روزنامه صبح ایران
وطن امروز
VATANEMROOZ.IR

شنبه | ۸ آبان ۱۴۰۰ | ۲۳ ربیع‌الاول ۱۴۴۳ | ۳۰ اکتبر ۲۰۲۱ | سال سیزدهم | شماره ۳۳۳۶ | ۸ صفحه | ۳۰۰۰ تومان

۱۱۸۳ سال و ۱۴ روز گذشت

VATAN-E-EMROOZ | VOL.13 | NO.3336 | SAT.OCT.30,2021 | ISSN:2008-2886

بازدید رئیس جمهور از مناطق زلزله‌زده خوزستان

دستور برای حل فوری مشکل زلزله‌زدگان اندیکا

صفحه ۴

بایدن قبل از شرکت در اجلاس «جی ۲۰» به دیدار پاپ رفت

عقل ناسالم آمریکا در بدن ناسالم اروپا

صفحه ۷

ایران روز چهارشنبه از حصول توافق با ۴+۱ برای از سرگیری مذاکرات تا ماه آینده خبر داد

وین؛ به زودی

نشریه آمریکایی ویک: اکنون نوبت بایدن است که تلاشی همراه با حسن‌نیت برای احیای برجام انجام دهد

صفحه ۲

بنزین در مدار آرامش

۹۷ درصد جایگاه‌های سوخت وارد مدار و بیش از ۱۴۰۰ جایگاه نیز به سامانه کارت هوشمند سوخت متصل شدند

وزیر نفت: غیر از سهمیه ماهانه یک سهمیه بنزین جبرانی نیز در آذرماه به مردم تعلق می‌گیرد

صفحه ۳

عکس: شانا

نیتروزئوس و حمله سایبری به سامانه سوخت

یادداشت

ابوالفضل عدالتی‌پور*: روز سه‌شنبه که خبر نفوذ به زیرساخت شبکه هوشمند سوخت کشور در رسانه‌ها اعلام شد خبرها و تحلیل‌های ضد و نقیضی از سوی کارشناسان مختلف شکل گرفت. اما اصل موضوع این حمله سایبری چه بوده و در مقیاس بزرگ‌تر چه اتفاقاتی منجر به این حمله شده است؟

در سامانه هوشمند سوخت از یک زیرساخت مجزا و ایزوله از اینترنت جهانی استفاده شده است. اینکه چگونه به یک شبکه خصوصی داخل کشور نفوذ شده، جای بحث کارشناسی فراوان دارد اما نکات قابل توجهی در این حملات وجود دارد.

این نوع شبکه‌ها که یک شبکه Air-Gap هستند مستقل از اینترنت جهانی سرویس‌دهی را انجام می‌دهند که نفوذ به این شبکه نشان از اطلاعات بالای نفوذگران از زیرساخت شبکه دارد و می‌توان احتمال داد بیشتر زیرساخت‌های کشور تحت تاثیر این حملات در آینده قرار بگیرند، همان‌طور که چندی پیش هم به زیرساخت ریلی کشور حملاتی شبیه به این انجام شده بود. از کار افتادن چنین سامانه‌ای به صورت سراسری در کل کشور و در یک زمان خاص، نشان از یک حمله حساب‌شده و از نوع APT* دارد.

اما در میان هیاهوی حملات سایبری اخیر این نکته شایان ذکر است که برای چنین سامانه زیرساختی مهم و حیاتی کشور چرا یک ساختار پشتیبان مجزا در یک شبکه کاملا مستتر که باید در چندین نقطه از کشور باشد در نظر گرفته نشده تا در چنین مواقع بحرانی به مدار سرویس‌دهی وارد شود.

این مورد و موارد دیگری که کارشناسان امنیت به آن اذعان دارند نشان از زیرساخت غیراصولی سیستم‌های حیاتی کشور دارد. چیزی که شاید زیاد در موردش خبررسانی نشد هک تابلوهای ترافیکی بود که آن هم در جای خود بسیار قابل بحث است و اینکه همزمانی این حملات با هم، وجود کدهای مخرب از مدت‌ها پیش در زیرساخت‌های کشور را نشان می‌دهد.

به بهانه این حملات بد نیست نیم‌نگاهی به پروژه Nitro Zeus بیندازیم.

