بخش نخست

مهندسان ضداجتماع

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

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

پیش از این‌که یک امپراتوری بین‌المللی زیرزمینی به راه بیاندازند، پیش از این‌که در هزاران کامپیوتر نفوذ کنند، پیش از این‌که امپراتوری آنلاین آن‌ها سالانه صدها میلیون دلار درآمد ایجادکند و پیش از این‌که فراری‌های تحت تعقیب پلیس‌بین‌الملل باشند؛ سم جین (SamJain) که اکنون ۴۱ ساله است و دانیل ساندین (DanielSundin) که اکنون ۳۳ ساله است، تنها دو کلاهبردار اینترنتی معمولی بودند.

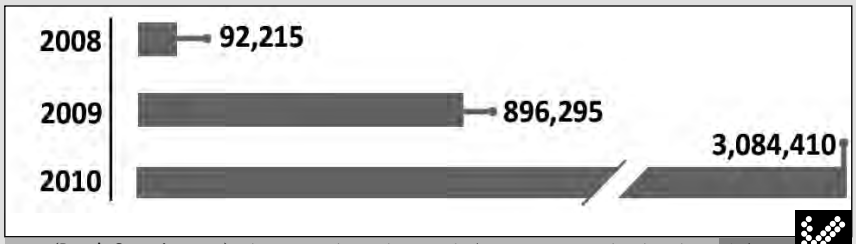
«در سایه تردید» عنوان بخش ثابتی است که عمدتاً به بررسی جنبه‌های حقوقی فضای سایبر، جرائم حوزه فناوری اطلاعات و تأثیرات آن بر این صنعت می‌پردازد.

IT Crimes

این دو در سال ۲۰۰۱ با یکدیگر ملاقات کرده و با مجموعه‌ای از ترفندها و شیادی‌های ساده‌کار خود را شروع‌کردند. با تکیه بر آشوب و دیوانگی ایجاد شده پس از حادثه یازدهم‌سپتامبر، جین‌ماسک‌های‌ضدسیاه‌زخم می‌فروخت. همچنین او با سوء استفاده از عجله و شتاب‌زدگی متقاضیان مهاجرتی که انگلیسی نمی‌دانستند، به راه‌اندازی سایتی کمک کرد که فرم‌های رایگان اداره مهاجرت امریکا را به متقاضیان می‌فروخت. آن دو با همکاری یکدیگر نسخه‌های جعلی نرم‌افزارهای مشهور را به فروش می‌رساندند و به اصطلاح «بازار خاکستری» به راه انداخته بودند. آن‌ها تمام این کالاهای جعلی و خطرناک را با روش‌های به شدت تهاجمی از جمله ترفندهای هکر کلاه سیاه نظیر «دزدی مرورگر» یا ترفندهای «اشتباه تایپی» (ثبت‌سایت‌هایی با نام‌های مشابه سایت‌های مشهور)، به فروش می‌رساندند. اما جین و ساندین خورده‌های فناوری نبودند؛ آن‌ها به کامپیوترهای قربانی‌ها نفوذ نمی‌کردند یا اطلاعات کارت‌های اعتباری را به سرقت نمی‌بردند.

