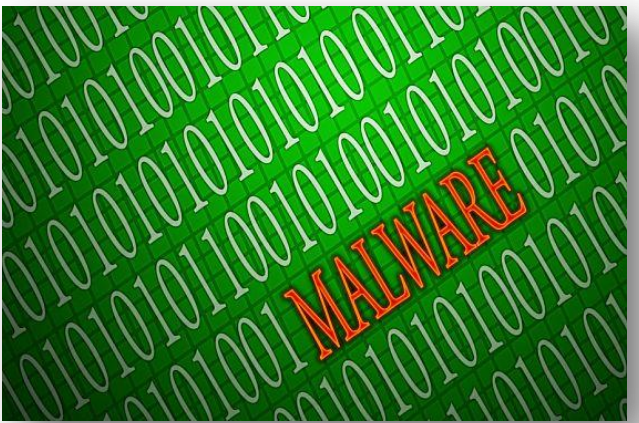
نیمه پنهان



فهرست

مقدمه

یک بدافزار رایانه‌ایبا وجود حجم کم می‌تواند اقداماتی فوق‌العاده خرابکارانه انجام دهد. به‌طوریکه امروزه انواع مختلف و متنوع بدافزارها به عنوان سلاح‌های نوین در جنگ سایبر به وفور مورد استفاده قرار می‌گیرد.

اولین بدافزار رایانه‌ای در سال ۱۹۸۵ به نام Brain نوشته شد و از آن به بعد برنامه‌نویسان حرفه‌ای با مقاصد مختلف اقدام به نوشتن بدافزار رایانه‌ای کردند. دلیل اینکه یک بدافزارمی‌تواند نوشته شود و سامانه‌های آلوده را از کار بیاندازد به ضعف‌هایی که متأسفانه در نوشتن سیستم‌عامل‌های مختلف برای رایانه‌ها وجود دارد،باز می‌گردد. برنامه نویسان اولیه سیستم‌عامل‌ها به تنها چیزی که فکر نمی‌کردند مسئله امنیت بود و در نتیجه وقتی محصولاتشان به بازار آمد مورد سوءاستفاده قرار گرفت. متأسفانه با ساختار فعلی رایانه‌هانیز حذف مشکلی به نام بدافزار رایانه‌ای عملاً غیرممکن می‌نماید و هر ساله بر میزان این تهدیدات افزوده می‌شود. تهدیداتی که امنیت ملی کشورها را به مخاطره می‌اندازد.

در این کتابچه ضمن آشنایی با اهداف ویروس‌نویسی به بررسی گوشه هایی نحوه استفاده سرویس های جاسوسی جهان از این ابزار می پردازیم.

فصل ۱

بررسی اهداف و انگیزه‌های شیوع بدافزارنویسی

بدافزارنویسان به دلایل گوناگونیاقدام به نوشتن بدافزارمی‌کنند که می‌تواند جنبه‌های مادی یا غیر مادی داشته باشد.عمده‌ترین دلایل نوشتن بدافزارهای رایانه‌ای عبارت است از:

- نارضایتی از شخص، سازمان ، یا کشور هدف

نارضایتی از عملکرد یک سازمان یا کشورمی‌تواند انگیزه نوشتن بدافزارباشد. به طور مثال در یک مورد نارضایتی دانشجویان از استادشان باعث تولید یک بدافزار شد.مقصود از نوشتن این بدافزار اثبات توانمندی دانشجویان به استادشان بود. چرا که استاد آن‌ها را بی سواد خطاب کرده بود.

- سرقت، تغییر و انهدام اطلاعات به جهت سوء استفاده مالی

به دست آوردن نام و رمز عبور کاربران جهت سوء استفاده مالی از دیگر اهداف بدافزارنویسان است که با ارسال کلیدهای زده شده توسط سامانه آلوده به مرکز خاصی می‌تواند به نویسنده بدافزار امکان سوء استفاده از این دسترسی‌ها را بدهد. سالانه میلیون‌ها دلار از حساب‌های کاربران رایانه‌ها در سراسر جهان برداشت می‌شود که عملاً امکان ردیابی آنان برای احقاق حقشان وجود ندارد.

