مدافعان

» منبع: نیوساینتیست » ترجمه: احمدشریف‌پور

چه کسی از پول، هویت و رازهای شما در برابر هکرهایی که قصد سرقت آن‌ها را دارند، محافظت خواهد کرد؟ ریچارد فیشر به گروهی از افراد خوش‌بین و امیدوار پیوسته تا ببیند، آیا آن‌ها آمادگی‌پذیرش چنین وظیفه‌ای رادارند یا خیر؟

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

۵ مارس ۲۰۱۱ ساعت ۱۰:۵۹:۵۹

زمان باقی مانده ۰۰:۵۰:۰۰

در تالاری ساکت و بدون پنجره در بریستول (غرب انگلستان)، لوسی رابسون و تیمش روی لپ‌تاپ‌هایشان خم شده بودند و این در حالی بود که ثانیه‌ها در همان زمان روی ساعت بزرگی که بالای سرشان قرار داشت، در حال شمارش معکوس بود. تا چند لحظه دیگر دشمن حمله بزرگ خود را آغاز می‌کرد. اما این مهاجمان از طریق درها و راه‌های ورودی معمول وارد نمی‌شدند. رابسون، در حال رقابت در فینال مسابقات امنیت سایبری انگلستان (UK Cyber Security Challenge) بود که در آزمایشگاه‌های اچ‌پی در بریستول برگزار می‌شد. شرکت‌کنندگان که اغلب نوجوان و برنامه‌نویسان مبتدی بودند، همه از خارج از دایره حرفه‌ای صنایع امنیت سایبری انتخاب شده بودند. هدف از برگزاری این مسابقات یافتن نسل جدیدی از افراد بود که مهارت‌های لازم را برای نبرد با تاریک‌ترین عناصر دنیای آنلاین داشته باشند. توانایی مقابله با هکرهایی که اسرار دولتی را به سرقت می‌برند، فعالیت‌های ناشناخته‌ای که باعث واردشدن خسارت می‌شوند و مجرمانی که به سرقت کارت‌های اعتباری می‌پردازند.

رگ‌های این صنعت به خون تازه نیاز دارد، زیرا طبیعت تهدیدها تغییرکرده است. مارتین سادلر کارمند آزمایشگاه‌های اچ‌پی می‌گوید: «پنج تا ده سال پیش، شما باید در برابر کودک باهوشی می‌ایستادید که سعی می‌کرد، صفحه اصلی یک سایت را به هم بریزد.» ناکام گذاشتن چنین حمله‌های نه چندان پیچیده، زمانی کار به نسبت آسانی بود، اما آن روزها دیگر گذشته است. هکرهایی را که چندی پیش به شبکه پلی‌استیشن سونی نفوذ کردند، در نظر بگیرید. آن‌ها به سادگی از تمام موانع امنیتی یکی از بزرگ‌ترین شرکت‌های الکترونیک دنیا گذشتند و اسامی، نشانی‌ها و به‌احتمال شماره کارت‌های اعتباری یک‌صد میلیون نفر را به سرقت بردند. پول‌های بادآورده به انگیزه‌ای برای شیطنت و سرگرمی هکرها تبدیل شده است. براساس اعلام دفتر دولتی جرائم سایبری و محافظت اطلاعات انگلیس، جرائم سایبری و مواردی نظیر سرقت کارت‌های اعتباری و جاسوسی صنعتی، به تنهایی سالانه ۲۷ میلیارد یورو به انگلستان خسارت وارد می‌کنند. این قضیه در بقیه نقاط دنیا نیز چندان متفاوت نیست.

در همین دوره، شکل جدیدی از فعالیت‌های غیرقانونی آنلاین که رهبران آن گروهی با نام «ناشناس» (Anonymous) هستند، رشد کرده که سایت‌ها را فلج کرد و اسرار دولتی و صنعتی را به سادگی افشا می‌کنند. یکی از داوران مسابقات امنیت سایبری می‌گوید: «ناشناس، گروهی متشکل از افراد معین و مشخصی نیست که به سراغ آن‌ها رفته و دستگیرشان کنید.» این نام در واقع پوششی برای اعضای دائم در حال تغییر و غیر رسمی است که ممکن است برای یک سال یا تنها سه ساعت فعال باشند. او می‌افزاید: «یکی از این اعضا ممکن است، مدیر یک بانک باشد که تصمیم می‌گیرد برای یک روز آدم بدی باشد. شما نمی‌توانید به سادگی در خیابان به صورت کسی سیلی بزنید، اما در وب می‌توانید.»

