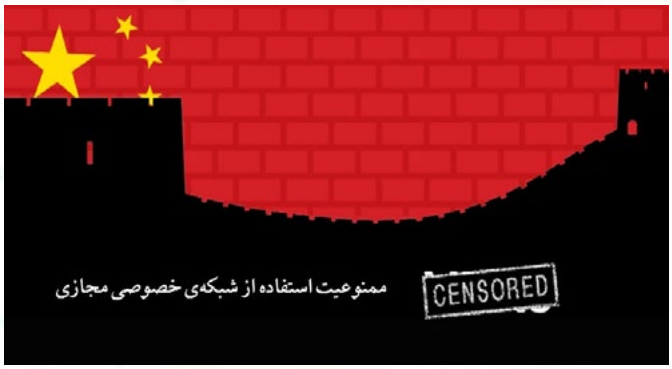
خبرنامه مدیریتی سراج
مرکز نرم‌افزار و سرویس وخدمات سازمان فضای مجازی سراج

اخبار فناوری اطلاعات و ارتباطات

۹۱

هفته نامه | سال دوم | شماره نود و یکم | ۹ بهمن ۱۳۹۵

سپر طلایی چین و ممنوعیت استفاده از شبکه‌ی خصوصی مجازی



مدت طولانی است که کشور چین به قوانین سخت‌گیرانه در خصوص سانسور اینترنت با استفاده از یک دیواره‌ی آتش قوی و بزرگ در این کشور شناخته می‌شود. این دیواره‌ی آتش، سپر طلایی چین نام دارد و محدودیت‌ها و سانسورهای مختلفی را در دسترسی کاربران به وب‌گاه‌های خارجی اعمال می‌کند.

این دیواره‌ی آتش بزرگ نزدیک به 171 مورد از هزار وب‌گاه برتر دنیا از جمله گوگل، فیس‌بوک، توییتر، تامبلر و دراپ‌باکس را مسدود کرده است. بنابراین برای دور زدن این محدودیت‌ها و دسترسی به این وب‌گاه‌ها، صدها هزار نفر از شهروندان چینی از شبکه‌ی خصوصی مجازی (VPN) استفاده می‌کنند.

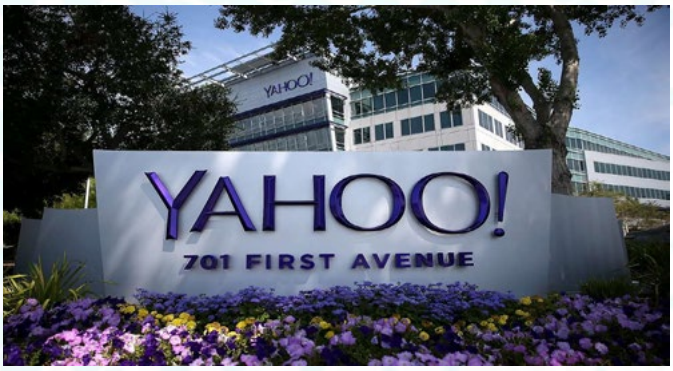
به گزارش خبرگزاری‌ها، اخیراً دولت چین اعلام کرده در تلاشی گسترده سعی دارد تمامی شبکه‌های خصوصی مجازی را از کار بیندازد و با این کار دسترسی به وب‌گاه‌های خارجی برای کاربران چینی بسیار سخت خواهد شد.

در برنامه‌ای با عنوان «پاک‌سازی» اتصالات اینترنت در چین، وزارت صنایع و فناوری این کشور اعلام کرد در یک تلاشِ 14 ماهه تمامی اتصالات VPN را از کار انداخته است. سرویس‌های VPN با رمزنگاری ترافیک کاربر و مسیریابی این ترافیک از طریق اتصالات راه دور، مکان کاربر در چین را مخفی کرده و می‌توانند محدودیت‌ها و سانسورها را دور بزنند.