- خودنمایی و اثبات توانمند بودن بدافزار نویس

بدافزار نویسان زیادی هستند که توانایی فکری بالایی داشته و همواره سعی می‌کنند با نوشتن یک بدافزار و قرار دادن نام اختصاری خود در آن به سایر افراد و گروه‌های برنامه نویس توانایی خود را اثبات کنند. البته این خودنمایی در همایش سالانه نفوذگران کلاه سفید نیز ظهور پیدا می‌کند و مدیران امنیت سازمان‌ها سعی در به استخدام در آوردن اینگونه افراد می‌کنند.

- حفاظت از برنامه‌های عرضه شده به بازار در مقابل تکثیر غیر مجاز

تعدادی از نرم‌افزارهای موجود در بازار به صورتی طراحی شده اند که چنانچه غیر مجاز تکثیر و مورد استفاده قرار گیرند اقدام به تکثیر بدافزاری در رایانه می‌کنند. این هشدار برای کسانی است که حقوق مالکیت معنوی تولید کنندگان نرم‌افزار را رعایت نمی‌کنند. البته اینکه صدمات نهایی این بدافزار به چه کسانی خواهد خورد خیلی کنترل شده نیست ولی به هر حال دوستان فرد استفاده کننده از نرم‌افزار به صورت غیر مجاز نیز در معرض خطر قرار دارند.

- نمایش ضعف‌های سیستم‌عامل‌ها و برنامه‌های کاربردی

اکثر سیستم‌عامل‌ها مخصوصا سیستم‌عامل داس و ویندوز دارای نقاط ضعف اساسی در حوزه امنیت هستند و برنامه نویسان سعی در فاش کردن این حفره‌ها دارند. نوشتن یک بدافزارمی‌تواند ضربه مهلکی به سیستم‌عامل مربوطه بزند. هم اکنون میلیون‌هابدافزار به واسطه ضعف سیستم‌عامل‌های مایکروسافت تولید و تکثیر شده است هرچند به واسطه محبوبیت این سیستم‌عامل‌ها کاربران نهایی آن‌هارا کنار نگذاشته‌اند و با مشکلات آن دست و پنجه نرم می‌کنند.

- تحقیقات دانشگاهی در آزمایشگاه‌های قرنطینه شده

در یک محیط دانشگاهی و علمی،متخصصان رایانه همواره پیگیر الگوریتم‌های برنامه‌سازی جدیدتر هستند در محیط‌های آزمایشگاهی می‌توان کدهای خطرناک تولید کرد و همینطور ضد آن کدها نیز به موازات تولید شده و در اختیار نرم افزارهای ضد بدافزار قرار داده می‌شود تا چنانچه دراثرسهلانگاریبدافزارازمحیطآزمایشگاهیخارجشدبهرایانه‌ها نتواند صدمه‌ای بزند.

- ایجاد تبلیغات برای محصول و شرکتی خاص

بر سر زبان افتادن نام تجاری و یا باز کردن صفحات وب محصول و یا شرکت خاصی می‌تواند انگیزه مالی برای نویسندگان بدافزار داشته باشد. البته در چنین حالتی خطری برای کاربران به وجود نمی‌آید ولی به هر حال علاوه بر سربار به وجود آمده می‌توان به ناخواسته بودن آن اشاره کرد که معمولا کاربران را کلافه می‌کند.

- مردم آزاری و لذت بردن از آزار دیگران

همواره افرادی هستند که سعی می‌کنند دیگران را اذیت کنند. این کار در حوزه فناوری اطلاعات نیز به صورت تولید و تکثیر بدافزار مشاهده می‌گردد. نوشتن پیغام آزاردهنده و نمایش عکس‌های ناخواسته می‌تواند این مردم آزاری را شدت دهد.

