گزارش
مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

بهمن ۱۴۰۰

امنیت سایبـــــری


بسم الله الرحمن الرحیم

فهرست

Iranian Council For
Defending The Truth

پیشگفتار

۱

پیشگفتار

مجمع ایرانی دفاع از حقیقت مادام همه تلاش خود را انجام می‌دهد که با به کارگیری شبکه‌ای از نخبگان در حوزه‌های مختلف سیاسی و شناختی گامی در جهت جلوگیری از ایجاد سوءتفاهم بردارد. در همین خصوص ما در مجمع ایرانی دفاع از حقیقت رسالت خود میدانیم تا با تهیه دیدبان‌هایی از موضوعاتی که به عنوان کارویژه برای خود انتخاب کرده‌ایم، چشم اندازی از مسیر را ارائه داده و در صورت توان پیشنهاداتی نیز برای کاهش این سوءتفاهم‌ها در آنان جای دهیم. ناگفته نماد که این دیدبان خود بخشی از راه حل کاهش سوءتفاهم است.

مجمع ایرانی دفاع از حقیقت
میز مطالعات امنیت

Iranian Council For
Defending The Truth

مقدمه

۲

مقدمه

اطلاع از اخبار و وضعیت فضای سایبر در ایالات متحده این امکان را فراهم می‌سازد تا با مسائل و مشکلات این حوزه سریع‌تر آشنا شده و هم‌چنین پیش از این که کشور ما نیز به آن مصائب و دشواری‌ها دچار گردد، راهکارهای اصلاحی را پیش‌بینی نماییم. از طرفی، با توجه به این که در اظهارات عمومی و جلسات رسمی مقامات این کشور برخی از نقاط ضعف دشمن در زمینه سایبری و فناوری‌های نوین بیان می‌گردد و با توجه به این نکته که بخش سایبری ایران توانایی آن را دارد که در تقابل با ایالات متحده از همین ضعف‌ها بهره‌برداری کند و به دشمن ضربه بزند؛ فلذا می‌توانیم از نقاط ضعف حریف استفاده نماییم و زمین بازی را به نفع خود تغییر دهیم و در موضع آفندی قرار بگیریم.

این تذکر ضروری است که با توجه به پیشگامی کشور امریکا در عرصه تکنولوژی، بررسی پیشرفت‌ها و برنامه‌ریزی‌های کلان این کشور در زمینه فناوری پیش‌بینی مقصد نهایی مسیر تکنولوژی در آینده را ممکن می‌سازد.

در بولتنی که در اختیار دارید اهم اخبار و اتفاقات کلان حوزه سایبر، تکنولوژی و فناوری‌های نوین جمع‌آوری شده است تا مخاطبین و فعالین در این زمینه بتوانند نسبت به وضعیت ایالات متحده از نگاهی جامع، کلان و به‌روز برخوردار شوند.

دیدکلی

در هفته‌ای که سپری شد با وجود آن که اخبار و گزارش‌های کمی را منتشر شد اما اتفاقات مهمی رخ داد که هر کدام می‌تواند مقدمه‌ای بر یک جریان خبری مستمر باشند. استمرار مناقشه اوکراین و روسیه همچنان ادامه دارد و از این رو این دو کشور پیش از ورود به درگیری نظامی و فیزیکی فعلاً در حال ارزیابی یکدیگر در عرصه سایبری هستند.

جاسوس‌افزار اسرائیلی پگاسوس نیز هم‌چون گذشته یک محور از گزارش ما را به خود اختصاص داده است. اخبار و گزارش‌های اخیر مدعی استفاده FBI و CIA از این نرم‌افزار به طور آزمایشی هستند.

در بخش بین الملل نیز حمله سایبری به دو شرکت بزرگ سوخت‌رسانی آلمان و اختلال‌آفرینی در سیستم‌های IT دیگر بنادر نفتی اروپا در محوریت قرار گرفته‌اند.

