قسمت دوم

مهندسان ضد اجتماع

چگونه دو شیاد با فروش نرم‌افزارهای جعلی یک امپراتوری به راه انداختند

» نویسنده: بنجامین والاس » منبع: وایرد، سپتامبر ۲۰۱۱ » ترجمه: احمدشریف‌پور

در قسمت قبلی مقاله خواندید که جین و ساندین با ایجاد رعب و وحشت در دل کاربران ناآگاه و فروش ترس‌افزارهایشان شرکتی را پایه‌گذاری کردند که درآمدی چند میلیون دلاری را برای آن‌ها به ارمغان آورد. در این قسمت خواهیم دید که آن‌ها چگونه این شرکت را به شرکتی بین‌المللی تبدیل کردند و در انتها چگونه شکایت سیمانتک باعث نابودی امپراتوری IMI شد.

«در سایه تردید» عنوان بخش ثابتی است که عمدتاً به بررسی جنبه‌های حقوقی فضای سایبر، جرائم حوزه فناوری اطلاعات و تأثیرات آن بر این صنعت می‌پردازد.

با گذر زمان، IMI خود را به یک موتور خلاقیت تبدیل کرد. گروه به‌صورت پیوسته در حال دستکاری و تغییر دادن بسته نرم‌افزارهای امنیتی (از برنامه‌های ضدویروس گرفته تا تمیزکننده‌های رجیستری و نرم‌افزارهای دیواره آتش)خود بود و آن‌ها را با نام‌های جدید مانند WinFix، ErrorSafe و DriveCleaner به بازار عرضه می‌کرد. شرکت به گونه‌ای خستگی‌ناپذیر، بازاریابی خود را بهبود می‌بخشید. تبلیغات محصولات متنوعی را برای مشتریان ارسال می‌کرد و پس از آن با استفاده از تحلیل‌های آماری پیچیده تعیین می‌کرد که کدام رویکرد اثربخش‌تر بوده است. روشی که در اواسط سال ۲۰۰۵ مورد استفاده قرار گرفت و به روش اسکنر معروف شد، جهشی بزرگ برای شرکت به ارمغان آورد. یک تبلیغ پاپ-آپ به کاربر هشدار می‌داد که یکی از درایوهایش آلوده است و پیشنهاد اجرای یک اسکن رایگان را مطرح می‌کرد. زمانی که این برنامه اسکنر دروغین نتایج بررسی خود را به نمایش می‌گذاشت؛ نتایجی که همواره نشان از آلودگی سیستم داشت، لینکی به نرم‌افزارهای IMI را نیز به همراه داشت و این نمونه‌ای موفق از هک اجتماعی بود. زیرا مشتریان احتمالی زمانی را صرف فرآیند «اسکن» کرده بودند و با نمایش نتایج آن به اندازه کافی ترسیده بودند و بنابراین احتمال بیشتری وجود داشت که نرم‌افزار را خریداری کنند.