درحالی‌که تنوع، انگیزه و هوش مجرمان به صورت نمایی رشد کرده است، مدافعان برای حفظ توانایی خود در این میدان در حال تلاش هستند. دانش فنی محض، دیگر به تنهایی جواب‌گو نخواهد بود. متخصصان کنونی امنیت سایبری به شدت نیازمند ارتقای دانش و توانایی‌های خود هستند. مسابقات امنیت سایبری، را اگر عملی از روی ناچاری ندانیم، خواهیم پذیرفت که فعالیتی لازم است.

سال گذشته چهار هزار نفر به امید انتخاب‌شدن به عنوان قهرمان نهایی امنیت سایبری در این مسابقات ثبت‌نام کردند. امروز و بعد از طی چندین مرحله رقابت فرسایشی، تنها سی نفر از آن‌ها باقی مانده‌اند. شرکت در دوره‌های گران‌قیمت آموزشی و کارورزی از جوایز برندگان این مسابقات خواهدبود. اما بیشترین سود نصیب حمایت‌کنندگان این مسابقات خواهد شد.

حمایت‌کنندگانی نظیر شرکت امنیتی سوفوس، کینتیک (Qinetiq) پیمانکار امور حفاظتی و آزمایشگاه دولتی علوم و فناوری دفاعی انگلیس که به این مسابقات به دید یک عملیات اکتشافی (کشف استعدادهای تازه) نگاه می‌کنند.

شرکت‌کنندگان پیش از این و در مراحل قبلی، دستورات خود را از مدیرعامل و مدیران فرضی یک شرکت تولیدی خیالی به نام Metal Box دریافت‌کرده‌اند. وظیفه امروز آن‌ها تأمین امنیت شبکه و سایت شرکت است، سپس آن‌ها به چند گروه با نام‌هایی نظیر انیگما، تورینگ و بامبی تقسیم خواهند شد.

آن‌ها آماده شروع نخستین تمرینات امروز هستند که توانایی‌های فنی، مهارت‌های فردی و کار تیمی آن‌ها را مورد آزمایش قرار خواهد داد. پس از آن داوران دو جایزه را، یکی به تیم برنده و دیگری به بهترین فرد شرکت کننده، اهدا خواهند کرد. شرکت‌کنندگان این مرحله شامل یک هنرپیشه حرفه‌ای، یک خوره کامپیوتر که موهایش را تا روی شانه‌هایش بلند کرده است،

یک پستچی از شمال انگلستان و رابسون هفده ساله تنها دختر این دوره از مسابقات هستند که در تیم انیگما به مبارزه خواهند پرداخت.

رابسون امنیت شبکه را به تنهایی و با مطالعه ویکی‌پدیا و کتاب‌هایی آموخته است که با پولی که از یک کار پاره‌وقت در یک سوپرمارکت، پس‌انداز شده بودند، خریداری کرده‌بود. او می‌گوید: «اگر این مسائل بر زندگی من تأثیر می‌گذارد، می‌خواهم بدانم که چگونه کار می‌کنند.» او همراه با پدرش (یک نصاب کفپوش) و مادرش (یک حسابدار ارشد دارای پروانه) در کرامر، شهری کوچک در سواحل شرقی انگلستان زندگی می‌کند. رابسون درمورد مادرش می‌گوید: «مطمئن باشید که "ارشد" و "دارای پروانه" از قلم نیفتد. چون خیلی مهم است.» او طوری صحبت می‌کند که انگار هر کلمه را پیش از گفتن پردازش می‌کند. موهای تیره و کوتاه او روی یقه یک لباس خاکستری و یک شال‌گردن مدروز ریخته است. سایر شرکت‌کنندگان تی‌شرت و شلوار جین پوشیده‌اند. رابسون به همراه دو دوستی که در طول دوره تابستانی کامپیوتر مدرسه ملاقات کرده بود، در این مسابقات شرکت کرد. تیم آن‌ها از شروع مسابقات تا مرحله پایانی خوش درخشیده بود و توانسته بودند مشکلات شناخته شده یک کامپیوتر خانگی را شناسایی و برطرف کنند. استوارت رنی دوست لوسی می‌گوید: «ما به واسطه لوسی است که به این مرحله رسیده‌ایم. کار او حرف نداشت.» اما امروز رنی در تیم بامبی قرار گرفته است که باید با تیم لوسی رقابت کند.