در قانون جدید، استفاده و راه‌اندازی سرویس VPN محلی بدون تأیید دولت، غیرقانونی محسوب شده و نیاز است تمامی اتصالات و کابل‌های VPN موجود در چین همگی دارای مجوز از نهادهای دولتی باشند.

علاوه بر این تمامی ارائه‌دهندگان سرویس اینترنت (ISP)، ارائه‌دهندگان سوریس آبر و نمایندگی‌های فروش VPN باید خود-بازرسی داشته و بر عملیات غیرقانونی بر روی کارگزارهای خود نظارت داشته باشند. ممنوعیت استفاده از سرویس VPN و اتصالات کابلی به سرعت اجرا شده و تا 11 فروردین ماه سال 97 برقرار خواهد بود.

یاهو تحت بازرسی: چرا نقض داده‌ی عظیم در این شرکت دیر اطلاع‌رسانی شده است؟



یاهو در شرایط سختی به سر می‌برد و در بررسی‌های سازمان بورس و اوراق بهادار آمریکا، از یاهو سؤال شده چرا در گزارش این نقض داده به مشتریان و سهام‌داران خود کُند عمل کرده است.

سازمان بورس و اوراق بهادار آمریکا بررسی‌هایی را برای نقض داده‌ی یاهو راه‌اندازی کرده است. این سازمان بیشتر تلاش می‌کند بفهمد آیا افشای این نقض داده توسط یاهو مطابق با قوانین امنیتی و مدنی بوده است یا خیر.

یاهو مدعی شده که در یک دوره‌ی سه ماهه با ارائه‌ی اسنادی با سازمان‌های اطلاعاتی، دولت‌های خارجی و سازمان‌های فدرال و ایالتی همکاری داشته تا به آن‌ها اطلاعاتی راجع‌به این حادثه‌ی امنیتی بدهد.

سال گذشته، شرکت یاهو دو نقض داده‌ی بزرگ را در تاریخ امنیت اینترنت، به کاربران خود اطلاع داد. این نقض داده‌ها بقدری بزرگ بود که گفته می‌شد نهادهای حکومتی و دولتی پشت این نفوذها بوده‌اند.

اولین نقض داده در شهریور ماه گزارش شد. آن زمان گفته می‌شد در این نفوذ نزدیک به 500 میلیون کاربر تحت تأثیر قرار گرفته‌اند. یاهو اعتراف کرد نفوذگران در این حمله اطلاعاتی مانند نام، آدرس رایانامه، شماره تلفن، تاریخ تولد، گذرواژه‌های درهم‌سازی‌شده به علاوه‌ی سؤالات و پاسخ‌های رمزنگاری شده یا نشده را به سرقت برده‌اند. ولی اطلاعات حساسی مانند اطلاعات حساب‌های بانکی و کارت‌های اعتباری از آسیب نفوذگران دور مانده‌اند.

مشکل اینجاست که تقویباً یک ماه قبل از اطلاع‌رسانی رسمی یاهو، نفوذگران اطلاعات 200 میلیون حساب کاربری یاهو را در وب تاریک به فروش گذاشتند. این اطلاعات مربوط به سال 2014 بود. این شرکت اعلام کرد در حال بررسی شرایط بوده درحالی‌که دو ماه قبل از آن، یاهو از این نقض داده‌ی عظیم باخبر شده است.

نفوذ دوم که در نوع خود بی‌سابقه‌ترین نفوذ تاریخ است، در آذر ماه اطلاع‌رسانی شد. یاهو در ادامه اعتراف کرد که نزدیک به 1 میلیارد حساب کاربری در معرض خطر قرار گرفته است.

در برنامه‌ی پاداش در ازای اشکال ارتش آمریکا ۱۱۸ آسیب‌پذیری وصله شد

ارتش آمریکا روز پنج‌شنبه نتایج اولین برنامه‌ی پاداش در ازای اشکال خود را به اشتراک گذاشت. این برنامه از 1 دی ماه به مدت 3 هفته در حال برگزاری بود و خبرها حاکی از آن است که این برنامه با موفقیت انجام شده است.

