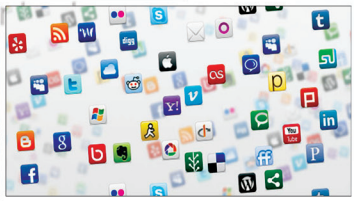
پایگاه تبیینی
و تحلیلی جزیان شناسی

دیدبان

www.Didban.ir



بررسی تاریخچه

جاسوسی دیجیتال


بسم الله
الرحمن
الرحيم

تاریخچه جاسوسی دیجیتال

شـاید به نظر برسد جاسوسی و پایش محصول قرن ۲۱ است اما همواره در تاریخ وجود داشته و قدمت آن را می‌توان با پیدایش تمدن‌ها یکی دانسـت. با پیشـرفت علم و دانش و ظهور فن‌آوری از دوربین و تلسـکوپ و رادیـو گرفته تـا دوربین‌های مدار بسته، ماهواره‌های جاسوسی، اینترنت، جی‌پی‌اس و ... روش‌های جاسوسـی و پایش بشر نیز دستخوش تحولات و پیچیدگی‌های بسیاری شده است. دوران جنگ سـرد میان آمریکا و روسیه را می‌توان یکی از مهم‌ترین عوامل پیشـرفت فناوری و گسـترش روش‌ها و ابزار جاسوسـی و پایش در تاریخ بشـر دانست چرا که نیروهای نظامی کشورهای درگیر، به ندرت به طور مسـتقیم در جنگ سـرد شرکت می‌کردنـد؛ ایـن نبرد بیشـتر توسـط آژانس‌های اطلاعاتـی مانند سـیا آمریـکا، MI۶ انگلسـتان، سـرویس اطلاعـات فـدرال آلمان غربـی، استاسـی آلمان شـرقی و کاگ‌ب شـوروی انجام می‌شـد و بـه همیـن دلیـل عملیات‌های جاسوسی نیاز دسـتگاه‌های اطلاعاتی بـه ابـزار و فن‌آوری‌های جاسوسـی و پایش را روز بـه روز افزایش می‌داد. بـه همین دلیـل طرف‌های درگیر سـرمایه‌گذاری هنگفتـی در پیشـرفت تکنولوژی و ابـداع ابزار و روش‌هـای جاسوسـی و اطلاعاتی کردنـد. برای نمونه می‌توان به پایگاه جاسوسـی اشلون، سازمان اطلاعاتی مشترک ایالات متحده و انگلستان اشاره کـرد که در جنگ جهانی دوم ایجاد شـد و از آن برضد شـوروی، چیـن، و هم‌پیمانان آنها اسـتفاده می‌شد.

جهان بـا حملات ۱۱ سـپتامبر وارد دوره جدیدی از جاسوسـی و پایش شـد. دولت آمریکا به بهانه محافظت مـردم آمریکا با تصویـب قوانین جدید امکان نظارت و پایـش شـدیدتر و جاسوسـی از تمامـی جنبه‌هـای زندگـی شـهروندان آمریکایـی و انجـام

عملیات‌های جاسوسی در جهان را برای خود افزایش و هموار کرد. از آن زمان به بعد بود که با گسترش فن‌آوری‌های پیشرفته ابزار پیچیده‌تر و پیشرفته‌تر جاسوسی و پایشی نیز ابداع و توسعه داده شد. فن‌آوری‌ها و دستگاه‌هایی که به دست شرکت‌های بزرگ آمریکایی که همگی از ارتباط نزدیکی با سازمان‌های اطلاعاتی و نظامی و دولتی این کشور دارند تولید شده‌اند.

این فن‌آوری‌ها و دستگاه‌ها نظیر اینترنت، تلفن‌های همراه، رایانه‌ها، دوربین‌های مدار بسته، جی. پی. اس‌ها و ... امکانات و گزینه‌های فراوانی نیز به سازمان‌های اطلاعاتی برای جاسوسی و پایش مردم نیز داده‌اند و در واقع می‌توان از آنها به عنوان شمشیر دولبه یاد کرد.

فن‌آوری‌های نوین و تجهیزات الکترونیکی چنان در تار و پود زندگی مردم عصر دیجیتال تنیده‌اند که تبدیل به تیغ دو لبه شده‌اند. به طوری که از یک سو برای تسهیل ارتباطات بین فردی تولید و از سوی دیگر به عنوان ابزاری برای جاسوسی و شنود به کار گرفته می‌شوند. اگرچه این ابزار نظیر دوربین‌های جاسوسی، دوربین‌های مداربسته، دستگاه‌های ضبط صدا ردیاب موبایل، جی. پی. اس و شنود صوتی در دسترس عموم مردم قرار دارد اما همین ابزار تله و طعمه‌ای برای جاسوسی و شنود توسط گردانندگان شبکه‌های جهانی ارتباطی نظیر مخابرات و اینترنت و غیره می‌شوند.

این گزارش با توجه به پیچیدگی و حساس بودن این فن‌آوری‌ها و افزایش تهدیدات امنیتی و سایبری

به بررسی برخی از حوزه‌های اصلی و روش‌ها و تکنیک‌های جاسوسی و پایشی با استفاده از فن‌آوری‌های نوین و تجهیزات سخت افزاری و نرم افزاری خواهد پرداخت.

جاسوسی و پایش اینترنتی

اینترنت به بزرگ‌ترین «ماشین جاسوسی و پایش اطلاعات» جهان تبدیل شده است و این در حالی رخ می‌دهد که به طور روز افزون شاهد این هستیم که اطلاعات شخصی بیشتر افراد نسبت به هر زمان دیگری در اینترنت قرار دارد و آن را به مثابه گنجینه با ارزشی از اطلاعات تبدیل کرده است.

دهه ۶۰ میلادی را می‌توان دهه پیدایش اینترنت نامید. آمریکا با هدف نظارت مجازی بر جهان و پس

از ارائه اینترنت در دهه ۹۰ میلادی با گسترش شبکه های اینترنتی در سراسر جهان، میلیاردها نفر را در دام تارهای عنکبوتی سیستم اطلاعاتی خود گرفتار کرد. طبق گزارشی که در سال ۲۰۱۱ منتشر شده در حال حاضر حدود ۲ میلیارد و ۲۰۰ میلیون نفر در جهان از اینترنت استفاده می کنند یعنی چیزی حدود یک سوم جمعیت کل جهان.

با استفاده روز افزون اینترنت در زندگی روزمره و پیوند خوردن دنیای حقیقی و دنیای مجازی و نفوذ اینترنت و فناوری‌های نوین در زندگی مردم دنیا، حاکمان اینترنت اگرچه بر حفظ حریم خصوصی تاکید می کنند به راحتی به تمامی ابعاد و زوایای زندگی افراد دسترسی پیدا کرده‌اند. این امکانات فرصت طلایی را برای جاسوسی از تمامی مردم دنیا برای آمریکا به وجود آورد. اما چرا اینترنت؟ اینترنت را می‌توان دریچه نفوذ به افکار و قلب‌ها دانست چرا که بسیاری از افراد افکار، اطلاعات شخصی، اطلاعات مهم، ارتباطات، احساسات، خواسته‌ها و بسیاری موارد دیگر را به راحتی در آن منتشر و آن را دو دستی تقدیم سازمان‌های اطلاعاتی و جاسوسی می کنند. آمریکا نیز با برنامه‌ای مدون و چند مرحله‌ای اقدام به بسترسازی استفاده از اینترنت در تمامی ابعاد زندگی واقعی و سایبری مردم جهان به وسیله لوازم و ابزار ارتباطاتی و الکترونیکی، بدون آنکه توجه و واکنش منفی افراد را برانگیزد کرد و توانست به خصوصی‌ترین زوایای زندگی آنها دسترسی و تسلط پیدا کند. در واقع هر وسیله‌ای که قابلیت اتصال به اینترنت را داشته باشد از آن می‌توان به عنوان یک ابزار جاسوسی و شنود و پایش استفاده کرد.

بر اساس قوانینی که دولت آمریکا وضع نموده، مدیریت شبکه های اینترنتی باید تمامی اطلاعاتی را که در شبکه جهانی رد و بدل می‌شود کنترل کرده و از آن‌ها استفاده لازم را به عمل آورد. بنابراین دیگر جای تعجب نیست، دولت آمریکا که خود را حافظ امنیت جهانی می‌داند، برای حفظ امنیت دو دنیای مجازی و حقیقی، اطلاعات مورد نیازش را با این توجیه از شبکه های اینترنتی بدست آورد.

دولت ایالات متحده آمریکا عملا حاکم مطلق

دنیای مجازی ماست. حاکمی که با در اختیار داشتن مدیریت منابع اینترنتی، مدیریت خدمات اینترنتی نظیر دامنه و فضای میزبانی به خوبی این فرصت را دارد، از تمام وقایعی که در شبکه جهانی رخ می‌دهد، مطلع گردد.

اما آمریکا چگونه این کار را انجام می‌دهد؟

مراکز کنترل اطلاعات و داده‌های اینترنتی

آژانس امنیت ملی آمریکا مشهور به NSA، یک آژانس دولتی آمریکا است که به نحوی زیر نظر سازمان دفاع ایالات متحده آمریکا اداره می‌شود. این سازمان در ۴ نوامبر سال ۱۹۵۲ تاسیس شد و وظیفه اصلی آن نظارت بر مخابرات و فعالیت‌های ماهواره‌ای و کشف رمز در ایالات متحده آمریکا می‌باشد.

این آژانس از اعضای کلیدی جامعه اطلاعاتی ایالات متحده آمریکا است و یکی از محرمانه‌ترین سازمان‌های جاسوسی در جهان به شمار می‌آید. البته کار این آژانس محدود به جاسوسی ارتباطات است و جاسوسی انسانی را شامل نمی‌شود. همچنین طبق قانون، فعالیت‌های جاسوسی این آژانس محدود به روابط خارجی است اما در برخی مواقع نظارتهای داخل مرزی را هم شامل می‌شود. مرکزاین آژانس در ایالت مریلند است.

شنود دایم ارتباطات از راه دور، در سراسر جهان (موبایل، فکس، ای. میل و ارتباطات انفورماتیک) و همچنین دریافت و تحلیل تصاویر ماهواره‌ای، در حوزهٔ وظایف سازمان امنیت ملی آمریکا (NSA) است. این آژانس - که مقرّ آن در فورت مید (مریلند، نزدیک واشنگتن) قرار دارد. صدهزار نفر را در استخدام خودش دارد که این افراد در مراکز مختلف در آمریکا و ایستگاه‌های شنود مستقر در خارج، به کار مشغول‌اند. این سازمان از بودجه سالانه‌ای معادل بیش از شانزده میلیارد دلار بهره می‌برد. به گفته جان پیک، کارشناس آمریکایی مسائل اطلاعاتی، آژانس امنیت ملی ایالات متحده، حدود ۹۵ درصد ارتباطات از راه دور را در سراسر جهان، تحت کنترل دارد. این حجم عظیم اطلاعات به وسیلهٔ ابرکامپیوترهای مجهز به نرم‌افزارهای تجزیه و تحلیل، مورد بررسی دقیق قرار می‌گیرد. البته رقم گفته شده از سوی این کارشناس آمریکایی، مورد قبول همهٔ اهل فن نیست، اما می‌توان با اطمینان گفت که توانایی آژانس امنیت ملی آمریکا در ره‌گیری اطلاعاتی بیش از پنجاه درصد ترافیک جهانی را شامل می‌شود. مدیر این آژانس، به هنگام یکی از معدود مصاحبه‌هایش با مطبوعات، اعلام کرده بود که او باید هر سه ساعت، اطلاعاتی معادل کل کتابخانه کنگره آمریکا را تحت اداره‌اش داشته باشد.

اطلاعات مورد تحلیل سازمان امنیت ملی آمریکا، به طور دائم از طریق حدود پنجاه ایستگاه شنود در بیست کشور جهان در سطح پنج قاره دریافت می‌شود. این ایستگاه‌ها وظیفه دارند علامات فرستاده شده از سوی ماهواره‌های مخابراتی را شنود کنند؛ البته عمده این علامات از سوی ماهواره‌های اینتل ست ارسال می‌گردد. مهم‌ترین ایستگاه‌های شنود در کشورهای انگلستان، نیوزیلند، استرالیا و آلمان مستقر هستند.

ایـن ایسـتگاه‌های ره‌گیـری علامات ماهـواره‌ای، اطلاعـات را دریافـت می‌کننـد؛ خـواه از طریـق ره‌گیـری مسـتقیم امواج فرسـتاده شـده از سـوی ماهـواره، یا از طریق دریافت علامـات ماهواره‌های ویـژه جمع‌آوری اطلاعات در فضا. این ماهواره‌های ره‌گیری که بـه نام‌های «مرکـوری»، «ترومپت»، یا «مانتور» شناخته می‌شـوند، همچنین قادر به ره‌گیری امواج رادیوالکتریک از مبدأ زمین هم هسـتند. برای انجام دقیق مأموریت، برخی از این ماهواره‌ها – مثل ماهواره‌هـای مرکوری – به آنتن‌هایـی مدوّر مجهز هسـتند که می‌توانند امواج خیلی سـبک را منعکس کنند؛ امواجی که سطحشـان می‌تواند تا سطح یک زمین فوتبال برابر باشد. این آنتن‌های عظیم می‌توانند امواج فرسـتاده شـده از سوی ایسـتگاه‌های تقویتی تلفن‌های همراه را دریافت کنند. شـایع اسـت که ۹ ماهواره از این دسـت در اطـراف زمین و در ارتفاع ۳۶ هـزار کیلومتری از سـطح زمین قـرار دارند. ۲ ماهـواره از این نوع، بر فراز قـارهٔ اروپا قرار دارند و اطلاعات دریافتی را به ایسـتگاه بزرگ منویت هیل در انگلستان ارسال می‌کنند.

