم کرد:

نرم‌افزار جاسوسی خانگی (Domestic Spyware)

نرم‌افزاری است که معمولا توسط صاحبان کامپیوترها بمنظور آگاهی یافتن از تاثیرات اینترنت برروی شبکه های کامپیوتری خودشان، خریداری و نصب می گردد. مدیران از این نرم افزار برای آگاهی از فعالیتهای آنلاین کارمندان استفاده می کنند. بعضی افراد نیز برای اطلاع از فعالیتهای سایر اعضاء خانواده استفاده می کنند (مانند مشاهده محتویات اتاقهای گفتگو توسط والدینی که کودکانشان در آنها شرکت می کنند)

یک شخص ثالث نیز می تواند نرم‌افزار جاسوسی را بدون آگاهی صاحب کامپیوتر نصب کند. مجریان قانون از نرم افزارهای جاسوسی برای آگاهی یافتن از فعالیت مجرمانی

استفاده میکنند که این مجرمان خود از همین نرم افزارهای جاسوسی برای حصول اطلاعات از کامپیوترهای شخصی به قصد دزدی دارایی‌ها استفاده کرده‌اند.

نرم افزار جاسوسی تجاری (Commercial Spyware)

این نرم‌افزار که بعنوان adware نیز شناخته می‌شود، نرم‌افزاری است که شرکتها برای تعقیب فعالیتهای وبگردی کاربران اینترنت استفاده می کنند. این شرکتها اغلب اطلاعات حاصل را به بازاریابان می فروشند و آنها کاربران را با تبلیغات خاص مورد هدف قرار می‌دهند – منظور تبلیغاتی است که با علائق کاربر مطابقت دارد و به احتمال زیاد برای وی جذاب است.

بدست آوردن اطلاعات به این سادگی موجب خوشحالی تبلیغ‌کنندگان می‌شود. سابقا، بازاریابان برای فهمیدن علائق افراد باید آنها را از طریق برگزاری مسابقات یا موارد مشابه تطمیع می کردند. آن روشهای کسب اطلاعات شخصی هنوز وجود دارد، اما در آن روشها قدرت خواندن و اطلاع از سرنوشت اطلاعات شخصی و پذیرفتن یا نپذیرفتن آنها توسط افراد وجود دارد. بهرحال، اطلاع از سلیقه‌های شما بصورت پنهانی با استفاده از نرم افزارهای جاسوسی بسیار آسانتر است و تصویر بسیار کاملتری به صنعت بازایابی ارائه می کند. در کل می توان ادعا کرد که نرم افزارهای جاسوسی همه جا هستند.

نرم‌افزارهای جاسوسی و مقابله با آنها (۲)

انواع و اهداف نرم‌افزارهای جاسوسی مختلف

نرم‌افزارجاسوسی هرچه نباشد، حداقل یک عامل آزاردهنده است که سرعت کامپیوتر را کم می‌کند، هارددیسک سیستم را بی‌جهت پر می‌کند و کامپیوتر شما را به هدفی برای تبلیغ‌کنندگان تبدیل می‌کند. فراتر از آگاهی از اطلاعات خصوصی شما، نرم‌افزار جاسوسی می‌تواند بعنوان ابزاری برای جرائمی مانند تقلب در شناسایی مورد استفاده قرار گیرد. در ادامه لیستی از انواع مختلف نرم‌افزارهای جاسوسی و هدفشان ارائه می‌شود.

ثبت‌کنندگان نشانی‌های وب و صفحات نمایش

ثبت‌کنندگان نشانی‌های وب، وب‌سایتها و صفحات دیده‌شده را ردیابی می‌کنند. ثبت‌کنندگان صفحه‌نمایش می‌توانند یک تصویر سیاه‌وسفید کوچک (برای کم‌کردن حجم تصویر) از صفحه پیش‌روی شما در هر زمان بگیرند و این تصاویر را بدون اطلاع شما ذخیره یا ارسال کنند. این روشها برای جاسوسی‌های خانگی متداول هستند.