ساعت ۱۱ است و حمله قرار است که شروع شود. عملیات مورد نظر شناسایی و مقابله با مجموعه‌ای از نفوذگران است که می‌خواهند به شبکه کامیوتری شرکت متال‌باکس نفوذ کنند. تیم‌ها هر یک در گوشه‌ای از تالار دورهم جمع شده و به‌وسیله موانعی از یکدیگر جدا شده‌اند. انتهای کابل‌هایی که به لپ‌تاپ‌های آن‌ها متصل است در لابه‌لای توده‌ای درهم از سیم‌ها و کابل‌ها در زیر میزی در همان نزدیکی گم می‌شود. این میز همان جایی است که برگزارکنندگان این رقابت به ریاست اندرو لایرد از کارمندان شرکت امنیتی کاسیدیان (Cassidian) مستقر در بریستول، به رهبری عملیات مشغول هستند. این تمرین روی شبیه‌ساز نرم‌افزاری به نام هات‌سیم Hotsim (سرنام

نفوذ به یک شبکه

راه‌های بسیاری برای از کار انداختن، دسترسی به اطلاعات یا نفوذ به یک شبکه وجود دارد؟ یک مدافع باید تمام این راه‌ها را بشناسد.

Hands on Training Simulator) انجام می‌شود که توسط کاسیدیان ساخته شده و به اندازه‌ای پایدار و قدرتمند است که می‌تواند دوره‌های آموزشی امنیت سایبری در ارتش‌های برزیل و فنلاند را مدیریت کند. هات‌سیم تمام ترافیک‌های روزمره‌ای را که از شبکه یک شرکت بزرگ انتظار می‌رود، بازسازی می‌کند. با بازسازی ترافیک‌هایی نظیر مرور وب توسط کارمندان، پیغام‌رسان‌های اینترنتی و تبادل ایمیل‌ها، نمایشگرهای لپ‌تاپ‌های تیم‌های شرکت‌کننده دقیقاً همان چیزی را نشان خواهد داد که تیم امنیت IT یک شرکت واقعی با آن روبه‌رو هستند.

تیم‌های شرکت‌کننده این ترافیک مجازی را برای یافتن نشانه‌های نفوذ بررسی می‌کنند. آن‌ها برای این کار از برنامه‌های استانداردی که فعالیت کارمندان را نشان می‌دهند، یک سیستم تشخیص نفوذ و یک فایروال برای اجتناب از تهدیدات خارجی استفاده می‌کنند. یک محافظ امنیت سایبری ماهر می‌داند که چگونه این ابزارها را برنامه‌ریزی کند تا حمله‌ها را تشخیص داده و آن‌ها را ناکام بگذارد. اگر شرکت‌کنندگان بتوانند این سه ابزار را (برنامه کنترل فعالیت کارمندان، سیستم تشخیص نفوذ و فایروال) مدیریت کنند، می‌توانند جلوی نفوذ را بگیرند.

اما تیم انیگما شروع بدی داشت و این تنها چند دقیقه پیش از نخستین نشانه‌های دردسر بود: دشمن علمیات اسکن پورت‌ها را شروع کرده است. پورت‌ها راه‌های نفوذ به شبکه هستند.

به مجموعه‌ای از شریان‌های ارتباطی فکر کنید که در داخل یک شهر گسترده شده‌اند و صدها یا هزاران مسیر مختلف را برای وسایل نقلیه متفاوت و به مقصدهای مختلف فراهم می‌کنند. به همین شکل، یک شبکه چندین هزار مسیر مجزا به نام پورت دارد که ترافیک از طریق آن منتقل می‌شود.

براساس قرارداد، ترافیک مرورگرها به طور معمول به پورت شماره هشتاد سرور وارد می‌شوند و ایمیل‌ها به پورت ۲۵ هدایت می‌شوند. نفوذگران احتمالی در تلاش برای یافتن ضعف‌هایی موجود در امنیت شبکه، هزاران نمونه از این پورت‌ها را اسکن می‌کنند. اما در نخستین تلاش‌هایشان برای امن‌کردن محیط شبکه، نه رابسون و نه هیچ یک از هم‌تیمی‌هایش متوجه این قضیه (شروع عملیات اسکن پورت) نشدند.