- ایجاد فرصت تجاری جهت ارایه سرویس بدافزار زدایی

نوشتن بدافزار و ضد آن به طور همزمان و فروش آن به یک شرکت ضد بدافزار برای پشتیبانی و جلو افتادن از سایر رقبا یکی دیگر از انگیزه‌های مادی بدافزارنویسان است. در اسفند ماه ۱۳۸۷ یک بدافزار قوی به نامVirutدر سراسر جهان پخش شدکه بلافاصله ضد بدافزار کسپرسکی بعد از دو روز روتین شناسایی و پاکسازی آن را به صورت کامل ارایه داد در حالی که دیگر محصولات حدود یک هفته طول کشید تا روتین شناسایی را عرضه کنند. در نهایت بعد از گذشت یک ماه فقط چند ضد بدافزار روتین پاکسازی را ارایه کردند که بعضا ایراداتی نیز داشته و الباقی نیز هنوز روتین پاکسازی را ارایه نکرده اند. حال سؤال اینجاست که چطور کسپرسکی توانست فقط در عرض ۴۸ ساعت روتین پاکسازی بدافزاری را ارایه دهد که از لحاظ پیچیدگی به شکلیبود که هیچ شرکت ضد بدافزاری نتوانست زیر یک ماه این روتین را ارایه دهد.

اهداف و انگیزه‌های دیگری نیز می‌توان برای نوشتن بدافزار متصور بود که دارای وزن کمتری است و ما از ذکر آنها چشم پوشی می‌کنیم.

موضوع نگارش بدافزارهای مختلف و انتشار آن تنها به تعدادی برنامه نویس یا انجمن‌های هکری محدود نمی‌شود. در ادامه تلاش می‌شود تا به بررسی رفتار برخی سازمان‌های رسمی‌که از بدافزارهای مختلف جهت پیشبرد اهداف خود استفاده می‌کنند، اشاره می‌شود.

سازمان‌های انتظامی‌و قضایی

سازمان‌های انتظامی‌و قضایی برخی کشورها (از قبیل پلیس و آگاهی) برای اثبات وقوع جرم و همینطور کشف جرم از مین گذاری در رایانه‌ها استفادهمی‌کنند به نحوی که وقتی به محل وقوع جرم رسیدند بتوانند از لایه‌های پنهان رایانه استفاده کرده تا به اهداف و اطلاعات کاربری که با آن کار می‌کرده برسند.

همکاری با شرکت‌های سیستم‌عامل‌نویس در این زمینه در همان اوایل کار آغاز شد تا با تعبیه درب‌های پشتی در سیستم‌عامل‌ها بتوانند آخرین اطلاعات پاک شده را بدست آورند. البته همواره شرکت‌های تولید کننده سیستم‌عامل مخصوصاً شرکت مایکروسافت این موضوع را انکار کرده است ولی همواره هکرها در بر ملا کردن اینگونه درب‌های پشتی سیستم‌عامل‌ها تعللی نکرده و توانسته‌اند درب‌های پشتی که چه به عمد و چه به سهو قرار داده شده را آشکار کنند. شرکت‌های سازنده نیز با ارسال وصله‌های امنیتی درب‌های پشتی آشکار شده مسدود می‌کنند، ولی معلوم نیست از طریق همین وصله‌هاچند درب پشتی دیگر اضافه می‌شود!

سازمان‌های امنیتی و اطلاعاتی

سازمان‌های اطلاعاتی امنیتی کشورها با ظهور پدیده بدافزارهای رایانه ای به فکر فرو رفتند تا به اصلی‌ترین مشکل خود که همان مشکلات جمع‌آوری اطلاعات از مردم کشور خود و یا افراد خارجی بود خاتمه بدهند، زیرا به دست

آوردناطلاعات از افراد و مراکز نظامی‌و امنیتی سایر کشورها فوق العاده مشکل‌زا و پرهزینه است.