هـر بار که شـما مکالمـه‌ای تلفنی با خـارج برقرار می‌کنیـد و انعـکاس صدای خودتان را در گوشـی می‌شـنوید (علامت مشخصه اسـتفاده از ماهواره در ارتباط با راه دور)، مطمئن باشید که این ایستگاه‌های زمینیِ آژانس امنیت ملی آمریکا هسـتند که مشغول دریافت مکالمهٔ شـما هسـتند. سـازمان امنیت ملی آمریکا روزانه میلیون‌ها ارتباط از راه دور را ره‌گیری می‌کند. تمام ارتباطی که به این ترتیب در چهارگوشهٔ جهان شنود می‌شوند، به فورت مید فرستاده شده، در آنجا غربال می‌شود؛ تنها بخش کوچکی از اطلاعات ارسالی مورد استفاده بعدی قرار می‌گیرد. اما عملیات غربال چگونه انجام می‌گیـرد؟ کامپیوترهایی مجهز بـه نرم‌افزارهای مخصوص، وظیفـهٔ تجزیه و تحلیل و غربـال اولیـه اطلاعـات را بـر عهده دارنـد. این کامپیوترهـا شـماره تلفن‌های خاصـی را در حافظهٔ خودشان ذخیره کرده‌اند که براساس آنها غربال اولیه را انجام می‌دهند و تنها آن دسـته از مکالماتی را که به وسیلهٔ این شماره‌ها صورت پذیرفته، نگه می‌دارند. این شماره‌ها عبارتند از: شماره تلفن وزارت‌خانه‌ها، سفارت‌خانه‌ها، روابط‌عمومی سازمان‌های بین‌المللی، سازمان‌های غیر دولتی، شرکت‌های بزرگ فعال در عرصه‌های حساس و مشکوک به رقابت با منافع ملی آمریکا در حوزه‌های مختلف؛ اما گزینش ارتباطات هم‌چنین از طریق شناسـایی صدای افراد هم صورت می‌گیرد. همین جا روشـن کنیم که میکروچیپ‌های کامپیوترهای کرای (Cray) که شناسـایی صداهای آشـنا را انجام می‌دهنـد، در فورت میـد و در یک کارخانهٔ ویژه ساخته می‌شوند. کامپیوترهای Cray متعلق به آژانس امنیت ملی آمریکا هماهنگ با بانک داده‌هایشـان، قادرند صداهای شخصیت‌های تحت مراقبت مثل شـخصیت‌های سیاسـی و دیپلماتیک، نظامی، رؤسـای شـرکت‌ها و حتی اعضای شناخته شـده جنبش‌های تروریسـتی یا شورشـیان و سران کارتل‌های مواد مخدر را شناسایی کنند.

شـمار ارتباطات گزینش شـده، حفظ شده و تفسیر شـده (ارتباطی کـه تحلیل یـا گزارشـی را در پی دارد) تقریبـاً به پانـزده مورد در روز بالغ می‌شـود. بی‌شـک ارتباطـات افراد بـر روی شـبکه اینترنت نیز تحت کنترل شـدید قـرار دارد؛ کامـلاً محتمل اسـت آژانس امنیت ملی ایالات متحـده با توجه به

محتوای روی شـبکه، هر لحظـه آنها را کنترل کند؛ میهن‌پرسـتی آمریکایـی به گونه‌ای اسـت که همه شـرکت‌های ارائـه دهنـده خدمـات اینترنتی - که اکثرشـان آمریکایی هسـتند - به آژانس امنیت ملی کشورشـان اجازه می‌دهند، داده‌های مشتریانشان را

کنتـرل کند و همین‌طـور ارتباطات اینترنتیشـان را؛ به عـلاوه اینکه برخـی سـایت‌های اینترنتی (اغلب آمریکایی)، گاهی بدون اطـلاع صاحبان آنها برای کنترل محتوای کامپیوترهای برخی کاربران اینترنتی، مورد اسـتفاده قرار می‌گیرد. مدتی است که به طور

مداوم این نجوا به گوش می‌رسد که شرکت بزرگ کامپیوتری «مایکروسـافت» پیوند نزدیکی با آژانس امنیـت ملی آمریـکا دارد؛ البته ایـن همکاری‌ها در چارچوب عملیات شـنود و ره‌گیری انجام می‌شود. باید بگوییم تنها، آژانس امنیت ملی آمریکا اینترنت را تحت کنترل ندارد؛ بلکه تقریباً تمام سـازمان‌های اطلاعاتی آمریکا سـرویس‌های ره‌گیـری و کنترل خاصّ خودشـان را (در مورد اینترنت) دارا هسـتند؛ ایـن موضـوع از CIA تا حتی سـرویس اطلاعاتی نیروی دریایی آمریکا را شامل می‌شود.

مرکز جاسوسی جهانی «اشلون»

اشلون واژه‌ای است که معمولا برای اشاره به یک سیستم جاسوسی جهانی (تأسیس در سال ۱۹۴۷) که سازمان‌های اطلاعاتی پنج کشور آمریکا، انگلستان، کانادا، استرالیا و نیوزیلند در آن نقش دارند و هم‌اکنون توسط آژانس امنیت ملی آمریکا هدایت می‌شود، به کار می‌رود. اشلون مقادیر عظیم تماس‌های تلفنی، پیام‌های ایمیل، دانلودهای اینترنتی، ارتباطات ماهواره‌ای و غیره را جمع‌آوری کرده، سپس اطلاعات مورد نظر را از طریق برنامه‌های اطلاعاتی تصفیه می‌کند.

بنا بر گزارش‌ها اشلون، در حدود ۹۰ درصد از ترافیک اینترنتی را وارسی می‌کند. آمریکا تلاش بسیاری کرده است تا این برنامه را از نظرها مخفی نگه دارد، حتی با توجه به اینکه دولت‌های استرالیا و نیوزیلند وجود این برنامه را تأیید نمودند. اشلون یک عملیات بسیار محرمانه است که دادگاه‌ها و مجالس ملی هیچ گونه نظارتی بر آن ندارند و در نتیجه کسی نمی‌داند که این برنامه‌ها چگونه مورد استفاده قرار می‌گیرند و یا اینکه استفاده از آنها مطابق با موازین قانونی است یا نه.

اشلون در فعالیت‌های تجاری نیز به جاسوسی می‌پردازد. برای مثال در سال ۱۹۹۰، آژانس امنیت ملی آمریکا از انعقاد یک قرارداد ۲۰۰ میلیون دلاری بین اندونزی و یک تولید کننده ماهواره ژاپنی مطلع شد. جرج بوش پدر در این معامله مداخله کرده و طرف اندونزی را قانع ساخت که این معامله را بین ژاپنی‌ها و شرکت AT&T (شرکتی که بعدها وارد برنامه استراق سمع از شهروندان آمریکایی شد) تقسیم کند.

بنا بر گزارشات، دولت آمریکا از برنامه اشلون برای جاسوسی صنعتی نیز بهره می‌گیرد که شامل تکنولوژی توربین بادی بدون دنده که توسط شرکت آلمانی «انرکون» (Enercon) طراحی شده بود و نیز تکنولوژی گفتار که توسط شرکت بلژیکی «هاسپی‌اندلرناوت» طراحی شده بود، می‌شود. این

جاسوسی‌های اقتصادی حتی به داخل آمریکا نیز سرایت کرده است. بر این اساس، برخی شرکت‌های آمریکایی مجبور می‌شوند تا از معاملات به نفع شرکت‌هایی که به طور مداوم پول به سوی دو حزب حاکم در آمریکا سرازیر می‌کنند، کنار بکشند.

مرکز جاسوسی یوتا

آژانس امنیت ملی امریکا برای رهگیری و ذخیره داده‌های الکترونیکی جمع آوری شده از سراسر جهان و شهروندان امریکایی، در حال ساخت بزرگ‌ترین مرکز جاسوسی جهان است.

این مرکز که در روستای دورافتاده بلافدیل در ایالت یوتا قرار دارد، قادر به پردازش داده‌هایی به حجم "یوتابایتز" (یک میلیون‌میلیارد گیگابایت) است.

فعالیت این تاسیسات ۲ میلیارد دلاری "رهگیری، کشف، تجزیه و تحلیل و ذخیره سازی حجم بالایی از ارتباطات جهانی از جمله محتوای مکالمات تلفنی، ایمیل‌های شخصی، پیام‌های متنی تلفن‌های همراه و جستجوهای اینترنتی را در بر می‌گیرد. "

بر اساس این گزارش، مرکز جاسوسی مذکور "مخفی‌ترین و دردسر سازترین آژانس اطلاعاتی در سراسر جهان به شمار می‌رود" و سالانه حدود ۶۵ مگاوات برق مصرف می‌کند. هزینه نگهداری این مرکز جاسوسی سالانه ۴۰ میلیون دلار است.

این مرکز جاسوسی سیگنال‌های ارتباطی را از زمان خروج از ماهواره‌ها تا هنگام حرکت در کابل‌های موجود در زیر زمین و زیر دریاها و شبکه‌های بین‌المللی، خارجی و داخلی رهگیری می‌کند.

آژانس امنیت ملی امریکا با استفاده از رایانه‌ای که احتمالا پر سرعت‌ترین ابر رایانه جهان به شمار می‌رود، قادر است از طریق لوازم خانگی نظیر یخچال فریزرها، اجاق‌ها و سیستم‌های روشنایی متصل به اینترنت، به جمع آوری داده بپردازد.

این تاسیسات از لحاظ تکنیکی به "وزارت امنیت داخلی امریکا" در جمع آوری اطلاعات درباره تهدیدهای سایبری و دستیابی به اهدافش در خصوص امنیت سایبری کمک می‌کند.

شبکه‌های اجتماعی

با ظهور رسانه‌ها و شبکه‌های اجتماعی و یکپارچگی سرویس‌های ارائه دهنده ایمیل و فضاهای مجازی و چت روم‌ها، جاسوسی آمریکا وارد فاز پیشرفته تر و مراحل پایانی خود شـد. با توسعه لوازم الکترونیکی هوشـمند نظیـر تلفن‌های همـراه، تبلت‌هـا و لوازم خانگی هوشـمند همچـون تلویزیون، کنسـول‌های بـازی و غیره که همگی امـکان ارتباط با اینترنت را دارند، مرحله جدیدی در جاسوسی سایبری آغاز شد و آن تلفیق و یکپارچگی انواع رسـانه‌های اجتماعی و سـرویس‌های ایمیل در چنین دستگاه‌هاسـت که چرخه جاسوسی را به طور چشمگیری کامل می کند. برای مثال تلفن‌های همراه هوشمند بهترین ابزار برای جاسوسی سایبری شـده‌اند. چرا که شما تنها با یک تلفن هوشـمند که قابلیت اتصال به اینترنت را دارد، می‌توانیـد وارد شـبکه‌های اجتماعـی و ایمیل‌های خود شـوید و به فعالیت بپردازید. این مساله شنود و پایش را بسیار راحت می کند. چرا که: ۱- به راحتی مکالمات و ارتباط تلفنی شنود می‌شوند. ۲- از طریق جی. پی. اس موقعیت مکانی و جغرافیایی شناسـایی می‌شـود و ۳- از طریق فعالیت‌هـای اینترنتی متوجه افکار و احساسـات و برنامه‌هـا و کارهایی که انجام می‌دهید می‌شوند.

اسـتفاده از اینترنـت روز به روز در حال گسـترش است، توسـعه تلفن‌های همراه هوشمندی که قابلیت ارتباط بـا فضای مجازی و سـایبری را دارند از این جهت رو به گسترش است که علاوه بر اینکه هویت فرد وارد شـده به فضای مجازی مشـخص می‌شود بلکه بـا اسـتفاده از سیسـتم موقعیت‌یـاب جهانی، GPS، موقعیت مکانی فرد نیز مشخص می‌شود.

این روزها فیس‌بوک تبدیـل به یکی از بزرگ‌ترین شـبکه های اجتماعی در جهان شده است و در حال حاضر حدود ۸۴۵ میلیون کاربر در سطح جهان دارد. در نگاه اول چیز بدی در مورد سـایت «فیس‌بوک» وجود ندارد. یک شـبکه اجتماعی که به شما کمک می کند تا با دوسـتان خود در ارتباط باشـید و حتی بتوانید دوسـتان قدیمـی خود را که سال‌هاسـت از آن‌ها بی خبر هسـتید، پیدا کنید. بسیار زیبا است که تصویر از کودک تازه متولد شده دوست خود را در صفحه مربوط به او ببینید و اولین نفری باشـید که به او تبریک می گویید.

یکـی از اولین مسـائل مربوط به فیـس بوک بحث رعایت حریم خصوصی کاربران اسـت. بسـیاری از کاربـران تصاویـر، کلیپ‌ها و یا مطالبـی را بر روی صفحه شـخصی خود منتشـر می کنند که علاقه ای ندارند تا دیگران هم به آن مطالب دسترسـی داشـته باشند.

در سال‌های اخیر موارد بسـیار زیادی از هک شدن حسـاب‌های کاربران در اعـداد میلیونی اتفاق افتاده است که به افشای اطلاعات شخصی میلیون‌ها کاربر در فضای مجازی منجر شـده اسـت. باج گیری‌ها، تهدیـد و آزار اذیت سـایبری از جملـه جدیدترین مشـکلات پیش روی بشر امروز اسـت که با شبکه اجتماعی فیس بوک ارتکاب به آن‌ها بسیار راحت‌تر شده است.

