The Dark Side Of The Net

علی احمدی
دانشجو مهندسی کامپیوتر
دانشکدگان فارابی دانشگاه تهران
ali.ahmadi9@ut.ac.ir

داستان از آنجا شروع می‌شود که افرادی در دنیای کامپیوتر وجود دارند که همیشه از هرگونه مصاحبه امتناع می‌کنند، و این افراد کسانی هستند که حساس‌ترین آسیب‌پذیری‌ها را کشف کرده، به شرکت‌ها و دولت‌ها می‌فروشند.

این موارد، بازارِ سیاهِ آسیب‌پذیری‌ها و اکسپلویت‌ها را تشکیل می‌دهد. ممکن است عجیب باشد ولی این موضوع کاملا قانونی است، زیرا اکثر خریداران آسیب‌پذیری‌ها دولت‌ها هستند، اما این معامله کاملا محرمانه است و همراه با هر معامله احتمالا قرارداد NDA (عدم افشای اطلاعات) وجود دارد، زیرا افراد خریدار می‌خواهند آسیب‌پذیری ناشناخته بماند و از طرف دیگر نمی‌خواهند کسی بداند که چه کسی آسیب‌پذیری را خریداری کرده است.

برای مثال اگر کسی یک Zeroday (یک آسیب‌پذیری ناشناخته در یک سیستم کامپیوتری) را با قیمت ۱۰۰,۰۰۰ دلار خریداری کند می‌تواند مانند خرید یک سلاح خطرناک باشد. اما اگر این Zeroday توسط شرکت سازنده نرم‌افزار شناسایی بشود به سرعت برای این آسیب‌پذیری به اصطلاح یک Patch ایجاد می‌کند، که باعث بی‌ارزشی کامل این آسیب‌پذیری می‌شود. در ادامه به شکل مختصر به گزارشات و تحقیقاتی که خانم Nicole Perlroth انجام داده، و همچنین اتفاقاتی که برای او افتاده می‌پردازیم.

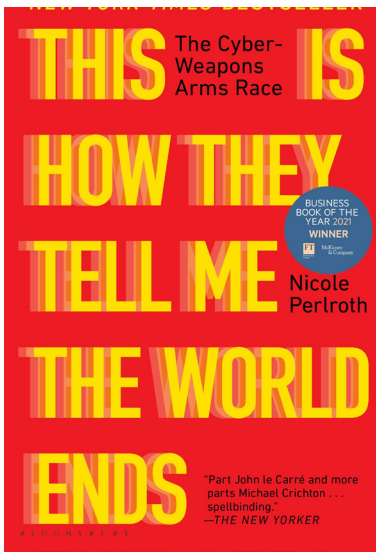
معرفی خانم Nicole و حوادثی که برای او اتفاق افتاد

خانم Nicole یک گزارشگر امنیت سایبری است که در نیویورک‌تایمز فعالیت می‌کرد. در واقع ایشان چندین مورد از مواقعی که مورد هدف حمله‌های سایبری قرار گرفتند را تاکنون مطرح کرده‌اند. اولین آنها به زمانی که به تایمز پیوسته بود مربوط می‌شود، چرا که حمله‌ای از طرف ارتش چین به تایمز صورت گرفت. تیم امنیتی تایمز ورود مشکوکی به سیستم‌های آنها مشاهده کرد: شخصی در طول چندین ماه ساعت ۱۰:۳۰ صبح به وقت پکن وارد سیستم‌های آنها می‌شد، و تا ساعت ۵:۰۰ به وقت پکن به دنبال منابع بود. پس از همکاری تایمز با FBI مشخص شد که این شخص در واقع به دنبال منابع یکی از همکاران خانم Nicole بود. فردی که درباره فسادهایی که در برخی از خانواده‌های حکومتی چین وجود دارد گزارشی تهیه می‌کرد. از آنجایی این اتفاق در نزدیکی انتخابات ۲۰۱۲ ریاست جمهوری آمریکا رخ داد، تایمز احتمال داد ممکن است هدف مخربی پشت این ماجرا باشد، اما بعداً مشخص شد که این یک حمله جاسوسی بود. یک Backdoor (بدافزاری که بعد از گرفتن دسترسی روی سیستم هدف نصب می‌شود تا بعداً امکان ارتباط مجدد و دسترسی وجود داشته باشد) روی کامپیوتری در شبکه داخلی تایمز قرارداده شده بود، و درواقع مهاجمان به ۵۳ کامپیوتر متعلق به کارمندان تایمز دسترسی داشتند. تمرکز این حمله روی خبرنگارانی بود که چین را پوشش می‌دادند.