به عنوان نمونهوظیفه اصلیآژانس امنیت ملی[1] آمریکا، مشهور به NSA، کهبه نحوی زیر نظر سازمان دفاع ایالات متحده آمریکا اداره می‌شود شنود دایم ارتباطات از راه دور، در سراسر جهان (تلفن همراه، نمابر، ایمیل و ارتباطات انفورماتیک) و همچنین دریافت و تحلیل تصاویر ماهواره‌ای است.

بی شک امروزه ارتباطات افراد بر روی شبکهبا استفاده از بدافزارهای رایانه ای به راحتی تحت کنترل شدید قرار دارد؛ واطلاعات ذخیره شده یا درحال تبادل جمع آوری می‌شود. در این روش در صورت صورت لو رفتن موضوع نیز مشکلی به وجود نمی‌آید.کاملاً محتمل است آژانس امنیت ملی ایالات متحده با توجه به محتواهای روی شبکه، هر لحظه آنها را کنترل کند؛ در آمریکا وضع به گونه ای است که همه شرکت‌های ارائه دهنده خدمات اینترنتی به آژانس امنیت ملی کشورشان اجازه می‌دهند، داده‌های مشتریانشان و همین طور ارتباطات اینترنتی‌شان را کنترل کنند ، به علاوه ، برخی سایت‌های اینترنتی (اغلب آمریکایی)، گاهی بدون اطلاع صاحبان آن‌ها برای کنترل محتوای رایانه‌های برخی کاربران اینترنتی، مورد استفاده قرار می‌گیرد. مدتی است که به طور مداوم این نجوا به گوش می‌رشد که شرکت بزرگ کامپیوتری «مایکروسافت» پیوند نزدیکی با آژانس امنیت ملی آمریکا دارد؛ البته این همکاری‌ها در چارچوب عملیات شنود و رهگیری انجام می‌شود. باید بگوییم تنها، آژانس امنیت ملی آمریکا اینترنت را تحت کنترل ندارد؛ بلکه تقریباً تمام سازمان‌های اطلاعاتی آمریکا سرویس‌های رهگیری و کنترل خاص خودشان را (در مورد اینترنت) دارا هستند.

---

[1] National Security Agency

فصل ۲

کارکرد پنهان دهکده جهانی

حضور بدافزاها در اوایل دهه هشتاد و استخدام بدافزار نویسان حرفه‌ای که میلیون‌ها دلار به رایانه‌ها صدمه زده بودند و عدم مجازات آن‌ها باعث شد تا به سرعت بازار نوشتن بدافزارهای هدایت شده داغ گردد. تا جایی که هر سازمانی سعی می‌کرد تا بیشترین بهره را از بدافزارها ببرد. این امر ،باعث گردید سازمان‌های جاسوسی سعی کنند از فرصت پیش آمده نهایت استفاده را بکنند. با عمومی‌شدن اینترنت در دهه ۹۰ نیز گرایش بدافزارها به سمت سرقت اطلاعات وتخریب آن‌ها پیش رفت. امروزه نیز اکثر بدافزارها جنبه تخریبی ندارند ولی اطلاعات حیاتی کاربر را در کسری از ثانیه به مراکز از پیش تعیین شده ارسال می‌کنند. در انحصار درآوردن موتورهای جستجو مانند گوگل و یاهو برای جمع آوری اطلاعات کاربران از دیگر روش‌هایی است که کشور آمریکا به دلیل داشتن توان مالی بالا توانسته است انجام دهد و با در اختیار

گذاشتن ظرفیت و سایر خدمات به صورت رایگان تقریباً تمامی کاربران سراسر جهان را به سمت خود سوق داده است و با استفاده از موتورهای تحلیل گر به راحتی می‌تواند کاربران را دسته بندی کرده و اهداف و تفکرات آنان را حدس بزنند.

