به‌نام خدا

اولین چالش سایبری دولت بایدن؛
اختلال سایبری در شبکه سوخت آمریکا

مرکز پژوهش‌ها
مجلس شورای اسلامی

معاونت مطالعات سیاسی

مشخصات گزارش

شماره مسلسل:
۲۶۰۱۷۵۵۸

تاریخ انتشار:
۱۴۰۰/۳/۱۷

مقدمه

جمعه ۱۷ اردیبهشت‌ماه ۱۴۰۰، هفتم می ۲۰۲۱، یکی از خطوط انتقال سوخت شرکت «کولونیال» آمریکا مورد حمله باج‌افزاری یک گروه هکری ساکن در اروپای شرقی به نام «دارک‌ساید» قرار گرفت و از کار افتاد.[1] این خط لوله روزانه ۵/۲ میلیون بشکه معادل ۴۵ درصد از نیاز بنزین، دیزل و سوخت جت ساحل شرقی ایالات متحده را تأمین می‌کند.[2] دولت بایدن روز یک‌شنبه ۹می ۲۰۲۱ (۱۹ اردیبهشت‌ماه ۱۴۰۰) اعلام وضعیت اضطراری کرد و شخص او تصریح کرد از ابعاد احتمالی این حادثه نگران است. هکرها ۱۰۰ گیگابایت از اطلاعات این شبکه را در اختیار گرفتند تا باج اعلام شده ازسوی شرکت تأمین شود؛ در غیر این‌صورت، اطلاعات سرورهای این شرکت را روی اینترنت منتشر خواهند کرد.[3]

تصویر ۱. خطوط لوله نفت کولونیال در جنوب شرقی آمریکا

1. https://www.bloomberg.com/news/articles/2021/05/09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown
2. https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html
3. https://www.abbc.com/news/business-57050690

در واکنش به این حمله، ابتدا کل عملیات این خط لوله متوقف شد تا سیستم‌های فناوری اطلاعات پشتیبان این خطوط لوله از حملات سایبری دامنه‌دارتر بعدی مصون بمانند و درنتیجه، بیش از ۱۰ هزار پمپ بنزین در سراسر جنوب شرقی آمریکا به‌ویژه کارولینا، ویرجینیا و جورجیا با کمبود سوخت مواجه شدند.[۱] با توجه به نبود راننده و تانکر سوخت کافی برای انتقال حجم سوخت انتقالی، کاهش سوخت بیش از یک هفته ادامه داشت و درنتیجه شرکت مجبور شد ۵ میلیون دلار پول دیجیتال به گروه هکری «دارک‌ساید» پرداخت کند.[۲] با این‌حال، قیمت متوسط هر گالن بنزین در روز چهارشنبه ۱۲ می ۲۰۲۱ (۲۲ اردیبهشت‌ماه ۱۴۰۰) به ۳ دلار افزایش یافت؛ قیمتی که از نوامبر ۲۰۱۴ تاکنون در این کشور تجربه نشده است.[۳] این قیمت همچنین یک جهش ۷ درصدی از چهارشنبه گذشته را نشان می‌دهد. علاوه‌بر این، صفوف طولانی در پمپ بنزین‌ها، ذخیره بنزین در پلاستیک، زدوخوردها میان رانندگان در برخی ایالت‌ها، قطع برق در ایالت میای و تبعات اجتماعی دیگری که این حمله را در پی داشت؛ سبب شد به‌رغم آنکه گروه هکری دسترسی به سرورهای خود را از دست بدهد و عملاً به باج درخواستی دست نیابد؛[۴] دولت بایدن در نخستین چالش سایبری جدی مردود شود.

نکات تحلیلی

- جو بایدن در سند «راهنمای استراتژیک موقت امنیت ملی آمریکا» که در مارس ۲۰۲۱ منتشر شد، تصریح کرده بود تهدیدهایی مانند بیماری‌های همه‌گیر، حملات سایبری و اطلاعات گمراه‌کننده هیچ مرز و دیواری نمی‌شناسد و پرداختن به آنها از اولویت‌های امنیت ملی آمریکاست.[۵] اما دولت وی به‌رغم موفقیت نسبی در مبارزه با همه‌گیری کرونا، نتوانسته است در حوزه مسائل سایبری توفیقی به‌دست آورد. این شکست هم به نوپدید بودن و متغیر بودن این حوزه در نسبت با موضوع امنیت ملی بازمی‌گردد و هم به دشواری سیاستگذاری و ساماندهی آژانس‌ها و نهادهای متعدد سایبری آمریکا.
- دیگر عصر و دوره‌ای که قدرت سیاسی با بازیگران صرفاً دولتی و کارتل‌ها و نهادهای اقتصادی تعریف می‌شد، پایان یافته است. یک گروه هکری بی‌نام و نشان که تنها اطلاعات موجود در مورد آنها صرفاً احتمالاتی در مورد محل سکونت اعضایش است، توانسته حکمرانی آمریکا بر یکی از معمول‌ترین کارکردهای یک دولت یعنی سوخت‌رسانی منظم را به چالش بکشد و این موضوع، معانی و پیامدهای محققانه پرشماری دارد.
- زبان و کانال و طرفین یک معادله قدرت، هیچ‌کدام در دست دولت آمریکا نیست. یک گروه هکری از خارج از مرزهای آمریکا، نظم سازوکار یک سیستم سوخت‌رسانی خصوصی درون مرزهای آمریکا را به‌هم می‌ریزد و از طریق کانال‌هایی که قابل شناسایی نیست، یعنی «دارک‌وب» طلب باج می‌کند و شرکت خصوصی هم از طریق پول دیجیتال که باز هم در اختیار دولت آمریکا نیست، بدان پاسخ می‌دهد. فناوری نه‌تنها ماهیت حکمرانی، بلکه بنیان آن را دچار چالش کرده است.