پس از موفقیت برنامه‌ی نفوذ به پنتاگون، این دومین برنامه‌ی پاداش در ازای اشکال بود که در سطح سازمان‌های دولتی انجام می‌شد. مقامات دولتی پورتال‌ها و پایگاه داده‌های خود را در اختیار نفوذگران کلاه سفید و محققان امنیتی قرار دادند تا بر روی آن تست نفوذ انجام داده و آسیب‌پذیری‌های ممکن را کشف کنند.

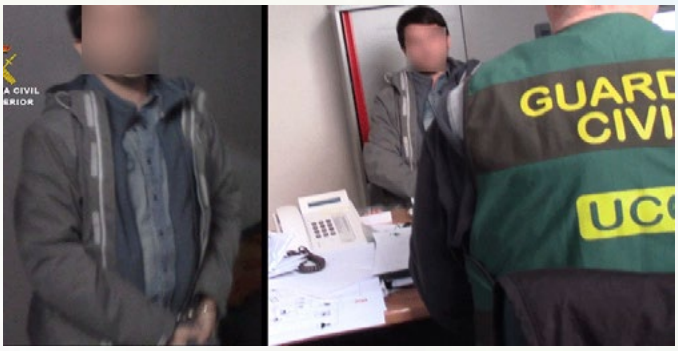
وزیر سابق ارتش آمریکا گفت: «ارتش در این برنامه توانست با گروهی از فناوری‌ها و محققان امنیتی به‌طور مستقیم در ارتباط باشد، موضوعی که شاید قبلاً از آن خودداری می‌کرد.»

ارتش آمریکا روز پنج‌شنبه اعلام کرد بیش از 400 گزارش آسیب‌پذیری دریافت کرده است که 118 مورد از آن‌ها منحصربفرد و عملیاتی هستند. به شرکت‌کنندگانی که اشکالی منحصربفرد را گزارش داده‌اند، بیشترین مقدار جایزه به مبلغ 100 هزار دلار پرداخت شده است. ارتش از 371 محقق امنیتی دعوت کرده بود تا در این برنامه شرکت کنند و 25 نفر از شرکت‌کنندگان از کارکنان دولتی از جمله 17 نفر نیروهای ارتش بودند.

ارتش همچنین جزئیات سطح بالایی از چندین آسیب‌پذیری بر روی وب‌گاه goarmy.com را به اشتراک گذاشت. این آسیب‌پذیری‌ها توسط یکی از شرکت‌کنندگان کشف شده بود و زنجیره‌ای از این آسیب‌پذیری‌ها دسترسی به وب‌گاه‌های داخلی وزارت دفاع آمریکا را بدون احراز هویت در اختیار مهاجمان قرار می‌داد.

برنامه‌های نفوذ به پنتاگون و برنامه‌ی پاداش در ازای اشکال ارتش توسط HackerOne برگزار شده است. HackerOne در یک پست گفت: «در سطح شبکه یک پروکسی باز وجود داشت که فرآیند مسیریابی نیز از طریق آن انجام می‌شد. به دلیل وجود آسیب‌پذیری در این پروکسی، محققان امنیتی می‌توانستند به شبکه‌های داخلی ارتش دست یابند. به خودی خود، هر یک از آسیب‌پذیری‌ها قابل توجه بودند ولی وقتی با یکدیگر ترکیب می‌شدند مسئله‌ای جدی رخ می‌داد.»

دستگیری نفوذگر روسی، نویسنده‌ی بدافزار NeverQuest



یک نفوذگر روسی که توسط FBI به جرم نفوذ به رایانه‌ها تحت تعقیب بود، اوایل این هفته در اسپانیا دستگیر و راهی زندان شد. هنوز در رابطه با استرداد این نفوذگر به آمریکا تصمیمی اتخاذ نشده است.

گواردیا سیویل، افسر آژانس اطلاعاتی اسپانیا، در فرودگاه بارسلونا این نفوذگر 32 ساله با نام استانیسلاو لیسو را با حکم بازداشت پلیس اینترپل و به درخواست FBI دستگیر کرده است.