امروزه سازمان‌های جاسوسی بیشترین استفاده را از فضای بوجود آمده می‌برند. یک فضای بسیار پیچیده با ظاهری ساده و کاربران عام، بهترین امکانی است که در عصر حاضر قدرت زیادی به این قبیل سازمان‌هامی‌دهد. جالب است که در حال حاضر با وجود تحریم نرم افزارهای حتی رایگان، تمامی‌ضد بدافزارهای غربی در کشور ما نماینده رسمی‌فروش داشته و ضد بدافزارهای قفل شکسته که در ایران مورد استفاده قرار می گیرند، به کندی در لیست سیاه ضدبدافزارهای خارجی قرار می گیرند!

در ادامه به منظور آشنایی خوانندگان به ذکر چند نمونه از پروژه‌های افشا شده در این زمینه می‌پردازیم.

بدافزارفانوس جادویی

فانوس جادویی[1] بدافزاری بود که در سال ۲۰۰۲ ماهیت جاسوسی آن لو رفت.فانوس جادویی توسط FBI طراحی و تولید شد. اولین گزارش‌هایی که در مورد این نرم افزار منتشر شد، مربوط به MSNBC (در نوامبر سال ۲۰۰۱) و آسوشیتدپرس است. این بدافزاردر لوای پیوست ایمیلو با سوء استفاده از رخنه‌های رایج موجود در سیستم‌عامل‌ها، در رایانه کاربران نصب می‌شود. به دنبال افشای عمومی‌این نرم افزار، مناقشات و بحث و گفتگوهای بسیاری در مورد «توانایی» یا «الزام» نرم افزارهای ضد بدافزار به شناسایی و ردگیری این جاسوس افزار FBI درگرفته است. در اینجا به عکس العمل دو مورد از شرکت‌های مطرح ضد بدافزار در این خصوص اشاره می‌شود:

---

[1] Magic Lantern

- شرکت تولید کننده ضد بدافزارمک آفی به مقامات FBI اطمینان داده که مکافی این نرم افزار را ردگیری نخواهد کرد!
- شرکت سیمانتک نیز در حال همکاری با FBI به منظور ممانعت از شناسایی این نرم‌افزار توسط نورتن است. به گفته یکی از محققان سیمانتک، محصولات ضد بدافزار نورتن به طور ویژه این تروجان را نادیده می‌گیرد.

همکاری‌های رسمی‌با مراکز و شرکت‌های حوزه ICT

کمیسیون اروپا پیش نویس قانونی را تهیه کرده است که شبکه‌های اینترنتی را ملزم می‌کند ریز اطلاعات تماس‌ها را حداقل تا ۶ ماه نگهداری کند. همچنین بر اساس همین پیش نویس، مراکز مخابراتی موظف به حفظ اطلاعات تماس‌ها حداقل تا یک سال هستند. این اطلاعات، شماره‌های گرفته شده، تماس‌های پاسخ داده شده و نشده، محل مورد استفاده، سایت‌های مشاهده شده و دیگر اطلاعات جهت بررسی‌ها و تحقیقات را شامل می‌شود.

همچنینگوگل، فهرستی از Search Stringها را از سرویس‌های جاسوسی جهان غرب همچون NSA ، CIA و سرویس‌های جدیدی که جایگزین K.G.B شده اند به شکل روزآمد دریافت می‌کند و بانکی از جستجوهای انجام شده بر اساس این رشته کلمات توسط تمامی‌جستجوگران در سرتاسر دنیا را در فهرستی جدید با اطلاعات بیشتر تهیه و به این سرویس‌ها ارسال می‌کند.این اطلاعات شامل آی پی، شماره تلفن (در صورت امکان)، موقعیت جغرافیایی، تاریخ و ساعت جستجو، سایر جستجوها، جستجوهای برگزیده و دیگر اطلاعات موجود است. علاوه بر اینگوگل، محتوای ایمیل‌های افراد در سرویس جی میل خود را برای شناخت علاقه‌مندی‌های کاربر بررسی کرده و تبلیغاتی متناسب با آن را به کاربر هنگام مشاهده ایمیل‌ها ارائه می‌دهد.