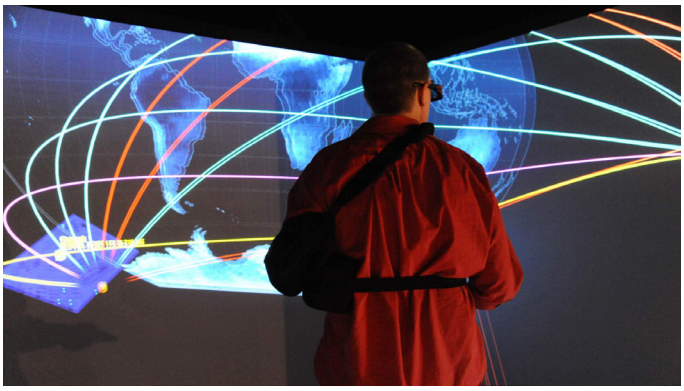
پس از گفت‌وگوی بسیار تایمز تصمیم گرفت این موضوع را به شکل عمومی مطرح کند. ترس آنها این بود که این موضوع باعث اخراج مدیران و همچنین کاهش ارزش سهام آنها شود. تایمز یکی از اولین شرکت‌هایی بود که پس از گوگل به شکل عمومی اعلام کرد که توسط چین هک شده است. پس از انتشار اخباری در مورد این موضوع چین مسئولیت حمله را برعهده نگرفت و گفت که قوانین چین به وضوح حملات آنلاین را ممنوع کرده و این خلاف قوانین ما است.

نتیجه اتفاقاتی که برای خانم Nicole افتاد چه شد؟

چند سال پس از این واقعه Nicole کنجکاو شد که در این موضوع تحقیقاتی انجام دهد و برای انتشار تحقیقاتش تصمیم گرفت آنها را به شکل کتاب منتشر کند.



نام کتابش «This is How They Tell Me the World Ends» بود. در همان سال‌ها Nicole هدف حملات دیگری نیز قرار گرفت. یک هشدار از تیمش دریافت کرده بود که شخصی در دارک وب به هر کس که بتواند به تلفن شخصی و حساب ایمیل او دسترسی پیدا کند، پول خوبی می‌دهد، که احتمال می‌رفت این قضیه مربوط به کتاب او باشد.



برای تحقیقات به آرژانتین سفر کرد و با شخصی به نام سزار سروتو (Cesar Cerrudo) آشنا شد. پیشنهاد او به Nicole این بود که اگر قصد آشنایی با بزرگان این حوزه را داری باید به Ekoparty (یک کنفرانس بزرگ امنیتی در بوئنوس آیرس) برود. Nicole به پیشنهاد Cesar در کنفرانس شرکت کرد و با تعجب افرادی را می‌دید که از شرکت‌های بزرگ در آنجا حضور داشتند که علاقه‌مند به خرید Zeroday بودند. آرژانتین به جایی تبدیل شده که بزرگان حوزه امنیت سایبری آن را هندِ توسعه‌ی بدافزار می‌نامند.

دولت‌ها و شرکت‌های زیادی برای خرید Zeroday در کنفرانس شرکت کرده بودند. خانم Nicole در این کنفرانس به جای استفاده از وسایل الکترونیکی از کاغذ و خودکار استفاده کرد تا امنیت مکالمات و گزارش‌هایی که انجام می‌دهد تضمین شده باشد. متاسفانه هیچ خریدار یا فروشنده‌ای حاضر به گفت‌وگو با Nicole نبود حتی وقتی به آنها نزدیک می‌شد برای سوال پرسیدن پراکنده می‌شدند.

بالاخره توانست با Ivan Arce که یکی از پدرخوانده‌های قدیمی حوزه امنیت است آشنا بشود. طبق گفته‌های او نسل‌های بعدی فرصت خوبی برای کسب ثروت از این حوزه دارند در حالی که شامل هیچ نوع مالیاتی نمی‌شود. تمام برداشت Nicole از کنفرانس همین بود.

