به‌نام ایزد یکتا

شمارش از صفر

داستان واقعی یک حمله روز صفر

Counting from Zero

By:

ALAN B. JOHNSTON

ترجمه:

مهندس محسن مصطفی جوکار

انتشارات پندار پارس

سرشناسه	:	جانستون، آلن بی. Johnston, Alan B.
عنوان و نام پدیدآور	:	شمارش از صفر : داستان واقعی یک حمله روز صفر/ آلن‌بی. جانستون ؛ ترجمه محسن مصطفی جوکار.
مشخصات نشر	:	تهران : پندار پارس، ۱۳۹۵.
مشخصات ظاهری	:	۲۷۰ ص.
شابک	:	۹۷۸-۶۰۰-۸۲۰۱-۰۴-۵ : ۱۹۵۰۰۰ ریال
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	عنوان اصلی: .Counting from zero, ۲۰۱۱
عنوان دیگر	:	داستان واقعی یک حمله روز صفر.
موضوع	:	داستان‌های انگلیسی -- قرن ۲۰م.
شناسه افزوده	:	مصطفی جوکار، محسن، مترجم
رده بندی کنگره	:	۱۳۹۵ ۸ش۲ج/PZ۳
رده بندی دیویی	:	۸۲۳/۹۱۴
شماره کتابشناسی ملی	:	۴۱۸۷۳۸۸

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸همراه: ۰۹۲۱۴۳۷۱۹۶۴ **info@pendarepars.com**

نام کتاب	:	**شمارش از صفر، داستان واقعی یک حمله روز صفر**
ناشر	:	**انتشارات پندار پارس**
تالیف	:	ALAN B. JOHNSTON
ترجمه	:	**محسن مصطفی جوکار**
چاپ نخست	:	**فروردین ماه ۹۵**
شمارگان	:	**۵۰۰ نسخه**
صفحه‌آرایی و ویراستاری	:	**مصطفی مصباحی**
چاپ، صحافی	:	**روز**
قیمت	:	**۱۹۵۰۰ تومان** **شابک : ۵-۰٤-۸۲۰۱-٦۰۰-۹۷۸**

تقدیم به

sYRQ6tKaYHkFcxJy7CMQLOoC0Q/WFoR8Onek2BBiZUY=

فهرست

مقدمه مترجم

در این داستان شخصی با نام میک اومالی که یک هکر و مختصص امنیت است با یک حمله روز صفر درگیر می‌شود و تلاش می‌کند منشا این حمله و سازندگان آن را پیدا کند. در طول این داستان برای میک اومالی اتفاق‌های جالبی می‌افتد و نویسنده کتاب تلاش کرده است که مصاحبه‌های او با یک مجله مربوط به امنیت را برای خوانندگان کتاب، آموزنده کند و به نوعی عشق را هم در داستان درگیر کند. داستان به گونه‌ای مبهم است و خواننده باید تکه‌ها را در کنار هم بگذارد و درنهایت هم سورپرایز خواهد شد. این کتاب به خطرات ناشی از بات‌نت‌ها و جدی گرفتن آن‌ها در دنیای اینترنت می‌پردازد و از سویی، نگاهی به کسب و کار تاریک در این زمینه می‌اندازد. کسانی که از تولید این بدافزارها پول‌های زیادی به جیب می‌زنند و از حملات روز صفر برای کسب درآمد و نه کمک به دنیای امنیت استفاده می‌کنند. میک اومالی داستان ما در طول خنثی کردن این روز صفر از سوی افراد مختلف تهدید می‌شود و سرانجام برای خنثی کردن این روز صفر به فکر در میان گذاشتن موضوع با دولت می‌افتد، اما در کمال ناباوری دارایی‌اش از سوی دولت مسدود و ممنوع الپرواز می‌شود. در نهایت میک اومالی به این نتیجه می‌رسد که پشت تمام این قضایا خود دولت‌ها قرار دارند و...

پیش گفتار

کد مخرب[1] برای آخرین بار کامپایل شده بود و برای آزمایش آماده بود.

مرد جوان نرم‌افزار را در کامپیوترش بارگذاری و به صورت تصادفی یک هدف را انتخاب کرد و سپس کلید ارسال را زد. او به تماشای نتیجه این کار نشسته بود.

در یک جای دور در دنیا، یک بسته اطلاعاتی از اینترنت بدون سر و صدا بر روی یک پورت فیلتر نشده وارد شده است. این بسته، از یک پروتکل که به ندرت استفاده می‌شود به طور موثر و عملی استفاده می‌کرد و به نظر می‌رسید که یک درخواست بی خطر باشد. با این حال، در پایان درخواست، این چیز کاملا متفاوتی بود: یک پیام به دقت دست کاری و قالب بندی شده که پس از آن منجر به اجرای خودکار یک کد می‌شد.

هیچکس از کامپیوتر استفاده نمی کرد – کامپیوتر به سادگی روشن و به شبکه متصل شده بود. برنامه پست الکترونیکی و یک مرورگر در حال اجرا بودند اما هیچکس به آنها نگاهی نمی‌کرد. صفحه نمایش برای صرفه جویی در مصرف برق خاموش شده بود. ناگهان، یک فرایند جدید بر روی کامپیوتر شروع به اجرا شدن کرد و در نتیجه یک بسته اطلاعاتی به سیستم وارد شده بود. یک فایل باینری شروع به دانلود شدن کرد و هنگامی که به پایان رسید، یک برنامه جدید را اجرا کرد.

این برنامه به عنوان یک مسافر که به کشور جدیدی رفته بود، شروع به نگاه کردن به اطراف و بررسی محل‌های جدید در سیستم می‌کرد، برنامه جست‌وجوی خود را شروع کرده بود. آن از تمام قابلیت‌های کامپیوتر، یک لیست تهیه کرده بود که ناچیز بودند. پردازنده با گیگاهرتز پایین که بسیار قدیمی بود و در حال اجرای یک سیستم عامل تجاری رایج و کد بسته بود. کامپیوتر به اندازه کافی حافظه داشت و یک دیسک سخت کوچک هم داشت اما برای برنامه‌ای که دانلود آن آغاز شده بود این دیسک سخت کوچک مقدار زیادی فضا داشت.

پس از اتمام دانلود، کار واقعی شروع شد. برنامه دوم به سراغ بررسی دقیق رکوردهای کامپیوتر رفت و همه نشانه‌های مربوط به فعالیت‌های اخیر خود را پاک کرد. این یک گزارش را به منبع فرستاد. این برنامه هر زمان که کامپیوتر روشن می‌شد، به صورت خودکار و مخفی خود را اجرا می‌کرد. موجودیت کلی آن از نظر پنهان بود.

مرد با پیام فرستاده شده بر روی موبایلش سردرگم شده و متوجه نشده بود که آیا این نخستین پیام فرستاده شده است یا خیر. او شروع به نگاه کردن به جزئیات کرد تا ببیند که چه اتفاقی افتاده است.

---

[1] Exploit

نخستین "زامبی" که شکار بزرگی نبود. به نظر نمی‌رسید که شامل هرگونه اطلاعات مخصوص و با ارزش و یا متعلق به شخص مهمی باشد. قابلیت‌های آن در بهترین حالت ناچیز بود – ظاهرا به سختی ارزش تلاش برای خطر کردن را داشت. این کامپیوتر احتمالا تنها یک سیستم در اتاق نشیمن یا اتاق خواب کسی بود اما هم اینک به طور کامل تحت کنترل او است!

با توجه به تعداد افراد دیگر در لیست، او از موفقیت خود احساس رضایت می‌کرد. او می‌دانست که تنها تعداد انگشت شماری از مردم در جهان تخصص شناسایی این کد مخرب را دارند چه برسد بخواهند در برابر آن از خود دفاع کنند.