پروژه اشلون[1]

مردم آمریکا سال‌ها است به نگاه‌های بی‌پروایانه میلیون‌ها ابزار جاسوسی در زندگی خصوصیشان عادت کرده‌اند. آمریکایی‌ها سال‌هااست که می‌دانند اگر کتاب‌های فهرست سیاه اف‌بی‌آی را از کتابخانه‌ای امانت بگیرند یا از کتاب فروشی‌ای بخرند، نام و مشخصات آنها، خود به خود، در اولویت‌های حساسیت برانگیز اف‌بی‌آی قرار می‌گیرند. اما مردم جهان هم از این حضور ناخوانده آمریکایی‌ها در حریم خصوصیشان آزرده خاطرند. در ۲۳ فوریه سال ۲۰۰۰ میلادی ، پارلمان اروپا گزارش تکان دهنده ای را منتشر ساخت که جهانیان را بهحیرت انداخت. دراین روز، به دنبال اختلافات تجاری اتحادیه اروپا با آمریکا، پس از شصت سال، پروژه جاسوسی سری اشلون فاش شد. اشلون نام رمز یک سامانه جاسوسی جهانی است که آژانس امنیت ملی آمریکا (NSA) آن را طراحی کرده است و علاوه بر آمریکا ، کشورهای انگلیس، کانادا، استرالیا و نیوزیلند در آن شرکت دارند.

طبق آخرین گزارش‌ها، سامانه جاسوسی از ۱۲۰ ماهواره ارتباطاتی، اکتشافی و نظارتی تشکیل شده که در مدارهای ثابت دور زمین می‌گردند. علاوه بر این ماهواره‌ها، تعداد بسیار زیادی گیرنده‌های زمینی در نقاط مختلف دنیا نصب شده است تا نقاط کور ماهواره‌ها را پوشش دهند.

این ماهواره‌ها و گیرنده‌ها وظیفه دارند روزانه حدود سه میلیارد تماس تلفنی، نمابر و ایمیل را ذخیره کرده، به رایانه‌های مادری که در این پنج کشور وجود دارند، انتقال دهند. این اطلاعات پس از ترجمه خودکار به زبان انگلیسی، تحت یک پردازش محتوایی دقیق قرار می‌گیرد.نرم افزارهای قدرتمند اشلون به فهرستی از واژه‌های کلیدی مجهزند که در صورت یافت شدن هر یک از آن واژه‌ها در

---

[1] ECHELON

متن گفتگوهای تلفنی یا نمابر و ایمیل، پرونده ویژهای برای آن اطلاعات تشکیل می‌شود و با تحلیل محتوای بقیه مطالب آن پرونده، میزان اهمیت خبر ذخیره شده مشخص می‌شود وبه آژانس اطلاعات امنیت ملی آمریکا ارسال می‌شود تا اقدامات جاسوسی بعدی درباره آن صورت گیرد. سامانه جمع آوری الکترونیک اشلون توسط آژانس بین المللی امنیت ملی آمریکا یا NSAانتخاب گردیده و طراحی شده است .

حوزه فعالیت اشلون بسیار گسترده است. این شبکه تار گونه در مسائل سیاسی، اقتصادی، فرهنگی و ... مهارت داشته ولی نقطه توجه و تمرکز آن بیشتر بر روی مسائل صنعتی و تجاری در حوزه اقتصاد می‌باشد. امروزه فعالیت سامانه جمع آوری الکترونیک اشلون برای همه آشکار گردیده است و اکثر کشورها در جهت مقابله با آن دست به اقداماتی زده اند. شاید بتوان یکی از راه‌های مقابله با آن را دقت در برقراری ارتباطات دانست. اما فرهنگ سازی و دادن اطلاعات کامل‌تر در خصوص اشلون می‌تواند خود باعث افزایش آگاهی‌های جامعه جهانی شود.