از این گذشته، قانون‌گذاری‌های ملی در حوزه سایبر در هر یک از بخش‌ها به فراخور عنوان ذکر شده ا ست .

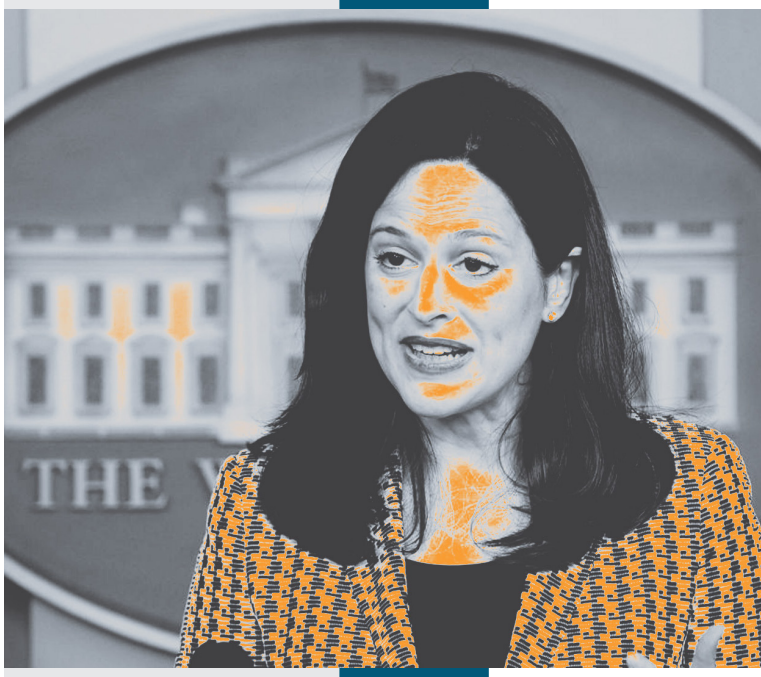
Iranian Council For
Defending The Truth

اخبار

۳

ایالات متحده

آن نوبرگر، معاون مشاور امنیت ملی، برای بحث در مورد مسائل سایبری به اروپا سفر می‌کند



آن نوبرگر، معاون مشاور امنیت ملی دولت بایدن در امور سایبری و فناوری های نوظهور، اوایل این هفته برای دیدار با مقامات اتحادیه اروپا و سازمان پیمان آتلانتیک شمالی به اروپا سفر کرد.

این دیدار در پی تشدید تنش ها و تهدیدهای تهاجم بین روسیه و اوکراین انجام می شود و بخشی از تلاش‌های دولت بایدن برای تقویت دفاع سایبری اوکراین و اروپا است. روسیه در گذشته زیرساخت‌های اوکراین را هدف قرار داده است و به نظر می‌رسد این بحران نیز تفاوتی با گذشته نداشته باشد. با این حال، ایالات متحده تیم‌هایی را به اوکراین و کشورهای اطراف خواهد فرستاد تا از وضعیت پدافند سایبری زیرساخت‌های حیاتی آنها پشتیبانی نماید و در صورت حملات سایبری روسیه به حفاظت از متحدان منطقه‌ای خود کمک کنند.

جامعه اطلاعاتی آمریکا درباره تهدیدات امنیتی ناشی از به اشتراک‌گذاری اطلاعات سلامت مردم با شرکت‌های خارجی هشدار داد

مرکز ملی ضد جاسوسی و امنیت (NCSC) در هشداری به صنعت متذکر شد که چندین شرکت آمریکایی با شرکت‌های چینی شراکت بالقوه خطرناکی دارند که شامل به اشتراک گذاری اطلاعات ژنتیکی و سایر اطلاعات زیست پزشکی است که می‌تواند برای نظارت به دولت چین تحویل داده شود.