لیسو به جرم ایجاد و انجام فعالیت مخرب با تروجان بانکی NeverQuest دستگیر شده است. این بدافزار مؤسسات مالی در سرتاسر جهان را هدف قرار داده و بالغ بر 5 میلیون دلار ضرر و زیان به بار آورده است.

این دستگیری پس از آن انجام شد که مقامات اطلاعاتی آمریکا اعلام کردند نفوذگران روسی پشت نفوذهای آبان ماه به انتخابات ریاست جمهوری آمریکا بوده‌اند و احتمالاً در انتخاب دونالد ترامپ به‌عنوان رئیس جمهور آمریکا تأثیرگذار بوده‌اند.

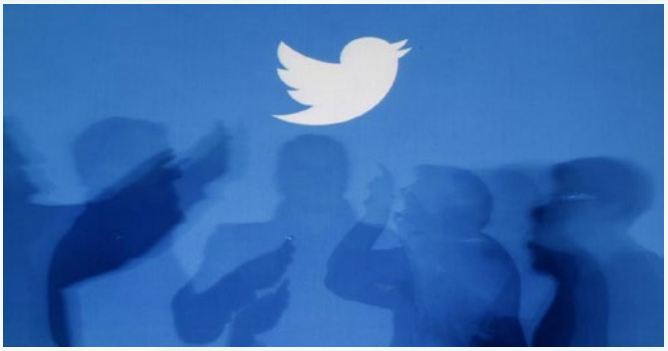
با این حال پلیس اسپانیا در بیانیه‌ای رسمی اعلام کرد با بررسی‌هایی که از سال 2014 شروع شده بود، FBI لیسو را تحت تعقب قرار داده بود. تروجان بانکی NeverQuest به کلاه‌برداران سایبری اجازه می‌داد به رایانه‌های افراد و مؤسسات مالی دسترسی یافته و داده‌های بانکی آن‌ها را به سرقت ببرند.

این بدافزار از طریق شبکه‌های اجتماعی، رایانامه‌ها و پروتکل‌های انتقال پرونده توزیع می‌شود و می‌تواند محتوای وب‌گاه‌های بانکی را دستکاری کرده و فرم‌های جعلی در آن قرار دهد. از طریق این فرم‌ها، مهاجمان می‌توانند گواهی‌نامه‌های حساب‌های کاربران را به دست آورند.

این بدافزار همچنین به مهاجمان اجازه می‌دهد با استفاده از کارگزار پردازش شبکه‌ی مجازی، کنترل دستگاه آلوده را در اختیار بگیرند. در ادامه از این رایانه‌ها برای ورود به حساب‌های بانکی و مالی قربانیان و کلاه‌برداری استفاده می‌شود.

افسر اسپانیایی در توضیحات خود گفت: «در بررسی که بر روی کارگزارهای لیسو در فرانسه و آلمان انجام دادیم، فهرستی از اطلاعات را در پایگاه داده‌های آن مشاهده کردیم که در این بین مانده حساب قربانیان نیز به چشم می‌خورد.

نفوذ به حساب توییتر بی‌بی‌سی و خبر جعلی تیراندازی به دونالد ترامپ



دیروز حساب توییتر متعلق به بی‌بی‌سی مورد نفوذ قرار گرفت و در آن پیامی بسیار عجیب منتشر شد. در این پیام آمده است: «آخرین اخبار: رئیس جمهور منتخب، دونالد ترامپ در اثر تیراندازی از ناحیه‌ی بازو زخمی شد.»

این پیام مدت کوتاهی پس از انتشار حذف شد و این خبرگزاری اعلام کرد این پیام نادرست بوده و از طرف نفوذگرانی که کنترل حساب کاربری را در دست داشتند منتشر شده است.