جمع‌آوری اطلاعات الکترونیکی در سراسر کره زمین صورت می‌گیرد. ایالات متحده، آمریکای لاتین، آسیای مرکزی و چین شمالی را کنترل می‌کند. اروپا، قسمت غربی روسیه تا اورال و آفریقا در عرصه مسئولیت انگلیس قرار دارد. استرالیا مشغول استراق سمع مکالمات از منطقه جنوب شرق آسیا و چین جنوبی است. نیوزلند در منطقه اقیانوسیه فعالیت می‌کند.

اطلاعات به دست آمده به حافظه مدرن ترین رایانه‌های موجود در مرکز بررسی اشلون ارسال و پیاده می‌شود. این اطلاعات از "دیکشنری‌های اشلون" رد می‌شود که شامل پایگاه‌های کلمات کلیدی که این پایگاه‌ها هر ماه در حال نوسازی مرتب است. این پایگاه واژه‌ها شامل اسامی‌افراد، ناوها، سازمان‌ها و کشورها و یک سری اصطلاحات ویژه است. شماره تلفن و فکس، آدرس ایمیل

در اینترنت که به اشخاص، تجار، سازمان‌ها یا سرویس‌های دولتی تعلق دارند، حکم کلید رمز را دارند. با استفاده از مجموعه معین کلیدها می‌توان اطلاعات ارزنده را کشف کرده و اطلاعات بی ارزش را بیرون انداخت. تجهیزات ویژه "اشلون" قادر استبه طور خودکار موضوع اطلاعات دریافت شده را طبقه بندی کند. دور کامل پردازش گزارش‌ها از پیاده کردن ماشینی سخن شفاهی تا ترجمه اتوماتیک از بیش از ۱۰۰ زبان، استخراج می‌شود. سامانه "اشلون" همچنین در برگیرنده ناوهای تجسسی و ایستگاه‌های گیرنده ای است که به سازمان‌های عضو پروژه (اداره ارتباطات وزارت دفاع استرالیا، دفتر ملی امنیت زلاند نوو اداره ارتباطات بسته کانادا) تعلق دارند. از این طریق پذیرش و انتقال اطلاعات پردازش شده صورت می‌گیرد.به گزارش خبرگزاری‌های خارجی، با کمک "اشلون" نظارت بر بیش از ۱۰ خط تلفن متعلق به خالد شیخ محمد، بالاترین مقام هم رده با بن لادن، صورت گرفت. اطلاعات به دست آمده همراه با اطلاعات به دست آمده از مأموران اجازه داد که این شخص را دستگیر کنند.

کشورها و سازمان‌های مختلف مدافع حقوق بشر مکرراً آمریکایی‌ها و شرکای آنها را به استفاده غیر تخصصی از این وسایل نیرومند متهم کرده اند. آن‌ها مدعی هستند که این ابزار در جهت جاسوسی اقتصادی، صنعتی، سیاسی و دیپلماتیک، استراق سمع مکالمات خصوصی و نظارت بر مکاتبات الکترونیکی خصوصی مردم فعالیت می‌کند.

در پایان باید گفت هر آنچه که به صورت رایگان در اختیار ما قرار می‌گیرد می‌تواند حاوی درب پشتی به منظور رخنه به سامانه‌های اطلاعاتی ما باشد و چنانچه اقدامات پیشگیرانه صورت نپذیرد باید قبول کرد که در زمین حریف بازی می‌کنیم و قطعا چنین پیش فرضی نتیجه برنده و بازنده بودن ما را رقم خواهد زد.