کمی بیشتر در مورد تاریخچه امنیت سایبری

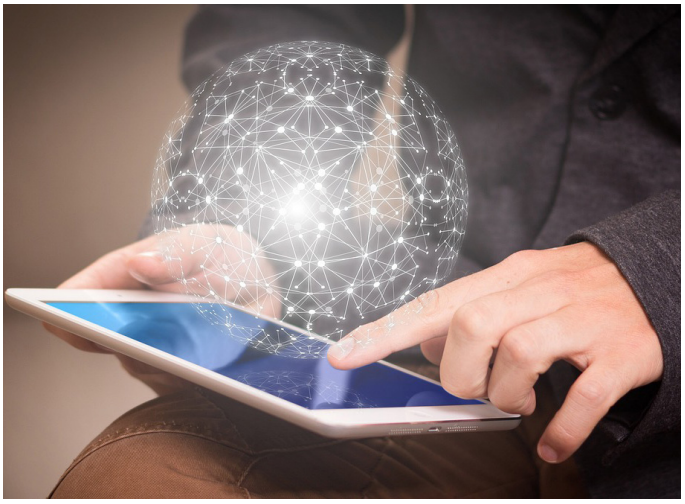
تا اینجا فهمیدیم که دنیای کنونی از افرادی تشکیل شده که برای نهادهای مخفی کار می‌کنند و هدف آنها ثروتی است که از این حوزه می‌توانند کسب کنند. ولی خب همیشه اینطور نیست. می‌توانیم در مورد زمانی سخن بگوییم که مایکروسافت یک شرکت تازه تاسیس بود و می‌خواست با Netscape رقابت کند. مایکروسافت در بازار کامپیوترهای شخصی خوب پیش رفته بود ولی در حوزه‌های دیگر ضعف زیادی داشت.

برای عقب نماندن از رقابت و شکست نخوردن، تمرکز مایکروسافت بر توسعه سریع و به موقع بود؛ درحالی که به امنیت نرم‌افزاری خود اهمیت چندانی نمی‌داد. در آن زمان هنوز پلتفرم‌های گزارش باگ وجود نداشتند که امکان گزارش باگ به تیم امنیتی وجود داشته باشد و معمولا چنین گزارشاتی توسط شرکت‌ها نادیده گرفته می‌شدند. کمبود چنین پلتفرمی باعث شد هانترها شروع به تشکیل انجمن‌هایی مانند Bugtraq کنند که شبیه نسخه‌های اولیه Reddit بود. این انجمن‌ها از نقص‌های امنیتی شرکت‌ها و محصولات آنها برای تمسخر استفاده می‌کردند و حتی در بعضی مواقع امکان سواستفاده نیز بود. این موضوع ادامه داشت تا زمانی که کرم‌های کامپیوتری مانند نیمدا از مایکروسافت برای تاثیرگذاری روی برخی از بزرگترین مشتریان مایکروسافت در دولت استفاده کردند. بیل گیتس کم‌کم شروع کرد به جدی گرفتن امنیت و او اعلام کرد که ما ساختار سازمانی خود را دوباره اولویت بندی می‌کنیم و امنیت خود را در اولویت قرار می‌دهیم. این موضوع به حقیقت پیوست، آن‌ها حتی دیتابیسی از افراد گزارش دهنده باگ و هکرهای خود تهیه کردند و دقیقا می‌دانستند که با چه کسی چگونه باید رفتار کنند و در ازای هر گزارش چه چیزی به او بدهند. گذشته از این موضوعات شرکت‌ها نگران نفوذ هکرهای دولتی و نظامی به سیستم‌هایشان بودند.

برای جلوگیری از این موارد، بانتی(مژدگانی) دادن در ازای گزارشات رونق پیدا کرد. این جریان به نوعی مسابقه بین دولت‌ها و شرکت‌ها تبدیل شد. مهم نبود که مایکروسافت یا هر شرکت دیگری چقدر بانتی می‌داد دولت‌ها برای دسترسی به همان باگ‌های امنیتی حاضر بودند مبالغی بدهند که شرکت‌ها توانایی رقابت با آن ارقام را به هیچ وجه نداشتند. برای مثال، مقدار بانتی اپل برای iOS چیزی نزدیک به ۲.۵ میلیون دلار است که یک واسط به نام Crowdfense با حداقل ۳ میلیون دلار بابت همان کار پرداخت می‌کند و برخی دولت‌ها قیمت‌های خیلی بالاتری را پیشنهاد دادند که اپل هرگز نمی‌تواند با اونا رقابت کند. در اینجا یک دوگانگی برای شرکت‌ها ایجاد می‌شود؛ زیرا اگر بخواهند در رقابت با دولت‌ها مقدار بانتی‌ها را افزایش دهند تشویقی برای مهندسان امنیتی شرکت می‌شود که شرکت را ترک کنند و در خارج از شرکت با فعالیت در این حوزه درآمد بیشتری نسبت به داخل شرکت داشته باشند. به همین دلیل محاسبات دقیقی در این بازی وجود دارد.