مسئول کنترل ترافیک عبوری از روتر شبکه، تونی شانون پسری ۲۸ ساله، چهارشانه، با اعتماد به نفس و ابروهای سوراخ شده بود. بعد از چند سال تجربه در صنعت IT، او دوباره برای تحصیل در رشته امنیت کامپیوتر در دانشگاه ترنت ناتینگهام ثبت‌نام کرده است. سبک و رفتار شانون اصلاً شبیه رابسون نیست. او تصور می‌کند که به‌وسیله جمله‌بندی‌های عجیب و غریب و خودنمایانه می‌توان داوران را تحت‌تأثیر قرار داد.

هنگامی که اوضاع شروع به خراب شدن می‌کند، او می‌گوید: «ما نابود شدیم، داریم مثل یک صندلی تاشوله می‌شویم.» و تیم واقعاً در برابر این حمله در حال له‌شدن بود و شانون، به‌رغم تمام گزافه‌گویی‌هایی که در گذشته کرده بود، هیچ کاری نمی‌توانست انجام دهد. عصبانیت در صدایش موج می‌زد.

> **سندی که کلمه «محرمانه» در محتویات آن وجود داشته باشد همانند نشانه‌ای است که به بدافزار می‌گوید: «هی، من چیز جالبی هستم.»**

زمان باقی مانده ۰۰:۳۱:۲۰

ظرف بیست دقیقه، سایت شرکت متال‌باکس هک شد. یک پیام ساده جایگزین صفحه اصلی سایت شده بود: "Pwned by /b" و پس از آن دنباله‌ای از حروف لاتین. و هنگامی که شما pwn (گرفتار) شوید، کار شما تمام است. این یکی از اصطلاحات دنیای اینترنت است.

تیم انیگما سعی می‌کند، صفحه خانگی را بازگرداند، اما یک نکته اساسی را فراموش‌کرده‌است: اگر آن‌ها ندانند که حمله‌کنندگان چگونه نفوذکرده‌اند، اصلاحات انجام شده توسط آن‌ها موقتی خواهدبود. تحقیقات بعدی نشان داد، هکرها از شیوه نفوذ با تزریق کد SQL استفاده‌کرده‌اند. SQL زبانی است که برای استخراج اطلاعات از یک پایگاه داده توسط سایت‌ها به‌کار برده می‌شود. بسیاری از خرده‌فروشان آنلاین برای به‌روزرسانی بی‌درنگ مجموعه محصولاتی که نمایش می‌دهند و ذخیره مشخصات خریداران از چنین پایگاه‌های داده‌ای استفاده‌می‌کنند. SQL استخراج چنین اطلاعاتی را خودکار ساخته و از این طریق زندگی را برای طراحان وب ساده‌تر می‌کند. اما اگر سایت‌ها بد طراحی شده باشند، هکرها می‌توانند از SQL علیه خودش استفاده کنند و با نفوذ به پایگاه داده اطلاعاتی را به سرقت ببرند. فرم‌هایی را درنظر بگیرید که در سایت‌ها برای واردکردن نام، آدرس و مشخصات کارت اعتباری به کار می‌روند. هر یک از این موارد می‌تواند دری احتمالی به قلمرو داخلی یک سایت بگشاید.

تیم انیگما تصور می‌کرد، حمله‌کننده از طریق یکی از این فرم‌ها و با واردکردن کدهای آلوده، یک پرس‌وجوی نادرست عمدی را به پایگاه داده ارسال‌کرده است. سایت بدساخت شرکت متال باکس نتوانست این پرس‌وجو را متوقف کند. این امر به هکر اجازه داد سایت را مجبور کند، اطلاعاتی را که قرار بود داده‌های مخفی پایگاه‌های داده باشند، آشکار کند. شاید این روشی بود که از طریق آن هکر موفق به سرقت رمز عبوری شده بود که بعدتر برای عوض کردن صفحه اصلی سایت به کار رفته بود.

زمان باقی مانده ۰۰:۱۳:۱۹

موضوع داشت جدی می‌شد. تا حالا حمله‌ها تنها یک سری خرابکاری‌های معمول بودند، اما اکنون هکرهای متال باکس قطعه بدافزار ویژه‌ای را به شبکه وارد کرده بودند که کلمات عبور، قراردادهای مالی و داده‌های شخصی حساس را ردیابی و سرقت می‌کرد. یافتن چنین داده‌هایی برای یک بدافزار بسیار ساده خواهد بود. به گفته لایرد «هر ایمیل یا سندی که در بالای آن کلمه «محرمانه» به چشم بخورد، همانند نشانه‌ای است که به بدافزار می‌گوید: هی! من چیز جالبی هستم.»