1. https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/
2. https://www.forbes.com/sites/melissaholzberg/2021/05/13/hackers-got-o-million-colonial-pipeline-reportedly-paid-a-ransom-in-cryptocurrency-contrary-to-claims/
3. https://www.fox2detroit.com/news/michigan-drivers-beware-memorial-day-gas-prices-could-break-3-a-gallon
4. https://www.thenationalnews.com/business/technology/colonial-pipeline-hackers-darkside-to-shut-down-after-losing-control-and-money-1,1223521
5. https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-security-strategic-guidance/

• ممکن است یک دولت از نظر آفندی و پدافندی، صاحب قدرت باشد و نهادها و آژانس‌های پرشماری را نیز بدین منظور در نظر گرفته باشد، اما نامتقارن بودن جنگ سایبری سبب شود از یک گروه کوچک هکری شکست بخورد. این شکست صرفاً نباید در تفاوت عرصه سایبر و در دیگر میدان‌های قدرت خلاصه شود و تصمیم‌گیران را به انفعال بکشاند. سیاستگذاری مبتنی‌بر یک نظام‌مندی و ارزیابی کارشناسانه می‌تواند کارکرد و بهره‌وری نهادها را اثبات کند.

• دو نکته مهم در مورد حمله باج‌افزارانه این گروه هکری که آن را با دیگر گروه‌ها متفاوت می‌کند، این است که اولاً این حمله نشان داد همچنان جرائم سایبری در حوزه زیست‌محیطی نیز امکان بروز دارد و این موضوع، خطر آشفتگی اجتماعی پس از حمله سایبری را گوشزد می‌کند. نکته دوم آن است که این گروه، تاکنون دو بار اقدام به اعطای کمک‌های مالی به گروه‌های خیریه کرده است که این موضوع نیز ممکن است از یک شکل نوین از پول‌شویی خبر دهد.

• یکی از موضوعات مهم در بحث پدافند غیرعامل، مبحث حفاظت از زیرساخت‌های حیاتی (Critical Infrastructure Protection) است. زیرساخت‌ها در هر کشوری در واقع بنیان اساسی جامعه آن کشور محسوب می‌شوند و آسیب به آن‌ها می‌تواند پیامدهای جبران‌ناپذیری را در کشورها ایجاد نماید. یکی از زیرساختهای مهم و اساسی در هر کشور، زیرساختهای مربوط به حوزه فضای سایبری است که به دلیل اهمیت و میزان تاثیرگذاری آن در دیگر زیرساخت‌های حیاتی تحت عنوان زیر ساخت حیاتی اطلاعاتی (Critical Information Infrastructure) توسط محققین این حوزه در دنیا مورد مطالعه و بررسی قرار میگیرد. با توجه به رشد روز افزون هوشمندسازی زیرساخت‌های اساسی مباحثی نظیر شهرهای هوشمند و ملاحظات امنیت سایبری آن از اهمیت خاصی برخوردار است. هوشمندسازی باعث میشود در سیستمهای کنترل صنعتی که مرکز اصلی کنترل و پایش اطلاعات در بسیاری از زیرساخت‌های حیاتی مانند سدها، نیروگاه‌ها، پالایشگاه‌ها و کارخانجات صنعتی و غیره، امنیت سایبری دغدغه بالایی را برای صاحبان این صنایع ایجاد کند. در نتیجه دولت‌ها باید در حوزه CIP سرمایه‌گذاری و توجه اساسی داشته باشند.

