ابزار جاسوسی دیداری

جاسوس‌های بین‌المللی تنها افرادی نیستند که به زیر نظر گرفتن رفتار اهدافشان علاقه‌مندند؛ تولیدکنندگان محصولات مختلف هم نیازمند کسب اطلاعات در مورد خریداران محصولاتشان هستند. این احتمال می‌رود که در آینده نه‌چندان دور، کمپانی‌های تجاری از ابزار جاسوسی برای دستیابی به این اطلاعات استفاده کنند. کمپانی المکس (Almax) مانکن بیونیکی به نام آیسی (EyeSee) ساخته است که در داخل چشمش دوربین مخصوص قرار دارد. این مانکن که تفاوت ظاهری چندانی با سایر مانکن‌ها ندارد، از طریق دوربین جاسازی شده در سرش و برنامه تشخیص چهره، قادر است سن، جنسیت و نژاد خریداران محصولات را تشخیص داده و اطلاعات مربوط به آنها را جمع‌آوری کند. ایده آیسی شناسایی راحت‌تر مشتریان هدف محصولات خاص است.

! اشیای بزرگ یا سنگین و همچنین ظروف شیشه‌ای، چینی و سایر اشیای شکستنی و ظروف حاوی مواد خوراکی و شیمیایی را در قفسه‌های پایین کابینت و کمد قرار دهید.

از گربه‌های جاسوس تا تلویزیون‌های هوشمند

نگاهی به روش‌های نوین جاسوسی و تجربیات قدیمی سازمان‌های اطلاعاتی

اخیرا یک نهنگ سفید در آب‌های نروژ مشاهده شده که کمربندی روی پشتش داشته که گفته می‌شود مخصوص نصب دوربین‌های فیلمبرداری گوپرو بوده است؛ بر روی گیره این کمربند کلماتی به روسی نوشته شده بود و همین امر مقامات نروژی را بر آن داشت تا احتمال استفاده روس‌ها از این نهنگ برای جاسوسی را مطرح کنند. البته استفاده از حیوانات برای جاسوسی بین سرویس‌های اطلاعاتی جهان معمول است. علاوه بر این سازمان‌های جاسوسی بزرگ جهان از شیوه‌های نوین و پیچیده‌تر برای جاسوسی از رقیبان خود استفاده می‌کنند.

وب‌سایت «ویکی‌لیکس» در گسترده‌ترین افشاگری در طول تاریخ علیه فعالیت‌های سازمان سیا با انتشار بیش از ۸هزار سند محرمانه از فعالیت‌های این سازمان از جاسوسی‌های گسترده و شیوه‌های جمع‌آوری اطلاعات از مردم در تمام نقاط جهان پرده برداشته است.

در این هزاران سند شیوه‌های جاسوسی سازمان سیا و نرم‌افزارهای مورد استفاده این سازمان برای جاسوسی از رایانه‌ها و تلفن‌های همراه هوشمند و وسایل خانگی در تمام نقاط جهان و حتی استفاده از حیواناتی مانند گربه برای جاسوسی افشا شده است؛ براساس اطلاعات منتشرشده از این بزرگ‌ترین افشاگری از سازمان‌های جاسوسی آمریکا و انگلیس می‌توان به موارد زیر اشاره کرد.

سیستم عامل مایکروسافت

بیشتر بدافزارهای جاسوسی سازمان CIA در سیستم عامل ویندوز مایکروسافت عمل می‌کنند. بسیاری از آنها با بارگذاری از طریق دستگاه‌های قابل حمل همچون درایو USB قابل انتقال هستند. سازمان جاسوسی آمریکا از پروژه‌ای به نام «کانگوروی خونین» جهت فراری دادن بدافزارهایش از کشف بهره می‌برد که آن‌قدر قدرت دارد که به رایانه‌های تحت پوشش پروژه بسیار امن «ایر گپ» (Air Gap) هم نفوذ می‌کند.