سپس خلاصه‌ای از آمار فعالیت را برای بررسی میزان انتشار این برنامه مخرب خواند و از هیجان زیاد نزدیک بود که از صندلی به پایین بیافتد.

هم اکنون، کد او تنها در عرض یک ساعت در حدود 123,412 کامپیوتر را در سراسر جهان آلوده کرده بود! با انجام کمی محاسبات از این نتیجه شگفت زده شده بود. کارهایی که می‌تواند با این همه کامپیوتر به صورت هماهنگ در سراسر جهان انجام شود...

تصمیم به ایجاد یک تغییر در کد کرد و چیز دیگری به آن اضافه کرد. یک هرزنامه بر روی صفحه نمایش ظاهر شد، با خونسردی به آن نگاه کرد و بدون هیچ فکری آن را حذف کرد.

سپس یک نام مستعار را به کد خود اضافه کرد : nØviz

بخش نخست

فصل صفر

یک ماه بعد...

میک اومالی – در مقایسه با قبل اکنون احساس راحتی بیشتری در یک خانه در ژاپن می‌کنم. (Ø نظر)

سرعت، نسبی است و سرعت اینترنت نیز به همین صورت است، میک اومالی همانطور که با سرعت 2Ø3 کیلومتر در ساعت در حال مسافرت بود به اینترنت با سرعت 4 Mb/s دسترسی داشت. این سرعت برای یک هواپیما کم بود اما برای یک وسیله نقلیه در جاده بسیار زیاد است اما با این وجود میک با یکی از موتورسیکلت‌های دوکاتی خود سریعتر از این سرعت را هم رفته بود. این برای یک قطار نیز زیاد بود مگر اینکه قطار از نوع Shinkansen باشد که میک هم اینک از توکیو سوار آن شده بود. او می‌دانست که قطار شروع به حرکت می‌کند و به زودی با سرعت بیشتری به راه خود ادامه خواهد داد.

میک نوشتن یک مطلب در بلاگ را تمام کرده بود و آن را در کسری از ثانیه به سرور خود آپلود کرد. این سرعت برای یک شبکه محلی سیمی کند بود اما برای یک شبکه بی سیم تلفن همراه سریع بود. این سرعت برای میک به عنوان کسی که از اینترنت بی سیم با سرعت بالا در سفرهای خود به دور دنیا استفاده می‌کرده، در حد معمولی بود. او نمی توانست زندگی بدون تلفن همراه خود که با چند فرکانس رادیویی کار می‌کرد را تصور کند.

میک غرق در افکار خود در مورد فرایند تبدیل شدن به یک فرد متخصص بود که ناگهان توسط یک احساس سوزن سوزن شدن در پشت گوش سمت راستش از این فکر بیرون پرید؛ این مربوط به هشدار

میکروفون بی سیمی بود که در پشت گوش خود گذاشته بود. یکی از دوستان دوره دانشجویی میک بود که این نمونه اولیه را در اختیار او قرار داد تا این تکنولوژی زیرپوستی را آزمایش کند و میک مشتاقانه آن را برای امتحان پذیرفت. کیفیت صدا بسیار عالی بود و هیچ نگرانی در مورد عدم وجود سیم وجود نداشت. این یک دستگاه بود که به هیچ منبع انرژی برای فعالیت خود نیاز نداشت [1] و تنها در صورت نیاز، تلفن همراه را به صورت بی سیم شارژ می‌کرد. او حتی می‌توانست با استفاده از این پیاده سازی، از فرامین صوتی برای شماره گیری و پاسخ به تماس ها استفاده کند اما این دامنه استفاده محدود بود. از زمان قرار دادن آن بر روی پوستش حتی یک تماس از دست رفته هم نداشت.

پیامی که از شبکه اجتماعی آمده بود به میک می‌گفت که دوست او با نام لارس وارد هیروشیما شده است و از یک صبحانه شخصی و البته به جز برنج بخارپز در حال لذت بردن است. میک برخی از وعده‌های غذایی عجیب و غریب و معماگونه که در بازدید پیشین خود از ژاپن [2] از آنها لذت برده بود را به یاد آورد. لارس مسیر GPS مربوط به دیروز خود را پست کرده بود که یک قطار با سرعت 3Ø1 km/h را نشان می‌داد که هر کسی به جز او شهامت سوار شدن آن را نداشت. میک اخم کرده به تلفن همرا خود نگاه کرد –بالاترین سرعتی که او طی کرده تنها 279 km/h بود.

بیرون از پنجره، حومه شهر با سرعت زیاد و به صورت پشت سرهم در حال طی شدن بود.

میک به خود لبخندی زد و به هفته هیجان انگیز پیش رو فکر می‌کرد. او در راه رفتن به یک کنفرانس امنیتی مربوط به اینترنت در هیروشیما بود؛ بهترین دوستان او از سراسر جهان در آنجا جمع شده بودند.

میک به عنوان یک "متخصص" امنیت در نظر گرفته شده بود؛ هرچند او از این واژه نفرت داشت و دلیلش این نبود که این واژه از او یک فرد با دانش بالا را می‌ساخت. با وجود اینکه او تنها ۲۴ سال داشت، تعداد کمی از افراد وجود داشتند که در مورد کامپیوتر و امنیت اینترنت بیشتر از او بدانند، اما روشن‌فکری؟

قطار تغییر مسیر می‌داد و میک از اینکه شتاب مورد انتظار را در بدن خود احساس نمی‌کرد متعجب شده بود. او حدس می‌زد که مسیر باید شیبدار شده باشد و به همین دلیل یک جست‌وجوی سریع اینترنتی را انجام داد که تایید می‌کرد مسیر ده درجه شیبدار شده است. تلفن همراه میک فوق العاده قدرتمند بود، با داشتن قدرت محاسباتی بالا و شبکه، از بیشتر کامپیوترهای رومیزی قدرتمندتر بود. کامپیوتر رومیزی او که در آپارتمانش در روستایی در شرق شهر نیویورک قرار داشت در مقایسه با

---

[1] Passive device

[2] Nihon

تلفن همراهش بسیار سریع‌تر بود. کامپیوترش به قدری سریع بود که حرارتی که تولید می‌کرد باعث شده بود تا او یک سیستم خنک کننده مایع و سفارشی را برای CPU طراحی کند – حتی یک فن هواپیما هم نمی‌توانست از ذوب شدن و سوختن یک پردازنده چند هسته‌ای مانند آن جلوگیری کند. میک با آرامش به بیرون از پنجره نگاه می‌کرد و از سوار شدن در یک قطار با تکنولوژی بالا لذت می‌برد.

خارج از کیوتو، قطار "Shinkansen Nozomi" که در انگلیسی "New Track Hope" ترجمه می‌شود، سرعت بالای 29Ø کیلومتر در ساعت را داشت که در نزدیکی شهر کوبه [۳] به 298 کیلومتر در ساعت نزدیک می‌شد. رد شدن قطارهای دیگر به ندرت صدای اضافی ایجاد می‌کردند یا باعث می‌شدند که قطار به لرزش درآید. سرعت نسبی بالای 5ØØ کیلومتر در ساعت چشمگیر بود.

قطعا قطاری از نوع فرمول ۱ بود !

میک از اینکه آنها چگونه در چنین سرعتی در تمام طول تونل ارتباط GPS با ماهواره را حفظ کرده بودند تعجب می‌کرد. GPS میک چند دقیقه پیش از کم کردن سرعت برای ورود به ایستگاه هیروشیما، سرعتی تا 299 کیلومتر در ساعت را ثبت کرده بود. میک در حالی که مایوس از این بود که نتوانسته بود رکورد لارس را تحت الشعاع قرار دهد، احتمالات دیگر را در نظر گرفته بود و این نکته در ذهنش نقش بسته بود که درجه بندی دستگاه لارس را باید بررسی کند تا از دقت آن مطمئن شود.