در عوض آن‌ها استادان مهندسی اجتماعی بودند که می‌توانستند مردم را وادار کنند که با رضایت‌کامل پولشان را به آن‌ها تقدیم کنند. این کار آنقدر سودآور بود که جین و ساندین می‌توانستند برنامه‌نویسان و طراحان و بازاریاب‌هایی را برای خود استخدام‌کنند. با این حال، شیوه کار آن‌ها هنوز غیرمتمرکز و خسته‌کننده بود. اما در آگوست سال ۲۰۰۳، کار جین و ساندین به لطف ظهور کرم بلستر (Blaster) با رونقی‌ناگهانی روبه‌رو شد. بلستر به سرعت صدها هزار ماشین را آلوده‌کرده و بیشترین سرعت آلوده‌سازی را در بین بدافزارهای آن دوره از آن خود کرد. علاوه بر این، بلستر وحشت بی‌سابقه‌ای را نیز در میان کاربران ایجاد کرد، به‌طوری که در چهار روز اول شیوع آن حدود چهل‌هزار کاربر کامپیوتر برای دریافت پشتیبانی و کمک با مایکروسافت تماس گرفتند. جین و ساندین امپراتوری خود را برپایه سوءاستفاده از ترس مردم؛ ترس از حمله‌های میکروبی یا ترس از بازگردانده شدن اتباع خارجی بنانهاده بودند و اکنون خطری وجود داشت که تقریباً هرکسی را که با یک کامپیوتر سروکار داشت، تهدید می‌کرد. این به معنی مخاطبان بالقوه فراوان برای یک برنامه تبلیغاتی دروغین آن‌ها بود. برای جین و ساندین که‌اکنون‌کار‌خود‌را‌تحت‌نام‌شرکت IMI (سرنام Innovative Marketing Inc) انجام می‌دادند، کاملاً واضح بود که باید از ترس ناشی از ویروس‌های کامپیوتری برای فروش برنامه‌های ضدویروس استفاده کنند.

در همان زمان، ساندین یک نرم‌افزار دیواره آتش با نام ComputerShield نوشته بود. کارایی این نرم‌افزار در حد برنامه‌های امنیتی معمول نبود، چون لازم نبود کارایی چندانی داشته باشد. هنر این برنامه در میزان فروش آن بود. پس از تغییر نام این برنامه به WinAntiVirus، شرکت IMI شروع به خرید مجموعه‌ای از تبلیغات پاپ‌آپ کرد که



نمودار۱ تعداد برنامه‌های ضدویروس جعلی که در سراسر دنیا توزیع شده‌اند (منبع: Panda Security).

هشدارهای دروغینی را درباره آلوده‌شدن هارددیسک‌های کاربران به نمایش درمی‌آوردند؛ این پیغام‌ها با مضامینی شبیه «۲۸۴ تهدید امنیتی جدی روی سیستم شما وجود دارد» به نمایش درمی‌آمدند. این تبلیغات به کاربر، پیشنهاد می‌کرد تا نسخه آزمایشی نرم‌افزار را دانلود کند یا ۳۹/۹۵ دلار را برای استفاده از نرم‌افزارهای بی‌کیفیت IMI بپردازد. هنگامی که چنین نرم‌افزاری نصب می‌شد، نسخه‌های آزمایشی با نمایش پاپ‌آپ‌های بیشتر درمرورگر کاربر، او را به ستوه‌آورده و وادار می‌کردند تا نسخه اصلی را خریداری کند. این برنامه واقعاً خنده‌دار به نظر می‌رسید؛ جین و ساندین، با سوء استفاده از ترس کاربران از ویروس‌ها، اقدام به گسترش نرم‌افزاری می‌کردند که خود در واقع یک ویروس دیگر بود و تازه کاربران را به پرداخت پول برای خرید مجوز آن مجبور می‌کردند.

این نقشه با موفقیت روبه‌رو شد. آن‌گونه که یکی از همکاران جین می‌گوید، مردم آن‌قدر از کرم بلستر ترسیده بودند که جین ادعا می‌کرد که می‌تواند از طریق فروش «قالب‌های یخ» نیز درآمد کسب کند. به زودی کار به جایی رسید که IMI ماهانه یک میلیون دلار درآمد کسب می‌کرد. جین و ساندین به سرعت توجه خود را از ترفندها و دیگر کارهای کوچک‌تر خود، معطوف این منبع درآمد جدید کردند. شرکت IMI برنامه اصلی خود را یافته بود.