نفوذ سیا به انواع گوشی‌های اندرویدی، اپل و همه نوع رایانه

سازمان جاسوسی آمریکا با همکاری همتای انگلیسی خود دست به ساخت بدافزاری به نام فرشته گریان Weeping Angel» زده که قادر است از تمام ابزارها و قطعات الکترونیکی که مردم استفاده می‌کنند، جاسوسی کند.

اگر قدرت این بدافزار آن‌گونه باشد که ویکی‌لیکس مدعی شده به راحتی قادر خواهد بود تمام وسایل الکترونیکی را از راه دور خاموش و روشن کند، هنگامی که این اتفاق رخ می‌دهد، حجم عظیمی از اطلاعات از قبیل مکان کاربر، پیام‌های فرستاده‌شده و حتی هر چیزی که توسط میکروفن دستگاه ضبط یا توسط دوربین دستگاه دیده‌شده باشد، در دسترس قرار می‌گیرد.

ناامنی تمام شبکه‌های اجتماعی

هنگامی که به راحتی می‌توان از خود دستگاه جاسوسی کرد، به تبع آن تمام پیام‌های ارسال‌شده در برنامه‌های اجتماعی نصب‌شده روی گوشی‌های هوشمند یا رایانه‌ها نیز قبل از رمزگذاری‌شدن و ارسال به فرد دیگری هک خواهند شد؛ بنا به گفته ویکی‌لیکس حتی اگر تمام اقدام‌های امنیتی و احتیاطی را رعایت کنیم، تمام فعالیت‌های ما در شبکه‌های اجتماعی در معرض دید ناظران پنهان است.

یکی از چشمگیرترین شیوه‌های جاسوسی که این اسناد افشاشده به تفصیل به آن پرداخته‌اند، برنامه «فرشته گریان» است که این امکان را در اختیار سازمان‌های جاسوسی و اطلاعاتی قرار می‌دهد که نرم‌افزارهای ویژه‌ای را بر تلویزیون‌های هوشمند قرار دهند که آنها را به وسایلی ضبط‌کننده پنهانی تبدیل کنند، به گونه‌ای که حتی هنگامی که به ظاهر خاموش هستند، قادرند تمام صداهای محیط اطراف خود را ضبط و به سرورهای اصلی منتقل کنند.

این برنامه تنها یکی از فناوری‌هایی است که توسط بخش ابزارهای نهفته «Embedded Devices Branch» ساخته شده؛ نهادی در سازمان سیا که بخش بیشتر اسناد منتشرشده به این نهاد اختصاص داده شده است.

ترورهای غیرقابل ردیابی با واژگونی خودرو

بخشی از این اسناد به ابزارهایی اشاره می‌کند که بکارگیری آنها بسیار خطرناک و وحشت‌آفرین است، به‌عنوان مثال در یکی از این اسناد توضیح داده شده که سازمان سیا می‌تواند از راه بسیار دور با هک کردن سیستم خودروها آنها را کنترل کند.

ویکی‌لیکس دراین‌باره می‌افزاید: «هدف از چنین کنترل‌هایی مشخص نیست، اما این امکان را در اختیار ماموران سازمان سیا قرار می‌دهد تا از این شیوه و با کنترل فرمان خودرو برای ترورهای غیرقابل ردیابی استفاده کند.»

گربه‌های جاسوس

در یکی از اسناد افشاشده تشریح‌شده که سازمان سیا با کار گذاشتن دستگاه‌های مختلف در بدن گربه‌ها از این حیوان برای جاسوسی از شوروی سابق استفاده می‌کرده است. بر اساس اعلام ویکی‌لیکس، سازمان سیا اقدام به نصب باتری در گوشت بدن گربه‌ها کرده، میکروفن‌هایی را در گوش این حیوان جاسازی کرده و سیم‌هایی را نیز در طول ستون‌فقراتش کار می‌گذارد، تا برای جاسوسی مناسب باشد.