حـدودا یک ماه پیـش بود که پخـش تصاویری از طریق سایت فیس بوک خانواده های چندین قربانی را در انگلسـتان شـوکه کـرد. افرادی کـه به دلیل ارتکاب به جرم‌های خشـن به زنـدان افتاده بودند به

وسیله قاچاق تلفن‌های همراه هوشمند به درون زندان توانسته بودند صفحه فیس بوک خود را به روز کرده و به خانواده قربانیان توهین کنند.

متاسفانه باید اذعان کرد که بعضی از جنایت‌های رخ داده در کشور ما هم به فیس بوک مرتبط است. استفاده از این شبکه برای دوست‌یابی یا حتی همسریابی باعث ایجاد مشکلات فراوان برای افراد مختلف شده است که متاسفانه در مواردی به قتل نیز منجر شده است.

اما نکته دیگر این مسئله است که در حال حاضر به طور متوسط و روزانه ۴ میلیارد پیام به شکل متن، عکس و یا فایل‌های صوتی و یا تصویری در این شبکه رد و بدل می‌شود. تعداد زیادی از این مطالب به وسیله کاربران به عنوان مطالب منفی و مضر اعلام شده و به وسیله سایت برداشته می‌شود. اما آیا تا به حال این سوال برای شما مطرح شده است که

چطور؟

سایت فیس بوک از طریق شرکت‌های الکترونیکی و اینترنتی کوچکتر به مانند "oDesk" بیش از هزاران نفر که عمدتا از اهالی فقیر آسیا، آفریقا یا آمریکای لاتین هستند را با دستمزد ساعتی ۱ دلار استخدام کرده و به آنان این وظیفه را محول می‌کند.

در این جا دو نگرانی وجود دارد: یکی این که این افراد از لحاظ امنیتی آن چنان که باید و شاید تایید نشده اند. این افراد از منازل خود در نقاط مختلف جهان به حساب‌های کاربری بخش زیادی از اعضای سایت دسترسی دارند و در صورتی که بخواهند می‌توانند نه فقط آن مطلب مضر و یا مورد اعتراض و بلکه به تمامی اطلاعات شخصی کاربران دسترسی داشته و از آن مطالب سوءاستفاده کنند.

مسئله بعد فشار بسیار زیادی است که به خود این افراد وارد می‌شود. عمده این افراد که این وظیفه را به عهده می‌گیرند جوان و در حال تحصیل هستند. حال تصور کنید که این افراد هر روز باید تصاویر وحشتناک و یا غیر اخلاقی را از نظر بگذرانند و یا متونی که در آن‌ها توهین‌های نژادی و یا فحاشی به کار رفته است را بخوانند. مسلما تاثیرات چنین کاری

در دراز مدت بسیار مخرب خواهد بود.

در یک نگاه کلی اگر فیس بوک را یک کشـور در نظر بگیریم، باید بگوییم که این کشـور از بسـیاری کشـورها پرجمعیت‌تر و ثروتمندتر اسـت. حال این «مدیران جهان سـومی» در حکم پلیس این کشـور بزرگ و پرجمعیت ظاهر شـده‌اند و سعی می‌کنند تا نظـم را در این محیط حفـظ کنند. اما باید گفت که نه تنها فیس بوک، بلکه سـایر شـبکه های اجتماعی مثـل «توئیتر» و «گوگل پـلاس» نیز در مورد این تیم مدیریتی خود سـکوت پیشـه کرده‌اند و خیلی میل ندارند تـا در مورد نحوه گزینـش و میزان حقوق و مزایای این افراد صحبت کنند.

کارشناسـان امنیـت فضای سـایبر حـدس می‌زنند که فیس بـوک چیزی در حـدود ۸۰۰ تا ۱۰۰۰ نفر مدیر این چنینی را از طریق شـرکت‌هایی همچون " oDesk " در سرتاسـر جهان استخدام کرده است. «گراهـام کلولـی» که مدیـر یک شـرکت امنیت سایبری اسـت این مسـئله را «یک راز کثیف که به خوبی مراقبت نشده است» می‌داند.

در حـال حاضر و با وجود این نگرانی‌ها و علی رغم اطلاعیه‌هایی که از طریق سـایت فیس بوک منتشـر شده است، هیچ مشـخص نیست که چگونه نظارتی بـر روی این افـراد صورت می‌گیـرد. در عین حال تقریبا هیچ گونه اقـدام امنیتی نیز بر روی رایانه های این افراد نیز صـورت نمی‌گیرد. در صورتی که این افراد بخواهند از این اطلاعات شـخصی علیه شخص دیگری اسـتفاده کنند یا بخواهند ایـن اطلاعات را به شـخص یا اشـخاص دیگری منتقل کننـد و یا به سادگی سیسـتم آن‌ها مورد حمله هکرها واقع شود، آن وقت مشـخص نیسـت که چه بر سـر اطلاعات شخصی کاربران خواهد آمد.

در آخرین مسـئله ای که در این رابطه اذهان عمومی را به خود جلب کرده اسـت، این اسـت که روزنامه تلگراف چاپ انگلسـتان در تحقیقاتی متوجه شـده اسـت که سایت فیس‌بوک بیشتر از میزانی که اعلام کرده بـود، با این «مدیـران اسـتخدامی» اطلاعات شـخصی کاربران را در میان می‌گذارد. این مدیران می‌تواننـد متوجـه شـوند که نـه تنها چـه کاربری محتوای مورد انتقاد را ارسـال کرده، حتی می‌توانند متوجه شـوند چه کاربر یـا کاربرانی ایـن محتوا را گزارش داده‌اند.

مطالعه جدید «شـورای مطالعات اطلاعاتی مدیترانه» در سال ۲۰۱۲ نشان می‌دهد که استفاده از رسانه های اجتماعـی به مثابـه ابزاری پیشـرو و جدید در جمع آوری اطلاعات تاکتیکی از منابع آشکار است.

یکـی از محققـان ایـن تحقیـق بـه نـام جـوزف فیتسـاناکیس ابراز می‌دارد: در این مطالعه ما نشـان می‌دهیـم که فیس بوک، توییتـر، یوتیوب، و دیگر شـبکه های اجتماعی از دید سـازمان‌های اطلاعاتی به عنوان کانال‌های شـدیدا باارزشـی برای کسـب اطلاعات به حسـاب می‌آیند. ما یافتـه های خود را بر اسـاس سـه مطالعه موردی اخیر بنا می‌کنیم که به عقیده ما عملکرد اطلاعاتی شـبکه های اجتماعی را نشان می‌دهند.

البته آنچه در این مطالعه بدان اشاره نمی‌شود، استفاده سازمان‌های جاسوسـی از شبکه های اجتماعی برای اهداف دیگر اسـت. این مطالعـه مخاطب را به باور این تفکر سوق می‌دهد که شبکه اجتماعی تنها یک ابزار جمع آوری اطلاعات هستند.

سـایت فیس بوک را گسـترده‌ترین ابزار جاسوسی

ساخت دست بشر نام گذاری کرده است. حتی اگر سازمان‌های جاسوسی آمریکا در ایجاد فیس بوک نقشی نداشته باشند، اما اکنون از این شبکه برای جمع آوری اطلاعات شخصی چند صد میلیون انسان با اندک هزینه ای اقدام می کند. البته جاسوسی از شهروندان فقط با اراده مدیران سایت‌های اینترنتی نیست بلکه این روند حتی ناخواسته و با وجود اعتراضات این سایت‌ها اد امه دارد و هر روز نظارت بر فضای مجازی در آمریکا بیشتر می‌شود.

جولیان آسانژ موسس وب سایت ویکی لیکس می گوید: فیسبوک تنفر آمیز ترین ابزار جاسوسی است که تاکنون ایجاد شده‌است. هر کس که نام و مشخصات دوستان خود را به شبکه اجتماعی فیسبوک اضافه می کند باید بداند که به شکل رایگان در خدمت دستگاه‌های اطلاعاتی آمریکاست و این گنجینه اطلاعاتی را برای آنها تکمیل می کند

به گفته وی فیسبوک یک گنجینه اطلاعاتی بسیار بزرگ از نام و پیشینه افراد است که کاربران آن را به شکل داوطلبانه در اختیار این شبکه اجتماعی قرار می‌دهند ولی این ابزار توسط دستگاه‌های امنیتی و اطلاعاتی آمریکا مورد بهره برداری قرار می گیرد. دسترسی این دستگاه‌های اطلاعاتی به اطلاعات ذخیره شده در فیسبوک آن را به یک ابزار خطرناک بدل کرده‌است.

البته باید گفت این نخستین بار نیست که دولت آمریکا در زمانی معاصر مقادیر عظیمی اطلاعات را جمع آوری و در پروژه های گوناگون به بررسی دقیق آنها می‌پردازد.

در طول مأموریت دولت «بوش»، «آژانس امنیت ملی» استخراج داده های مربوط به میلیون‌ها شهروند آمریکایی (مکالمات تلفنی، نامه های الکترونیک، فکس و دیگر منابع) را با هدف به اصطلاح کشف اعضای احتمالی شبکه های تروریستی و نظارت بر آنها، در قالب برنامه ای سری بدون مجوز قضایی آغاز کرد. دولت مزبور همچنین کوشید پروژه عظیم دیگری را با نام «آگاهی جامع اطلاعاتی» و به منظور ایجاد یک پایگاه اطلاعاتی دیگر با هدف جست وجوی الگوهای رفتاری و یا گرایش‌های موجود در نامه های الکترونیک، مکالمات تلفنی، معاملات مالی، اطلاعات مربوط به روادیدها و غیره، و در نتیجه شناسایی و به اصطلاح «دشمنان»، به اجرا درآورد. این برنامه پس از مشاهده واکنش بسیار منفی مردم، از سوی کنگره متوقف گردید.

حال، در شمار پروژه های جاسوسی رنگارنگ آمریکا که هدفی جز کنترل کامل شهروندان خود و جهان را دنبال نمی کنند، می‌توان به عملیات این کشور در جهت کنترل شبکه های اجتماعی اینترنت اشاره کرد.

شایان ذکر است که این گونه پروژه‌ها شهروندان را چه در آمریکای لاتین و چه در آمریکای شمالی و یا دیگر کشورهای جهان به شدت نگران و مضطرب ساخته است، چرا که نقطه آغازین نظارت گسترده بر مردم را تجاوز به حریم خصوصی و اجتماعی آنان و نقض آزادی فردی و حقوق شخصی تشکیل می‌دهد. این اندیشه که سازمان‌های اطلاعاتی و نظامی بر زندگی شهروندان نظارت کامل داشته، آنها را مظنونانی بالقوه قلمداد کنند و بدین شکل از اقدامات خشونت آمیز آینده جلوگیری به عمل

آورند، بسیار مستبدانه است و دکترین امنیت ملی را به خاطر می‌آورد. چنین به نظر می‌رسد که دستگاه امنیت ملی آمریکا با اجرای پروژه های بیش از پیش مداخله گرانه و ضددموکراتیک خود روز به روز گسترش بیشتری می‌یابد، تا بدانجا که دیگر از کنترل خارج گردیده است. حال که شهروندان بسیاری کشورها بیش از هر زمان نسبت به نظام‌های خود خشمگین اند، به اقدامات اعتراض آمیز روی می‌آورند و خواستار تغییرات اقتصادی، اجتماعی و سیاسی‌اند، لازم است تمامی این پروژه‌ها شناسایی و به چالش کشانده شود.

در واقع هر کاربر شبکه اینترنت، به محض اتصال به این شبکه و با هر کلیک نا خواسته انبوهی از اطلاعات شخصی و غیر شخصی را به گردانندگان آن می‌دهد یا در واقع از وی این اطلاعات را می‌ربایند. کارشناسان کامپیوتر اظهار می‌دارند حتی نصب محیط‌هایی مانند ویندوز، با اتصال به اینترنت کلیه اطلاعات کاربر و عملیات اینترنتی وی را به شرکت عامل یعنی مایکروسافت منتقل می‌سازد و تنها در بعضی از مواقع است که هشداری مبنی بر دزدی اطلاعات دریافت می‌شود.

شیوع سایت‌های شبکه‌های اجتماعی و وب‌سایت‌های اشتراک تصاویر ویدئویی دولت آمریکا را تشویق کرده است که تأثیر بیشتری بر ساختارسیاسی کشورهای‌دیگر بگذارد، ضمن اینکه بخش قابل‌توجهی از جمع‌آوری اطلاعات و نشان کردن کیس‌های جاسوسی و به کارگیری آن‌ها در شبکه‌های اجتماعی از جمله فیس‌بوک اتفاق می‌افتد.

در زمان انتخابات ایران، کاربران ایرانی بالای ۹۰ درصد مخاطبان توئیتر را تشکیل می‌دادند. پس از انتخابات ایران، ۴۰۰ میلیون توئیت در کتابخانه ملی آمریکا، برای

بررسی و تحلیل محتوا ثبت شد. این نشان‌دهنده جمع‌آوری و آنالیز اطلاعات است.

«رابرت گیتس» وزیر دفاع آمریکا در ژوئن ۲۰۰۹ اعلام کرد، تکنولوژی‌های رسانه‌های اجتماعی همچون توئیتر که نقشی حیاتی در مستندسازی و هماهنگی اعتراضات در ایران به ویژه تهران داشتند، یک دارایی استراتژیک عظیم برای آمریکا محسوب می‌شوند.

گوگل؛ بزرگ‌ترین دستگاه جاسوسی دنیا

بسیاری از ما وقتی اسم گوگل به میان می‌آید، تصویری از یک موتور جست‌وجوی مشهور در ذهن مان نقش می‌بندد. این شرکت اینترنتی، هم‌اکنون خدمات مختلفی را به کاربران سراسر جهان ارائه می‌دهد. جست‌وجوی اطلاعات، پست الکترونیک (رایانامه)، گفت‌وگوی آنلاین (چت)، خواننده خوراک (فیدریدر) از مهم‌ترین این خدمات هستند اما خدمات گوگل به این‌ها منتهی نمی‌شود. گوگل ده‌ها سرویس مختلف را برای کاربران عرضه می‌کند.