رقابت در این حوزه از کجا و توسط چه کسانی شروع شد؟

یکی از عملیات‌هایی که در این حوزه معروف است و جیمز گاسلر در آن مشارکت داشته Gunman بود. ماجرا از این قرار است که



سرویس اطلاعاتی فرانسه به دولت آمریکا گفته بود که روسیه در حال شنود ارتباط بین ماست، و پیش فرض این است که روسیه در حال جاسوسی است. مشکل از سفارت آمریکا داخل مسکو شروع شد و این پروژه توسط NSA با نام Gunman شروع شد. در آن زمان آن‌ها در حال ساختن سفارت جدید در مسکو بودند و ابزارهای جاسوسی پیدا میکردند حتی در داخل بتن دیوار! در عمل کل سفارت جدید تبدیل شده بود به دستگاه شنود شوروی. دو دسته از بهترین افراد NSA برای بررسی ابزارهای داخل سفارت آمدند. توانستند با بررسی یک ماشین تحریر با اشعه ایکس یک سیم‌پیچ اضافه در پشت آن پیدا کنند. این سیم‌پیچ یک مغناطیس‌سنج کوچک بود که کوچکترین اختلالی را در میدان مغناطیسی ثبت می‌کرد و با فشرده شدن هر دکمه از دستگاه تایپ، کلید فشرده شده را ضبط می‌کرد و به دستگاهی که در دودکش سفارت مخفی شده بود می‌فرستاد و از آنجا از طریق امواج رادیویی اطلاعات به شوروی فرستاده می‌شد. حتی شوروی این توانایی را داشت که دستگاه را از راه دور غیرفعال کند، که در بعضی مواقع احتمال شناسایی آن نباشد. پس از کشف این مورد توسط نیروهای NSA، آمریکا متوجه شد که از این نظر از شوروی بسیار عقب است و اگر خودشان را به شوروی نرسانند احتمال شکست در جنگ‌های سایبری بیشتر خواهد شد. شروع رقابت برسر توسعه اکسپلویت و خریدوفروش زیرودی از همینجا بود.

یکی از برنامه‌های NSA این بود که برای هر فناوری جدیدی که به بازار وارد می‌شود، راهی برای نفوذ به آن پیدا کنند. چون NSA افراد متخصص خودش را داشت، اوایل کار در بازار زیرودی هیچ نقشی نداشت و از خارج از سازمان خریدی انجام نمی‌شد. اما به لطف ادوارد اسنودن مشخص شد که NSA در سال ۲۰۱۳ حدود ۲۵ میلیون دلار خرید در این حوزه داشته است. طبق گفته Nicole افرادی در NSA بودند که آنها به عنوان افرادی توصیف می‌شدند که شما برای ممکن کردن غیرممکن‌ها پیش آنها می‌روید. هزینه‌های زیاد NSA برای خریدهای خارج از شرکت باعث شد که این افراد که حقوق عادی ادارات دولتی را داشتند تصمیم بگیرند NSA را ترک کنند و با هم آزمایشگاه تحقیقاتی خود را راه اندازی کنند و با هدف توسعه ابزارهای جاسوسی برای کارفرمای سابق خود یعنی NSA یا حتی آژانس‌های دیگر کار کنند. این چیزی بود که شرکت‌ها هم از آن می‌ترسیدند.

نتیجه

شرکت‌های نرم‌افزاری مثل مایکروسافت امنیت خودشان را جدی می‌گیرند، ولی از طرفی دولت کشور خودشان در تلاش است تا مشکلی در محصولات آنها پیدا کند تا اطلاعاتی را از دولت‌های خارجی بدست بیاورد.

این فقط آمریکا و روسیه نیستند که در این حوزه فعالیت می‌کنند، اکنون در سراسر جهان اکثر کشورها برای نفوذ به راه های ارتباطی دیگر کشورها یا مردم در حال جمع‌آوری اطلاعات هستند، برخی از این کشورها مثل چین از این اکسپلویت‌ها برای جاسوسی از مردم خودشان استفاده می‌کنند، و برخی نیز مانند کره شمالی برای کسب درآمد از طریق سرقت از بانک‌ها و توسعه باج‌افزار در جهان استفاده می‌کنند. این امر زندگی انسان‌ها را ناامن میکند در حالی که هدف اولیه‌ی رونق این موارد افزایش امنیت بود.

منابع

This Is How They Tell Me the World Ends: The Cyberweapons Arms Race