پنهان‌کاری سازمان سیا از آسیب‌پذیری وسایل الکترونیکی

ویکی‌لیکس درباره انگیزه خود از افشای چنین اسنادی ضمن بیان این‌که قصد دارد به مباحث پیرامون قدرت سازمان‌های اطلاعاتی و جاسوسی جهان و میزان امنیت سایبری دامن بزند، می‌نویسد که سازمان سیا با پنهان‌کاری درباره آسیب‌پذیری وسایل الکترونیکی و گوشی‌های هوشمند از نقاط ضعف آنها در راستای مقاصد خود استفاده می‌کرده است، هنگامی که سازمان سیا می‌تواند از طریق وسایل الکترونیکی و گوشی‌ها و خودروهای هوشمند از تمام مردم جهان جاسوسی کند، هر هکر و دولتی می‌تواند این کار را انجام دهد.

۱۰ شیوه کلاسیک جاسوسی در دنیا

۱. نظارت مخفیانه: نظارت مخفیانه هنوز هم در عملیات جاسوسی به کار می‌رود. دوربین‌های مخفی در مکان‌های غیرمعمول، تجهیزات صوتی برای گوش دادن و ضبط مکالمات یا حتی یک پیپ دارای گیرنده که جاسوس با آن ارتباطات رادیویی اطراف را تشخیص می‌داد. در سال ۲۰۰۳، سازمان سیا از رباتی به نام «چارلی» خبر داد که به شکل ماهی ساخته شده است. ماموریت واقعی این دستگاه هرگز فاش نشد، اما کارشناسان معتقدند برای نمونه‌برداری و آزمایش آب اطراف تاسیسات هسته‌ای ساخته‌شده است. زمانی که این روبات رونمایی شد، آسوشیتدپرس با دانشمندی که روبات را دیده بود، مصاحبه کرد. او گفت این روبات آن‌قدر واقعی به نظر می‌رسد که ممکن است توسط دیگر موجودات دریا شکار شود. بسیاری از موسسات و نهادها برای نظارت بر محیط‌زیست از ماهی‌های روبات استفاده می‌کنند.

۲. تراشه‌های کوچک و قابل‌اطمینان: در طول دهه ۱۹۶۰، مدارهای یکپارچه (تراشه) تحولی عظیم محسوب می‌شدند. قبل از این تحول، فرستنده‌ها غیرقابل‌اعتماد نبودند و باتری‌های بزرگ می‌خواستند. این تراشه‌ها مصرف انرژی را کم کردند، صددرصد قابل‌اعتماد بودند و جای بسیار کمی می‌گرفتند، یعنی می‌شد هرجایی آنها را جاسازی کرد.

۳. جاسازی در اشیا (Dead Drop): در این روش جاسوس‌ها شیء یا پیامی را در وسیله‌ای جاسازی می‌کردند. سکه‌های توخالی وسیله مناسبی برای انتقال پیام بودند. با اینکه فضای داخل سکه بسیار کم بود، ماموروها می‌توانستند در آن یک مایکرودات (Microdot) قرار دهند. سیستم نوشتن میکرو در دهه‌های ۱۹۶۰ و ۱۹۷۰ توسط سیا اختراع شد. برای خواندن پیام‌های مخفی به یک ذره‌بین بسیار قوی نیاز بود. معروف‌ترین مورد جاسوسی با سکه تو خالی در سال ۱۹۵۳ اتفاق افتاد که یک جاسوس روسی اشتباهی سکه خود را به یک پسربچه روزنامه‌فروش داد. زمانی که سکه از دست پسر افتاد، پیام از آن بیرون آمد. چهار سال طول کشید تا افبی‌آی توانست دستورالعمل نوشته‌شده در آن را رمزگشایی کند.