■ پروژه Nitro Zeus چیست؟

در نخستین روزهای حضور باراک اوباما در کاخ سفید، هزاران افسر ارشد اطلاعاتی و نظامی ایالات‌متحده آمریکا مشغول کار روی پروژه‌ای شدند که با هدف فلج کردن و از کار انداختن تمام زیرساخت‌های حساس در ایران تشکیل شده بود. نام این طرح و پروژه «Nitro Zeus» بود و اگر به شکل عملیاتی اجرا می‌شد، قادر به از کار انداختن بخش‌های مهمی از زیرساخت‌های اقتصادی و اجتماعی در ایران بود، از جمله نیروگاه‌های برق، خطوط ارتباطی تلفن و حتی تجهیزات دفاع هوایی. این پروژه میلیون‌ها دلار هزینه داشته است تا بر اساس آن اقدام به طراحی و جاگذاری تجهیزات سایبری و الکترونیک در شبکه‌های رایانه‌ای ایران شده و در زمان مورد نیاز همه این ابزارها به عنوان یک ارتش آماده به خدمت، به کار گرفته شوند. این موضوعی است که «نیویورک‌تایمز» و همچنین وب‌سایت «Buzz Feed» به آن پرداخته‌اند. بر اساس این گزارش‌ها، پروژه Nitro Zeus به عنوان یک نقشه احتمال و در صورت به نتیجه نرسیدن مذاکرات هسته‌ای میان ایران و آمریکا مطرح شده بود. از آنجا که ایالات‌متحده از بابت حمله ناگهانی اسرائیل به ایران و وارد کردن آمریکا به یک جنگ ناخواسته نگرانی داشت، این پروژه را برای جلوگیری از چنین جنگی یا حداقل کوچک و محدود کردن آن راه‌اندازی کرده بود. نیویورک‌تایمز همچنین در گزارش خود اشاره کرد ایالات‌متحده پروژه و نقشه‌ای محدودتر برای از کار انداختن تأسیسات هسته‌ای فردو، در نظر داشته و پیاده کرده است، زیرا تأسیسات هسته‌ای در فهرست اولویت‌های ایالات‌متحده و رژیم مجعول صهیونیستی از بالاترین رتبه برخوردار بوده‌اند و این موضوع از زمانی که استاکس‌نت بیش از هزار سانتریفیوژ را در نطنز از کار انداخت در دست بررسی و اقدام بوده است. اما از آنجا که نفوذ به سایت فردو با مشکلات بیشتری همراه بوده است، این پروژه و نقشه به شکل اختصاصی بر نفوذ به این سایت با استفاده از یک بدافزار برای از کار انداختن تجهیزات و سیستم‌های رایانه‌ای سایت، طراحی شده بود. این گزارش‌ها نشان می‌دهد بدافزاری نظیر استاکس‌نت، تنها بخش کوچکی از این پروژه بزرگ بوده است. البته پروژه «Nitro Zeus» ریشه در دولت بوش دارد ولی سال‌های ۲۰۰۹ و ۲۰۱۰ به تکامل رسید. در آن سال‌ها اوباما از ژنرال آلن در ستاد فرماندهی مرکزی ارتش ایالات‌متحده خواست طرحی را برای مقابله با ایران در صورت شکست مذاکرات [برجام] آماده کند. یکی از مهم‌ترین بخش‌های این پروژه درباره نحوه به‌کارگیری ویروس استاکس‌نت است. آنگونه که گزارش BuzzFeed از محتوای مستند Zero Day بیان کرده، استاکس‌نت از مدت‌ها قبل مشغول عملیات بوده و آمریکا و اسرائیل توافق کرده بودند این ویروس به شکلی محدود، تنها تعدادی اندک از رایانه‌ها در ایران را آلوده کند تا سایر کشورها از آن مطلع نشوند اما سال ۲۰۰۹ یکباره این کرم بدافزار، برخی رایانه‌های خارج از پروژه را نیز آلوده کرد و به این ترتیب این عملیات افشا شد. گزارش Buzz Feed اشاره کرده که نسخه‌ای بسیار تهاجمی‌تر از استاکس‌نت توسط اسرائیلی‌ها طراحی و علیه ایران به کار گرفته شد که منجر به عصبانیت و آشفتگی متحدان آمریکایی شد. در این مورد یکی از منابع آمریکا به مستندسازان Zero Day گفته است: «این امر منجر به از بین رفتن سری بودن عملیات شد. دوستان اسرائیلی ما ابزاری که مشترک طراحی شده بود را یکجانبه به کار گرفتند و به این ترتیب عملیات را از حالت سری بیرون آورده و حتی احتمال بروز جنگ را ایجاد کردند».