اخطاریه هشدار می‌دهد که "ضرر قرارگرفتن اطلاعات DNA افراد در اختیار طرفین ناخواسته، ابدی و مانا خواهد بود و نه تنها بر همان فرد، بلکه بر بستگان آنها و احتمالاً نسل‌های آینده نیز تاثیر می‌گذارد."

NCSC از سال گذشته شروع به هشدار درباره خطرات همکاری با نهادهای چینی در مورد موضوعاتی مانند بیوتکنولوژی و هوش مصنوعی کرد. مایک اورلاندو، مدیر اجرایی NCSC در آن زمان گفت:« ما فکر می‌کنیم که بسیاری از این فناوری‌ها در خطر هستند. اگر برتری خود را در این حوزه ها از دست بدهیم... ممکن است به عنوان یک ابرقدرت بین المللی تحت الشعاع قرار بگیریم.»

پگاسوس

طبق گزارش‌ها FBI و CIA نرم‌افزارهای جاسوسی گروه NSO را خریداری کرده‌اند

برای اولین بار، FBI آزمایش نرم افزارهای جاسوسی NSO را تایید کرد

FBI چگونگی استفاده از جاسوس افزار پگاسوس را در تحقیقات جنایی مورد بررسی قرار داد، اما هرگز آن را در هیچ تحقیقی به کار نگرفت. به گزارش مجله نیویورک تایمز، اف‌بی‌آی تصمیم گرفت تابستان گذشته این نرم‌افزار جاسوسی را مستقر نکند، زمانی که واشنگتن پست و ۱۶ شریک رسانه‌ای دریافتند که از جاسوس‌افزارPegasus برای هدف قرار دادن تلفن‌های فعالان، مدیران و روزنامه‌نگاران در سراسر جهان استفاده می‌شود.

دیگر اخبار جاسوس‌افزارها: طبق گزارش تایمز اسرائیل، پلیس اسرائیل از نرم‌افزار جاسوسی برای هک کردن یک فرد کلیدی درگیر در پرونده جنایی علیه بنیامین نتانیاهو، نخست‌وزیر سابق، استفاده کرده است. مشخص نیست که آیا پگاسوس در این موضوع نقش داشته است یا خیر، اما رسانه های اسرائیلی گزارش دادند که مقامات این هک را به عنوان بخشی از تحقیقات در مورد گزارش‌هایی مبنی بر استفاده غیرقانونی پلیس این کشور از نرم افزارهای جاسوسی NSO کشف کردند. نتانیاهو این افشاگری را "زلزله" خواند.

جاسوس‌افزار Pegasus در تلفن‌های دیپلمات‌های فنلاندی شناسایی شد

وزارت خارجه فنلاند اعلام کرد که ابزار هک Pegasus گروه NSO در تلفن‌های دیپلمات‌های فنلاند شناسایی شده است. این خبر جدیدترین مورد از یک سلسله افشاگری است که نشان می‌دهد نرم‌افزار جاسوسی قدرتمند گروه NSO برای اهدافی غیر از وظایف اعلام‌شده ضدتروریسم و مطابق قانون استفاده شده است.

وزارت خارجه فنلاند گفت اطلاعات ذخیره شده در تلفن‌ها عمومی یا طبقه‌بندی شده در پایین‌ترین سطح است و بنابراین این نقض خطر امنیتی قابل توجهی ایجاد نمی‌کند. اخیرا چندین افشاگری مربوط به NSO Group منتشر شده است، از جمله اینکه FBI نرم افزار جاسوسی NSO Group را خریداری کرده، اما هرگز از آن استفاده نکرده است و اینکه گروه NSO تلاش کرده است تا دسترسی به معماری تلفن Signal-ing System ۷ را خریداری کند، که به NSO اجازه می‌دهد تا موقعیت مکانی یک دستگاه را ردیابی و به صورت پنهانی مسیر تماس‌های تلفنی و پیامک‌ها را نیز تغییر دهد.