۴. جک در جعبه: جاسوس‌ها باید مانند ارواح باشند؛ آرام و بی‌سروصدا. برای جلوگیری از شناسایی‌شدن، از نقشه‌هایی استفاده می‌کردند که روی ابریشم چاپ می‌شدند تا خش‌خش نکنند. در اواخر دهه ۱۹۳۰ و اواسط ۱۹۴۰، MI۹ از دکمه سرآستین‌هایی استفاده می‌کرد که قطب‌نما داشتند. یکی از

تاکتیک‌هایی که والاس وارنست از آن گفتند «جک در جعبه» نام داشت. این تکنیک ساده درواقع یک چمدان بود که آدمکی دقیقا شبیه به مامور در آن بود. ماموری که در خودرو تحت تعقیب بود، منتظر فرصتی مناسب می‌ماند و «جک در جعبه» را باز می‌کرد. با اینکه تنها پنج ثانیه از دید پلیس‌ها خارج می‌شدند، اما همین مدت برای جاسوس‌ها کافی بود تا در سایه‌ها ناپدید شوند.

۵. نوشته قابل اشتعال: اگر جاسوسی گیر بیفتد و نوشته‌ای مهم همراهش باشد، چه باید بکند؟ در طی جنگ جهانی دوم، جاسوس‌ها می‌توانستند نوشته‌ها و اطلاعات حساس را در دفترچه‌ای قابل اشتعال یادداشت کنند. در این دفترچه ورقی وجود داشت که توسط مدادی خاص مشتعل می‌شد. این ورق مانند نارنجک عمل می‌کرد، در عرض چند ثانیه مشتعل می‌شد و کل دفترچه را می‌سوزاند. پس از ورق‌های قابل اشتعال، ورق‌های قابل‌حل در آب اختراع شد، «ماموران می‌توانستند در هنگام خطر بلافاصله ورق را در توالت یا آب بیندازند.»

۶. مسموم کردن: در اواسط دهه ۱۹۶۰، بسیاری از مأموران مجبور می‌شدند نوشیدنی‌های دیگران را مسموم کنند. در کتاب «روش‌های حیله‌گری و فریبِ سازمان سیا» روش‌های زیادی برای ریختن پودر یا قرص در نوشیدنی‌ها بدون جلب‌توجه ذکرشده است. زنان جاسوس به دلیل داشتن دستکش و دستمال در این زمینه موفق‌تر بودند. هنگام روشن کردن سیگار

دیگران، از جعبه کبریت استفاده می‌شد تا قرص یا پودری را در نوشیدنی فرد موردنظر بریزند. تنها با یک تکان در مچ دست.

۷. پنهان در برابر دیدگان همه: «پنهان نگاری» درواقع پنهان کردن پیامی مخفی در انظار عمومی است. والاس از شعبده‌بازی به نام «جان مالهالند» گفت که در سال ۱۹۵۳ مشاور سازمان سیا شد و تاکتیک‌های جدیدی از این نوع به آنها آموخت. یکی از روش‌های ارتباط نحوه گره زدن بند کفش بود. نحوه بستن گره کفش می‌توانست پیام‌هایی مانند «دنبالم بیا» یا «شخص دیگری را آوردم» داشته باشد. این تاکتیک هنوز هم بسیار موثر است. گروه‌های تروریستی مانند القاعده از این روش استفاده می‌کنند. در یک مورد گزارش شد که القاعده اسنادی محرمانه را در یک فیلم ویدیویی مستهجن تعبیه کرده بود.

۸. گیرنده اسناد: امروزه جاسوس‌ها به‌راحتی از اسکنرهای کوچک استفاده می‌کنند. اما سالیان پیش، جاسوس‌ها از تکنیک‌های دیگری استفاده می‌کردند. موزه سازمان سیا از دوران جنگ جهانی دوم وسیله‌ای دارد که برای برداشت اطلاعات و بخشی از اسناد به کار می‌رفت. هنگامی که این وسیله را از میان فاصله بسته نشده یک پاکت نامه عبور می‌دادند، محل تماسش با کاغذ را پاره می‌کرد و قسمتی از مدرک را بدون این‌که کسی متوجه شود، بیرون می‌آورد. در این روش پاکت همچنان باز نشده باقی می‌ماند.