علاوه بر این، شرکت IMI روش‌هایی را به کار می‌برد تا اطمینان حاصل کند که تبلیغاتش روی بیشترین کامپیوترهای ممکن دیده شود. یکی از مدیران سابق شرکت می‌گوید: «اندکی پس از این‌که کرم بلاستر سود فرصت و سود فراوانی را برای IMI به همراه آورد، ساندین حدود سه میلیون دلار را صرف خرید یک سایت دوست‌یابی بزرگسالان مستقر در کاستاریکا کرد و به این ترتیب، ساندین به میلیون‌ها کاربر این سایت در سراسر جهان دسترسی داشت. یکی از چالش‌هایی که IMI با آن روبه‌رو بود، رها شدن از دست مشتریان عصبانی بود که پول خود را می‌خواستند. هدف اصلی این بود که تا حد ممکن پولی به مشتریان بازگردانده نشود و در عین حال مشتریان از تماس گرفتن با شرکت‌ها و بانک‌های تأمین کننده کارت‌های اعتباری‌شان بازداشته شوند، زیرا این کار روابط بانکی و مالی IMI را به خطر می‌انداخت. مسئله این نبود که محصولات IMI بی خاصیت بودند، زیرا بسیاری از کاربران هیچ راهی برای فهمیدن این موضوع نداشتند. اما در بسیاری از موارد نرم‌افزارهای ضدویروس کاربران، برنامه‌های IMI را آلوده و خطرناک معرفی کرده و این کار نصب آن‌ها را با دشواری روبه‌رو می‌کرد یا سرعت کامپیوتر را تا حد زیادی کاهش می‌داد. این شرکت، مراکز خدمات تلفنی متعددی را برای پشتیبانی از زبان‌های مختلف راه‌اندازی کرد که به طور معمول کاربران را به پاک کردن سایر نرم‌افزارهای امنیتی‌شان ترغیب می‌کرد. این ترفند باعث آرام شدن تماس گیرندگان می‌شد، مجوز دسترسی بدون محدودیت را برای نرم‌افزارهای IMI فراهم می‌کرد و سرعت کامپیوتر را به حالت عادی بازمی‌گرداند. برنامه‌های IMI هنوز بی‌خاصیت بودند یا تأثیرشان بسیار اندک بود، اما آن هشدارهای ناراحت‌کننده دیگر به نمایش درنمی‌آمدند و مشتریان نگران و عصبی به این توهم گرفتار می‌شدند که نرم‌افزار جدید خریداری شده واقعاً کارش را به انجام رسانیده است.

در نتیجه، این تجارت با رشدی ناگهانی و تقریباً بی‌وقفه مواجه شد. بین سال‌های ۲۰۰۴ تا ۲۰۰۶، درآمد ناخالص سالانه از ۱۱ میلیون دلار به ۵۳ میلیون دلار رسید. در ژانویه ۲۰۰۴، دفتر اوکراین IMI حدود ۷۰ کارمند داشت. چهار سال بعد بیش از ششصد نفر در این دفتر کار می‌کردند. این دفتر تمام تجملات و جزئیات اداره‌های استاندارد را فراهم کرده بود. دپارتمان منابع انسانی، کلاس‌های آموزش زبان انگلیسی برگزار می‌کرد و هر جمعه نوشیدنی رایگان توزیع می‌شد. تفریحات دسته‌جمعی نظیر بولینگ و مهمانی‌های تولد برگزار می‌شد و شرکت حتی یک سالن ورزشی کوچک هم داشت. شرکت IMI برای یک گروه بیست و چند ساله از خوره‌های نرم‌افزار اوکراینی که تا پیش از این شغلی نداشتند، محل لذت‌بخشی برای کار به شمار می‌آمد.

اما از جهات دیگر، IMI به هیچ وجه مانند شرکت‌های معمول دیگر نبود. کارمندان سابق IMI می‌گویند که آن‌ها نام واقعی یکدیگر را نمی‌دانستند و در عوض هرشخص یک نام مستعار آنلاین داشت. سایت اصلی شرکت با زیرکی تمام، درباره دست‌اندرکاران و کارمندان شرکت هیچ اطلاعاتی بروز نمی‌داد. قراردادها به گفته یکی از تازه‌کاران شرکت «بسیار عجیب» و بدون مهر و امضاهای معمول مدیران شرکت بود. حقوق کارمندان به‌صورت نقدی پرداخت می‌شد. براساس ایمیلی که توسط یکی از مدیران اوکراینی شرکت IMI نوشته شده بود و به همراه اسناد دادگاه منتشر شد، «دستمزدها تا حد ممکن از دید ارگان‌های مالیاتی، پلیس و هر شخص دیگری مخفی نگه داشته می‌شد. به جای عقد قرارداد با ISPها پول فقط به حساب‌های مخفی خارجی آن‌ها واریز می‌شد. این امر به ما امکان می‌داد که تا حدود ۲۰ درصد در هزینه‌های مالیاتی احتمالی صرفه‌جویی کنیم.»