در چند سال بعدی، افراد و شرکت‌های فراوان دیگری از این ایده تقلید کردند. به این ترتیب، طی مدت کوتاهی کاربران کامپیوتر در محاصره هشدارهای ترسناک از سوی انواع مختلف تولیدکنندگان برنامه‌های ضدویروس قرار گرفتند. این نسل از نرم‌افزارها که «ترس‌افزار» نامیده می‌شدند، به زهرآلودترین بلایای اینترنتی تبدیل شدند. براساس تحقیقات شرکت امنیتی پاندا در سال ۲۰۰۹، هر ماه به طور میانگین ۳۵ میلیون کامپیوتر به این ترس‌افزارها آلوده می‌شدند. دیرک کولبرگ یکی از محققان ارشد سوفوس که در زمینه تهدیدات کامپیوتری تحقیق می‌کند، می‌گوید: «هنوز هم ترس‌افزارها بهترین امید تبهکاران برای تبدیل سیستم‌های در معرض خطر به پول نقد هستند.» و IMI که تا همین اواخر «گوگِل ترس‌افزارها» بود، طی چند سال از یک گروه کوچک و خانگی هکرها به یک قدرت بین‌المللی و سازمانی پیچیده با صدها کارمند و دفاتری در چهار قاره تبدیل شده بود. چندین

جین و ساندین در دو چیز مشترک بودند. نخست تکبر و خود برتربینی که تا حد تحقیر دیگران پیش می‌رفت و دوم علاقه‌ای که به مرزهای تاریک تجارت الکترونیک داشتند.

مرکز پشتیبانی تلفنی در اوهایو، آرژانتین و هند وجود داشت و محصولاتش را با حدود هزار نشان تجاری و نه زبان مختلف به فروش می‌رساند. بین سال‌های ۲۰۰۲ تا ۲۰۰۸ میلادی، IMI صدها میلیون دلار سود را نصیب صاحبان خود کرده است.

کارمندان IMI نام واقعی یکدیگر را نمی‌دانستند، هرکس تنها با یک اسم مستعار آنلاین می‌شد.

برخلاف سایر کارآفرینان اینترنتی جوان که در شروع هزاره جدید کسب‌وکارهای بزرگی را راه‌اندازی کردند، داستان سم جین و دانیل ساندین در پروفایل‌ها و نمودارهای متملقانه و در کتاب‌های متعدد و فیلم‌های دیوید فینچر آورده نشد. اما اگر روش شیادانه آن را در نظر نگیریم، IMI را می‌توان یکی از قابل‌توجه‌ترین استارت‌آپ‌های دهه گذشته به شمار آورد! استعداد این زوج در مهندسی اجتماعی به اندازه تمام محصولات و ویژگی‌های نوآورانه‌ای است که شرکتی همانند فیس‌بوک عرضه کرده است و روش هوشمندانه و قابل‌توجهی که این شرکت در قبال توسعه نرم‌افزار و بازاریابی اتخاذ کرده بود، هر هفته نوآوری تازه‌ای را عرضه می‌کرد. به ظاهر داستان IMI چیزی نیست که دو بنیان‌گذار آن، تمایلی به بازگوکردن آن داشته باشند. درواقع، مکان اقامت هیچ یک از آن‌ها مشخص نیست و حکم دستگیری هردو صادر شده است. اما به لطف مجموعه‌ای از پرونده‌های قضایی و شکایت‌های جنایی که در طی سال‌های اخیر ضد آن‌ها به دادگاه عرضه شده است و همچنین برپایه مصاحبه‌هایی که با کارکنان سابق شرکت انجام شده‌است، می‌توان به تصویری از نحوه ایجاد ترس‌افزار در این شرکت دست یافت و فهمید که چگونه این دست‌فروش‌های دوره‌گرد به دو مولتی‌میلیونر تبدیل شده‌اند.