۹. دستگاه ارسال پیام‌های کدگذاری شده: مدت‌ها قبل از اختراع موبایل، بخش فنیِ سازمان سیا درحال اختراع یک سیستم ارتباطی با برد کم یا SRAC بود. با استفاده از این دستگاه دو مأمور می‌توانستند بدون حضور در یک مکان، باهم ارتباط برقرار کنند. در این دستگاه از اسم رمزهایی مانند DISCUS یا BUSTER استفاده می‌شد و شبیه یک ماشین‌حساب بزرگ بود. مأموران می‌توانستند با این دستگاه در فاصله ۳۰۰متری باهم ارتباط برقرار کنند. گاهی ممکن بود سیگنال قطع شود، اما بازهم در ابزار جاسوسی پیشرفت و تحولی بزرگ بود.

۱۰. دست‌به‌دست کردن سریع: این روش از دوران جنگ سرد وجود داشته است. این تکنیک اختراع شد تا در محیط‌های حساس که جاسوسان آمریکایی مدام تحت نظر بودند، بتوانند بسته‌ها و اسناد را به یکدیگر منتقل کنند. مأمور در ظاهر درحال انجام یک کار عادی است؛ اما درواقع دارد نقشه می‌کشد چیزی را به مأمور دیگری منتقل کند. این دست‌به‌دست کردن به‌سرعت در کوچه‌ها، راه‌پله‌مترو یا گوشه کنارهای خیابان‌ها صورت می‌گرفت.

۵ ابزار جاسوسی واقعی عصر مدرن

۶-ابزار جاسوسی دوران جنگ سرد

جاسوسی به اندازه تمدن بشریت قدمت دارد. در قوانین حمورابی و همچنین کتاب عهد عتیق یهودیان از جاسوسی به‌عنوان روشی برای چیره شدن بر دشمنان یاد شده است، اما پیشرفت‌های تکنولوژی باعث شکوفایی روش‌های ابتدایی جاسوسی شده.

۵-چتر مخصوص

در طول جنگ سرد که دوران طلای گجت‌های جاسوسی جیمز باندی بود، یک آدمکش بلغاری از چتری برای شلیک سم رایسین به یک پناهنده رژیم شوروی در لندن استفاده کرد؛ سم مهلکی که طرفداران سریال Breaking Bad با آن آشنا هستند. سازمان اطلاعات شوروی هم در آن دوران، ماتیکی با نام بوسه مرگ ساخته بود که یک گلوله را در فاصله نزدیک شلیک می‌کرد؛ گجت‌هایی مرگبار که تنها نوک کوه یخ ابزار جاسوسی دوران جنگ سرد هستند.

۴-گربه‌های جاسوس و تکنیک‌های فکرخوانی

در طول جنگ سرد ایده‌های عجیبی برای ساخت ابزار جاسوسی ارایه شد. برخلاف سیستم طبیعی گوش حیوانات که نویزهای پس‌زمینه را حذف کرده و قابلیت تمرکز بر یک صدا را دارد، دستگاه‌های استراق سمع قدیمی تمامی صداها را با هم ضبط می‌کردند و کیفیت بسیار پایینی داشتند. به همین دلیل در بین دهه‌های ۵۰ و ۶۰ میلادی، ایده‌ای در سازمان اطلاعاتی آمریکا مطرح شد که از گوش حیوانات برای بهبود کیفیت صداهای ضبط شده توسط دستگاه‌های استراق سمع، استفاده شود. جاسوسان در گوش گربه‌ها میکروفن جاسازی کرده، در جمجمه این حیوانات فرستنده رادیویی می‌گذاشتند و در شکم آنها باتری دستگاه ضبط صدا را قرار می‌دادند. از دم گربه‌ها هم به‌عنوان آنتن استفاده می‌شد. سپس ساعت‌های زیادی صرف تعلیم این حیوانات می‌شد تا برای جاسوسی آماده شوند؛ اما در هنگام عملیات، غرایز حیوانی بر گربه‌ها غلبه می‌کرد و کل عملیات خراب می‌شد. هاوتون در همین رابطه می‌گوید:

آموزش گربه‌ها بازدهی بالایی ندارد. گاهی وقت‌ها این گربه‌های میلیون دلاری در حین عملیات به دنبال غذا سر گردان می‌شدند و گاهی هم در خیابان با ماشین تصادف می‌کردند و می‌مردند.