ایستگاه قطار در هیروشیما مملو از شلوغی و صداهای بلند و ناهنجار بود که میک عاشق آن بود. او از چالش‌های حمل و نقل عمومی و عبور و مرور در یک کشور که نمی توانست به زبان آنها صحبت کند یا حتی علایم و نشانه‌ها را بخواند لذت می‌برد. امروز او منتظر دیدن سیستم اتوبوس برقی هیروشیما بود.

میک خواست از ایستگاه خارج شود که با تعجب ایستاد، او یک مرد مسن‌تر از خود را دید که بر روی جدول نشسته و در حال سرکشیدن رامن [۴] بود.

پیش خود گفت؛ این گونتر است؟

سابقه دوستی میک با گونتر شافر [۵] به پنج سال پیش بازمی‌گشت و پس از یک فاجعه کوتاه، در راه‌اندازی یک شرکت به عنوان مشاور کسب و کار به او کمک کرده بود. گونتر همچنین مدت‌ها پیش موفق شده بود که میک را به کنفرانس‌های بین المللی مانند آنچه که این هفته برگزار می‌شود دعوت کند. این کنفرانس‌ها یک پلتفرم کامل برای میک بودند تا در اینترنت و امنیت کامپیوتر بهتر شده و

---

[3] Kobe

[4] Ramen یک غذای ژاپنی

[5] Gunter Schafer

دیگران را نیز در این زمینه متقاعد کند. از نظر میک تمام این صنعت سر خود را در شن فرو برده بود (یا شاید در جایی دیگر) – ظاهرا هیچکس در مورد آنچه در دنیای خارج وجود دارد ایده‌ای نداشت و از اتحاد در حال تحول متخصصان امنیت و جرم و جنایات سازمان یافته، انواع حملات پیچیده درحال شکل‌گیری بود.

خبر خوب این بود که ابزارهای بزرگ امنیتی و روش‌های مختلف در دسترس بودند که اینترنت را برای استفاده امن می‌کردند و اما خبر بد این بود که تنها شمار کمی از افراد از آن استفاده می‌کردند. ماموریت شخصی میک این بود که آن را تغییر دهد.

گونتر برای همیشه در این صنعت بوده و مورد احترام همگان بود. میک حدس می‌زد که او باید در حدود ۳۵ تا ۳۹ سال داشته باشد و به نظر می‌رسید که همه را بشناسد. او همچنین یک مجموعه شگفت انگیز و عتیقه از گرامافون‌هایی که توسط ادیسون ساخته شده بودند داشت که میک آن‌ها را در خانه او در مونیخ آلمان دیده بود.

گونتر وقتی که دید میک به طرف او می‌آید با صدای بلند گفت "میک! حالت چطوره؟".

گونتر تنها دوست نزدیک میک بود که او می‌توانست به طور اتفاقی با او ملاقات کند. نرم‌افزار به میک می‌گفت که محل سکونت او تا چه حد به دوستانش نزدیک است و در زمان نزدیک شدن به خانه دوستانش به او پیام می‌داد. با این حال گونتر دوست نداشت کسی در مورد محل سکونتش و جایی که می‌رفت چیزی بداند و تلفن همراه او همیشه عمدا اطلاعات نادرست را گزارش می‌داد – گونتر آن را موقعیت جغرافیایی مبهم[6] می‌نامید – که میک آن را آزاردهنده می‌نامید. اگر او نیاز داشت با گونتر در جایی ملاقات کند باید نرم‌افزاری که خود گونتر نوشته بود را اجرا می‌کرد – گونتر تنها پس از این کار اطلاعات حساس را به اشتراک می‌گذاشت. میک واقعا نمی‌توانست از چیزی شکایت کند – او تمام دوستان و خانواده‌اش را مجبور کرده بود که با استفاده از PGP برای او ایمیل‌های رمزگذاری شده بفرستند. درواقع او از خواندن ایمیل‌های رمزگذاری نشده خودداری می‌کرد. او همچنین در مورد کامپیوترش و امنیت اینترنت که شامل مکالمه صوتی و تصویری امن در اینترنت است بسیار دقیق بود و وسواس داشت.

دوستان میک همه در صنعت کامپیوتر و امنیت بودند و در مورد رفتارهای غیرعادی او فکر نمی‌کردند اما افراد دیگر احتمالا به رفتارهای غیرعادی او فکر می‌کردند و معمولا وقتی که میک مرتکب اشتباهی می‌شد سعی می‌کرد که آن را برای فرد مورد نظر توضیح دهد. او یکسری از عادت‌ها را داشت که در

[6] Geofuzzing

طول سالیان برای او به وجود آمده بودند و حتی در صورت سعی کردن هم نمی‌توانست از دست آنها خلاص شود.

به عنوان یک مهندس کامپیوتر و برنامه نویس، میک تمام عملیات داخلی کامپیوترش و ارتباط دستگاه‌ها را می‌دانست. به عنوان یک متخصص امنیت، او تمام راه‌هایی که از طریق آن‌ها کامپیوترش می‌توانست به خطر بیافتد یا تحت کنترل کسی دربیاید، اطلاعاتش از بین رفته و یا دزدیده شوند را می‌دانست. در نتیجه، او هرگز از برنامه‌ها یا نرم‌افزارهایی که شخصا مورد بررسی قرار نداده بود بر روی کامپیوترش استفاده نمی‌کرد و برنامه‌ها را شخصا بررسی و کامپایل می‌کرد. او به طور دقیق تمام اطلاعات بر روی کامپیوترش را رمزگذاری می‌کرد، به طوری که تنها خودش می‌توانست از آن‌ها استفاده کند. میک تقریبا همیشه از صدا، تصویر و پیام‌های فوری امن با دوستان و همکاران خود استفاده می‌کرد. تنها استثنا در این مورد می‌توانست یک تماس کوتاه با دوست جدید یا همکارش باشد که بخواهد به آنها توضیح دهد که چگونه می‌توانند نرم‌افزارهای مربوط به امن سازی صدا را دانلود و نصب کنند؛ سپس آنها می‌توانند بر روی یک کانال رمزگذاری شده در اینترنت با هم صحبت کنند. میک در مورد کلمه عبور خود نیز بسیار دقیق بود و هر هفته آن را عوض می‌کرد. او نسبت به اینکه کامپیوترش و ارتباطات‌های آن امن هستند مطمئن بود اما آموزش و تجربه‌های او در این زمینه به او یاد می‌داد که هرگز این طور فکر نکند. او این کار را برای مدت زمان طولانی و به طور منظم انجام می‌داد؛ وگرنه شب خوابش نمی‌برد.

میک از گونتر پرسید "حالت چطوره و در حال حاظر چی کار میکنی؟"

گونتر از جایش بلند شد و پاسخ داد "پیش از آمدن به هتل مقداری غذا خوردم". در آن سوی پیش‌خوان، صندوقدار به گونتر یک سینی پلاستیکی همراه با یک سند ناخوانا را تحویل داد که به خوبی چاپ شده بود. او چند سکه در سینی گذاشت و یک رسید تحویل گرفت و به دنبال میک خارج شد.

آن ها با هم در خیابانی از هیروشیما سوار تراموا[۷] شدند.

گونتر با توجه به رابطه بین میک و لیز کلایتون[۸] که در تلاش برای ایجاد یک رابطه رسمی بودند اما به دلیل وجود برخی از مشکلات با هم درگیری‌هایی داشتند پرسید "هم اینک رابطه بین شما و لیز چطور است؟"

میک پاسخ داد "گفتنش سخته اما حدس میزنم هم اکنون تنها با هم دوست هستیم". طی دوازده ماه گذشته آنها چند بار از هم جدا شده بودند. هرچند، موضوع پیچیده‌تر از این بود.