تعدادی از کارمندان که از شیوه‌های کاری IMI ترسیده بودند، شرکت را ترک کردند. اما تعداد قابل توجهی در شرکت باقی ماندند. یکی از کارمندان سابق IMI می‌گوید: «در کشور ما (اوکراین) فرار از سرویس‌های مالیاتی یا هرچیز دیگری، کاملاً طبیعی بود.» کارمندان سابق شرکت، برای آوردن نام IMI در رزومه‌هایشان هیچ تردیدی به خود راه نمی‌دادند. برخی از آن‌ها حتی به شرکت‌های معتبر بین‌المللی نظیر مایکروسافت و بارکلیز راه یافتند.

در همین زمان و هزاران مایل دورتر، جین و ساندین درگیر موج جدیدی از مشکلات قانونی بودند. جین با شکایت سیمانتیک درگیر بود که سابقه آن به نرم‌افزارهای بازار خاکستری بازمی‌گشت که سیمانتیک ادعا کرده بود، جعلی و تقلبی هستند. سایت گرین کارت او که برای فریب دادن مهاجران، ظاهری شبیه نمایندگی رسمی وزارت کشور داشت، در نهایت توجه مسئولان ذی‌ربط را به خود جلب کرد. این اتفاق زمانی رخ داد که در دسامبر سال ۲۰۰۳، مأمورین مانع از ورود وی به ایالات متحده شده و لپ‌تاپ او را توقیف کردند. او در آن زمان چکی بی‌محل به مبلغ یک میلیون دلار با خود داشت. او به سرعت به برزیل رفت و آنجا بین ریو، سائوپائولو و فلوریانوپولیس در رفت‌وآمد بود و براساس شواهد و مدارک در هتل‌ها زندگی می‌کرد. پدر و مادرش به وکلا گفته بودند که از محل اقامت او بی‌اطلاع هستند. پس از این‌که پلیس ایالات‌متحده و کانادا کارمندان جین و ساندین را برای بازجویی فراخواندند، بسیاری از کارمندان شرکت را ترک کردند. ساندین نیز جابه‌جا شدن‌های مکرر را آغاز کرد. ابتدا به کانادا رفت و بعد به‌صورت ناگهانی با ام‌و M3 جدیدش را در ونکوور جا گذاشته و به زادگاهش یعنی سوئد بازگشت.

اما تمام این مشکلات تأثیر چندانی در توقف برنامه ترس‌افزارهای IMI نداشت. از حدود سال ۲۰۰۷، شرکت خلاقیت و نحوه کارش را خبیثانه‌تر کرد. شبکه‌های اصلی تبلیغات IMI را تحریم کردند. به همین دلیل، شرکت تعدادی آژانس جعلی تبلیغات آنلاین به راه انداخت که بنرهای تبلیغاتی را در سایت‌های مشهور نظیر

اکونومیست، eHarmony و سایت لیگ برتر بیس‌بال به نمایش در می‌آوردند. برنامه‌نویسان IMI کدهای مخربی را در این تبلیغات مخفی‌کرده بودند. این کدها باعث می‌شدند که اگر کسی از دفاتر سایت‌های میزبان تبلیغات به آن‌ها نگاه می‌کرد، تبلیغات شرکت‌های مشهور نظیر Travelocity، Priceline و Weight Watcher را مشاهده کند. اما اگر یک کاربر معمولی به سراغ این تبلیغات می‌رفت، آگهی‌های خرید و فروش ماشین‌های دست دوم و قرص‌های رژیمی را می‌دید. زمانی‌که کاربران روی این تبلیغات کلیک می‌کردند، مرورگر آن‌ها به سایت‌های فروش نرم‌افزارهای ضدویروس هدایت می‌شد یا بدتر از آن یک دانلود خودکار آغاز می‌شد و در تمام این مدت، IMI درگیر نبردی بی‌امان با شرکت‌های امنیتی شناخته شده بود و به‌صورت دائمی نرم‌افزارهایش را دستکاری می‌کرد تا از ثبت شدن آن‌ها در پایگاه داده تهدیدات امنیتی شناخته شده جلوگیری کند.