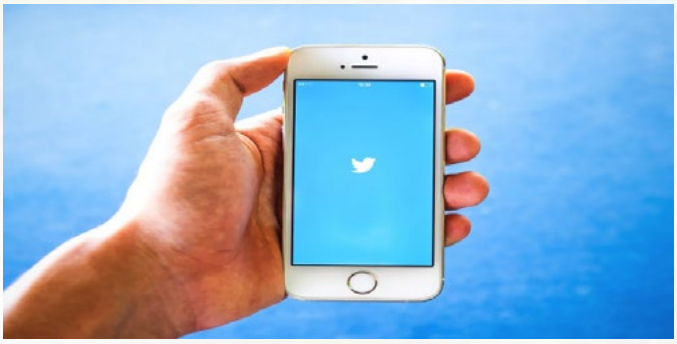
بی‌بی‌سی اعلام کرد در حال حاضر نمی‌داند چه کسانی پشت این حملات هستند و گفت: «ما در حال پیگیری ماجرا هستیم و گام‌هایی را طی می‌کنیم تا مطمئن شویم چنین اتفاقاتی دیگر رخ نخواهد داد.»گروه نفوذ OurMine کنترل حساب مورد نفوذ قرار گرفته را در دست گرفتند و توییتی را از آن منتشر کردند که این نقض را افشاء کرد. در پیام گروه OurMine آمده است: «ما فعالیت‌های غیرعادی را در این حساب کاربری شناسایی کردیم. این حساب توسط یک نفر مورد نفوذ قرار گرفته بود و ما سعی کردیم این اشکال را برطرف کنیم.» گروه OurMine با فاصله‌ی کوتاهی از انتشار پیام زنده بودن ترامپ، توییت خود را ارسال کرد.

براساس گزارش بی‌بی‌سی که پس از این نفوذ با گروه OurMine تماس گرفت، این گروه نفوذ آمریکایی مسئول نفوذ به حساب توییتر بی‌بی‌سی و انتشار خبر کشته شدن دونالد ترامپ نبوده است.

گروه نفوذ OurMine گفت: «ما در مرحله‌ی اول به حساب بی‌بی‌سی نفوذ نکردیم. ما بعد از مشاهده‌ی فعالیت‌های مشکوک در این حساب، دوباره به آن نفوذ کردیم تا مطمئن شویم که نفوذ رخ داده یا خیر. ولی متأسفانه این حساب مورد نفوذ قرار گرفته بود. ما فقط توییتی در این حساب ارسال کردیم و اطلاع دادیم که این حساب مورد نفوذ قرار گرفته است. ما هیچ‌گاه به هیچ حسابی بدون دلیل نفوذ نمی‌کنیم. ما یک گروه نفوذ امنیتی هستیم.»

گروه OurMine در گذشته توانسته بود به چند حساب کاربری سطح بالا در توییتر نفوذ کند. از جمله‌ی این حساب‌های توییتر، می‌توان نت‌فلیکس، Marvel و سایر شرکت‌ها را نام برد. هرچند، این گروه نفوذ هیچ‌گاه سعی نکرده اخبار نادرست یا بدافزار را از طریق این نفوذها توزیع کند و بیشتر نشان دادن ضعف امنیتی در حساب‌های قربانی مدنظر این گروه بوده است.

ناتو: نفوذگران سایبری هر ماه ۵۰۰ بار به اتحادیه حمله می‌کنند



سخنگوی ارتش اتحادیه‌ی ناتو اعلام کرد ناتو به هدفی برای تمام نفوذگران در سراسر دنیا تبدیل شده است و به‌طور میانگین هر ماه 500 حمله‌ی سایبری علیه این اتحادیه انجام می‌شود. این حملات در سال گذشته نسبت به سال 2015 افزایش 60 درصدی داشته است.

برای شناسایی مهاجمان بررسی‌های زیادی صورت گرفته است ولی در بسیاری از موارد، کشف اینکه حمله توسط چه کسانی انجام شده، کار بسیار دشواری است. سخنگوی این اتحادیه گفت: «دولت‌های خارجی، مهاجمان سایبری و تروریست‌ها می‌توانند منشأ این حملات باشند با این حال انتساب حملات کار سختی است. البته بسیاری از کشورها دارای منابع بزرگی در حوزه‌ی سایبری هستند و مسئولیت بسیاری از حملات علیه ناتو برعهده‌ی چنین کشورهایی است.»