---

[۷] واگن برقی

[8] Liz Clayton

گونتر در حالی که به سرعت به برنامه کنفراس در تلفن همراهش نگاه می‌کرد پرسید "شما چه روزی ارائه داری؟"

-"من پنجشنبه، تو چطور؟"

گونتر گفت "من این هفته سخنرانی ندارم – فقط استراحت می‌کنم و از خوردن سوشی لذت می‌برم"

میک می‌دانست که گونتر این هفته آرامش نخواهد داشت – او کسی را نمی‌شناخت که سخت‌کوش‌تر از گونتر باشد. گونتر همچنین یکی از با استعدادترین برنامه‌نویسانی بود که میک می‌شناخت و همیشه بر روی یک پروژه برای خود یا مشتری در حال کار بود.

میک بلند شد و گفت "من باید پیاده بشم"

گونتر گفت "من چهار راه بعدی پیاده میشم. بعدا با شما صحبت می‌کنم"

میک از تراموا پیاده شد و از خیابان عبور کرد و به لابی هتلی که قرار بود برای یک هفته آنجا بماند وارد شد. او در درجه نخست، هتل را از سرعت اینترنت بی‌سیم آن، راحتی تخت خوابش و احساسی که در لابی آن داشت مورد قضاوت قرار داد. او عاشق هتل‌هایی بود که لابی‌های بزرگ با صندلی‌های راحت و چشم انداز خوب داشتند و اسپراسو نیز همه جا وجود داشته باشد. به نظر نمی‌رسید که این هتل لابی بزرگی داشته باشد اما میک می‌دانست که حتما یک شبکه بی‌سیم عالی دارد که توسط برگزار کننده کنفرانس ایجاد شده است.

یک گروه کر ملایم با تعظیم و احترام و حرکات دیگر[9] مورد استقبال و توجه میک قرار گرفت. او عاشق آهنگ‌های ژاپنی بود ازجمله آهنگ کوتاهی که در سکوی‌های قطار و ایستگاه‌های مترو پخش می‌شد. میک همچنین از اینکه خیلی از چیزها را به ژاپنی متوجه نمی‌شد لذت می‌برد و به جای معنا بر روی حرکات سر و دست تمرکز می‌کرد. این متوجه نشدن به او یادآوری می‌کرد که هر روز چقدر باید صحبت می‌کرد؛ در صورتی که اکنون نیازی به آن نیست. او می‌توانست یک روز کامل در ژاپن بدون اینکه با کسی گفتگویی داشته باشد به مترو و فروشگاه برود.

پس از اینکه احوال پرسی تمام شد میک گفت "لطفا بررسی کنید".

آن خانم پرسید "اسمتون؟"

میک گفت "الک رابرتسون[10]" و پاسپورت خود را درآورد. میک یکی از پاسپورت‌های خود را به درستی بیرون آورد – او سه پاسپورت با نام‌های مختلف داشت. دوستان و همکارانش او را با نام

---

[9] Bowing and Bobbing

[10] Alec Robertson

میک اومالی[11] می‌شناختند اما این یکی از نام‌هایش بود که در ۱۸ سالگی هنگامی که یک شهروند آمریکایی شده بود برای خود انتخاب کرده بود. او برای خانواده‌اش و هر وقت که می‌خواست رد خود را مخفی کند "الک رابرتسون" بود که نام پاسپورت بریتانیاییش بود.

میک از نام‌های متعدد استفاده می‌کرد و هویت‌های مختلف برایش به یک عادت تبدیل شده بود که البته این کمی ظاهرسازی هم بود. از آنجا که او دوست نداشت پاسپورت یا دیگر مدارک شناسایی خود را نشان دهد، در بررسی‌های هتل از هویت قدیمی خود که الک بود استفاده می‌کرد. او می‌دانست که در برخی از نقاط جهان، هتل‌ها این اطلاعات را شبانه به پلیس گزارش می‌دهند. میک پیامدهای عدم حفظ حریم خصوصی یا کاغذهایی که سفرها و فعالیت‌های او را ترسیم می‌کردند دوست نداشت. این تنها یکی از راه‌های بی‌شمار حفظ حریم خصوصی بود که توسط پایگاه‌های اطلاعاتی به هم پیوسته به طور پی‌درپی ضعیف شده بود. میک در مخفی کردن ردپای دیجیتالی خود یک متخصص بود و از رمزگذاری و گمنام سازی[12] استفاده می‌کرد؛ او به خوبی در زندگی روزمره خود این تئوری را عملی کرده بود.

البته میک می‌دانست اگر کسی مانند دولت بخواهد او را ردیابی کند، هیچ مشکلی برای این کار نخواهد داشت. در کشوری که در صورت جست‌وجوی او هر دو پاسپورتش پیدا خواهد شد، این رویکرد او بدون خطر نخواهد بود. خوشبختانه میک چند کار را برای رئیس سازمان ملی استاندارد آن کشور خاص انجام داده بود. در صورت وجود خطر، چند تماس تلفنی می‌توانست چند ساعت بعد به او کمک کند، هرچند پس از آزادیش مشکوک بودن این قضیه قابل انکار نیست.

پس از دریافت اطلاعات میک و اشتباه تلفظ کردن اسمش، آن زن گفت "آقای رورستون[13]، به هیروشیما خوش آمدید". چند دقیقه بعد میک چمدانش را در اتاق باز کرد. او یک ارتباط امن اینترنت را برقرار کرد و مقداری پول را از حساب بانکی خود منتقل کرد. این یک کارت بانکی مخصوص[14] برداشت پول بود که برای این سفر تهیه شده بود. این کار ردپای تراکنش‌های مالی میک را برای پیگیری، سخت‌تر می‌کرد و برخی از صورت حساب‌های بانکی را هر ماه تولید می‌کرد، اما مدیریت آن به صورتی که به نظر می‌رسید دشوار نبود.

میک در کنفرانش ثبت نام کرده و آماده بود تا ببیند که کدام یک از دوستان او در آنجا هستند که ناگهان هنگام عصر وضعیت تغییر کرد. شبکه اجتماعی میک با یک پست در مورد یک حمله که شبیه

---

11 Mick O'Malley

12 Anonymization

13 Rovertson

14 Pre-Paid Bank Card

به گسترش آتش سوزی در اینترنت بود به صدا درآمد – این شبیه به یک حمله روز صفر[۱۵] بود که هیچ کس، پیش‌تر این نوع حمله را ندیده بود.

هنگامی که یک آسیب‌پذیری جدید در نرم‌افزاری کشف می‌شود، این یک مسابقه بین برنامه‌نویس کامپیوتر که تلاش می‌کند برنامه را تعمیر کند و مهاجم که سعی می‌کند از این باگ استفاده کرده و کامپیوترهایی که از این برنامه استفاده می‌کنند را در اختیار بگیرد است.

با گذشت زمان کافی، نرم‌افزار می‌تواند تعمیر شود یا در اصطلاح کامپیوتری "وصله [۱۶]" شود و آسیب‌پذیری مورد نظر را پردازش کرده و مانع حمله توسط برنامه‌های مخرب کامپیوتری مانند ویروس‌ها و کرم‌ها شود. روز صفر اشاره به وضعیتی دارد که آسیب‌پذیری در همان روز کشف شده و به طور فعال توسط مهاجم استفاده می‌شود. به دیگر سخن، هیچ زمانی (صفر روز) بین اینکه حمله کشف می‌شود و آن برای آلوده کردن و کنترل کامپیوترها استفاده می‌شود وجود ندارد.

