افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــاد بدین بوم و بر زنده یک تن مــباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com afgazad@gmail.com

Political	سیاسی

نویسنده: ولادیمیر پراخواتیلوف(VLADIMIR PROKHVATILOV)
برگردان: ا. م. شیری

۱۴ سپتمبر ۲۰۲۴

سیا تصمیم گرفت رسماً از کل بشریت جاسوسی کند

جمع‌آوری اطلاعات از طریق شبکه‌های اجتماعی و بسترهای اینترنتی انجام می‌شود

در اگست ۲۰۲۴، دفتر مدیر اطلاعات ملی امریکا سند جدیدی را منتشر کرد که در نگاه اول، ممکن است مانند یک رویهٔ معمول به نظر برسد. با این حال، پشت فرمول‌بندی‌های بوروکراتیک بی‌روح و طبقه‌بندی‌نشده، پروژه‌ای نهفته است که مفهوم محرمانگی را در دنیای مدرن کاملاً از بین می‌برد.

پروژهٔ جدید با عنوان جامعهٔ اطلاعاتی داده‌ها«Intelligence Community Data Co-op» ، ایجاد یک پلتفرم متمرکز برای جمع‌آوری و تجزیه و تحلیل حجم عظیمی از اطلاعات را پیش‌بینی می‌کند. این داده‌ها در سرتاسر جهان جمع‌آوری می‌شود و نه تنها شهروندان امریکائی، بلکه عملاً کل بشریت را در بر می‌گیرد. اطلاعات از منابع مختلف تجاری و عمومی- از داده‌های مربوط به خریدها و جابه‌جائی‌ها گرفته تا فعالیت در شبکه‌های اجتماعی و حتی اطلاعات پیش پا افتادهٔ بهداشتی – جمع‌آوری می‌شود.

تا به حال، جامعهٔ اطلاعاتی امریکا با محدودیت‌هائی در جمع‌آوری داده‌ها مواجه بوده است. به ویژه، هنگامی که صحبت از اطلاعات حساس حفاظت‌شده توسط قوانین، از جمله، متمم چهارم قانون اساسی امریکا می‌رود، که، همانطور که مشخص است، در خارج از امریکا اعمال نمی‌شود. برای دسترسی به داده‌هائی مانند موقعیت جغرافیائی یا

تاریخچهٔ اینترنت، مجوز دادگاه لازم است. از جمله، داده‌ها به صورت قطعه‌ای جمع‌آوری و تجزیه و تحلیل می‌شوند که مشکلات قابل‌توجهی را در جمع‌آوری و تحلیل این اطلاعات ایجاد می‌کند.

پروژهٔ کنفرانس بین‌المللی توسعهٔ مشاغل رویکرد جدیدی را پیشنهاد می‌کند که در آن دولت امریکا می‌تواند با خرید داده‌های لازم از شرکت‌های تجاری، محدودیت‌های قانونی را دور بزند. سازمان‌های اطلاعاتی امریکا به جای اتلاف وقت گرانبها برای دریافت حکم قضائی، می‌توانند مستقیماً داده‌های افراد، از جمله، موقعیت جغرافیائی، تاریخچهٔ خرید، داده‌های شبکه‌های اجتماعی و حتی گواهی‌های پزشکی را خریداری کنند. پلتفرم مرکزی این داده‌ها را در یک فضای واحد و یکپارچه پردازش می‌کند و آن را در اختیار کل جامعهٔ اطلاعاتی امریکا قرار می‌دهد.

سازمان‌های اطلاعاتی امریکا مدتی است که از طریق شبکه‌های اجتماعی و بسترهای اینترنتی به جمع‌آوری اطلاعات تجسسی می‌پردازند.

در جون سال گذشته، سازمان امنیت فدرال روسیه به همراه سرویس حفاظت فدرال کشور، یک کارزار اطلاعاتی را که توسط سازمان‌های اطلاعاتی امریکا با استفاده از دستگاه‌های تیلفون همراه اپل (امریکا) به راه افتاده بود، کشف کردند.