روسیه و اوکراین

مجرمان سایبری از قوانین ارز دیجیتال روسیه ناامید شدند

مقامات روسیه قانون جدیدی را برای تنظیم ارزهای دیجیتال معرفی کردند. این قانون را می‌توان با تمایل دولت روسیه برای کنترل بازارهای دارک وب و بخش باج افزار آن که در دو سال گذشته پربار شده، مرتبط دانست.

از آنجایی که بسیاری از جرایم اقتصادی سایبری که از روسیه عملیات می‌کنند از ارزهای دیجیتال برای انتقال ثروت بهره می‌برند، این قانون باندهای باج افزار این کشور را تحت تأثیر قرار خواهد داد.

اخیراً سرویس‌های امنیتی روسیه اعضای گروه REvil را به درخواست ایالات متحده دستگیر کردند و این امر بر تصور مجرمان سایبری که طی سال‌ها روسیه را مکانی مناسب برای تعدی به اهداف خارجی و بدون مجازات می‌دانستند، تأثیر خواهد گذاشت. قوانین جدید، پولشویی‌هایی که توسط گروه‌های بزهکار انجام می‌شوند را نیز تحت تأثیر می‌گذارند.

یکی از توصیه‌های کلیدی بانک روسیه ممنوعیت مبادلات محلی به عنوان تنها ابزار برای ارتقای ثبات مالی، امنیت ملی و حمایت از مصرف کننده است.

یاداشت بانک روسیه اساساً به جرایم سایبری اختصاص ندارد. در عوض، نگاهی واقع بینانه به خطرات بالقوه ارزهای دیجیتال برای اقتصاد و امنیت انرژی کشورهای در حال توسعه دارد. بانک سه توصیه عمده دارد:

- ممنوعیت کامل استخراج ارزهای دیجیتال در روسیه.
- تعطیلی صرافی‌های ارز دیجیتال محلی.
- افزودن جریمه به قوانین موجود که استفاده از ارز دیجیتال برای خرید مستقیم را ممنوع می کند، اگرچه مانع از خرید یا مالکیت ارزهای دیجیتال از صرافی‌های خارجی نمی شود.

بانک نگران است که سرمایه‌گذاری گسترده در ارزهای دیجیتال به طور قابل‌توجهی عرضه پول ملی را کاهش دهد، سرمایه‌گذاری محلی را کاهش دهد و نوسانات بازار می‌تواند ثروت محلی را به طور کامل از بین ببرد.

همچنین بانک روسیه اشاره می‌کند که استخراج بیت کوین خطری برای امنیت انرژی این کشور خواهد بود و به طور بالقوه نیاز به برقی فراتر از توان تولیدی کشور روسیه دارد. با ایجاد قانون کریپتو، دولت روسیه یک مبنای قانونی برای تسلط بر کسب و کارهای مجرمانه باج افزاری ایجاد کرده است.


CRYPTORUBLE
GOLD STORAGE COIN

با مشاهده حملات سایبری جدید، ترس اوکراین از حمله روسیه افزایش یافت

حساب‌های رسمی ایمیلی متعلق به قوه قضاییه اوکراین، ایمیل‌هایی با ظاهری درست همراه با پیوست‌های حاوی نرم‌افزارهای مخرب ارسال نموده اند. مرکز ارتباطات استراتژیک و امنیت اطلاعات اوکراین گفت: اگر گیرندگان پیوست‌ها را باز کنند، هکرها می‌توانند به سیستم‌های رایانه‌ای شان دسترسی پنهانی داشته باشند.

این مرکز گفت، مشخص نیست که آیا هکرهای ارسال کننده ایمیل به برخی از حساب‌های ایمیل قوه قضاییه دسترسی پیدا کرده اند یا به کل سیستم ایمیلی.