میک وب‌سایت و بلاگ شخصی خود را چک کرد و با احساس دلهره متوجه آن شد که آنها هم اینک مورد حمله قرار گرفته و آلوده شده‌اند. به جای مطالب او در وب‌سایت، یک بنر بزرگ با عبارت "کربن سمی است" در سایت وجود داشت – که این عبارت ظاهرا اشاره به خطرات ناشی از تغییرات آب و هوا داشت. میک برخی از وب‌سایت‌های دیگر را نیز بررسی کرد و بیش از نیمی از آنها همین پیام را نشان می‌دادند. به طور خاص، به نظر می‌رسید که سایت‌های دولت ایالات متحده امریکا به طور یکنواخت پایین آورده شده‌اند (هک شده‌اند). وقتی میک متوجه شد که این یکی از بزرگترین حمله‌های اینترنتی است، قلبش به شدت می‌زد. با وجود این شرایط، او به خود لبخند می‌زد و اینکه این اتفاق به او گوشزد می‌کند که در چه مرحله‌ای قرار دارد و این یک موقعیت مناسب برای اوست – احاطه شده توسط همکارانش. او تنها باید از یک چیز مطمئن می‌شد.

میک به سرعت به مرکز عملیات شبکه یا همان NOC[۱۷] مربوط به سرورهای کنفرانس یا شبکه بی‌سیم رفت. در طول مسیر، وب‌سایت کنفرانس را چک کرد و از اینکه می‌دید هنوز فعال است و به نظر نمی‌رسد که آلوده شده باشد آرام شد. به سرعت در را باز کرد و از چیزی که بر روی میز می‌دید و مربوط به دستیار NOC بود وحشت زده شد. میک مستقیما به سمت مسیریابی که در آنجا قرار داشت رفت. کابل‌هایی که مسیریاب را به اینترنت وصل می‌کرد برداشت و با یک حرکت، آنها را از سرور جدا کرد.

---

۱۵ Zero day

۱۶ Patch

۱۷ Network Operations Center

ناگهان یک نفر سر میک فریاد زد و گفت "هی مرد چی کار میکنی، این اینترنت ما بود" و همان طور که میک به طرف او برمی گشت دست‌هایش را به آرامی بالا برد و امیدوار بود که آن فرد یک گارد امنیتی نباشد.

میک گفت "میدونم و به خاطر این متاسفم. اما بچه‌ها، چیزی در مورد روز صفر وب سرور شنیدید؟" و همه آنها به جز یکی سرشان را تکان دادند. همانطور که هر یک از آنها وب‌سایت‌های مورد علاقه خود را نگاه می‌کردند و آن را برای خودشان تائید می‌کردند میک وضعیت را به سرعت برای آنها توضیح داد "سرورهای شما هنوز مورد حمله قرار نگرفته و من فورا نیاز به جداسازی آنها از اینترنت دارم. پس ما می‌توانیم یک محیط نظارتی راه‌اندازی کرده و در صورت بروز حمله آن را مشاهده کنیم. در ضمن من میک اومالی هستم. می‌تونم به شما کمک کنم؟" و همانطور که نفس نفس می‌زد حرفهایش را به پایان رساند.

یکی از آنها پاسخ داد "حتما، لطفا شروع کنید. تنها من باید سرپرست را از انجام این کار آگاه سازم. یک صفحه مربوط به قطع شدن وب‌سایت ایجاد می‌کنم و با نوشتن یک گزارش کوچک به بقیه افراد اطلاع دهم که در شبکه چه اتفاقی می‌افتد...این کار ما برخی از افرادی که در خارج از اینجا هستند را عصبانی خواهد کرد".

میک پرسید "آیا در این اطراف جایی وجود دارد که بتوانیم کارمان را شروع کنیم؟" و به اتاق کوچکی که در آن طرف NOC وجود داشت نگاه کرد.

- "بریم".

میک دستور داد "من به تمام کامپیوترهایی که شما در اینجا یا در هر یک از بخش‌های مختلف شبکه راه‌اندازی کرده‌اید نیاز دارم. ما باید یک طعمه برای دام آماده کنیم، پس می‌توانیم مهاجم را در زمان ورود، به دام بیاندازیم" و کارکنان NOC شروع به تنظیم مجدد چیزها طبق دستور او کردند.

میک به دوستان خود پیام‌هایی را فرستاد و چیزی که در ذهنش بود را برای آنها توضیح داد و از آنها خواست که در عرض ده دقیقه دیگر او را در اتاق ملاقات کنند. میک در مواقع این چنینی، از برنامه پیام رسان نظیر به نظیر[۱۸] خود قدردانی می‌کرد؛ این برنامه یک پروژه متن باز شخصی بود که برای دوستان و خانواده‌اش ساخته بود و می‌توانست حتی بدون اتصال به سرورهای اینترنت نیز اجرا شود.

سپس با استفاده از تلفن همراهش سعی کرد از راه دور به وب سرور خود وارد شود؛ اما نتوانست. او توانایی وارد شدن به سرور دیگری که گزارش‌های مربوط به وب سرور در آن ذخیره شده بود را داشت؛ فایل‌هایی که فعالیت‌ها و عملیات انجام شده بر روی یک کامپیوتر را که یک دنباله از آدرس‌های

[18] Peer-to-Peer

پیمایش شده دیجیتالی بود لحظه به لحظه ثبت و ضبط می‌کردند. او این کار را به عنوان یک تضمین برای پوشش وضعیت‌هایی درست مانند این ایجاد کرده بود. برای میک اینکه دست‌کم می‌تواند به گزارش‌ها دسترسی داشته باشد جالب بود – آنها توسط مهاجم پاک نشده بودند – هرچند شامل جزئیات به اندازه‌ای که مورد نیاز او باشد نبودند. به جز شش نفر از دوستان نزدیک و هم دانشگاهی میک که در مقابلش ایستاده بودند و به وضعیت موجود نگاه می‌کردند فرد دیگری حضور نداشت. میک به آنها نگاهی کرد و سپس ذهن خود را بر روی کاری که در دست داشت متمرکز کرد. او به هرکس دستوری داد.

–" لارس یک تله سطح پایین را در سرور نصب کرد و یک دامپ[۱۹] کامل را در یک درایو آفلاین انجام داد. لیز مسیریاب[۲۰] را برای فرستادن تمام ترافیک ورودی از طریق این زیرشبکه پیکربندی کرد. شخص دیگری به سراغ فایروال رفت و آنالیز نفوذ و ثبت ورود به سیستم را در آن راه‌اندازی کرد. ما تنها یک فرصت داریم و بنابراین باید به نتایج درست برسیم. اجازه دهید این تله را تنظیم کنیم". گروه پراکنده شده و شروع به انجام کار کردند.

لارس الواستورم[۲۱] دوست سازنده یکی از محبوبترین سیستم عامل‌های متن باز بود و در میان چیزهای دیگر یک متخصص در زمینه امنیت هسته هم بود – هسته[۲۲]، بخش مرکزی یا هسته هر سیستم عاملی در کامپیوتر است. لارس از دانشگاه هلسینکی[۲۳] در فنلاند مورد استقبال قرار گرفته بود و تقریبا به اندازه میک مسافرت کرده بود.

در دقایق بعدی بحث‌ها بسیار کم شده بود اما در عوض مقدار زیادی نوشتن و گاهی هم فحش و ناسزا گویی وجود داشت. تکنسین‌های محلی به افراد، گذرواژه‌هایی که آنها برای کار کردن بر روی کامپیوترها به آن نیاز دارند را دادند. میک اکنون خود را با طرح شبکه آشنا کرده بود و دقیقا جایی که می‌خواست تله فعال شود را می‌دانست.

یک مرد با قد کوتاه که در اتاق راه می‌رفت سوالی پرسید "چه اتفاقی داره اینجا میافته؟". یکی از تکنسین‌ها متعجب از جایش بلند شد و به میک نگاه کرد. میک به لیز که افسوس می‌خورد نگاهی کرد و به سمت آن مرد رفت. لیز گاهی به آنها در موقعیت‌های دشوار مانند این کمک کرده بود.