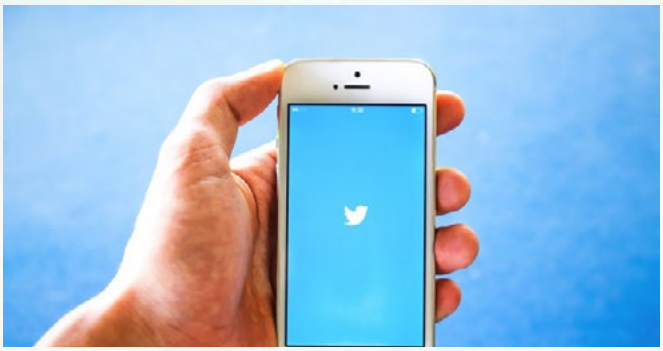
ناتو اواسط سال 2016 تصمیم گرفت حملات سایبری را نیز مانند حملات مسلحانه‌ی معمولی قلمداد کند و به نفوذگران خارجی هشدار داد در صورت حمله به دولت‌های عضو اتحادیه، طبق ماده‌ی 5 با آن‌ها برخورد خواهد شد.

در اغلب موارد این‌گونه تصور می‌شود که دولت روسیه پشت بسیاری از نفوذهای سایبری است. همان‌طور که در انتخابات ریاست جمهوری آمریکا نیز گفته می‌شود کرملین با کمک شهروندان خود در آمریکا، در روند انتخابات دخالت کرده و نفوذهای متعددی را علیه حزب دموکرات انجام داده است.

همزمان دولت‌های اروپایی نیز در خصوص حملات سایبری روسیه و نفوذ به رایانه‌های این کشورها هشدار دادند. کشورهای اروپایی ادعا می‌کنند دولت روسیه سعی دارد با نفوذهای سایبری در روند انتخابات کشورهای دیگر اختلال ایجاد کند.

در طرف دیگر، دولت روسیه تمامی این ادعاها و اتهامات را رد کرده و اعلام کرد دولت روسیه خود هدف حملات سایبری دولت‌های خارجی قرار گرفته است. دولت روسیه در دی ماه اعلام کرد شواهدی پیدا کرده که سرویس‌های اطلاعاتی از کشورهای خارجی تلاش می‌کنند مؤسسات مالی و بانک‌های روسیه را از کار بیندازند.

نفوذ به حساب توییتر نیویورک تایمز و خبر جعلی حمله‌ی موشکی روسیه به آمریکا

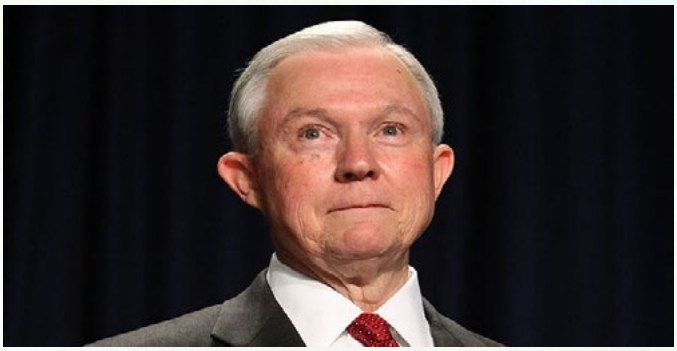


نیوریورک تایمز در حال بررسی نفوذ به حساب توییتر خودش است که توسط OurMine انجام شده و در روز یکشنبه خبرهایی جعلی را منتشر کرده است.