سم جین

در سال ۱۹۹۱ زمانی که شایلش کومار جین ملقب به «سم» پس از سه سال تحصیل از دانشگاه پن (Penn State) فارغ‌التحصیل شد و به دره سیلیکون آمد، بی‌توجهی او به اخلاقیات کاملاً مشهود بود. سه ماه پس از ورود به دره سیلیکون زمانی که تلاش می کرد با نام جعلی کریستوفر روبیو یک حساب جاری باز کند، به دلیل استفاده از مدارک جعلی دستگیر شد. پدر او که یک مهندس بود و در کارخانه وستینگ‌هاوس در پیتس‌بورگ کار می‌کرد، در نامه‌ای که برای تقاضای عفو پسرش به قاضی دادگاه نوشته بود، ادعا کرده بود که پسرش تاکنون هیچ‌گاه دردسری ایجاد نکرده است و وضعیت ایجادشده را به یک «کابوس برای خود و همسرش» تعبیر کرده بود. دو همکار دیگر جین در یک شرکت نوپای مرتبط با دکه‌های فروش بلیت؛ که محل کار بعدی جین بود، به یادمی‌آورند که وی با سوزاندن‌عمدی پای خود و انداختن گناه آن به گردن مشکلات کامپیوترش، یک لپ‌تاپ رایگان به عنوان غرامت دریافت کرده بود.

جین جثه ریزی داشت و همواره از ظاهرش ناراضی بود. همکلاسی‌های سابق او می‌گویند که همیشه برای مخفی‌کردن سیم‌های ارتودنسی دهانش، لب‌هایش را به فرمی خاص

نمودار۱ شایلش کومار جین (چپ) و دانیل ساندین (راست) استادان مهندسی اجتماعی بودند و با شیوه‌های خاص خود مردم را وادار می‌کردند که با طیب خاطر پول‌هایشان را در ازای نرم‌افزارهای جعلی به آن‌ها تقدیم کنند.
تصویرسازی از: آلوارو تاپیا هیدالگو (Alvaro Tapia Hidalgo)

جمع می‌کرد و تصمیم داشت برای خلاص‌شدن از شر عینک چشمش را جراحی‌کند. جک پالادینو (Jack Palladino) یکی از وکلای دعاوی برجسته سان‌فرانسیسکو که از سال ۲۰۰۶ با IMI کار می‌کرد و با جین هم دوست شده بود، دید دلسوزانه‌تری نسبت به شخصیت وی دارد. او جین را یک نابغه عجیب و غریب می‌بیند که خشونت رفتاری وی ناشی از مشکل در برقراری ارتباط با مردم بوده است. مستقل از دلایل زیربنایی، جین با جهان‌بینی منفی که داشت، همه اطرافیانش را می‌آزرد. دیدگاه او این بود: «یا سر بقیه را کلاه بگذار یا سرت را کلاه می‌گذارند.»

در زمانی که حباب دات‌کام در حال ترکیدن بود، جین موقعیت شغلی خود را در مرزهای ناآشکار بازاریابی اینترنتی و کلاهبرداری علنی مستحکم‌کرد. با پولی که از شرط‌بندی بر سر مسابقات فوتبال به چنگ آورده‌بود، به همراه گروهی دیگر، شرکتی به نام eFront را تأسیس‌کرد که با خرید چند دوجین سایت‌های کوچک، اما پرمحتوا به توزیع آگهی‌های تبلیغاتی در این سایت‌ها پرداخت. این ایده بسیار پیشرفته‌تر از زمان خودش بود و این شرکت مستقر در کاستامدیا در کالیفرنیا به سرعت به یکی از برترین شرکت‌های حباب دات‌کام تبدیل شد. شرکت Media Metrix از تحلیل‌گران بازار، eFront را به عنوان یکی از بیست شبکه پرترافیک اینترنت معرفی کرد. کمتر از یک‌سال بعد، مشخص شد داده‌هایی که درباره eFront به تحلیل‌گران Media Metrix ارائه شده بود، دستکاری شده بودند و به همین دلیل eFront از هم پاشید. بسیاری از کارکنان eFront معتقد بودند، جین مسئول این قضیه بوده است، اما او در آن زمان این اتهام را رد کرد. در بهار سال ۲۰۰۱ درهای eFront برای همیشه بسته شد و جین برای تجدید قوا به هاوایی رفت.