---

[19] Dump

[20] Router

[21] Lars Elvström

[22] Kernel

[23] Helsinki

لیز موهای برس کشیده‌اش را به کنار صورتش برده بود و با یک گیره آنها را بسته بود. او لبخند زد و گفت "سلام! من لیز کلایتون[۲۴] هستم و شما؟"

-" ند ایورسون[۲۵] و مسئول این شبکه هستم یا دست‌کم بودم..."

در حالی که میک مشغول کار کردن بود لیز گفت "درسته ند"، امیدوارم بتوانیم اوضاع را به سرعت بین افراد تقسیم کنیم.

میک گفت "اجازه دهید آنچه که قرار است انجام دهیم را توضیح بدهم. وب سرور شما هنوز به حمله روز صفر آلوده نشده و بنابراین ما در حال راه‌اندازی مانیتورینگ و ثبت پیام‌ها هستیم و می‌توانیم تلاش کنیم تا ببینیم که حمله به چه صورتی اتفاق می‌افتد. با کمک تکنسین‌های شما، ما مسیریاب‌ها و فایروال‌ها را پیکربندی مجدد کردیم و به این ترتیب می‌توانیم ببینیم که حمله به چه صورتی کار می‌کند و چگونه می‌توانیم در برابر آن از خود محافظت کنیم."

ند پرسید "چرا نمی‌توانید تنها گزارش‌های مربوط به سرورهای آلوده شده را نگاه کنید؟"

لیز توضیح داد "ما پیش‌تر سعی کردیم – حمله گزارش‌ها را پاک و به طور کامل مسیر را پنهان می‌کند. هنوز هیچ‌کس اطلاعاتی در مورد این حمله برای تجزیه و تحلیل کردن آن ندارد". لیز به میک که در حال استراحت کردن بود نگاه کرد و فهمید که هم اینک اوضاع چندان خطرناک نیست.

-"بسیار خب، اما سرور من آلوده شده است؟ من ترجیح میدم به زودی از آلوده شدن آن جلوگیری کنم".

میک گفت "هووم...ما می‌توانیم وب سرور شما را با یک سرور ساختگی جایگزین کنیم. به این ترتیب سایت واقعی شما امن خواهد ماند. تنها باید آن را به سرعت راه‌اندازی کنیم – هر چیز دیگری در چند دقیقه آماده دسترسی خواهد بود."

میک ادامه داد "زمانی که کار ما انجام شد شما می‌توانید همه چیز را به حالت پیشین برگردانید".

با توجه به اینکه لیز می‌دانست که باید بیشتر شب را در آنجا بماند گفت "البته، ما این کار را انجام خواهیم داد".

همانطور که لیز قدم زنان به محل پیشین خود برمی گشت، غرغر کنان به میک گفت "تو به من مدیون هستی". این تنها لبخندی در گوشه لب لیز بود که میک از او دیده بود.

---

[24] Liz Clayton

[25] Ned Iverson

کمتر از پانزده دقیقه بعد، بسیاری از افرادی که در اتاق بودند به اطراف نگاه می‌کردند و از خودشان احساس رضایت می‌کردند. میک دید که سرپرست به او اشاره می‌کند. تنها دو نفر هنوز با عصبانیت مشغول به کار بودند. گونتر با سرعت زیادی در حال تایپ کردن بود و در حالی که یک زن با موهای تیره که میک پیش‌تر متوجه آن نشده بود در پشت صندلی ایستاد، با حرکت دست به او جهت را نشان داد. کدهایی که در صفحه نمایش وجود داشت، نشان دهنده تنظیمات و پیکربندی پیچیده فایروال بود. گونتر لحظه‌ای بعد انگشت شستش را به او نشان داد و آن زن نشست و به میک لبخند زد و این کار باعث شد که میک چیزی که به آن فکر می‌کند را فراموش کند.

او کیست؟

میک با هر یک از گروه‌ها صحبت کرد و تنظیمات و پیکربندی آنها را تائید کرد. در نهایت آنها آماده بودند.

میک همانطور که هیجان زده شده بود گفت "بسیار خب، اجازه دهید که دوباره به اینترنت وصل شویم".

یکی از تکنسین‌ها پاسخ داد "اووووم، تنها می‌توانم یک لینک را فعال کنم و اتصال دهنده‌های دیگر به هم پیوند خورده‌اند". میک بعدها در مورد این احساس بدی خواهد داشت اما اکنون در حالت مقاومت در برابر تهدید بود. پس از متصل کردن کابل اترنت به اینترنت، یکی از تکنسین‌ها گزارش داد "ما فعال هستیم!".

همه بی سر و صدا نشسته بودند و بی صبرانه به صفحه نمایش نگاه می‌کردند. تنها یک دقیقه زمان برد.

گونتر همانطور که حرکت اطلاعات بر روی صفحه نمایش خود را تماشا می‌کرد فریاد زد "فکر می‌کنم گرفتیمش". افراد دیگر نیز به صفحه نمایش خودشان نگاه کردند – برخی از صفحه نمایش‌ها فعالیت-هایی را نشان می‌دادند و برخی خیر. میک صفحه مرورگر خود را که مربوط به وب‌سایت کنفرانس بود نوسازی[۲۶] کرد؛ صفحه "کربن سمی است" به میک نشان داده شد. اینکه چطور اینقدر سریع اتفاق افتاده است میک را شگفت زده کرد.

همه افراد به طور همزمان بخشی از اطلاعات که مربوط به گزارش‌ها بود را می‌خواستند. میک به تمام آنها گوش می‌داد و گاهی دوباره می‌خواست که آن را تکرار کنند. پاسخ در ذهن او شروع به شفاف شدن کرد و یک حقیقت آن را تائید می‌کرد.

---

[26] Refresh

میک همانطور که به سمت لارس خم می‌شد پرسید "لارس، فعالیتی بر روی پورت 443 می‌بینی؟".

لارس جواب داد "بله، یک ارتباط HTTPS که همزمان با حمله به پورت 443 آمده است". میک دستش را پشت او گذاشت.

فهمیدم!

میک نگاهی به تیم کرد و در حالی که می‌خندید گفت "از همه متشکرم" – من به تمام گزارش‌های آرشیو شده بر روی دایرکتوری اصلی برای تائید نیاز دارم اما فکر می‌کنم که ما ماهیت حمله را پیدا کرده باشیم. او درحالی که آنها را نادیده گرفته بود گفت " سپاس دوباره به‌خاطر تمام کمک‌های شما ".

لیز پرسید "میک، مرحله بعدی چیه؟".

میک همانطور که نشسته بود و در حال گرفتن کد منبع وب سرور بود پاسخ داد "زمان نوشتن یک وصله است". او شروع کرد به نوشتن یا برنامه‌نویسی کردن تا وب سرور را تغییر داده و آسیب پذیری آن را برطرف کند و از موفقیت‌آمیز بودن حمله جلوگیری کند.

همانطور که شبکه در حال آماده شدن بود، دیگران یا سرشان را برای استراحت بر روی میز گذاشته بودند و یا اینکه به تلفن‌های همراه خود نگاه می‌کردند. همه در مورد حمله زمزمه می‌کردند که کار چه کسی بوده یا نیست.

چند ساعت بعد میک وصله را نوشت. آن را بررسی کرده و در سرور جایی که مردم نرم‌افزارها را دانلود می‌کردند آن را آپلود کرد – وصله آماده برای تائید، انتشار و نصب در سراسر اینترنت بود. روز صفر تقریبا تمام شده بود.

یک نفر پشت سر میک با فریاد گفت "یک دقیقه صبر کنید، شما این کد را به صورت ناشناس بررسی کردید!". میک برگشت و زنی را دید که پیش‌تر با گونتر کار می‌کرد. آن خانم از نظر لباس پوشیدن در میان بقیه افرادی که در کنار میک بودند متمایز بود، او یک پیراهن بافتنی، یک دامن تیره و بوت پوشیده بود.