حساب @nytvideo حساب ویدئویی توییتر متعلق به روزنامه‌ی آمریکایی نیویورک تایمز است که بیش از 250 هزار دنبال‌کننده دارد. دیروز ساعت 9:40 در این حساب یک خبر جعلی درباره‌ی حمله‌ی موشکی روسیه علیه آمریکا منتشر شد. این خبر در مورد حمله‌ی موشکی باعنوان بیانیه‌ای از طرف ولادیمیر پوتین منتشر شده بود. این خبرهای جعلی به سرعت حذف شد در حالی‌که در توییت‌های دیگری به دخالت گروه OurMine در انتشار خبرهای جعلی اشاره شده بود. این گروه نفوذ که در دی ماه نیز به حساب توییتر نت‌فلیکس حمله کرده بود، در تلاش است با این کار به شناساندن وب‌گاه و سرویس‌های نفوذ خود بپردازد و در حال حاضر با نفوذهای خود به حساب‌های سطح بالای توییتر شناخته می‌شود.

در فهرست قربانیان این گروه که به حساب‌های توییتر آن‌ها نفوذ شده می‌توان مدیرعامل فیس‌بوک، مارک زوکربرگ، مدیرعامل فعلی و سابق توییتر و مدیرعامل گوگل را مشاهده کرد. در پیامی که توسط OurMine ارسال شده بود، تأیید شد که این گروه مسئول نفوذ به حساب موسیقی سونی در توییتر بوده و خبرهای جعلی در خصوص مرگ بریتنی اسپیرز منتشر کرده است.

دادستان منتخب ترامپ: باید در رمزنگاری‌ها دربِ پشتی داشته باشیم



جف سشنز، دادستان کلِ منتخب ترامپ، معتقد است استفاده از رمزنگاری‌های قوی بسیار عالی است ولی باید مقامات راهی برای شکستن آن داشته باشند.

باتوجه به اهمیت رمزنگاری، سشنز معتقد است نهادهای امنیتی و بررسی‌کننده‌ی جرائم باید راهی برای دور زدن این حفاظت‌ها داشته باشند. به‌نظر می‌رسد دیدگاه‌های سشنز با دیدگاه رئیس جمهور فعلی آمریکا، دونالد ترامپ هماهنگ است.

در بحثی که بین اپل و FBI در باز کردن قفل آیفون تیرانداز در حادثه‌ی سان‌برنادیو پیش آمد، ترامپ معتقد بود اپل باید با نهادهای اطلاعاتی همکاری می‌کرد و در غیر این‌صورت تحریم می‌شد. ترامپ می‌گوید: «آن‌ها فکر می‌کنند کی هستند؟ هیچ‌کس. ما باید در چنین مواردی بتوانیم تلفن همراه را باز کنیم.»

تمامی دیدگاه‌های ترامپ در خصوص رمزنگاری، امنیت برخط و هرچیز مرتبط با رایانه به‌روز نبوده و نشان می‌دهد او هیچ درکی از این مباحث ندارد. این موضوع را می‌توان از حساب توییتر او فهمید. دیدگاه‌های سشنز نیز بازتابی از دیدگاه‌های ترامپ است هرچند او به‌طور صریح در این‌باره اظهارنظر نکرده است.

از سشنز سوال شد که آیا استفاده از رمزنگاری قوی را برای حفاظت از آمریکا در برابر حملات سایبری مفید می‌داند و او در پاسخ گفت: «رمزنگاری موضوعی مهم و ارزشمند است. همچنین ضروری است که نهادهای امنیتی و بررسی‌کننده‌ی جرائم قادر باشند در صورت لزوم و برای پیشبرد امنیت ملی و تحقیقات جنایی آن را رمزگشایی کنند.»

بنابراین تنها راهی که به ذهن همگان برای دور زدن رمزنگاری می‌رسد، استفاده از دربِ پشتی در ویژگی‌های امنیتی است و این خواست نهادهای اطلاعاتی نیز هست. با قدرت گرفتن افرادی همچون سشنز نمی‌توان گفت که در آینده چه اتفاقی خواهد افتاد. قوانین تضعیف امنیت سایبری بدون شک مخالفت‌هایی بدنبال خواهد داشت.