همچنین، سازمان سیا برای دهه‌ها مبالغ زیادی خرج پروژه‌ای به نام استارگیت کرد که در آن از تکنیک‌های ذهن خوانی و تله پاتی برای دسترسی به اطلاعات محرمانه استفاده می‌شد. حتی در بعضی موارد، مخدرهایی مانند LSD برای کنترل ذهن به کار می‌رفتند؛ اما پس از مدتی این پروژه‌ها با شکست مواجه شدند.

۳-میکروفن تصویری

برخلاف تصور عمومی، تنها سازمان‌های اطلاعاتی نیستند که بر روی ابزار جاسوسی کار می‌کنند؛ مدتی پیش در دانشگاهی در تگزاس، دانشمندان بر روی روشی برای بازسازی مکالمات از طریق تصاویر کار کردند. در کنفرانس ۲۰۱۴ SIGGRAPH، این ایده مطرح شد که می‌توان با ضبط تصاویر محیطی که در آن مکالمه‌ای صورت گرفته، کلمات ردوبدل شده را بازسازی کرد.

از آنجایی که از اصوات به صورت موج در محیط منتشر می‌شوند، وقتی از محیطی که در آن صدا وجود دارد تصویری گرفته شود، امواج صوتی که با چشم غیرمسلح قابل رویت نیستند در داخل تصاویر ضبط می‌شوند. این تصاویر پس از آنالیز، مکالمات صورت گرفته را آشکار می‌کند. با استفاده از این ابزار جاسوسی، استراق سمع بدون نیاز به میکروفن هم امکان‌پذیر است.

۲-هک ایمپلنت‌های پزشکی

هک کردن ایمپلنت‌های پزشکی فقط در سریال Homeland امکان‌پذیر نیست؛ تمامی دستگاه‌های پزشکی مانند پمپ‌های انسولین، ایمپلنت‌های الکتروشوک و ضربان‌سازهای قلبی که به‌صورت وایرلس قابل کنترل‌اند و با باتری استفاده می‌کنند، هم قابل هک کردن هستند. در کنفرانس بلک هت سکیوریتی (Black Hat Security) سال ۲۰۱۱ در لاس وگاس، هکری به نام جروم رد کلیف (Jerome Radcliffe) نشان داد که پمپ انسولین مورد استفاده خودش را هک کرده است. چندسال گذشته هم ضربات سازهای وایرلس بیماران قلبی قابل هک شناخته شد. با وجود این که تاکنون پرونده‌ای در مورد استفاده غیرقانونی از ایمپلنت‌های پزشکی برای اهداف جاسوسی ثبت نشده، دیوان محاسبات آمریکا، سازمان غذا و دارو را ملزم کرده است که کمپانی‌های سازنده چنین ایمپلنت‌هایی را مجبور به برطرف کردن ضعف‌های موجود در محصولاتشان کند.

۱-کدهای غیرقابل‌رمزگشایی

رمزگذاری امن اطلاعات از اهداف اصلی سازمان‌های جاسوسی است؛ کدهایی که توسط هیچ هکری قابل شکستن نباشند. در همین رابطه برخی بر این باورند که رمزگذاری کوانتمی راه‌حل دستیابی به این هدف است. این روش با استفاده از قوانین فیزیک ذرات بنیادی، پیام‌ها را تنها برای گیرنده آنها قابل رمزگشایی می‌کند. رمزگذاری کوانتمی هنوز در مراحل ابتدایی توسعه قرار دارد، اما در آینده نزدیک با عملی شدن آن، دولت‌ها و سازمان‌های جاسوسی سرمایه‌گذاری‌های عظیمی برای استفاده از این تکنولوژی انجام خواهند داد. به اعتقاد هاوتون، نخستین کشوری که از این ابزار جاسوسی برای رسیدن به اهدافش استفاده کند، بسیار جلوتر از سایر کشورها خواهد بود.