میک گفت "درسته".

آن خانم پرسید "اما چگونه از سوی بقیه مردم برای نوشتن این وصله قابل اعتماد هستید؟".

میک شانه‌ای بالا انداخت و گفت "نمی‌خواهم اما مشکلی وجود ندارد. چک کردن آن به صورت ناشناس از صدمه زدن به شخص خاصی جلوگیری می‌کند؛ وگرنه گسترش آن را متوقف می‌کند. ما تنها نیاز به انتشار این وصله داریم پس می‌توانیم این روز صفر را به پایان برسانیم."

آن خانم همانطور که سرش را تکان می‌داد گفت "اهمیتی نمی‌دهید که هیچکس متوجه نخواهد شد که شما حمله را متوقف کرده‌اید؟ شما دیوانه هستید!".

میک که از لهجه آن خانم خوشش آمده بود پرسید "متشکرم. و شما...". آن خانم قطعا اهل اروپای شرقی یا شاید صربستانی بود اما انگلیسی او بسیار عالی بود.

آن خانم با اشاره به اینکه تولید کننده فایروال را به خوبی می‌شناسد گفت "من کاترینا پترسکو[۲۷] از شرکت F.T.L (یک تولید کننده مطرح فایروال) در سان فرانسیسکو هستم". میک می‌دانست که F.T.L ابزارهای امنیتی زیادی را به فروش می‌رساند و نمی‌خواست که آن خانم را در مورد چیزهای بدی که با آن روبرو است با خبر کند.

میک همانطور که دستش را برای دست دادن دراز می‌کرد گفت "میک اومالی – به هر حال از کمک شما متشکرم. با فایروال موفق باشید".

آن خانم با او دست داد و گفت "قابلی ندارد".

برخی از تکنسین‌ها پشت میک و لیز استاده بودند تا به آنها کمک کنند که با همدیگر NOC را به حالت نخست برگردانند. هنگامی که این کار انجام شد، میک کاترینا را در گوشه‌ای از اتاق دید؛ کاترینا متوجه میک شد و به او نزدیک شد.

کاترینا گفت "خب، به من بگو که چگونه این کار را انجام دادی".

میک پرسید "منظور شما کشف حمله است؟" و وقتی که دید کاترینا سرش را تکان می‌دهد ادامه داد."من در طول سال‌ها چندین حمله را دیده‌ام اما این یکی غیرعادی بود. معمولا این روزها مرورگرها هستند که آلوده می‌شوند اما در این مورد این وب‌سرور بود که آلوده شده و صفحات وب را نشان می‌داد. ردیابی که ما از طریق برنامه Wireshark انجام دادیم آن را تائید کرد –یک درخواست برای مرور یک وب‌سایت بود که پیش‌تر آلوده شده بود."

– "و پورت 443 ؟".

– "سرعت تکثیر نشان می‌داد که کرم از یک روش رایج حمل داده که مسدود نشده است استفاده می‌کند. معمولا پورت 443 برای ترافیک رمزگذاری شده وب باز نگه داشته می‌شود. خوشحالم که ما زمان زیادی صبر نکردیم."

---

[27] Kateryna Petrescu

– "به هر حال، این وصله یک تکه زیبا از کد بود. شما در زندگی حرفه‌ای خود باید به عنوان یک توسعه دهنده نرم‌افزار کار کرده باشید. درسته؟ "

میک جواب داد "بله، برای مدت طولانی" و سپس ادامه داد "به هر حال وقتی که فهمیدم حمله چگونه کار می‌کند، دنبال کردن آن بی اهمیت بود و اشکال را پیدا کردم. باورتان بشود یا نه، این تنها یک حمله از نوع سرریز بافر[۲۸] بود". میک موضوع را عوض کرد" شما پیش‌تر در نیهون[۲۹] بوده‌اید؟...منظور من ژاپن است". چند روز پیش گونتر پیشنهاد کرده بود که به افتخار سفر آنها به ژاپن همه منحصرا باید از کلمه ژاپنی برای کشورشان استفاده می‌کردند – Nihon . این کاربرد در شبکه اجتماعی توسط افراد زیادی استفاده می‌شد و اکنون میک با آن آشنا بود. او در تلاش برای این بود که بگوید ژاپن یا ژاپنی.

کاترینا گفت "تنها یک بار – من چند سال پیش در توکیو و یوکوهاما بودم".

آنها در مورد چهار بازدیدی که میک از ژاپن داشته و بازدید پیشین کاترینا و کنفرانس‌هایی که به طور منظم در آن حضور داشته بحث کردند. میک متوجه شد که نقش کاترینا از حضورش بدان معنی است که او باید در بسیاری از کنفرانس‌های مشابه که میک در آن بوده نیز حضور داشته باشد.

لیز برای میک که بیشتر پیکربندی‌های NOC را بازگردانده بود دست تکان داد و از اتاق خارج شد. میک هم برای لیز دست تکان داد و گفت "متشکرم!". لیز پشت سر کاترینا بود و کاترینا سرش را برگرداند و لیز را نگاه کرد.

کاترینا پرسید "لیز کلایتون، درسته؟".

میک گفت "بله، ما همیشه دوست هم بوده‌ایم". میک فکر می‌کرد که به خاطر استفاده از واژه "دوست" واکنش خاصی را در چشم‌های کاترینا دیده است.

این می‌تواند یک کنفرانس واقعی باشد.

---

[28] Buffer Overflow

[29] Nihon

فصل ۱

از وبلاگ the Security and Other Lies :

چه تفاوتی بین یک کرم و ویروس وجود دارد؟ dieraptorzdie (نام مصاحبه کننده)

dieraptorzdie، این پرسش خوبی است. ویروس‌ها و کرم‌ها انواع مختلفی از "Malware" هستند که این نام کوتاهی برای برنامه مخرب[1] است. معمولا Malware بدون آگاهی شما بر روی کامپیوتر نصب می‌شود و ممکن است اطلاعات را به سرقت برده، آنها را حذف کند، کامپیوتر را به دستگاهی برای فرستادن هرزنامه تبدیل کند و یا کارهایی را انجام دهد که دوست ندارید.

هم یک ویروس و هم یک کرم تلاش خواهند کرد که به کامپیوترهای دیگر گسترش پیدا کرده و یا تکثیر شوند – تفاوت در چگونگی انجام این تکثیر است. اگر Malware تلاش کند که خود را با چسباندن به تکه دیگری از نرم‌افزار یا اطلاعات تکثیر کند – معادل یک میزبان بیولوژیکی – آن وقت، آن را ویروس می‌نامیم. این کار ممکن است از طریق یک ایمیل انجام شود که آن را باز می‌کنید و یا از یک صفحه وب که از آن بازدید کرده‌اید دانلود شود.

اگر Malware طوری طراحی شده باشد که خود انتشار باشد – آن وقت بدون کمک برنامه‌های دیگر و از طریق اینترنت خود را گسترش می‌هد که به صورت کرم شناخته می‌شود. این واژه اشاره به راهی دارد که Malware "کرم" از طریق شبکه منتشر می‌شود. وقتی کامپیوتر به اینترنت متصل شده است می‌تواند انواع پیام‌ها را از کامپیوترهای دیگر دریافت کند. مهاجم می‌تواند یک دسته از پیام‌ها را به کامپیوتر شما ارسال کند (گاهی این "اسکن پورت" شناخته می‌شود) و تلاش کند تا به صورت ناخواسته Malware را نصب کند. این کار می‌تواند هر زمان که به اینترنت وصل می‌شوید رخ دهد و حتی برای اینکه این نوع از حمله اتفاق بیافتد لازم نیست حتما ایمیل خود را چک کنید و یا وب را مرور کنید.