مثلاً Google Docs ابزار بسیار سودمند آنلاینی است که جایگزین خوبی برای ورد (word)و اکسل (Excel) مایکروسافت محسوب می‌شود. همه‌جا هم در دسترس است و می‌توانید اسنادتان را به سادگی به اشتراک بگذارید و به طور گروهی آنها را ویرایش کنید.

گوگل‌ارث (GoogleEarth) که برای مشاهده کره زمین و مکان‌های مختلف آن به صورت مجازی است.

سرویس آمار بازدید سایت گوگل (Google Analytics)، ابزاری بسیار کامل است. هر نوع اطلاعاتی در مورد بازدیدکنندگان سایتتان که بخواهید به شما می‌دهد. اکثر شهرهای ایران را می‌شناسد و بازدیدکنندگانتان از هر شهری را به شما اطلاع می‌دهد.

گوگل دسک‌تاپ، ابزار جست‌وجوی داخل رایانه شخصی شما که تمام فایل‌های داخل رایانه‌تان را به سرعت و مانند جست و جو ی اینترنت برای شما می‌یابد. کافی است آن را نصب کنید و به آن فرصت

بدهید تا فایل‌های داخل رایانه شما را شناسایی کند. گـوگل دسـک‌تاپ در کنار موتور جسـت‌وجوی خود، امکانات بسیار جالب دیگری به نام Gadget هم دارد که شـامل انواع ابزار کاربردی و سرگرمی جالب می‌شود.

مترجم گوگل (Google Translator) متون شما را به ۳۶ زبان مختلف می‌تواند ترجمه کند.

خدمات گـوگل محدود به این‌ها نیسـت و شـامل مـوارد بیشـتری در حوزه خرید و فروش، پاسـخ به سؤالات و ... می‌شود.

گوگل عـلاوه بر این‌ها سـایت‌های زیـادی را هم خریـداری کرده اسـت. سـایت‌هایی کـه کاربران زیـادی در آنهـا فعالیـت می‌کننـد. مثـلاً یوتیوب (Youtube) سـایتی اسـت که کاربران می‌توانند فیلم‌هـا را در آن به اشـتراک بگذارند. این سـایت توسط گوگل خریداری شده است.

وجه اشـتراک این سـایت‌ها و خدمات مختلف در تعداد بسـیار کاربرانشان است. کاربرانی که اکنون با کلمه کاربری (Account) که در گوگل دارند از خدمات این سایت‌ها بهره‌مند می‌شوند.

رایگان!؟

همه موارد بالا از خدمات مفیدی است که گوگل به کاربران خود می‌دهد اما آیا تا به حال این سؤال برای شـما پیش آمده که این همه خدمات، چرا برای شما "رایگان" عرضه می‌شود؟

همه ما شنیده‌ایم و می‌دانیم که انجام این کارها برای گوگل هزینـه زیادی دارد، سـرمایه‌گذاران بزرگی باید پول خرج کنند، مهندسـان زیادی در حوزه‌های مختلف باید دورهم جمع شوند، قطعات فنی زیادی مثل سـرورها و چیزهای دیگر باید سـاخته شـده و در کنـار هم قرار گیرند تا چیـزی به عنوان گوگل و خدمات آن در صفحه مرورگر ما عینیت پیدا کند.

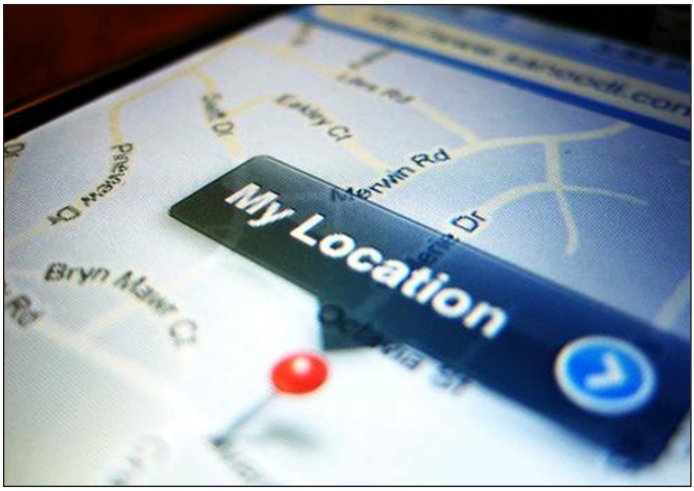
اسـتفاده از این همه، بـرای ما تقریباً هیـچ هزینه‌ای ندارد. ظاهراً همه چیز مجانی است. اما چرا!؟

تبلیغات و ....

در محیـط اینترنـت سـایت‌هایی کـه بازدیدکننده بیشـتری را به خود جلب کنند، محل مناسـبی برای کسـب اطلاعـات از کاربـران و همچنیـن تبلیغات بـرای آنها می‌شـوند. گوگل نیز از این امر مسـتثنی نیست؛ اما گوگل هیچ تبلیغی را در صفحه اول خود نمی‌گذارد. گوگل با توجه به نوع جست‌وجویی که شما انجام می‌دهید، برای شـما تبلیغات مرتبط نشان می‌دهد.

همچنیـن گوگل با توجه به محتوای نامه‌هایی که در صندوق ایمیلتان دارید، به شـما تبلیغ نشان می‌دهد. یعنی با توجه به محتوای نامه‌هایی که شما برای افراد دیگر می‌فرستید یا برای شما می‌آید، به شما تبلیغات مرتبط نشان می‌دهد.

کار از ایـن بـه بعد کمـی مخفیانه‌تر می‌شـود، این سـایت می‌تواند با تحلیل و بررسـی جسـت‌وجوها و همچنیـن محتوای نامه‌هـا و همچنین صفحاتی که کاربران به آنها مراجعه می‌کنند (یعنی اطلاعاتی که نیاز کاربران هسـت) به اطلاعات ذی‌قیمتی در مورد کاربرانش دست پیدا کند. این اطلاعات می‌تواند در مورد تک‌تک کاربران یا اقشـار خاصی از کاربران در محدوده‌هـای مکانی یا زمانی خاص باشـد. مثلاً می‌تواند بفهمد که نویسـنده متنی که یک حسـاب کاربـری در گوگل دارد به دنبال چـه چیزهایی در گوگل بوده یا برای دسـته کسـانی که در محدوده مکانی "اسـتان تهران" زندگی می‌کنند چه چیزهایی



اهمیت دارد. حتـی می‌تواند بفهمد کاربران اینترنت در مثلاً اسـتان "آذربایجان غربی" یا شهرستان "فسا" در "اسـتان فارس" در زمان عیدنوروز بیشتر به دنبال چه چیزهایی هستند. او می‌تواند از این طریق بسیاری از خواسته‌ها و سلایق ما و جامعه‌ای که در آن هستیم را بفهمد.

شـاید این‌ها خیلـی برای ما اهمیت نداشـته باشـد ولی برای برخی افراد و شـرکت‌ها اطلاعات بسـیار مفید وحتی حیاتی قلمداد می‌شـوند. چطور؟ اگر با بحث‌های بازاریابی و تولید و فروش محصول آشـنا باشـید، به دست آوردن نیاز و سـلیقه مخاطب برای تولیدکننـدگان اهمیت زیادی دارد. گوگل با تحلیل محتوای اطلاعاتی که از کاربران به دسـت می‌آورد (مثل اطلاعات مکانی، نوع جسـت‌وجوها، محتوای نامه‌هـا و ...)، اطلاعـات بسـیار ذی‌قیمتـی بـرای شرکت‌های مختلف تهیه می‌کند و اینجاست که باید برای به دسـت آوردن این اطلاعات پول خرج کرد. یک‌سری از اطلاعات دم دسـتی‌تر در اختیار عموم قرار داده می‌شـود تا قـدرت گوگل نشـان داده شـود و ایجـاد جذابیت کند مثل اطلاعاتی کـه در مـورد بیشـترین کلمات جست‌وجو شده از شـهرهای مختلف جهـان می‌توانیـد روی سـایت گوگل ببینید.

تا اینجای مسأله را شاید بتوان با استناد به توافقنامه‌ای که در ابتدای اسـتفاده از گوگل و یا هنگام عضویت در آن می‌خوانید و قبول می‌کنید، هضم کرد.

شـما با قبول ایـن توافقنامه، به گـوگل این اجازه را می‌دهید که از اطلاعات شـما این گونه استفاده‌ها را انجام دهد.

بـه هرصورت باید بدانیم که گـوگل چیزی بیش از آنچه که ما هزینـه آن را می‌پردازیم، به ما نمی‌دهد. هزینه‌ای که ما به گوگل می‌پردازیم، همان اسـتفاده کردن ما از گوگل اسـت. کافی اسـت کـه ما وارد سایت گوگل شویم و از خدماتش مثل جست‌وجوی عبارات و عکس‌ها، استفاده از جی‌میل و ... استفاده کنیم تا هزینه این خدمات را پرداخته باشیم!

اما چیز دیگری در این بین هسـت که مسأله را برای کاربران حسـاس‌تر می‌کند. آیا گـوگل می‌تواند به عنوان یک بازوی اطلاعاتی- امنیتی برای به دسـت آوردن اطلاعـات از مـردم و یـا مبارزه با دشـمنان دولت‌ها استفاده شود؟

پاسـخ این مسأله، مثبت اسـت و با توجه به دلایل و شـواهدی که در ادامه مطلب به آنها اشاره می‌شود، دولت آمریکا خود یکی ازحامیان اصلی آن است.

– گوگل از شما چه می‌داند؟

اطلاع از وضعیت علمی، نظامی، اقتصادی، فرهنگی و به هرصـورت اطلاع از وضـع دولت‌های دیگر و نیروهای مرتبط با آنان، نقش اساسی در تأمین امنیت یـک دولت خاص (در اینجا یعنـی آمریکا) خواهد داشـت. برای آمریـکا اهمیت زیـادی دارد تا بداند محققان کشـور "الف" در زمینه پژوهش‌های علمی صنعتـی خاص، به چه نتایجی دسـت یافته‌اند؟ برای آنهـا اطلاع از وضعیـت اقتصـادی و فرهنگی یک کشور خیلی مهم اسـت. همچنین در زمینه‌هایی که به آن نـام تروریسـم می‌دهند، شـناخت تحرکات تروریسـت‌ها و گروه‌هایی از این دسـت برایشـان اهمیت حیاتی دارد.

دسـتیابی به این اطلاعـات از جمله مواردی اسـت که هزینه زیادی برای کسـانی کـه این اطلاعات را می‌خواهند، دارد.

گوگل چگونه می‌تواند در تأمین اهداف مزبور نقش ایفا کند؟ باید دید که گوگل چقدر در کسـب این اطلاعات مفید اسـت؟ آیا گوگل می‌تواند وضعیت تحقیقات علمی صنعتی یک جامعه خاص را بفهمد؟ آیا گـوگل می‌تواند ارتباطات بیـن افراد مختلف و احیاناً تروریست‌ها را آشکار کند؟

اسـتفاده شـما از معمول‌ترین خدمات گوگل یعنی جست‌وجوی اطلاعات (Search)، اطلاعات زیر را در اختیار گوگل قرار می‌دهد:

۱– شـماره IP رایانه شما: این شماره بسته به شرایط، مـکان رایانه شـما و اطلاعات مرتبطـی را در دنیای اینترنت نشـان می‌دهد؛ مثلاً اینکه شـما از چه ISP (شـرکت تامین کننده اینترنت) اسـتفاده می‌کنید و شـهری که هم اکنون در آن هسـتید و چیزهایی از این قبیل.

۲– نوع سیسـتم‌عامل (مثل ویندوز xp) و مرورگری که شـما با آن کار می‌کنید (مثل فایرفاکس) و دقت صفحه نمایش شما (مثلا ۸۰۰ در ۶۰۰)

۳– کلماتی که توسط گوگل، جست‌وجو کرده‌اید.

۴– تمام سایت‌هایی که از طریق صفحه جست‌وجوی گوگل وارد آنها شده‌اید.

۵– اگر شما دارای یک حساب جی– میل (Gmail) در گوگل باشـید، باید اطلاعات زیر را به موارد بالا اضافه کنید:

– چه کسانی به شما نامه فرستاده‌اند.

– کسانی که از شما نامه دریافت داشته‌اند.

– محتوای همه نامه‌های شما.

حتی اگر شـما در جی‌میل، حسـابی نداشـته باشید، نامه‌هایی که برای دارندگان جی‌میل ارسـال کرده یا از آنها دریافت کرده‌اید شامل این موضوع می‌شوند.

اسـتفاده شـما از خدمـات مختلـف گـوگل (مثل خبرخوان) و سـایت‌های وابسـته، اطلاعات بسـیار بیشـتری در اختیار گوگل می‌گذارد؛ مثلاً اگر شـما در شـبکه اجتماعی اُرکات (Orkut) عضو باشید، تمام ارتباطات و فعالیت‌های شـما در این شـبکه در اختیار گوگل است.

موارد دیگری هم هسـتند که برای کاربران کشور ما فعلاً (!) کاربرد و اهمیتی ندارند، ولی به آنها اشـاره می‌شود.