دانیل ساندین

تقریباً در همین زمان بود که جین توسط یکی از دوستان با دانیل ساندین آشنا شد و این دو به سرعت همکاری‌شان را شروع کردند. ساندین در شانزده سالگی از مدرسه اخراج شده و پس از آن سوئد را به قصد آریزونا ترک کرده بود. در آریزونا او با نوشتن برنامه‌های ردگیری ترافیک برای سایت‌های غیراخلاقی، روزگار می‌گذراند. او که قدبلند و به شدت لاغر بود، از بیماری گوارشی ازدیاد باکتری (Bacterial Overgrowth Syndrome) رنج می‌برد که این امر افزایش وزن را برای او غیرممکن می‌کرد. او نیز همانند جین از ماندن در آپارتمانش راضی بود و ترجیح می‌داد از طریق ماشین‌ها با مردم ارتباط برقرار کند. البته، او در زندگی آنلاین نیز وسواسی بود و مدام اشتباهات نگارشی دیگران را اصلاح می‌کرد و بسیاری از ایده‌ها را احمقانه می‌پنداشت. او عاشق جمع‌آوری محتواهای مستهجن بود و به گفته یکی از همکارانش آرشیوی ۷ ترابایتی از این محتواها داشت.

هرچند که همکاری جین و ساندین اغلب‌مجازی بود (ساندین به سیاتل رفت، در حالی که جین هاوایی را به قصد لاس‌وگاس ترک کرد)، اما بسیار به هم احساس نزدیکی می‌کردند. جین و ساندین در دو چیز مشترک بودند. نخست تکبر و خود برتربینی که تا حد تحقیر دیگران پیش‌می‌رفت و دوم علاقه‌ای که به مرزهای تاریک تجارت الکترونیک داشتند. ساندین تعدادی سایت غیراخلاقی راه‌اندازی کرده‌بود و از طریق ارسال اسپم درآمد کسب می‌کرد. جین نیز جذب هوش تجاری دوستش‌شده بود. ساندین از نخستین کسانی بود که ارزش و سود برون‌سپاری را درک کردند و در اواخر سال ۲۰۰۱ او کارهای طراحی رابط کاربری و کدنویسی را به برنامه‌نویسانی در آرژانتین، هند و اوکراین واگذار کرده بود. جین به این نتیجه رسید که می‌توان اززیرساخت نرم‌افزاری که ساندین در حال آماده‌کردن آن است، برای ایجاد تجارتی بسیار بزرگ‌تر استفاده کرد.

در روزهای نخست شکل‌گیری، کارکنان IMI از تعدادی برنامه‌نویس و بازاریاب جوان پراکنده در سراسر کشور تشکیل شده بود که ارتباط چندان محکمی با هم نداشتند. دوست سابق جین، یعنی کریستی راس که محل نمایش تبلیغات را کنترل می‌کرد، یک دانشجوی حقوق کالج بوستون به نام مارک دوسوزا که برقراری ارتباط با شرکت‌های صادرکننده کارت‌های‌اعتباری را برعهده داشت و یک دانش‌آموز دبیرستانی خوره برنامه‌نویسی اهل سینسیناتی به نام جیمز رنو که گاهی مجبور می‌شد، به دلیل تذکرات مادرش برنامه گفت‌وگویی با جین را قطع کند، از جمله این کارکنان بودند. همه آن‌ها از طریق چت و ایمیل با هم در ارتباط بودند و تقریباً هیچ‌گاه همدیگر را از نزدیک ملاقات نکرده بودند. حروف روی صفحه کلید راس از فرط استفاده مداوم تقریباً پاک شده بودند ودوسوزا که بعد از فارغ‌التحصیلی وقتش را میان بحرین و تورنتو تقسیم‌کرده‌بود، در طول شش سال همکاری تنها یک بار جین را از نزدیک دیده بود. بالاخره در پایان سال ۲۰۰۱میلادی، IMI صاحب یک دفترمرکزی در اوکراین شد تا بتواند از نیروی کار ارزان برنامه‌نویسی در این کشور استفاده کند.قسمت دوم این ماجرا را در شماره آتی ماهنامه از نظر خواهید گذراند.