این حملات سایبری در حالی انجام می‌شود که روسیه به افزایش نیرو در مرز خود با اوکراین ادامه می‌دهد. یک مقام ارشد وزارت امور خارجه ایالات متحده گفت احتمالاً مقامات ارشد امریکا و روسیه در این هفته برای آرام کردن اوضاع صحبت خواهند کرد. مقامات اوکراینی بر این باورند که روسیه مسئول حملات سایبری اخیر است که سیستم‌های کامپیوتری دولتی را از کار انداخته است.

بین‌الملل

استراتژی امنیت سایبری بریتانیا بر برگشت‌پذیری تمرکز دارد

دولت بریتانیا اولین استراتژی امنیت سایبری دولتی خود را در قالب یک طرح چند میلیون پوندی برای کمک به محافظت بهتر از خدمات عمومی حیاتی در برابر خطر فزاینده حملات سایبری راه اندازی کرد.

بر اساس بیانیه دولت، بخش خدمات عمومی بریتانیا جهت حفاظت بیشتر در برابر خطر توقف خدمات توسط تهدیدات سایبری خصمانه تقویت خواهد شد. عموم مردم نیز از طریق یک سرویس گزارش آسیب‌پذیری جدید که به افراد امکان گزارش ضعف‌های خدمات دیجیتالی را می‌دهد، قادر هستند در این تلاش مشارکت کنند.

این استراتژی جدید با سرمایه گذاری ۳۷.۸ میلیون پوندی برای کمک به مقامات محلی جهت تقویت برگشت‌پذیری سایبری خود، محافظت از خدمات و داده‌های ضروری که شهروندان به آنها متکی هستند، تأمین مالی می‌شود. وزیر استیو بارکلی گفت : بریتانیا در حال حاضر سومین کشور در جهان است که در فضای سایبری از سوی کشورهای متخاصم هدف قرار می‌گیرد.

استراتژی جدید رئوس کلی ارتقای انعطاف پذیری سایبری ملی را با به اشتراک‌گذاری بهتر داده‌ها، تخصصی نمودن و بهبود قابلیت‌ها توسط دولت مرکزی و بخش عمومی طرح ریزی می‌کند تا دولت بتواند به صورت یکپارچه دفاع کند. از ۷۷۷ حادثه مدیریت شده توسط مرکز ملی امنیت سایبری بین سپتامبر ۲۰۲۰ تا آگوست ۲۰۲۱، حدود ۴۰ درصد مربوط به بخش عمومی بوده است.

در سال ۲۰۲۰، شورای کلیولند و هکنی هر دو مورد حملات باج افزاری قرار گرفتند که بر مالیات، وام‌ها و لیست انتظار مسکن تأثیر گذاشت. شورای شهر گلاستر نیز در سال ۲۰۲۱ مورد حمله سایبری قرار گرفت.

به دنبال انتشار استراتژی اخیر امنیت سایبری ملی که از همه بخش‌های جامعه می‌خواهد تا نقش خود را در تقویت نقاط قوت اقتصادی بریتانیا در فضای سایبری، از طریق تنوع بیشتر در نیروی کار، ارتقاء سطح بخش سایبری در تمام مناطق بریتانیا ، گسترش قابلیت های تهاجمی و تدافعی سایبری و اولویت دادن به امنیت سایبری در محیط های کاری، اتاق های مدیریت و زنجیره های تامین دیجیتال، ایفا کنند.

اطلاعیه های کلیدی در استراتژی عبارتند از:

• ایجاد یک مرکز جدید هماهنگی سایبری دولتی (GCCC)، برای هماهنگی بهتر تلاش‌های امنیت سایبری در بخش عمومی.

• یک سرویس جدید گزارش دهی آسیب پذیری بین دولتی، که به محققان امنیتی و اعضای عمومی این امکان را می دهد تا مسائل مربوط به خدمات دیجیتال بخش عمومی را که شناسایی می کنند، به راحتی گزارش کنند. این امر سازمان‌ها را قادر می سازد تا هر مشکل شناسایی شده را سریع‌تر برطرف کنند.