به عنـوان مثال Latitude ابزاری اسـت که امکان بـه اشـتراک‌گذاری اطلاعـات در مـورد موقعیت

جغرافیایی افراد از طریق تلفن همراه را در سرویس My Location فراهم می‌کند. اگر چه در این سرویس کاربر با انتخاب یک گزینه به گوگل اعلام می‌کند موقعیت جغرافیایی او را شناسایی نکند، این شرکت در سرور خود آخرین اطلاعات مربوط به موقعیت فیزیکی او را در سرور خود نگه می‌دارد. آیا می‌دانستید گوگل از طریق این سرویس از عمر باتری گوشی شما و دیگر اطلاعاتی که به ظاهراً اهمیتی ندارند هم مطلع می‌شود؟

بررسی جست‌وجوها

بهتر است ادامه گزارش را برای شمایی بنویسیم که می‌خواهید کارتان از دید شخص سومی مانند گوگل مخفی بماند. بسیاری از مردم به هر دلیل می‌خواهند مقصودشان از جست‌وجوهایی که در شبکه انجام می‌دهند، پنهان بماند اما گوگل مجموع جست‌وجوهایی را که از طریق دستگاه رایانه هر شخص انجام شده می‌داند. آمار استفاده از سرویس‌های مختلفی که از طریق این رایانه انجام شده (مثل ایمیل و...) را هم دارد. برایش خیلی سخت نیست تا بفهمد کدام جست‌وجو واقعی و کدام برای ردگم‌کردن است. حتی گوگل می‌داند که از صفحات جست‌وجویی که برای‌مان فراهم کرده، در چه سایت‌هایی کلیک کرده‌ایم. فرض کنید لابلای جست‌وجوهایی که انجام می‌دهیم چند جست‌وجوی بی‌ربط به موضوع هم بکنیم تا طرفمان (یعنی گوگل) منظور ما را نفهمد و مثلاً رد گم می‌کنیم اما بدلیل اینکه کل عملیات ما تحت‌نظر گوگل انجام پذیرفته، خیلی نمی‌توانیم به پوشیده‌ماندن کارمان اطمینان داشته باشیم.

بررسی نامه‌های الکترونیک

یکی دیگر از چیزهایی که به ذهن می‌رسد این است که محتوای نامه‌های ما را بررسی کند. اگر مواردی از ارتباطات مشکوک در آنها یافت، مسأله را دنبال می‌کند تا به سرنخ‌های بیشتر و مدارک محکم‌تر برسد و نهایتاً این امور به مراجع خاص آن ارجاع می‌شود.

شاید بگوییم که ما برای ارتباط با افراد بیگانه ایمیل‌ها را با نام مستعار می‌سازیم و از اطلاعات با عنوان مستعار استفاده می‌کنیم. البته کار خوبی است، اما اصلاً نباید به آن اطمینان کرد. اجازه بدهید مثال: بسیار پیش‌آمده که در صندوق ایمیل شما که به نام مستعار ایجاد کرده‌اید- نامه‌ای برای دوستتان فرستاده باشید. کافی است دوست شما در پاسخ ایمیل شما، نام واقعی شما را ببرد. یعنی تمام زحمات شما برای مخفی ماندن هویتتان بر باد رفت؛ ادامه این ماجرا مساوی است با لو رفتن اطلاعات بیشتر در مورد هویت شما و دوستانتان.

شاید بگویید «من یک ایمیل برای ارتباطات ناشناس دارم و یک ایمیل دیگر برای ارتباط با دوستانم.» خب این هم راه حل بهتری است اما هنوز اطمینان بخش نیست. هر بار که از گوگل استفاده می‌کنید، گوگل رایانه شما را با یک کوکی (با شماره شناسایی یکتا) شناسایی می‌کند. این کوکی دو سال روی رایانه شما اعتبار دارد و با هربار استفاده از گوگل، مجدداً احیا می‌شود. خب وقتی ببیند یک بار از ایمیل ۱ و بار دیگر از ایمیل ۲ روی این رایانه استفاده شده، احتمال زیادی می‌دهد که هر دو متعلق به یک نفر باشد.

اگر صندوق ایمیل شما در گوگل (Gmail) باشد، گـوگل تمـام ایمیل‌هایی که از آن ارسـال یا به آن آمده باشد را می‌داند.

کسـانی که بـا ریاضیـات و آمار سـر و کار دارند، می‌دانند که خیلی راحت می‌توان از طریق "گراف"، ارتباط بین ایمیل‌ها، هویت‌ها را تشخیص داد.

البته شکل بالا، مثال بسیار سـاده‌ای از گراف مزبور اسـت. از طریق تحلیل محتـوای ایمیل‌ها می‌توان به موضوع ارتباطات بین ایمیل‌ها پی برد.

ایمیل‌ها از نظر ارتباطات کاری، ارتباطات دوسـتانه، ارتباطـات خانوادگـی و عاطفـی و ... می‌توانـد دسـته‌بندی شـود. رایانه‌ها و مـکان جغرافیایی آنها هم معلومند. مشـکل بتوان در چنین شبکه‌ای هویت مخفی داشـت. شـواهد زیادی در دسـت هست که نشـان می‌دهد اطلاعـات حتی پس از حـذف آنها توسـط کاربران، در سـرورهای گـوگل نگهداری می‌شود.

بررسی گفتوگوهای آنلاین (چت)

گفت و گوهای ما در محیط‌های چت (chat) حاوی اطلاعات زیادی اسـت و همانند ایمیل‌ها قابل تحلیل و پیگیری هسـتند. بررسی استفاده ما از سرویس‌های مختلف گوگل

وقتی اسـتفاده کاربران از خدمـات مختلف گوگل به این موارد اضافه می‌شود، مسـأله ابعاد جدیدتری به خود می‌گیرد. خدمـات مختلفی که گوگل روی سایت خود فراهم کرده، موجب اشتیاق هرچه بیشتر کاربران برای اسـتفاده از گوگل می‌شود. البته برای اسـتفاده از بسـیاری از این خدمات باید در گوگل یک حساب کاربری ایجاد نمود. استفاده از فیدریدر (یا خواننـده خوراک) سـایت‌های موردعلاقه ما را برای گوگل معلوم می‌نماید. اسـتفاده ما از سرویس گـوگل‌ارث (Google Earth)، مکان‌های مهم و مـورد توجه ما را بـرای گوگل معلوم می‌سـازد. از ایـن طریق راحت می‌توان فهمید شـما در کجا کار می‌کنید یا خانه‌تان کجاسـت؟ یـا مکان‌های مهم و مورد توجه شما چه جاهایی هستند؟ «»

آیا گمان می‌کنید تنها خودتان از محتویات Gmail شـخصی خود باخبرید؟ آیا گوشـی تلفن همراهتان فقط کارهایی را کـه می‌خواهید انجام می‌دهد؟ آیا موتورهای جستجو هویت شما و آنچه را که جستجو می‌کنیـد، تنهـا نزد خـود نگه می‌دارنـد؟ «گوگل» ایمیل‌های مـا را می‌خواند تـا آگهی‌های تجاری به آن‌ها ارسـال کند. زمانی که از "Google Map" استفاده می‌کنیم، آن‌ها می‌دانند که چگونه ما از نقطه آ به نقطه ب می‌رویم. زمانی که از موتور جستجوی گوگل استفاده می‌کنیم، آن‌ها می‌دانند که دنبال چه چیزی هستیم. آن‌ها تمام این اطلاعات را می‌خوانند، اما ما با آن‌ها معامله‌ای می‌کنیم مبنی بر این که از این اطلاعات علیه خودمان استفاده نکنند، تا به شعارشان یعنی «بد نباش!» (Don't Be Evil) پایبند باشند. اما آیا واقعا این گونه است؟

پیش‌بینی آینده برای سازمان سیا

کمپانـی Recorded Future یـک شـرکت نرم‌افزاری واقع در شـهر کمبریج ایالت ماساچوست در آمریکا اسـت که در حـوزه اطلاعات وب و نیز تحلیل‌هـای پیش‌بینانه فعالیت می‌کند. این شـرکت با اسـتفاده از ابـزاری به نام «موتـور تحلیلی موقتی» (emporal analytics engine)، ابـزار

پیش‌بینی و تحلیل را به متخصصین ارائه می‌کند تا آن‌ها بتوانند با بررسی منابع موجود در اینترنت و بازیافت، اندازه‌گیری و تصویرسازی اطلاعات، شبکه‌ها و الگوها را در گذشته، حال و آینده نشان دهند. نرم‌افزار این شرکت منابع را تحلیل کرده و «لینک‌هایی نامرئی» بین اسناد ایجاد می‌کند تا لینک‌هایی که آن‌ها را به یکدیگر پیوند می‌زند و نیز افراد، نهادها و وقایع مربوط به آن‌ها را شناسایی کند. این شرکت در سال ۲۰۰۸ و توسط فردی به نام «کریستوفر آهلبرگ» (Christopher Ahlberg) تشکیل یافته و تا نوامبر ۲۰۱۱ دارای ۲۰ کارمند بود. گوگل در ۳ می ۲۰۱۰ و سازمان سیا از طریق شاخه‌های سرمایه‌گذاری خود یعنی «گوگل‌ونچرز» (Google Ventures) و "این-کیو-تل" (In-Q-Tel) در این شرکت سرمایه‌گذاری کرده‌اند. Recorded Future Inc. شرکتی است که تمام اطلاعات موجود در صفحات وب را بررسی می‌کند تا بداند چه کسی، چه چیز، کی، کجا و چرا – یعنی برای مثال، چه کسی، برای چه به کجا می‌رود.

البته این اولین باری نیست که سیا و گوگل در یک پروژه مشترک سرمایه‌گذاری می‌کنند. «این-کیو-تل» شاخه سرمایه‌گذاری سیا که در تکنولوژی‌های آتی و ثمرده سرمایه‌گذاری می‌کند

در گذشته در شرکتی به نام «کی‌هول» (Keyhole) سرمایه‌گذاری کرد. این شرکت در سال ۲۰۰۴ به وسیله گوگل خریداری شد تا از آن به عنوان آغازی برای «گوگل‌ارث» (Google Earth) استفاده شود.

گوگل؛ جاسوس آژانس امنیت ملی

پس از حملات سایبری به گوگل در سال ۲۰۱۰ که ادعا می‌شود از جانب هکرهای چینی انجام گرفت، این شرکت تصمیم گرفت با عقد قراردادی با آژانس امنیت ملی حفاظت سایبری در مقابل این گونه حملات را به این سازمان جاسوسی واگذار کند. این امر نگرانی‌های بسیاری در میان فعالین

حمایت از حفظ حریم خصوصی در آمریکا برانگیخت به گونه‌ای که «مرکز اطلاعات حریم خصوصی الکترونیک» (Electronic Privacy Information Center) درخواست کرد، اطلاعات مرتبط با این قرارداد منتشر شود.

با این حال، «ریچارد لئون» (Richard Leon)، قاضی دادگاه فدرال، اعلام کرد که هیچ کس حق ندارد بداند که آیا گوگل برای آژانس امنیت ملی جاسوسی می‌کند یا نه. وی گفت: «آژانس امنیت ملی آمریکا مجبور نیست که هیچ یک از فعالیت‌های سازمان یا هر نوع اطلاعات مرتبط با این فعالیت‌ها را منتشر کند.» حال مشخص نیست که شرکت گوگل – محبوب‌ترین وب‌سایت جهان – وارد چه نوع معامله‌ای با آژانس امنیت ملی آمریکا شده است.

رسوایی‌های Wi–Fi و اندروید

در سال ۲۰۱۰ اعلام شد که اتومبیل‌های تصویربرداری خیابانی گوگل که در بیش از سی کشور جهان مشغول فیلمبرداری از خیابان‌ها و خانه‌ها بودند، به شبکه‌های اینترنت بی‌سیم نفوذ کرده و تمام اطلاعات مبادله شده در آن‌ها را می‌ربودند. شرکت گوگل در ابتدا اعلام کرد که فقط شبکه‌های را محل‌یابی می‌کردند اما بعدها اذعان کرد که اتومبیل‌های این شرکت حین فیلمبرداری ارتباطات شبکه‌های وای‌فای رمزگذاری نشده را ضبط کرده و آن‌ها را به سرورهای گوگل ارسال کرده‌اند. متعاقب این امر اروپایی‌ها شرکت را تحت تعقیب قضای قرار دادند و قانونگذاران آمریکایی نیز خواهان توضیح «کمیسیون فدرال بازرگانی» (Federal Trade Commision)

شـدند. در ایالـت ارگـون نیـز شـکایتی علیـه گـوگل مطـرح شـد. در سـال ۲۰۱۰ و متعاقـب اعتراضات وسیعی که نسـبت بدیـن امر صورت گرفت، شـرکت گوگل مجبور شد که به کار این سیستم خاتمه دهد. در حقیقت گوگل توانسـت با این کار به آدرس‌ها و رمزهای ایمیل‌های اینترنتی و همچنین هر نوع ارتباطاتی که از طریق سیستم‌های بی‌سیم رد و بدل می‌شدند، دست یابد.

سال گذشته نیز گزارش‌هایی مخابره شد مبنی بر اینکه گوشـی‌های تلفن همراه «اندرویـد» (Android) گوگل و «آیفون» (iPhone) شـرکت اپل به طور مـداوم محل خود را به شـرکت‌های سـازنده خود مخابـره می‌کنند. گوگل و اپـل اطلاعات مربوط به مکان‌هـا را به عنوان بخشـی از رقابت بـرای ایجاد پایگاه‌هـای عظیم داده که می‌تواننـد مکان مردم را از طریق تلفن‌های همراه شناسایی کنند، جمع‌آوری می‌کنند. این پایگاه‌هـای داده می‌توانند به آن‌ها در دسـتیابی به بازار ۹/۲ میلیارد دلاری خدمات مکان-محـور که انتظار می‌رود در سـال ۲۰۱۴ بالغ بر ۳/۸ میلیارد دلار شود، یاری خواهند رساند.