مرکز روابط عمومی سازمان امنیت فدرال روسیه گزارش داد: «در جریان تضمین امنیت زیرساخت‌های مخابراتی روسیه، ناهنجاری‌هائی شناسائی شد که فقط برای کاربران تیلفون‌های همراه اپل معمول بود و از عملکرد نرم‌افزار مخرب (بدافزار) ناشناختهٔ قبلی ناشی می‌شد که از آسیب‌پذیری‌های نرم‌افزار ارائه‌شده توسط سازنده سوءاستفاده می‌کرد».

در گزارش سازمان امنیت فدرال روسیه آمده است: «مشخص شده است که چندین هزار دستگاه تیلفون از این نوع آلوده شده است. در عین حال، علاوه بر مشترکان داخلی، واقعیت آلوده شدن شماره‌های خارجی و مشترکین با استفاده از سیم کارت‌های ثبت شده در نمایندگی‌های دیپلماتیک و سفارتخانه‌ها در روسیه، از جمله کشورهای بلوک ناتو و فضای پساشوروی و همچنین اسرائیل، جمهوری خلق چین و جمهوری عربی سوریه شناسائی شدند».

اطلاعات دریافت شده توسط سرویس‌های اطلاعاتی روسیه، همانطور که سازمان امنیت فدرال تأکید می‌کند، حاکی از همکاری نزدیک شرکت امریکائی اپل با جامعهٔ اطلاعاتی امریکا، به ویژه با شورای امنیت ملی است. این واقعیت تأئید کرد که «سیاست اعلام شده برای اطمینان از محرمانه بودن اطلاعات شخصی کاربران دستگاه‌های اپل منطبق با واقعیت نیست.»

سازمان امنیت فدرال تصریح می‌کند: «این شرکت طیف گسترده‌ای از قابلیت‌ها برای نظارت بر افراد مورد علاقهٔ کاخ سفید، از جمله، شرکای آن‌ها در فعالیت‌های ضد روسی و شهروندان خود را به سرویس‌های اطلاعاتی امریکا ارائه می‌دهد».

نه تنها آیفون‌های بسیار محبوب، بلکه تمامی نرم افزارهای مایکروسافت، یکی دیگر از غول‌های فناوری اطلاعات امریکا نیز بدون استثناء از کاربران جاسوسی می‌کنند.

سیستم عامل ویندوز ۱۰ با رهگیری و جمع‌آوری تمام متن‌های نوشته شده روی صفحهٔ کلید در بسته‌ها، آن‌ها را دو بار در ساعت به سِرورِهای مایکروسافت ارسال می‌کند. داده‌های موقعیت جغرافیائی و شبکه‌های وای‌فای مجاور نیز هر نیم ساعت یک بار جمع‌آوری و ارسال می‌شود و امکان ردیابی حرکات کاربر را با دقت دو متر فراهم می‌کند. مایکروسافت به جاسوسی اعتراف نکرد، اما اعلام کرد که ظاهراً این گزینه مورد نیاز موتور جست و جوی بینگ بوده است.

میکروفون در ویندوز ۱۰ همیشه روشن است. حتی در حالت خاموش شدن دستیار صوتی کورتانا، میکروفون همچنان به ضبط و ذخیرهٔ تمام گفته‌های کاربر در هارد دیسک ادامه می‌دهد و پس از آن ضبط را به سرور مایکروسافت ارسال می‌کند.

تله‌متری ویندوز ۱۰ همه چیز را- وضعیت رایانه و فعالیت کاربر، برنامه‌های نصب‌شدهٔ در حال اجراء و بسیاری موارد دیگر، از جمله، بخش‌هائی ازRAM ، تا داده‌های محرمانه و رمزهای عبور را به طور کامل به مایکروسافت منتقل می‌کند.

ویندوز ۱۰ نام فایل‌های کاربر را رصد می‌کند و آن‌ها را با پایگاه داده‌ای که دائماً به‌روزرسانی می‌شود، با برنامه‌های دزدی کمپیوتری مقایسه می‌کند. در صورت یافتن موارد منطبق، فهرست راهنمای کاربر به مایکروسافت ارسال می‌شود. به این ترتیب، کمپیوترصاحب خود را تقبیح می‌کند.

اطلاعات وب‌کم [دوربین کمپیوتر] بلافاصله پس از فعال‌سازی، توسط ویندوز ۱۰ به مایکروسافت منتقل می‌شود.