برای افزایش میزان فروش، IMI ترس‌افزارهایش را ترسناک‌تر کرد. دیگر به جای مشاهده پیغام مشکلات سیستمی، یک کاربر ممکن بود با پیغامی مواجه شود که به او می‌گفت: «کامپیوتر دیگری به اطلاعات سیستم شما دسترسی پیدا کرده است.» بدتر از آن، پاپ‌آپ‌هایی ظاهر می‌شدند که مضمون آن‌ها این بود: «محتوای غیراخلاقی غیرقانونی در سیستم شما یافت شده است.» و سپس نرم‌افزار یک گالری از تصاویر بدنانگشتی غیر اخلاقی را که مثلاً از درایوهای کامپیوتر کاربر استخراج شده بود، به او نشان می‌داد و فهرستی از سایت‌های غیرقانونی نیز به آن افزوده می‌شد یا پیغامی با مضمون «تهدیدهای جدی برای ازدواج یا پیشرفت شغلی» به نمایش درمی‌آمد، مگر این‌که کاربر هزینه خرید نرم‌افزار پاک‌سازی درایو را پرداخت می‌کرد. اکنون که دیگر نگرانی‌های قدیمی درباره کرم بلاستر فروکش کرده بود، IMI تصمیم گرفت، ترس از طلاق، بیکاری و حتی زندان را مورد آزمایش قرار دهد.

جک پالادینو، بازرس سابق و دوست ساندین، معتقد است که دو بنیان‌گذار IMI چندان در این قضایای افراطی مقصر نبودند. او تقصیر را متوجه همکاران افراطی، مدیران میانی جاه‌طلب و فشار رشد فزآینده اقتصادی می‌داند. او می‌گوید: «کنترل این اسب سرکش دیگر به دست آنان نبود، بلکه این اسب بود که آنان را به دنبال خود می‌کشید.»

به هر حال، این رشد فزآینده تأثیر خود را نشان داد. به گفته کولبرگ که یک متخصص امنیتی است، IMI در سال ۲۰۰۸ تقریباً حدود ۱۸۰ میلیون دلار، از نرم‌افزارهای امنیتی خود درآمد داشته است. در همان زمان، IMI در زمینه محتوای غیراخلاقی و دیگر بازارها نیز فعالیت می‌کرد. اما به زودی این بنیان‌گذاران IMI بودند و نه مشتریان، که در معرض گرفتار شدن پشت میله‌های زندان قرار گرفتند.

در بهار سال ۲۰۰۸، پس از این‌که جین در کالیفرنیا و در ارتباط با شکایت قبلی سیمانتیک تحت تعقیب قرار گرفت، به ایالات متحده برگشت و به عمارتی در سان‌فرانسیسکو نقل مکان کرد. او با به خدمت گرفتن وکلای گران‌قیمت و قدرتمند آماده دفاع از خود می‌شد. اما با زیاد شدن فشارها، به ظاهر جین راهبرد خود را تغییر داد. در ماه دسامبر، کمیسیون تجارت فدرال که بیش از ۱۳۰۰ مورد شکایت از IMI و محصولاتش دریافت کرده بود، شکواییه‌ای را علیه شرکت و اعضای اصلی آن به جریان انداخت. جین در جلسه استماعی

> **زمانی که پالادینو برای آخرین بار جین را درست پیش از ناپدیدشدنش دیده بود، به شدت شیفته دیدگاه جین درباره ایجاد تغییراتی انقلابی در صنعت تجهیزات پزشکی شده بود.**