اندروید و اپل، ردیاب‌هایی که قربانیانشان با کمال میل آن‌ها را با خود حمل می‌کنند

بـر اسـاس تحقیـق جدیدی که به وسـیله «سـامی کامـکار» (Samy Kamkar)، تحلیلگـر مسـائل امنیتی، انجام گرفته گوشی اندروید در هر چند ثانیه یکبار موقعیت خود را شناسایی کرده و حداقل چند بار در هر سـاعت ایـن داده‌ها را به گـوگل مخابره می‌کنـد. این گوشـی همچنین نام، مـکان و قدرت سیگنال هر نوع شبکه Wi-Fi نزدیک را نیز مخابره می‌کند. شرکت گوگل تاکنون از ارائه توضیحی در مورد این اطلاعات امتناع کرده است.

چـرا Google Earth رژیـم صهیونیستی را نشان نمی‌دهد

از سـال ۲۰۰۵ تاکنون که گوگل سیستم Google Earth را راه‌انـدازی کـرده اسـت، این شـرکت تبدیل بـه برترین ارائـه دهنده تصاویـر ماهواره‌ای با قابلیت تفکیک بالا شـده اسـت. در سـال ۲۰۱۰، سیسـتم Google Earth جهانیان را قادر سـاخت که ویرانی‌های پس از زلزله هائیتی را مشاهده کنند. پـس از زلزله و سـونامی مرگ‌بار ژاپـن نیز گوگل همین امـکان را فراهم آورد. گـوگل می‌تواند تنها با یک کلیـک تمام جهان و حوادث دوردسـت‌ها را در صفحه نمایشـگر شـما ظاهر کند. با این حال

یک کشـور وجـود دارد کـه گوگل آن را به شما نشـان نخواهد داد: رژیم صهیونیستی!

در سـال ۱۹۹۷، کنگره «قانون تفویض اختیارات دفـاع ملی» را تصویب کرد. بخشی از این قانون با عنوان «ممنوعیت جمع‌آوری و انتشار تصاویر ماهواره‌ای مربوط به اسـرائیل» شـناخته می‌شود. بر اسـاس این قانـون انتشـار تصاویر ماهواره‌ای رژیم صهیونیستی با تفکیک بالا ممنوع اسـت. این قانـون علاوه بر رژیم صهیونیستی، شامل سرزمین‌های اشـغالی نیـز می‌شـود به همیـن دلیل اسـت که سـازمان دیده‌بـان حقوق بشـر نمی‌تواند در گزارش‌هـای خود تصاویر واضحـی از نوار غزه ارائه کند. البته اخیـرا ترکیه اعلام کرده که ماهواره «گوک‌تورک» (ترک آسـمانی) پـس از پرتاب در سال ۲۰۱۳، تصاویری با تفکیک‌پذیری بالا از رژیم صهیونیسـتی منتشـر خواهد کرد. این نکته نیز شایان ذکر اسـت که شـرکت گوگل ارتباطـات نزدیکی با رژیم اشـغالگر صهیونیسـتی دارند. مؤسسـین این شـرکت بارها به رژیم صهیونیستی سفر کرده و یک مرکز تحقیق و توسعه در «تل‌آویو» تأسیس کرده‌اند.

سایر جاسوسی‌های گوگل

بـه جرئـت می‌تـوان گفت کـه تمـام نرم‌افزارها و خدمات ارائه شده به وسیله گوگل دارای عنصری از جاسوسی هستند. برای مثال این شرکت حساب‌های Gmail افراد را به صورت پیوسته مورد بررسی قرار می‌دهـد تا با توجه به لغات و عبارات کلیدی مندرج در ایمیل‌های آن‌ها، تبلیغات ارائه شـده برای حساب مذکـور را هدفمند سـازد. در نرم‌افـزار وب‌گردی Google Chrome نیـز در هنگام نصب شـدن یک شـماره شناسـایی (ID) تولید می‌کند که تمام جسـتجوهای انجام شده به وسـیله کاربر به نام ID مذکور ثبت می‌شود.

لوازم الکترونیکی هوشمند جاسوسان پنهان در خانه‌ها

با پیشـرفت ابزارهای برقی هوشمند و استفاده هرچه بیشـتر آنها به عنوان بخشـی از ابزارآلات ساختمان، امکان جاسوسـی خانه‌هابسیار آسـان‌تر گشته است. رییس سازمان سیا، دیوید پترائوس با تایید این مطلب اظهار داشت که آمریکاییان با استفاده از این وسایل این امکان را به سـازمان‌های جاسوسـی می‌دهند تا زندگی شـخصی و خصوصی آنها را راحت‌تر تحت کنترل و نظارت قرار دهند.

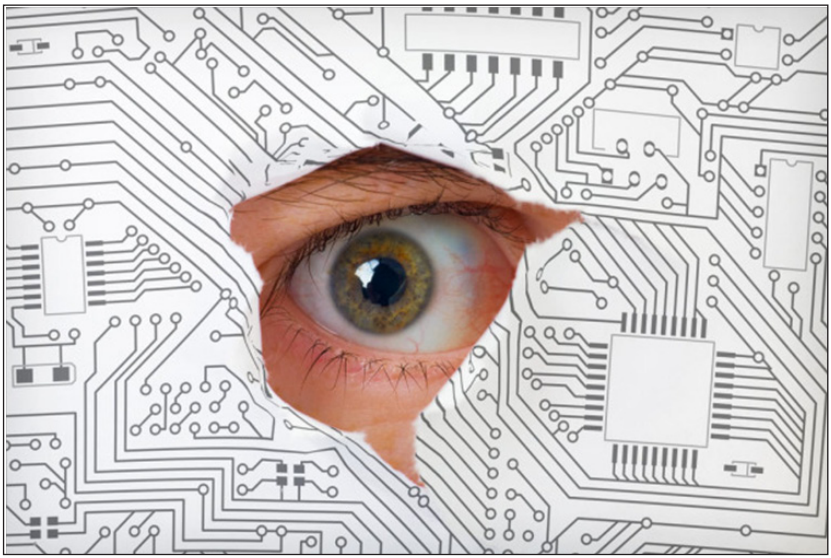
دیوید پترائوس طی سخنان خود در نشست «این‌کیوتل» که پیرامون عملیات‌های سرمایه‌گذاری سیا در بخش فناوری بود، بیان داشت که این وسایل جدید همچون یخچال، اجاق گاز، و سامانه برق خانه که به اینترنت متصل می‌شوند می‌توانند «مفهوم رازداری و پنهان‌کاری ما را تغییر دهد.»

وی افزود: «چنین ابزارهایی را می‌توان به وسیله فناوری‌هایی چون شناسایی فرکانس رادیویی، شبکه‌های حسی، و سرورهای جاسازی‌شده کوچک که همگی با استفاده از محاسبات فراوان، کم‌هزینه، و پرقدرت به نسل بعدی اینترنت متصل می‌شوند مکان‌یابی، شناسایی، رصد، و از راه دور کنترل کرد.»

گفتنی است که در حال حاضر یکی از بزرگ‌ترین شرکت‌های سازنده ریزپردازنده به نام ARM پردازنده‌های جدیدی را ساخته است که می‌توانند تقریباً درون تمامی وسایل خانگی جاسازی شده و به اینترنت وصل شوند تا از این طریق بتوان آنها را به همراه دیگر وسایل از راه دور تحت کنترل گرفت. این شرکت نام این محصول را «اینترنت اشیاء» گذاشته است.

سؤالی که مطرح است این است که این اطلاعات برای تحلیل و بررسی به کجا فرستاده خواهند شد. در حال حاضر سازمان امنیت ملی آمریکا NSA دست به ساخت یک تأسیسات به شدت یکپارچه و مستحکم ۲ میلیارد دلاری در اعماق صحرای یوتای آمریکا زده است که دورتادور آن را کوه فرا گرفته است. قرار است این تأسیسات در ماه سپتامبر ۲۰۱۳ به طور کامل مورد بهره‌برداری قرار بگیرد.

وبگاه خبری گیزمو که در مورد وسایل برقی و فناوری‌های جدید فعالیت می‌کند در مورد این مرکز گفته است: «مرکز داده‌های یوتا کانون شبکه جهانی اطلاعات (GIG) به حساب می‌آید. این مرکز یک پروژه نظامی است که با چندین یوتابایت



داده سروکار دارد؛ میزان این داده‌های به حدی زیاد است که در حال حاضر واحد شمارش دیگری برای آن وجود ندارد.»

ایـن وبگاه می‌افزایـد: «این مرکز بـا وجود هر یک از پست‌های شـنود، ماهواره‌های جاسوسی، و مرکز داده NSA که به آن متصل می‌شـوند سبب می‌شود تا NSA تبدیل به بزرگ‌ترین سـازمان جاسوسـی جهان شود.»

– تلویزیون هوشمند جاسوسی در مقابل دیدگان شما

تلویزیون‌های پیشـرفته پلاسـما و LED مدل ۲۰۱۲ سامسـونگ، ویژگی‌هایـی دارنـد که پیـش از این هیچگاه شـاهد نبودیم، آنها مجهز به دوربین HD، دو میکروفـن و نرم‌افزارهایـی بـرای دنبال کردن و تشخیص چهره و تشخیص صدا هستند.

بـا کمک این ویژگی‌هـا، خریدار ایـن تلویزیون‌ها می‌تواند با شـیوه‌ای نوین بر تلویزیون وضوح بالای خود کنترل داشته باشد، این تلویزیون‌ها دیگر بیشتر شبیه یک رایانه شخصی شـده‌اند و درست به همین دلیل، ممکن اسـت هدف بعدی هکرها قرار بگیرند، هکرهایـی که می‌خواهند شـما و خانواده‌تان را دید بزنند و صدایتان را بشـنوند و اطلاعات شخصی شما را جمع‌آوری کنند.

دوربیـن وبی و اتصال به اینترنت چیزهای تازه‌ای در تلویزیون‌های پیشرفته نیستند، اما از آنجا که می‌توان اپلیکیشـن‌های ثالث را روی ایـن تلویزیون‌ها نصب کرد، پیشـبینی اینکه بشـود به کمک یک اپلیکیشن مخرب و دوربین و میکروفن تلویزیون، امنیت حریم خصوصـی خریدار را به مخاطره انداخت، پیشـبینی بعیدی به نظر نمی‌رسد.

دوربین و میکروفن‌ها، در بالای صفحه سـری ۸۰۰۰ پلاسمای سامسونگ و LED های مدل‌های ۷۵۰۰ و ۸۰۰۰ES متصل هسـتند، وقتی تلویزیون به اینترنت متصل شـود، کاربر امکان می‌یابد از طریق سرویس ابری سامسـونگ از اپلیکیشـن‌های موجود استفاده

کند.

ایـن تلویزیون‌ها، با اسـتفاده از نرم‌افزار تشـخیص چهـره، کاربرانشـان را شناسـایی می‌کننـد، به این معنی که تشـخیص می‌دهنـد کدام عضـو خانواده جلوی تلویزیون اسـت و تلویزیـون را برای هر فرد شخصی‌سازی می‌کنند. این تلویزیون‌ها می‌توانند به فرمان‌های صوتی هم گوش بدهند.

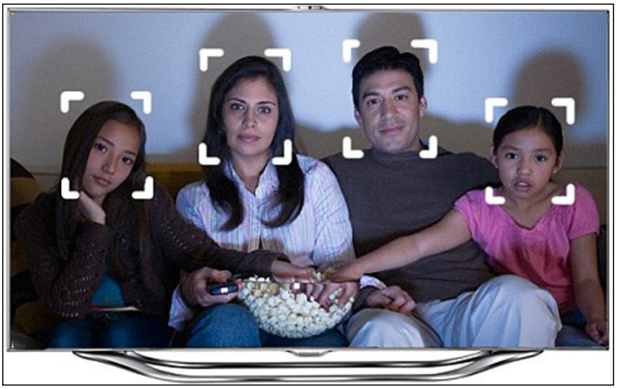
مساله نگران‌کننده امکان سـوء استفاده از دوربین و میکروفن تلویزیون اسـت، گرچه می‌تـوان دوربین و میکروفن را به شـیوه نرم‌افزاری غیرفعال کرد، اما راه اطمینان‌بخشی برای غیرفعال کردن سخت‌افزاری آنها وجود نـدارد. در تلویزیون‌ها دیگر میکروفن و دوربین به صورت وسایل جانبی با یک کابل USB به تلویزیون متصل می‌شوند و به این ترتیب اگر مایل به استفاده از آنها نباشید و می‌خواهید کاملا از امنیت و حریم شـخصی خود مطمئن باشید، آنها را متصل نکنید.

به تازگی سامسـونگ گفته است، در حال کار روی اپلیکیشنی است که تلویزیون‌های هوشمند را تبدیل به یک سیسـتم امنیتی می‌کند، به عبارتی به کاربران اجـازه می‌دهد از راه دور با گوشـی یـا تبلت خود، منظره منزلشـان را ببینند. سؤالی که پیش می‌آید این است که آیا افرد بداندیشی پیدا نمی‌شـوند که بتوانند به نوعی با برنامه‌های مخـرب، همین کار را بکننـد؟ آیـا اطلاعاتی که از طریق این اپ خاص به گوشـی کاربـران می‌رسـد، رمزگزاری شده خواهد بود؟

پروژه عینک گوگل مخوف‌ترین پروژه جاسوسی جهان

ماه‌ها اسـت که در مورد عینک گوگل خبرهایی به گوش می‌رسـد. حالا این شرکت رسـما اطلاعاتی در مورد پروژه‌اش منتشـر کرده است و می‌توانید با Google Glass آشنا شوید؛ و این، اولین تصاویر منتشر شده از طرف گوگل هستند که نشان می‌دهند عینک این شرکت چه شکلی خواهد داشت. گجتی که در فیلم‌های تخیلی سال‌ها آن را می‌دیدیم، حالا در حال تبدیل شـدن به یک محصول واقعی اسـت. گوگل یـک صفحه در گوگل پـلاس برای عینک واقعیت افزوده‌اش ایجاد کـرده و می‌گوید تعدادی از کارمندانش مشـغول تست این کامپیوتر پوشیدنی هستند.