• یک رژیم حفاظتی جدید و دقیق تر برای کل دولت، که شامل ارزیابی قوی از برنامه ها و آسیب پذیری های ادارات می شود. این امر برای اولین بار تصویر دقیق تری از سلامت سایبری را در اختیار دولت مرکزی قرار می دهد.

تامین کننده سوخت آلمان پس از حمله سایبری اعلام وضعیت اضطراری کرد

این حمله گروه Oiltanking GmbH و Mabanaft GmbH را هدف قرار داد. Oiltanking در مجموع ۱۳ مخزن را اداره می کند و مشتریان معمولی گوناگون و همچنین شرکت‌های بزرگ مانند شل را شامل می‌شود.

یک خبرگزاری آلمانی Handelsblatt که برای اولین بار این خبر را منتشر کرد، اظهار داشت که "تمامی سیستم‌های بارگیری و تخلیه نفتکش از کار افتاده اند." به گزارش Computer Weekly، به نظر می‌رسد این حمله بر سیستم‌های خودکار مورد استفاده برای پر کردن و تخلیه مخازن ذخیره سوخت در ۱۳ مرکز تاسیساتی آلمان تأثیر گذاشته است.

طبق گزارش دیگر روزنامه آلمانی، اشپیگل، از آن جایی که در حال حاضر ۲۶ شرکت در بازار سوخت مشغول به فعالیت هستند، خطر قطع عرضه در صنعت سوخت آلمان وجود ندارد.

شل، یکی از بزرگترین مشتریان این شرکت، همچنین اعلام کرد مادامی که آنها برای حل این مشکل تلاش می‌کنند، مسیر عرضه نفت را به انبارهای جایگزین تغییر خواهد داد.

این حمله در حالی صورت گرفت که آلمان که به شدت به نفت روسیه وابسته است، در نظر دارد در صورت تهاجم بیشتر روسیه به اوکراین، از قرارداد خط لوله گاز با روسیه خارج شود. آژانس‌های اطلاعاتی آلمان همچنین هفته گذشته هشداری درباره حملات سایبری توسط APT۲۷، یک گروه هکری مستقر در چین، صادر کرد.

مقامات اروپایی: سلسله حملات سایبری به بخش های نفت و شیمیایی اروپا احتمالا هماهنگ و مرتبط به هم نیستند

دادستان‌های اروپایی و مقامات امنیت سایبری در حال بررسی حمله باج‌افزاری هستند که چند بندر مهم نفتی را تحت تأثیر قرار داده است. این حمله تنها چند روز پس از هک دو شرکت آلمانی رخ داد که تأمین‌کنندگان نفت را مجبور ساخت مسیر انتقال محصولات خود را به مخاذن جایگزین تغییر دهند.

این حملات سازمان هایی را در بلژیک، هلند و آلمان از جمله برخی از بزرگترین بنادر منطقه هدف قرار دادند. مقامات امنیت سایبری این کشورها روز پنجشنبه اعلام کردند که شاهدی دال بر ارتباط این حملات به یکدیگر وجود ندارد.

در یک گزارش داخلی از اداره فدرال امنیت اطلاعات آلمان (BSI) آمده است که گروه بلک‌کت (Black-Cat)، که در تعدادی از حملات اخیر دست داشته ، پشت حمله اخیر به دو شرکت صنعت نفت آلمان بوده است.

میانمار همزمان با اعلام قانون جدید امنیت سایبری، VPN ها را نیز ممنوع کرد

طبق گزارش‌ها، دولت نظامی میانمار قرار است قانون محدودکننده جدیدی را برای امنیت سایبری تصویب کند که استفاده از شبکه‌های خصوصی مجازی (VPN) را جرم انگاری می‌کند. VPN ها شهروندان را قادر می‌سازد قوانین اینترنتی دولتی را دور بزنند و به سایت‌های ممنوعه مانند فیس‌بوک دسترسی داشته باشند.