آن‌گونه که از نشانه‌ها برمی‌آمد، بدافزار در حال قطعه‌قطعه‌کردن اسناد به اجزای بسیار کوچک و رمزگذاری آن‌ها بود. بدافزار برای این‌که بتواند بدون جلب توجه اطلاعات سرقت

جرائم مجازی، دنیای واقعی

سال ۲۰۲۰ است. شما در محله‌ای ناشناس گم شده‌اید، زیرا می‌خواستید از ازدحام راه‌های اصلی فرار کنید. اما اصلاً نگران نیستید: زیرا سیستم ناوبری ماشین‌تان شما را به مسیرهای خلوت و درست هدایت خواهد کرد. سیستم ناوبری که با میلیاردها حسگر تعبیه شده، در مسیرها ارتباط برقرارمی‌کند که این حسگرها از به‌وجودآمدن گره‌های ترافیکی جلوگیری می‌کنند. اما آیا می‌توانید به سیستم ناوبری ماهواره‌ای اعتماد کنید؟ اگر هکرها می‌توانند به یک سایت نفوذ کنند، به طورحتم می‌توانند در کار این شبکه‌های حسگر هم تداخل ایجاد کرده و باعث راهنمایی‌های اشتباه در مقیاس شهری شوند. ماشین‌ها برای تصادف با یکدیگر به جایی هدایت می‌شوند؛ شاید در انتهای یک خیابان دورافتاده، یعنی جایی که کسی منتظر است تا از شما سرقت کند. اگر این سناریو به نظر شما غیرممکن است، در نظر داشته باشید که میلیاردها حسگر متصل به هم، به زودی در شهرها و املاک ما نصب خواهند شد که انبوهی از اطلاعات را در مورد شما و محیط اطرافتان تولید خواهند کرد. چندین گیگابایت از داده‌های حساس در سراسر آنچه‌که «اینترنت اشیا» (Internet of Things) نامیده می‌شود، سرگردان خواهد بود؛ شبکه‌ای جهانی از اشیای متصل به هم که به‌صورت پیوسته تحت نظارت و بررسی خواهند بود.

مارتین سادلر از آزمایشگاه‌های اچ‌پی در برستول انگلستان می‌گوید: «دنیای حسگرها مشکلات جدیدی را به‌وجود خواهد آورد.» او در ادامه می‌افزاید: «چنین دنیایی به وضوح به نوع جدیدی از نگهبانان نیاز خواهد داشت تا از افتادن کنترل آن به دستان خرابکاران جلوگیری کنند. زمان آن رسیده که آموزش نسل جدید محافظان سایبری را آغاز کنیم.»

شده را بیرون بکشد، تمام این اجزای کوچک را در پیام‌هایی که به پرس‌وجوهای DNS معروف هستند، مخفی می‌کرد. به‌طور معمول، چنین پرس‌وجوهایی معمولاً هر زمان که کسی به سروری در خارج از شبکه متصل شود، ارسال خواهند شد.

هنگامی که شما مثلاً به دنبال سایت نیوساینتیست می‌گردید، مرورگر شما تقاضایی را برای سروری ارسال می‌کند که این آدرس اینترنتی متنی را به یک آدرس واقعی که دنباله‌ای طولانی و غیرقابل حفظ کردن از اعداد است، ترجمه می‌کند. چون این پرس‌وجوها بخش عظیمی از ترافیک معمول وب را به یک شبکه داخلی به‌وجود می‌آورند، به آسانی و بدون برانگیختن حساسیت می‌توان بیت‌های اطلاعات اضافی (سرقت شده) را در داخل آن‌ها مخفی کرده و بیرون از شبکه انتقال داد.

به همین دلیل، بدافزار می‌تواند به سادگی قطعات رمزگذاری شده اسناد را در قالب هزاران پرس‌وجوی DNS خارجی ارسال کند. هنگامی که آن‌ها به سلامت از شبکه خارج شدند، حمله‌کننده می‌تواند به سادگی آن‌ها را دوباره در مقصد سرهم کرده و به اسناد اصلی دست یابد. به این نوع حمله استخراج از طریق DNS می‌گویند.