یکی از نکاتی که در تک تک سـرویس‌های جدید کمپانی گـوگل لمس می‌شـود میل به تغییر شـیوه زندگی به حالت مدرن است. هم اکنون این کمپانی پـرده از پـروژه شـگفت انگیز و جدید خـود یعنی عینک هوشـمند بر می‌دارد. عینک‌های آنلاینی که می‌تواننـد بهترین گجت بـرای همراهی و کمک به شما و یا سازمان‌های جاسوسی باشند.



در فیلم‌های تخیلی حتماً تا کنون ابزارهای هوشمند بسیاری را مانند عینک، ساعت مچی و ... دیده‌اید که به نقش اول فیلم در رسیدن به هدف خود کمک می‌کنند. عینک هوشمند گوگل نیز قرار است به شما در انجام کارهای روزانه کمک کند با این تفاوت که منبع اصلی این عینک برای جمع آوری اطلاعات سرویس‌های دیگر گوگل و شاید اطلاعات موجود دیگر در اینترنت است. این عینک در حقیقت شامل یک نمایشگر برای نمایش محتوا به شما و یک سیستم تشخیص صدا و حرکت چشم است تا بتواند خواسته های شما را انجام دهد. تنها کافی است برای استفاده از اینترنت و کمک گرفتن از این دستگاه در کارهای روزانه خود در اینترنت صحبت کنید تا همه چیز برای شما انجام شود.

هنوز از طرف کمپانی گوگل اطلاعات زیادی درباره این عینک‌های هوشمند که یکی از محصولات فیزیکی گوگل هستند انتشار نیافته است اما با دیدن ویدئو انتشار یافته در سایت رسمی گوگل می‌توان حدس‌هایی از چگونگی کار این عینک و امکاناتی که قرار است در اختیار استفاده کنندگان خود بگذارد بزنیم. گوگل هم اکنون پروژه تولید این عینک‌ها را Project Glass نام گذاری کرده است و از کاربران خود می‌خواهد تا می‌توانند پیشنهاد های جدیدی برای افزایش کارایی این عینک‌های هوشمند بدهند.

این عینک‌ها از دیگر سرویس‌های ارائه شده توسط کمپانی گوگل مانند شبکه مجازی گوگل پلاس، نقشه گوگل، سرویس تشخیص گفتار، گوگل موزیک، تقویم گوگل و ... استفاده می‌کند و برای پردازش اطلاعات بعید نیست تصمیم گرفته شود از سیستم عامل اندروید استفاده شود. گوگل با توسعه سرویس‌های مختلف هم اکنون قدرت انجام پروژه های زیادی را دارد که هر کدام از آن‌ها می‌توانند به تحولات بزرگی در تکنولوژی تبدیل شوند. در واقع هر آنچه که شما می‌گویید، می‌بینید، می‌شنوید و

انجام می‌دهید تماما قابل پایش و جاسوسی می‌شوند. این عینک تداعی بخش فیلم پلیس آهنی و ترمیناتور است که بازیگر نقش اول آن آرنولد شوارتزینگر با عینکی شبیه عینک گوگل به پردازش و شناسایی محیط اطراف خود می‌کرد.

فضای ابری (Cloud Storage)

به تازگی شرکت‌های اینترنتی نظیر گوگل، یاهو، آمازون، سونی، ال‌جی، دراپ باکس، مایکروسافت

و دیگر شرکت‌های بزرگ دنیا اقدام به ارائه فضاهای ذخیره سازی مجازی یه به اصطلاح ابری آن هم به صورت رایگان و با حجم بسیار بالا کرده‌اند.
شعار خدمات ابری این است که از این پس فایل‌ها و داده‌ها و مستندات مهم و پرکاربرد خود را می‌توانید در فضای ابری ذخیره کنید و از آن پس از هر جای جهان به آنها دسترسی داشته باشید و یا با دیگران به اشتراک بگذارید.

اما فضای ابری چه خطراتی می‌تواند با خود به همراه داشته باشد؟ تا کنون امکان جاسوسی از اطلاعات و ایمیل‌ها و چت‌ها در اینترنت وجود داشت اما از این پس امکان جاسوسی فایل‌های مهم و حساس شما نیز برای سازمان‌های جاسوسی آمریکا میسر شده است. در واقع این خود ما هستیم که فایل‌های مهم و گاهی حساس و امنیتی خود را تقدیم این آژانس‌ها خواهیم کرد.
گوگل بزرگ‌ترین ماشین جاسوسی جهان اخیرا فضای مجازی گوگل داکس Google Docs را به گوگل درایو Google Drive تغییر داد و حجم آن را به ۵ گیگابایت افزایش داد. آن هم به صورت رایگان. با تبلیغات گسترده‌ای ک در این زمینه شد گوگل هدف از این اقدام را فراهم کردن شرایط مورد نیاز برای کاربران خود به منظور در دسترس بودن دائمی اسناد و فایل‌های مهم خود در هر مکان و هر زمان عنوان کرد.

گوگل درایو یا Google Drive نام سرویس جدیدی است که به وسیله آن شما می توانید همه فایل هایتان را در یکجا ذخیره کنید و با هر کس که می خواهید به اشتراک بگذارید. گوگل درایو به شما ۵ گیگابایت فضای ابری ارائه می دهد و شما می توانید با پرداخت هزینه آن را تا یک ترابایت افزایش دهید. اما اگر بخواهیم به امکانات متنوعی که گوگل

برای فضای ذخیره سازی ابری خود در نظر گرفته است اشاره کنیم:

می توانید با گوگل درایو تمامی کارهایی که در گوگل داکز تا کنون انجام داده اید را تجربه کنید، فایل های مختلف بسازید و یا ویرایش کنید.

با گوگل درایو دیگر نیاز ندارید که در ایمیل هایی که از طریق سرویس جیمیل ارسال می کنید فایل ها را پیوست کنید (Attachment) و تنها کافی است لینک فایل مورد نظر موجود در گوگل درایو را در ایمیل خود وارد کنید و گیرنده آن را دریافت خواهد کرد!

همچنین شما برای به اشتراک گذاری عکس ها و یا فیلم هایتان در گوگل پلاس تنها کافی است از گوگل درایو خود فایل را انتخاب کنید، به همین آسانی.

مهمترین خاصیت فضای گوگل درایو این است که به شما امکان می دهد بتوانید بیش از ۳۰ فرمت فایل را از طریق مرورگر خود باز کنید و دیگر نیازی ندارید برنامه ها را بر روی سیستم خود نصب کنید (HD video,,,... ,Microsoft Office Adobe Illustrator and Photoshop)

گوگل درایو به شما امکان می دهد به صورت چند نفره بر روی یک فایل ویرایش انجام دهید و تمامی تغییران به همراه نام ویرایش کننده ذخیره می گردد و شما می توانید به حالت های گذشته برگردید. شما می توانید از طریق مرورگر، گوشی تلفن هوشمند و یا رایانه خود به گوگل درایو دسترسی داشته باشید.

اما به‌طور کلی، پردازش ابری با چندین خطر امنیتی مجزا، اما مرتبط باهم مواجه است. علاوه بر این که ممکن است اطلاعات ذخیره شده، توسط مهاجمان به سرقت رفته یا در اثر خرابی سیستم از بین برود، ممکن است تأمین کننده خدمات ابری نیز از این اطلاعات سوء استفاده کند یا در اثر فشارهای دولت آن را افشا کند. واضح است که این خطرات امنیتی پیامدهای وخیمی را درپی دارند.

در سال ۲۰۰۸ تنها یک بیت اطلاعات معیوب در پیغام‌هایی که بین سرورهای مورد استفاده خدمات S۳ آمازون

(سـرنام Simple Storage Service) ردوبـدل می‌شـد، به خاموشـی سیسـتم برای چندین ساعت منجر شـد. خدمات مذکـور، فضای ذخیره‌سـازی آنلایـن را در مقیاس گیگابایـت در اختیار کاربران قـرار می‌دهنـد. در اوایل سـال ۲۰۰۹ یـک هکر با حدس زدن پاسخ سـؤال امنیتی ایمیل شخصی یکی از کارمندان توییتر توانسـت تمام اسـناد موجود در حسـاب Google Apps را که توسـط وی مورد اسـتفاده قرار می گرفت، به دسـت آورد و بخشی از این اسناد را برای رسانه‌ها ارسال کند. مدتی بعد یک اشکال نرم‌افزاری محدودیت‌های به اشتراک گذاری اسـناد برخی از کاربران Google Docs را حذف کـرد. به این ترتیب، هریک از کاربرانی که سـندی را با آن‌ها به اشـتراک گذاشـته بودید می‌توانسـت تمام اسـناد مشترک شما و سایر کاربران را ببیند. در مـاه اکتبر و در پی خرابی یکی از سـرورهای بخش Danger از شـرکت مایکروسافت که تأمین کننده فضای ذخیره‌سـازی اسـت، اطلاعات یـک میلیون گوشی هوشمند T-Mobile Sidekick از دست رفـت. البتـه بخش زیـادی از این اطلاعـات بعدها بازیابی شد. پیتر مل، رهبر یک گروه امنیتی خدمات ابری در مؤسسه ملی اسـتاندارد و فناوری (NIST) ایالات متحـده واقـع در Githersburg از ایالت مریلنـد می گوید: «حیطـه حمله‌ها بـه نرم‌افزارهایی که توسـط ابرهای عمومی عرضه می‌شـوند، بسیار گسـترده‌تر اسـت. تمام مشـتریان به تمام ابزارهای موجـود در نرم‌افزار ابری دسترسـی دارند. اگر این نرم‌افزارها تنها یک نقطه‌ضعف داشـته باشـند، یک مهاجم می‌تواند به تمام اطلاعات آن‌ها دست یابد.»

خدمات ذخیره سـازی اطلاعات بر مبنـای فناوری ابری و پلتفرم های به اشتراک گذاری فایل خطرات گسـترده ای را از نظر امنیتی برای صاحبان مشاغل به ارمغان می آورند.

این پلاتفرم هـا و خدمات علیرغم مزایایی که دارند باعث می شـوند شـرکت های امنیتـی در صورت فقـدان یـا سـرقت اطلاعـات از این طریـق دچار خسـاراتی غیرقابـل جبران شـوند. شـرکت امنیتی سـوفوس در گزارش تازه خود که بـه همین منظور منتشر کرده، به کاربران این خدمات هشدار داده که در زمان استفاده از سرویس هایی مانند Dropbox هشیار باشـند. زیرا این سـرویس ها اطلاعات را در اماکنی ناشـناخته و به شیوه های ذخیره می کنند که لزومـا قابل اعتماد نبوده و از نظـر امنیتی مورد تایید متخصصان نیستند.

اگـر چه بـا اسـتفاده از این شـیوه دیگـر لزومی به تخصیص منابع محلی برای ذخیره سـازی اطلاعات و صـرف هزینه برای این کار وجـود ندارد، اما قبل از این کار باید از ایمن سـازی سرویس های ذخیره سـازی اطلاعات به طور دقیق اطمینان کسب کرد تا از مشکلات بعدی جلوگیری شود. امروزه مهاجمان آنلایـن با حملـه به سـرویس های اینترنتـی ناایمن ابری موفق به سـرقت اطلاعات ارزشـمندی شده و خسـارات مادی و معنوی غیرقابل جبرانی به شرکت های تجاری وارد می کنند.

ویروس‌های جاسوسی

حدود ۲ سـال قبل بود که سـر و صدای عظیمی در

دنیای تکنولوژی به پا شد . ترس از وجود یک بدافزار فوق العاده پیشـرفته ، قدرتمند و بسیار خطرناک که برنامه ی هسته ای ایران را هدف قرار داده بود . یک نام در این بین شنیده میشد . STUXNET ؛ کرمی که لقب پیشرفته ترین ویروس جاسوسی تاریخ را از آن خود کرد و مقالات زیادی راجع به آن نوشته شد . بعد از مدتی مسـئولین برنامه های هسـته ای ایران خبر از حل مشـکل دادند . گذشت و گذشت تا روز یکم ماه سپتامبر سال ۲۰۱۱ که محققان ظاهرا بدافزار دیگـری را پیدا کرده بودنـد . اما خیلی در مورد آن توضیحاتی داده نشـد . اما ظاهـرا خبرهایی از دنیای امنیت به گوش میرسـد . اسـتاکس نت ۲ ، استاکس نت جدید ، نسـخه پیشـرفته تر استاکس نت ، فرزند اسـتاکس نت و نام هایی دیگر . همه این اسـامی به این دلیل انتخاب شده اند تا قدرت این بدافزار را بار دیگر به همگان یادآوری کنند .

طبقـه گفته هـای شـرکت امنیتی سـیمانتک ، این بدافزار اولین بار در سیسـتم هـای کامپیوتری اروپا مشاهده شده اسـت که کدهایی مشابه کدهای کرم مشـهور اسـتاکس نت دارد و میتواند پیش زمینه ای برای انجام حملات بزرگ کامپیوتری علیه سیسـتم های حیاتی زیر ساختی در آینده باشد .