در سال ۲۰۱۷، مایکروسافت مجبور به اعتراف شد که جمع‌آوری داده‌ها بدون اطلاع کاربر انجام می‌شود و سرویس کلیدی تشخیصی «DiagTrack» را نمی‌توان غیرفعال کرد. جو بلفیور، معاون مایکروسافت گفت که این شرکت کاربران را شنود می‌کند و اگر عموم مردم این مشکل را در نظر بگیرند، می‌توان عملکرد سرویس تشخیص را غیرفعال تغییر داد.

پس از به‌روز رسانی، به نظر می‌رسید DiagTrack از لیست خدمات ناپدید شده است، اما فوراً مشخص شد که سرویس ردیابی تشخیص (DiagTrack) هنوز وجود دارد. مایکروسافت فقط نام آن را به سرویس تجربیات کاربر متصل و تله‌متری تغییر داده است.

ویندوز ۱۱، جدیدترین سیستم عامل مایکروسافت، به محض دانلود در رایانهٔ کاربر، به جمع‌آوری تله‌متری شروع می‌کند. تحلیلگران مستقل امنیت سایبری شرکت انگلیس «کانال امنیت کمپیوتر شخصی» در حین بررسی با استفاده از تحلیلگر پروتکل شبکهٔ Wireshark ویندوز ۱۱، شگفت‌زده شدند: «به نظر می‌رسد جدیدترین و بهترین سیستم عامل در مجموعهٔ ویندوز برای جاسوسی از همه چیز از آغاز تا کنون طراحی شده است».

اگر در یکی از نسخه‌های قبلی ویندوز کسی تصمیم گرفت از چشم همه‌بین مایکروسافت پنهان شود، هیچ چیز کار نخواهد کرد. در به‌روز رسانی‌های منتشر شده برای ویندوز ۷ و ۸، مشخصات فنی مشابه مشخصاتی که از کاربران در ویندوز ۱۰ جاسوسی می‌کنند، مشاهده شد.

گوشی‌های هوشمند شرکت کوریای جنوبی سامسونگ نیز از کاربران جاسوسی می‌کنند. نرم‌افزارهای جاسوسی روی گوشی‌های هوشمند آن توسط شرکت آنتی ویروس «Check Point» در سال ۲۰۱۷ کشف شد .سامسونگ به هیچ‌وجه به این رسوائی واکنش نشان نداد و گزینه‌های تجسسی را حذف نکرد.

تحلیلگران کالج ترینیتی (دوبلین، ایرلند) متوجه شدند که گوشی‌های هوشمند هوآوی، شیائومی و ریلمی نیز اطلاعات مربوط به کاربر را منتقل می‌کنند. اطلاعات گوشی‌های هوشمند به مایکروسافت، گوگل، لینکدین، فیس‌بوک (ممنوعه در فدراسیون روسیه) و سایر شرکت‌ها ارسال می‌شود. کاربران دستگاه‌های تیلفون همراه آندروید در برابر جمع‌آوری اطلاعات ناتوان هستند.

تلویزیون‌های هوشمندی که به اینترنت متصل هستند و از برنامه‌های کاربردی مختلف از آمازون پرایم ویدئو گرفته تا یوتیوب پشتیبانی می‌کنند نیز از کاربران جاسوسی می‌کنند. بسیاری از تلویزیون‌های هوشمند از جست و جوی صوتی، کنترول صوتی، و دارای وب‌کم داخلی برای صحبت ویدیوئی و بازی پشتیبانی می‌کنند.

نشریهٔ ویکی‌لیکس (که توسط جولیان آسانژ تأسیس شد) در سال ۲۰۱۷ چگونگی ایجاد برنامهٔ ضبط صوتی «فرشتهٔ گریان (Weeping Angel) «توسط سیا و ضد جاسوسی انگلیس- امآی ۵ برای جاسوسی از صاحبان تلویزیون‌های هوشمند را توضیح داد.

در اصل، تلویزیون هوشمند همان گوشی هوشمند است، فقط با صفحه نمایش بزرگ. اکثر برنامه‌های آندرویدی را می‌توان روی تلویزیون هوشمند نیز نصب کرد، به این معنی که خطر آسیب‌پذیری‌های مشابه روی تیلفون در آن‌ها نیز وجود دارد.