هم ویروس‌ها و هم کرم‌ها می‌توانند به سرعت پخش شوند و در یک زمان کوتاه بسیاری از خسارت‌ها را به بار بیاورند.

---

[1] Malicious Software

یکسری از کارها وجود دارد که با انجام دادن آنها می‌توانید از کامپیوتر خود محافظت کنید. نرم‌افزار آنتی ویروسی که بر روی کامپیوتر خود نصب می‌کنید می‌تواند به حفاظت در برابر ویروس‌ها کمک کند: آنتی ویروس هرچیزی که دانلود و نصب می‌کنید را بررسی و نظارت می‌کند و اگر ویروسی وجود داشته باشد آن را پاک می‌کند. فایروال می‌تواند برای محافظت در برابر انواع مختلفی از کرم‌ها استفاده شود. هدف فایروال در شبکه، جلوگیری از ترافیک ناخواسته اینترنت است درحالی که به ترافیک مجاز اجازه ورود را می‌دهد. واژه "فایروال" از صنعت ساخت و ساز می‌آید که در معنای واقعی کلمه یعنی یک دیوار ضد آتش بین اتاق‌ها و یا ساختمان. اگر یک فایروال در شبکه خود داشته باشید، می‌تواند برنامه‌های پویش پورت را متوقف کرده و تنها به ترافیکی که می‌خواهید از اینترنت به سیستمتان وارد شود اجازه دهد.

اما بهترین دفاع در برابر کرم‌ها و ویروس‌ها این است که مطمئن شوید که یک سیستم‌عامل امن را اجرا می‌کنید و آن را با وصله‌ها به‌روز نگه داشته‌اید. همچنین باید در مورد هر تکه از نرم‌افزار که بر روی کامپیوتر خود نصب و یا دانلود می‌کنید بسیار دقت کنید. باید فورا هر به‌روزرسانی نرم‌افزار و وصله‌ها که در دسترس قرار می‌گیرند را نصب کنید – بسیاری از آنها نقص‌های امنیتی شناخته شده را برطرف می‌کنند. خود من تنها نرم‌افزارهایی را نصب می‌کنم که خودم آنها را کامپال کرده و کد منبع آنها را بررسی کرده‌ام. دست‌کم، باید به کسی که نرم‌افزار را نوشته است اطمینان داشته باشید؛ وگرنه، کامپیوتر خود را در معرض خطر خواهید یافت...

-> آیا به پرسش شما در این هفته پاسخ داده نشده؟ لطفا استدلال‌های خود را در بخش خاصی از انجمن که مربوط به آن است بیان کنید.

فصل ۲

رئیس جلسه شروع به صحبت کرد "از همه برای حضور در این جلسه تشکر می‌کنم" و به تیم خود در اطراف اتاق نگاه کرد. او شرکت Cloud 8++ را از صفر ساخته بود. همچنین در حوزه صنعت نیز رشد کرده بود و از علاقه‌مندان[1] به کسب و کار خانگی، امروزه به یک شرکت تبدیل شده بود. آنها از مقدار زیادی از موفقیت‌ها و سود نامشروع در طول سال برخوردار بودند اما همه چیز در حال تغییر بود.

– "پیش از هر چیز، یک گزارش در مورد پیشرفت حمله جدید می‌خواهم".

یکی از افراد پاسخ داد "همه چیز همانطور که انتظار می‌رفت انجام شد و میزان موفقیت در برابر وب سرورهای هدف ۱۰۰٪ بود".

– "زمان قطع شدن بسیار زیاد نبود اما چشم‌گیر بود. به ما گفته بودید که پیش از اینکه سرورها دوباره بالا بیایند و آماده شوند، یک روز یا بیشتر زمان لازم است. ما زمان کافی برای نصب نرم‌افزارهایمان را داریم؟".

– "برای نصب نرم‌افزارهایمان زمان داریم. این حمله خاص در جهت یک برنامه متن باز که جامعه بزرگ و فعالی از توسعه دهندگان را دارد کارگردانی شده است. آنها بسیار سریع سازماندهی شده و در عرض چهار ساعت یک وصله را نوشته و آپلود کردند و تقریبا بی‌درنگ پس از آن وب سرورها شروع به بالا آمدن کردند. بیشتر سرورها در دوازده ساعت وصله شدند."

– "آیا چیزی وجود دارد که بتوانیم با استفاده از آن در آینده از این کار جلوگیری کنیم؟"

– "حمله بعدی روز صفر ما علیه یک نرم‌افزار تجاری است؛ پس نیازی نیست که در مورد جامعه متن باز نگران باشیم. افزون بر این، مشاور ما دارای ایده‌هایی است در مورد اینکه چگونه می‌توانیم اجتماع را تقسیم و قطعه قطعه کرده و واکنش آنها را در آینده کاهش دهیم".

رئیس جلسه پرسید "و حمله خاموش؟".

---

[1] Hobbyists

آن مرد پیش از اینکه ادامه دهد یک لحظه مکث کرد و گفت "اگرچه ما هنوز آمار دقیقی را نداریم اما بسیار موثر است. من یک مراجعه معکوس[۲] را در مورد آدرس IP که به من داده بودید انجام دادم".

– "هنوز آن را انجام نداده‌اید!"

– "خب، انجام دادم.آدرس متعلق به شرکت UBK بود که یک شرکت دولتی است که ارائه دهنده خدمات برای شرکت دیگری است. تا آنجا که می‌دانم آن‌ها یک هدف اصلی برای ما نیستند. چرا ما باید از حمله خاموش بر روی آنها استفاده کنیم؟".

رئیس جلسه بر روی میز کوبید و فریاد زد "شما نباید نگران این باشید! و لازم نیست که در آینده این را انجام دهید!".

آن مرد همانطور که تلاش می‌کرد موضوع را تغییر دهد گفت "دست‌کم آماده حرکت به فاز ۲ هستیم".

رئیس جلسه پاسخ داد "نه آماده نیستیم" و افرادی که در کنار میز نشسته بودند را متعجب کرد. افراد در حالی که از این پاسخ گیج شده بودند به اطراف نگاه می‌کردند.

– "به آزمایش حملات ادامه می‌دهیم. باید به طور کامل پاسخ و واکنش مربوط به خطر را برای هر یک درک کنیم". اتاق برای لحظه‌ای ساکت شد.

– "بسیار خب، می‌دانم که همه شما چه فکری می‌کنید – این دیوانه است! می‌دانیم که حملات کار می‌کنند و همچنین می‌دانیم که یک واکنش وجود خواهد داشت – پس چه اهمیتی دارد؟ چرا باید به آزمایش ادامه دهیم؟ "

– "این یک بحث نیست. تصمیمی که گرفته‌ام را گفتم. آنقدر به آزمایش ادامه می‌دهیم تا بگویم که چه زمان آماده هستیم".

یک نفر دیگر با تاکید پرسید "این یک جهت جدید از سوی حامیان ماست؟" و به محض اینکه این حرف را زد همه افراد حاضر در اتاق فهمیدند که این حرف باید درست باشد.

– "آقایان، زمان در حال تغییر است. همه شما نقش اساسی و انکارناپذیری که حامیان ما در کسب و کارمان بازی می‌کنند را می‌دانید. حتی با دستور جدید و زیرساخت‌های کنترلی، نیاز به حفاظت در برابر ردیابی و رسیدگی به درآمدهایمان داریم. هم اینک، همه باید بر روی وظیفه‌ای که در دست داریم تمرکز کنیم. به طور منظم گزارش وضعیت کنونی را تا پیش از رسیدن به آزمایش بعدی می‌خواهم. حرف دیگری برای گفتن ندارم!"

---

[2] Reverse lookup