برخلاف استاکس نت که سیستم های خاص "اسکادا" شرکت زیمنس را هدف قرار میداد و در واقع هدفش ایجاد اختلال در برنامه های هسته ای ایران بود ، این بدافزار جدید یک Backdoor (درب پشتی) روی سیستم نصب کرده و به جمع آوری اطلاعاتی مثل اسناد مربوط به طرح ها میپردازد . این اطلاعات میتواند در حملاتی که ممکن است در آینده رخ دهند مورد استفاده قرار بگیرد .

این بدافزار برای اجرا روی سیستم های ویندوزی نوشته شده است . متخصصان به دلیل ایجاد فایل هایی با پیشوند "~DQ." به آن لقب "دوکیو" (Duqu) را داده اند . این بدافزار همچنین یک دسترسی از راه دور ایجاد میکند . البته دوکیو با نصب دیگر "سارقان اطلاعاتی" (منظور ماژول هایی است که برای سرقت اطلاعات طراحی شده اند) میتواند کلیدهای فشرده شده را ثبت کرده و همچنین اطلاعات دیگر سیستم را نیز به سرقت ببرد .

یکی از مدیران شرکت سیمانتک گفته است که نمونه هایی از این بدافزار را در هفت یا هشت کمپانی اروپایی پیدا کرده اند . البته او مشخصات و موقعیت مکانی آن شرکت ها را فاش نکرده است . وی همچنین تاکید کرد که از هویت مشتریان محافظت خواهد شد .

به گفته سیمانتک این احتمال وجود دارد که سازندگان استاکس نت ، دوکیو را نوشته باشند یا افراد دیگری که به کد استاکس نت دسترسی داشته اند .

شباهت کدهای دوکیو با استاکس نت زیاد است ، اما با این حال در بحث انجام فعالیت های خرابکارانه ، کاملا با هم متفاوت هستند . استاکس نت سعی در ایجاد اختلال در سیستم های کنترل صنعتی داشت ، اما دوکیو هدف خود را ایجاد دسترسی از راه دور انتخاب کرده است . سازندگان دوکیو از این قابلیت به منظور جمع آوری اطلاعات و بهره گیری از آنها در حملات بعدی استفاده خواهند کرد .

هنوز مشخص نیست که دوکیو چگونه یک سیستم را آلوده میکند . جالب اینجاست که این بدافزار از هیچگونه آسیب پذیری هم استفاده نمیکند . وی همچنین ادامه میدهد که ممکن است این آلودگی از طریق روش های مهندسی اجتماعی صورت بگیرد . مثل باز کردن یک ایمیل حاوی ضمیمه ی آلوده و یا کلیک کردن بروی یک لینک مخرب که باعث آلودگی سیستم میشود . وی همچنین ابراز امیدواری کرد که در روزهای آینده بتوانند جزئیات بیشتری در مورد دوکیو بدست بیاورند .

طبق گفته های شرکت سیمانتک ، دو نوع مختلف از دوکیو کشف شده است . یکی از آنها در تاریخ ۱ سپتامبر سال جاری کشف شد . محققان میگویند یکی از انواع دوکیو از گواهی دیجیتال معتبر مربوط به یک شرکت تایوانی استفاده میکند . چیزی که در استاکس نت هم به چشم میخورد و از گواهی های به سرقت رفته ی شرکت Realtek استفاده شده بود .

دوکیو همچنین از یک سرور دستور-کنترل برای آپلود و دانلود اطلاعات مورد نظرش که به نظر میرسد چیزی مثل فایل های JPG باشند ، استفاده میکند . البته این اطلاعات به صورت رمزنگاری شده ارسال و دریافت میشوند . دوکیو طوری برنامه نویسی شده است که پس از ۳۶ روز به صورت اتوماتیک خود را از روی سیستم حذف میکند . اطلاعات فنی دیگری در مورد دوکیو که توسط سیمانتک و یک آزمایشگاه ناشناخته (به احتمال زیاد آزمایشگاه امنیتی CrySyS) دیگر جمع آوری

شـده اسـت را میتوانید در این فایل PDF مشاهده کنید .

در همین حال شـرکت مک آفی هم بیکار ننشسته و پسـتی راجع به دوکیو در بـلاگ خود میگذارد . در این پسـت آمده است که دوکیو به منظور جاسوسی و همچنین انجام حملات هدفمند علیه وبسایت های ارائه دهنده گواهی های دیجیتال طراحی شده است . تصویری نیز توسط شرکت سیمانتک تهیه شده است کـه در آن اسـتاکس نت و دوکیو را با هم مقایسـه کرده اند .

Feature	Stuxnet	Duqu
Modular malware	✓	✓
Kernel driver based rootkit	✓	✓ very similar
Valid digital signature on driver	Realtek, JMicron	XXXXX
Injection based on A/V list	✓	✓ seems based on Stux.
Imports based on checksum	✓	✓ different alg.
3 Config files, all encrypted, etc.	✓	✓ almost the same
Keylogger module	?	✓
PLC functionality	✓	× (different goal)
Infection through local shares	✓	No proof, but seems so
Exploits	✓	?
0-day exploits	✓	?
DLL injection to system processes	✓	✓
DLL with modules as resources	✓ (many)	✓ (one)
RPC communication	✓	✓
RPC control in LAN	✓	?
RPC Based C&C	✓	?
Port 80/443, TLS based C&C	?	✓
Special "magic" keys, e.g. 790522, AE	✓	✓ lots of similar
Virtual file based access to modules	✓	✓
Usage of LZO lib	?	✓ multiple
Visual C++ payload	✓	✓
UPX compressed payload,	✓	✓
Careful error handling	✓	✓
Deactivation timer	✓	✓
Initial Delay	? Some	✓ 15 mins
Configurable starting in safe mode/dbg	✓	✓ (exactly same mech.)

```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
        LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
        return nil
        end
```

فلیم بوده است. ویتالی کاملیوک، کارشناس ارشد بدافزار در شرکت نرم افزارهای امنیتی کاسپرسکی کاشف فلیم است. وی به عنوان عضوی در یک گروه کارشناسی به دنبال کد بدافزاری رایانه ای بود که گفته می شد اطلاعات رایانه های داخل ایران را از بین برده بود.

۲- ویژگی های فلیم چیست؟

۲-۱- کد فلیم از ویروس استاکس نت خیلی بزرگتر است. کد فلیم ۲۰ مگابایت حجم دارد در حالی که کد استاکس نت فقط ۵۰۰ کیلو بایت بود. بنابراین، فلیم بزرگترین بدافزاری است که تا کنون مشاهده شده است.

۲-۲- زبان برنامه نویسی استفاده شده برای نوشتن این بدافزار لوا نام دارد که تا کنون در هیچ بدافزاری استفاده نشده بود. شرکت کسپراسکی می گوید از این زبان برنامه نویسی بیشتر در نوشتن بازی های رایانه ای استفاده می شود زیرا می توان دائما کدهای جدید به آن اضافه کرد و آن را ارتقا داد. استفاده از زبان برنامه نویسی لوا نشان می دهد طراح این ویروس در نظر دارد این ویروس را دائما رشد داده و تقویت کند.

۲-۳- فلیم از مارس ۲۰۱۰ فعال بوده است.

۳- فلیم چگونه عمل می کند؟

۳-۱- بر خلاف استاکس نت فقط برای جاسوسی و جمع آوری اطلاعات طراحی شده است. این ویروس تواناییهایی بیش از این دارد. این ویروس از صفحه نمایشگر رایانه عکس می گیرد و میکروفون رایانه را روشن می کند تا مکالمات محیط ضبط شود. بعدا اطلاعات گردآوری شده به منبع منتشر کننده ویروس منتقل می شود.

آقای میکو هیپونن مدیر عامل شرکت امنیتی F-Secure معتقد است که این گواهی های دیجیتال جعلی از شرکت تایوانی C-Media به سرقت رفته اند . وی همچنین در پاسخ به اینکه دوکیو توسط آمریکا و یا اسرائیل و به منظور هدف قرار دادن ایران نوشته شده است ، اظهار بی اطلاعی کرد .

ویروس شعله خطرناک ترین جاسوسی غرب علیه ایران

اما چندی پیش کارشناسان از انتشار بدافزار به شدت پیچیده جدیدی خبر داده اند که کشورهای خاورمیانه و به خصوص ایران را هدف قرار داده است. محققان چندین شرکت امنیتی غربی و شرکت های تحقیقاتی هم شناسایی این بدافزار به نام Flamer را تایید کرده و از آغاز بررسی ها و تجزیه و تحلیل آن خبر داده اند.

متخصصان مرکز ماهر در ایران Flamer را عامل سرقت حجم گسترده ای از اطلاعات در هفته های اخیر توصیف کرده و می گویند این بدافزار به دنبال انتشار بدافزارهای مشابهی مانند استاکس نت و دیوکو عرضه شده است.

- فلیم چگونه کشف شد؟

ظاهرا شرکت نرم افزاری کسپراسکی در روسیه کاشف

۳-۲- تیم مارر و دیوید وینستاین، روز ۱۰ خرداد در فارین پالیسی نوشتند: «بنا بر اعلام کاسپرسکی بدافزارهای دیگری هم وجود دارند که می توانند صدا را ضبط کنند اما نکته اصلی در مورد فلیم کامل بودن آن است، یعنی توانایی آن برای به سرقت بردن اطلاعات از شیوه های بسیار متنوع».

۳-۳- مارک کلایتون روز ۱۰ خرداد درباره شیوه عمل فلیم در کریستین ساینس مانیتور نوشته است: «کارشناسان می گویند به علت بزرگی و پیچیدگی ویروس فلیم کشف کامل برنامه آن و این که چه کارهایی انجام داده است سال ها زمان می برد. با این حال، از یافته هایی که تاکنون بدست آمده مشخص شده است که ویروس فلیم می تواند از طریق یو اس بی، بلوتوث یا دیگر ابزارها در یک شبکه گسترش پیدا کند. در دستگاه های آلوده، این ویروس می تواند برای اجرا شدن منتظر نرم افزارهای خاصی شود و سپس به تصاویر دست یابد، میکروفون های داخلی را برای ضبط مکالمات روشن کرده و ئی میل ها و چت ها را رهگیری کند. این ویروس می تواند اطلاعات بدست آمده را بسته بندی و رمزگذاری کرده و آنها را برای رایانه های مشخصی در سراسر جهان بفرستد».

۳-۴- به زبان فنی می توان گفت ویروس فلیم مانند یک «کرم» عمل می کند به این صورت که بدون نیاز به دخالت انسان گسترش می یابد و برای رساندن اطلاعات ربوده شده به دست گردانندگانش کانال هایی را برای خود باز می کند.

۴- چه کسی فلیم را ساخته است؟

۴-۱- شرکت کاسپرسکی عقیده دارد این ویروس با توجه به پیچیدگی و مکان جغرافیایی رایانه های آلوده احتمال ساخته یک ملت-دولت است و نه یک شرکت و موسسه خصوصی یا گروهی از هکرها.

۴-۲- موشه یعلون، معاون رئیس کابینه اسرائیل و وزیر امور راهبردی اسرائیل روز سه شنبه ۸ خرداد تقریبا به صراحت تایید می کند که اسراییل این ویروس را ساخته است. وی به رادیو نظامی اسرائیل گفته است: «به نظر منطقی می آید که فرض کنیم هر کس که تهدید ایران را تهدیدی جدی تلقی می کند، تدابیر مختلف، که شامل اینها (حملات سایبری با ویروس فلیم) می شود را برای صدمه زدن به آن (ایران) اتخاذ خواهد کرد. اسرائیل از این نعمت برخوردار بوده که دارای فناوری پیشرفته (رایانه ای) بوده است. این ابزار (فناوری پیشرفته) که ما (اسرائیل) به آن افتخار می کنیم باب انواع فرصت ها را بر روی ما می گشاید.

۴-۳- مارک کلایتون روز ۱۰ خرداد در کریستین ساینس مانیتور می نویسد: «کارشناسان شرکت کاسپراسکای معتقدند به احتمال زیاد یک کشور این ویروس را ساخته است. آنها معتقدند این ویروس نه نتها بسیار پیچیده است بلکه کار اصلی آن جاسوسی اطلاعات است. یکی از شرکای اتحادیه بین المللی مخابرات نیز که در این تحقیقات همکاری می کند با این ارزیابی موافق است. شرکت کرایسیس لب (CrySyS Lab) مستقر در دانشگاه فن آوری و اقتصاد در بوداپست مجارستان گزارشی از بررسی های خود از ویروس فلیم منتشر کرد. در گزارش این شرکت آمده است: «نتایج بررسی های فنی ما این فرضیه را تایید می کند که سرویس دولتی یک کشور با بودجه و تلاش قابل توجهی این ویروس را ساخته است».

چشم انداز آینده

اگرچه تلاش‌های غرب برای جاسوسی از مردم و به ویژه ایران به طور روزافزون ابعاد تازه‌ای به خود می گیرد اما می‌توان با اتخاذ تدابیری این حفره‌های امنیتی را مسدود کرد. اگرچه امنیت هرگز ۱۰۰ درصدی نخواهد بود اما با راهبردهای کارشناسی شده و آموزش می‌توان از وقوع جاسوسی و حملات دیجیتالی و سایبری جلوگیری کرد. استفاده از نرم افزارهای امنیتی جدید و به روز، آموزش همگانی و اطلاع رسانی در مورد خطرات و تهدیدهای موجود در اینترنت و ....، جلوگیری از مهندسی اجتماعی برای انجام عملیات جاسوسی سایبری، تشکیل پلیس اینترنتی و فضای سایبر و به کارگیری از اینترنت ملی بهترین می‌توانند از بهترین رویکردها برای مقابله با جاسوسی عصر نوین در حال حاضر باشند.

نظرات، انتقادات و پیشنهادات
خود را برای دیدبان ارسال کنید:
didban@mail.com

www.didban.ir

Designer : Kamal Zakeri