دولت امریکا تخمین می‌زند که استخراج از طریق DNS تاکنون باعث خروج بیش از بیست ترابایت داده از شبکه‌های دپارتمان‌ها و آژانس‌های دولتی امریکا شده باشد، اما چون سارقان اطلاعات سرقت شده را رمزگذاری می‌کنند، به سختی می‌توان گفت که چه چیزهایی به سرقت رفته است. لایرد می‌گوید: «آن‌ها نمی‌دانند که این داده‌ها چه بوده‌اند یا به کجا منتقل شده‌اند.» و این یک سرقت بی عیب و نقص است.

تیم انیگما نتوانست این نفوذ را ردگیری کند و شرکت متال باکس در حال از دست دادن داده‌ها است: تا کنون دو هزار سند از طریق شبکه به بیرون منتقل شده‌اند. رابسون، که اغلب آرام و خونسرد است، هراسان به نظر می‌رسد و با عجله جزئیات این حمله را ثبت می‌کند. در همین حین بقیه سعی دارند بفهمند که چه اتفاقی در حال رخ دادن است. تالار بدون در و پنجره و مملو از فریادهای اعضای تیم‌ها آکنده از بوی عرق شده است. زمانی که تیم از طریق DNS به سرقت پی برد، دیگر خیلی دیر شده بود.

زمان باقی مانده ۰۰:۰۲:۵۸

حمله‌کنندگان هات‌سیم، دسترسی تمام کارمندان متال باکس، حتی اعضای تیم امنیتی را به حساب‌هایشان مسدود کرده‌اند. اگر شما سه بار کلمه عبوری را اشتباه وارد کرده باشید و دسترسی شما به حسابتان قفل (مسدود) شده باشد، می‌دانید که این وضعیت چگونه است. چنین حمله‌ای معمولاً پوششی برای یک حمله بزرگ‌تر است، اما امروز این دیگر پایان راه است.

رئیس مسابقات لایرد دستور می‌دهد: «دست‌هایتان را از روی صفحه‌کلید بردارید.» اعضای تیم به صندلی‌هایشان تکیه می‌دهند و گیج و سرگردان به نظر می‌رسند. رابسون می‌گوید: «سرم درد می‌کند.» و شانون به ساعت خیره شده است.

رابسون، شانون و سایر اعضای تیم برای نخستین‌بار آنچه را که افراد تیم‌های امنیتی با آن روبه‌رو هستند، تجربه کرده‌اند. در تمام دنیا، متخصصان امنیت سایبری تحت فشار قرار دارند. آن‌ها هیچ‌گاه نمی‌دانند که حمله بعدی کی و چرا صورت خواهد گرفت.

۶ مارس ۲۰۱۱، ساعت ۱۳:۳۰:۰۰

ترتیب دهندگان مسابقات در آستانه اعلام نتایج و معرفی برندگان در جشن پایانی مسابقات هستند که در بریستول و در محلی جذاب‌تر از آن تالار برگزار می‌شود. امروز یک‌شنبه‌ای سرد و لذت‌بخش است و تلألو خورشید روی جام‌ها و قاشق و چنگال‌ها چشم را خیره می‌کند.

تیم انیگما جایزه بزرگ را نبرده و این جایزه نصیب تیم بامبی شده است که برنده انفرادی، یعنی دن سامرز پستچی نیز جز همین تیم است. اما تیم انیگما روحیه خوبی دارد.

روی صحنه تالار، رابسون جایزه‌ای را به‌واسطه عملکرد مناسبش تا رسیدن به مرحله فینال دریافت می‌کند: امکان شرکت در دوره کارآموزی امنیت دیجیتال در شرکت کینتک. حتی شانون هم در وضعیت خوبی به سر می‌برد.

او که برنده یک دوره آموزشی شده است، می‌گوید: «از امشب دیگر در خواب دندان قروچه نخواهم کرد.» هنگامی که مراسم در سالن رو به اتمام است، رابسون بیرون سالن در حال نوشتن یک پیام کوتاه روی موبایلش است. سال آینده او در دانشگاه در رشته علوم کامپیوتر تحصیل خواهد کرد و شاید هم یک سال استراحت کند.

در همین هنگام، کسی در جایی، به مجموعه کابل‌های درهم تنیده، پردازنده‌ها و سرورهایی که در سراسر دنیا به هم وصل شده‌اند، متصل خواهد شد که به یقین اهداف تاریکی را در سر می‌پرورد.