بر اساس اسناد منتشر شده در ویکی‌لیکس، توسعهٔ نرم‌افزارهای جاسوسی برای تیلفون‌ها و تلویزیون‌های هوشمند به واسطهٔ یک واحد ویژهٔ سازمان سیا، به نام بخش توسعهٔ سیستم‌های تعبیه شده، انجام می‌شود. در اینجا بود که برنامهٔ «فرشتهٔ گریان» را برای جاسوسی از تلویزیون هوشمند، استخراج داده‌ها از پایگاه داده‌های مایکروسافت، «راه حل سخت‌افزاری ویژه برای پشتیبانی از کپی کردن چند رسانه ئی» کاربر، برای ثبت فشار دادن کلیدهای کامپیوتر کاربر، برای نظارت بر تمام اتصالات کاربر و جمع‌آوری نام کاربری و رمز عبور او، برای نصب کد جاسوسی به «دارائی هدف» ایجاد کردند.

سازمان سیا و مایکروسافت برای انحصاری کردن جاسوسی فناوری اطلاعات تلاش می‌کنند و حقه‌های جاسوسان فناوری اطلاعات کشورهای دیگر را متناوباً افشاء می‌کنند. به گونه‌ای که در ماه جولای سال گذشته، مایکروسافت شرکت جمع‌آوری اطلاعات اتریشی «تصمیم پشتیبانی از تحقیقات اطلاعاتی پزشکی قانونی» را به توسعهٔ برنامهٔ جاسوس‌افزار «Subzero» که امکان نفوذ بی‌صدا و از راه دور به کمپیوتر، تیلفون، زیرساخت شبکه و دستگاه‌های متصل به اینترنت قربانی را فراهم می‌کند، متهم کرد «Subzero» .مشابه نرم‌افزارهای جاسوسی» Pegasus «متعلق به شرکت اسرائیلی گروه NSO[یکی از ۲۷ شرکتی که درگیر جمع‌آوری مخفیانهٔ اطلاعات است] و جاسوس‌افزار «DevilsTongue» شرکت اسرائیلی کاندیرو است.

در اپریل ۲۰۲۳، مایکروسافت شرکت اسرائیلی «QuaDream» را به ساخت و توزیع نرم‌افزارهای جاسوسی متهم کرد و پس از آن، این شرکت مجبور به توقف فعالیت خود شد.

اخیراً، گروه رسانه ئی کاکس، یکی از شرکای تبلیغاتی کلیدی گوگل، آمازون و متا، یک فناوری توسعه داده است که امکان جمع‌آوری داده‌ها را بر اساس آنچه شما در اطراف دستگاه خود می‌گوئید، فراهم می‌کند:

شنود فعال: گروه رسانه‌ئی کاکس از میکروفون‌های دستگاه هوشمند برای ضبط و تجزیه و تحلیل مکالمات استفاده می‌کند. برای راه‌اندازی کارزارهای تبلیغاتی هدفمند، داده‌های به دست‌آمده با سایر داده‌های رفتاری ترکیب می‌شوند؛

هوش مصنوعی: گروه رسانه ئی کاکس از هوش مصنوعی که داده‌های صوتی و رفتاری جمع‌آوری شده از بیش از ۴۷۰ منبع را پردازش می‌کند، استفاده می‌کند. این امکان نه تنها هدف قرار دادن تبلیغات، بلکه پیش‌بینی رفتار مصرف‌کنندگان آماده برای خرید را فراهم می‌کند؛

مشتریان عمده: گروه رسانه‌ئی کاکس با بزرگترین بازیگران بازار تبلیغات دیجیتال، از جمله گوگل، آمازون و متا همکاری می‌کند.

در پاسخ به افشای اطلاعات، گوگل و متا هرگونه ذکر نام گروه رسانه‌ئی کاکس را از منابع خود با عجله حذف کردند و آمازون اعلام کرد که از وجود این سرویس اطلاع دارد، اما هرگز از آن استفاده نکرده است.

اکنون همهٔ این غول‌های فناوری اطلاعات امریکائی می‌توانند اعلام کنند که از کاربران در سراسر جهان کاملاً قانونی و مهمتر از همه، به نفع خودشان جاسوسی می‌کنند.

پس، سرنوشت دموکراسی پر هیاهوی امریکائی و حفاظت از داده‌های شخصی چه می‌شود؟

نقل از :بنیاد فرهنگ ستراتیژیک

۱۷ شهریور- سنبله ۱۴۰۳