که در سن‌خوزه، در ژانویه سال ۲۰۰۹ برگزار شد، حضور نیافت، ارتباطش را با وکلایش قطع کرد و سرانجام ناپدید شد. حکم دستگیری وی صادر شد، اما از آن زمان تاکنون دیگر خبری از او شنیده نشده است. در آوریل سال ۲۰۰۹ پلیس مخفی اوکراین، با ماسک و مسلسل‌های خودکار به دفاتر سابق IMI در کیف حمله کرد. در پایان سال گذشته (۲۰۱۰) ساندین نیز در کنار جین به فهرست فراریان اینترپل افزوده شد. در غیاب بنیان‌گذاران، کمیسیون تجارت فدرال (FTC) در دعوای خود علیه جین و ساندین برنده شد. مارک دو سوزا و پدرش موریس که به راه‌اندازی حساب‌های تجاری IMI کمک کرده بودند، با پرداخت ۸/۲ میلیون دلار آزاد شدند. جیمز رنو با پرداخت ۱۸ هزار دلار، جریمه ۱/۹ میلیون دلاری خود را به حال تعلیق درآورد و پرونده کریستی روس هنوز در جریان است.

پالادینو در داستان IMI ردپایی از تراژدی می‌بیند. او می‌گوید: «این زیانی بزرگ است. آن‌ها جوان‌های خوب و با استعدادی بودند که از راه راست خارج شدند.» با نگاه به ظهور و سقوط امپراتوری جین و ساندین، سخت است که دیدگاه او را رد کنیم. تنها به کمک تبلیغات پاپ‌آپ و سیستم توزیع آنلاین، جین و ساندین توانستند چهل میلیون دلار نرم‌افزار را به میلیون‌ها کاربر بفروشند. در بهترین زمان‌های این دهه، آن‌ها سازمانی را راه‌اندازی و اداره کردند تا این نرم‌افزارها را تولید کرده و به فروش برسانند. اگر آن‌ها این مهارت‌ها را صرف نرم‌افزارهایی کرده بودند که ارزش نصب و استفاده را داشت، شاید اکنون به شخصیت‌هایی قابل تحسین تبدیل شده بودند، در عوض اکنون آن‌ها فراری هستند. گفته می‌شود که ساندین به سوئد بازگشته است و این کشور قوانین محکمی دارد که از شهروندانش در برابر قوانین استرداد مجرمان محافظت می‌کند. اما جین که گفته می‌شود، به آب و هوای گرم علاقه دارد، به احتمال به برزیل رفته است. اما هیچ یک از افرادی که این دو را می‌شناسند فکر نمی‌کنند که آن‌ها دست از کارکشیده و در حال استراحت هستند.

زمانی که پالادینو برای آخرین بار جین را درست پیش از ناپدیدشدنش دیده بود، به شدت شیفته دیدگاه جین درباره ایجاد تغییراتی انقلابی در صنعت تجهیزات پزشکی شده بود. او می‌گوید: «من تقریباً درباره مطرح کردن این موضوع مردد بودم، اکنون دیگر پلیس امریکا به دنبال مردی کوتاه با پوستی تیره در مجامع مرتبط با سلامت و پزشکی خواهد بود.»

در حالی که IMI به ظاهر از دور خارج شده است، نسل جدیدی از جین‌ها و ساندین‌ها بدون آرام و قرار روی طرح‌های جدید ترس‌افزارها کار می‌کنند. نوید‌بخش‌ترین بخش بازار برای آنان شبکه‌های اجتماعی است، جایی که پست‌های گمراه‌کننده به سادگی می‌تواند کاربران را به دام بیاندازد. کمپین‌های جدید ترس‌افزارها به تدریج به نتایج جست‌وجوهای گوگل نیز راه یافته است و خود را در قالب پست‌هایی درباره مراسم ازدواج خاندان سلطنتی، زمان ملاقات‌های عمومی هنرپیشه‌ها و حتی مشاهده فیلم کشته شدن اسامه بن‌لادن مخفی کرده است. و این جنبه دسیسه‌آمیز مهندسی اجتماعی است و هیچ راهی برای از بین بردن تهدیدات سیستمی در مغزهای فریب خورنده ما وجود ندارد.