معانی و ملاحظات برای جمهوری اسلامی ایران

• نباید حمله به یک سایت غیرمرتبط و پایین آوردن نمای آن با حمله به زیرساخت‌های حیاتی یکسان دانست. از این روست که باید توجه داشت تأمین امنیت سایبری زیرساخت‌های سایبری کشور، فوری‌تر و آنی‌تر از تأمین امنیت سایبری سایت‌های خبری و حتی پایگاه‌های داده است. چرا که زیرساخت‌های سایبری همچون لایه زیرین درگاه‌های خدمات نیازهای حیاتی جامعه است و با خدشه و اشکال در این زیرساخت‌ها، عملاً زیرساخت‌های پشتیبان نیازهای روزمره شهروندان جامعه مانند برق، آب، مخابرات و حتی اینترنت دچار اختلال خواهد شد. در نتیجه ارزیابی امنیت سایبری این زیرساخت‌ها براساس یک نقشه جامع زیرساختی در کشور به ویژه متناسب با طرح آمایش سرزمین ضروری است.

• تعدد مراکز تصمیم‌گیری و ارزیابی حملات سایبری و حتی پاسخگویی و مقابله سبب می‌شود حملات اولاً ابعاد و پیامدهایی فراتر از انتظار داشته باشد و ثانیاً پاسخ‌های بازدارنده‌ای پیدا نکند. مهم‌ترین موضوع در امنیت سایبری جمهوری اسلامی ایران، فقدان یک استراتژی منسجم و پس از آن نبود فرماندهی واحد در شناسایی، ارزیابی و پاسخگویی به حملات سایبری است. به صورت مشخص، اکنون چهار نهاد متولی این حوزه عبارتند از قرارگاه پدافند سایبری سازمان پدافندغیرعامل، افتاء، وزارت ارتباطات و پلیس فتا. براساس سند پیشگیری و مقابله با حوادث فضای مجازی مصوب چهل و چهارمین جلسه شورای عالی فضای

مجازی، آن دسته از حوادث فضای مجازی که درحوزه مردم، کسب وکارهای خصوصی و مؤسسات غیردولتی و غیر زیرساختی به وقوع می‌پیوندد، توسط نیروی انتظامی جمهوری اسلامی، آن دسته از حوادث فضای مجازی که در حوزه دستگاه‌های غیر زیرساختی رخ می‌دهد، از طریق وزارت ارتباطات و فناوری اطلاعات و آن دسته از حوادثی که در حوزه دستگاه‌های زیرساختی اتفاق می‌افتد توسط مرکز مدیریت راهبردی افتا مورد رسیدگی قرار خواهد گرفت. این در حالی است که قانون تشکیل سازمان پدافند غیرعامل همچنان به تصویب مجلس نرسیده است. همچنین ایجاد آمادگی لازم در عالی‌ترین سطح به منظور صیانت از زیرساخت‌های حیاتی در برابر حملات اینترنتی و دفاع مناسب در برابر هرگونه حمله در چارچوب مصوبات شورای عالی فضای مجازی به کمیسیون عالی امنیت مرکز ملی فضای مجازی سپرده شده و از سویی دیگر، ابلاغیه‌های مرکز مدیریت راهبردی افتا برای کلیه دستگاه‌های موضوع ماده ۲۹ قانون برنامه ششم الزام‌آور نیست. در نتیجه با یک آشفتگی سازمانی و پراکندگی اداری روبروییم که موازی‌کاری و تداخل مأموریتی و بعضاً خنثی‌سازی مأموریتی را به دنبال دارد.

- سرعت بالای رخدادهای فناورانه، هوشمندسازی خدمات و شکل حکمرانی را به یک امر بدیهی تبدیل کرده است. این هوشمندسازی باید مبتنی بر یک رویکرد ایجابی و براساس اتکاء بر توان داخلی کشور باشد. پیش از آنکه براساس ملاحظات بودجه و همچنین دقت‌های فنی ورود به بازار امنیت سایبری در بخش خصوصی به قدرت سیاسی در ایران تحمیل شود، باید مبتنی بر مقررات حداقلی و براساس یک نگاه دقیق و فراگیر نسبت به برون‌سپاری برخی اقدامات حفاظتی و سخت‌افزاری اقدام کرد. مدرن‌سازی خدمات در حوزه‌های مختلف شهروندی به دلیل تغییر در سبک زندگی حتماً صورت خواهد گرفت. در نتیجه باید در فضای استارت‌آپی پدیدآمده امروز، از توان بالای چهره‌ها و شرکت‌های دانش‌بنیان هم‌راستا با اعتماد به خلاقیت و دانش آنان و البته سطح‌بندی برون‌سپاری استفاده کرد و با نگاه پیش‌دستانه، زمینه شکل‌گیری صنعت امنیت سایبری در بخش خصوصی را فراهم نمود. اگرچه اهمیت الکترونیک‌سازی خدمات و آنلاین‌سازی زیرساخت‌ها نباید ملاحظات حفاظتی و دقت‌های امنیتی را کمرنگ کند و از سویی دیگر، ارائه هر گونه خدمات در حوزه زیرساخت را از بخش خصوصی منع کرد.