با توجه به تمام این موارد لزوم افزایش امنیت در زیرساخت‌های کشور به‌شدت به چشم می‌خورد که تجهیزات تنها می‌تواند نیمی از این امنیت را شامل شود و نیمه گمشده دیگر این پازل، عدم دانش کافی مسؤولان و مدیران مربوط است.

*** کارشناس امنیت اطلاعات**

پی‌نوشت

* یک تهدید پیشرفته و مستمر یا APT، حمله پیچیده و مداومی است که در آن، یک مهاجم بدون اینکه شناسایی شود در یک شبکه حضور پیدا می‌کند تا در یک دوره زمانی طولانی، اطلاعات حساس را به سرقت ببرد. حمله APT برای نفوذ به یک سازمان خاص، با هدف گریز از اقدامات امنیتی موجود و عدم شناسایی، به دقت برنامه‌ریزی و طراحی می‌شود.

تیترهای امروز

رئیس قوه قضائیه:

هفت تپه را تنها نمی‌گذاریم

صفحه ۲

ارتش ترکیه مناطقی در حومه شمالی حلب را با گلوله‌های خمپاره هدف قرار داد

التهاب در شمال سوریه

صفحه ۷

آیا طالبان دیدگاه همسایگانش درباره مشارکت همه اقوام افغانستان در قدرت را می‌پذیرد؟

دولت فراگیر از شعار تا عمل

■ استقبال طالبان از نشست تهران

صفحه ۲

نگاهی به تازه‌ترین فیلم اصغر فرهادی قهرمان و تکرار ساختارگرایی

قهرمان کُشی

صفحه ۸

نگاه

صادرات لوازم خانگی نتیجه اعتماد به توان داخل

مهدی باقری: ایران سال ۹۸ زمان حضور شرکت‌های کره‌ای از صادرات لوازم خانگی ۱۷۰ میلیون دلار ارزآوری داشت؛ این در حالی است که سال ۹۹ بعد از خروج شرکت‌های ال‌جی و سامسونگ ۲۰۰ میلیون دلار صادرات داشته‌ایم و پیش‌بینی می‌شود با حمایت از این صنعت و ممنوعیت واردات لوازم خانگی، در ۱۰ سال آینده با توجه به رشد سالانه ۱۸ درصدی صادرات لوازم خانگی به صادرات ۹۰۰ میلیون دلاری در سال ۱۴۰۹ و صادرات بیش از یک میلیارد دلاری در سال ۱۴۱۰ برسیم. دستور اخیر رهبر حکیم انقلاب مبنی بر ممنوعیت واردات لوازم خانگی کره‌ای گام نخست حرکت صنعت لوازم خانگی به این سو است.

در مقیاس جهانی صادرات لوازم خانگی بعد از مشتقات نفتی، یکی از مهم‌ترین و ارزآورترین صنایع در دنیا محسوب می‌شود و به عنوان مثال چین سالانه ۹۳ میلیارد دلار، آلمان بیش از ۱۴ میلیارد دلار و ترکیه ۱۳ میلیارد دلار از صادرات لوازم خانگی ارزآوری دارند. در ایران نیز بعد از خروج شرکت‌های کره‌ای، توجه ویژه‌ای به این صنعت شد و به همین علت امروز صادرات لوازم خانگی یکی از مهم‌ترین صادرات ایران به کشورهای مختلف دنیاست.

از آنجا که در دهه‌های ۷۰ و ۸۰ اعتماد کمتری به توان داخلی بود، شرکت‌های مختلف مانند ال‌جی و سامسونگ به بازار لوازم خانگی ایران وارد شدند. آن زمان کمتر کسی فکر می‌کرد روزی بتوان از صادرات لوازم خانگی ارزآوری کرد و در این صنعت به خودکفایی رسید.

ادامه در صفحه ۶