VPN ها در میانمار به ویژه در طول قطعی اینترنت تحمیلی توسط ارتش، که از زمان کودتای نظامی فوریه گذشته برای هفته‌ها ادامه داشته است، بسیار حیاتی هستند. طی سال گذشته، دولت نظامی نظارت بر اینترنت را افزایش داده، کنترل شرکت‌های مخابراتی و ارائه دهندگان خدمات اینترنتی را به منظور نظارت بر شهروندان خود و سانسور گفتار آنلاین مستحکم کرده است. محدودیت‌های اینترنت در سراسر آسیای جنوب شرقی در حال گسترش است. کامبوج کنترل‌های اینترنت به سبک چین را اتخاذ نموده و درگاه اینترنتی ایجاد کرده است که از طریق آن تمام ترافیک وب ردیابی و نظارت می‌گردد.

اینترنت کره شمالی در تزلزل است

هر وب سایت در کره شمالی حداقل دو مورد در ماه گذشته دچار قطعی کامل شده است. به نظر می‌رسد اینترنت این کشور با دو قطعی کامل مواجه شده که احتمالاً ناشی از حمله ردّ سرویس توزیع شده (DDoS) بوده است.

کارشناسان فکر می‌کنند که این اختلالات نتیجه حملات سایبری علیه کره شمالی باشد، گرچه حدس‌های محتمل دیگری نیز وجود دارد.

کره شمالی قطعی‌های متناوبی را تجربه کرده است تا اینکه طی یک حادثه در ۱۴ ژانویه تمام وب سایت های این کشور فلج شد به نحوی که دامنه‌های اینترنتی که به ".kp" ختم می‌شدند و متعلق به وب سایت‌های رسانه‌های دولتی کره شمالی بودند، از کار افتادند.

یک تناقض بر سر دسترسی به فناوری در کره شمالی وجود دارد. در حالی که حدود ۱۰ درصد از مردم کره شمالی تلفن هوشمند دارند و رایانه‌های شخصی در دسترس هستند، اکثریت شهروندان از دسترسی به شبکه جهانی وب محروم هستند. آن‌ها می‌توانند به اینترانت کشور، شامل وب‌سایت‌های خبری کره شمالی، آشپزی و موضوعات بی‌ضرر دسترسی داشته باشند، اما نمی‌توانند به وب‌سایت‌های خارجی نزدیک شوند.

کاربران تلفن همراه قادر به برقراری تماس با خارج از کشور یا دسترسی به شبکه جهانی نیستند.

نحوه اختلال در اتصالات نشان می‌دهد که کل زیرساخت فناوری اطلاعات کره شمالی توسط یک حمله ردّ سرویس توزیع شده (DDOS) آسیب دیده است. شبکه وب کره شمالی تنها حدود ۱۰۰۰ آدرس وب دارد و برای تعداد انگشت شماری از مقامات دولتی قابل دسترسی است. شرکت های فناوری آمریکایی که اینترنت کره شمالی را رصد می کنند، بیان نمودند که به نظر می رسد شبکه اینترنت در این کشور متحمل یک حمله DDoS شده و در آن تجهیزات اینترنتی هدف تحت تأثیر ترافیک ساختگی قرار گرفته است.

همچنین قطعی‌های اینترنت می‌تواند نتیجه کمبود برق داخلی یا سایر مسائل زیرساختی محلی باشد، اما ماهیت قطعی‌های اخیر را کارشناسان غیرعادی می‌دانند. به نظر می‌رسد قطعی اینترنت اغلب در کره شمالی اتفاق می افتد، برای نمونه سال گذشته در پی یک به روز رسانی نرم افزاری ناکارآمد، رسانه‌های دولتی از دسترس خارج شدند.

برخی گمانه‌زنی‌ها نیز اختلالات ایجاد شده را نتیجه اقدامات ایالات متحده، چین یا هر کشور دیگری می‌دانند که با کره شمالی دشمنی دارند.


http://www

ICDT.IR