گزارش
مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

خرداد ۱۴۰۰

امنیت سایبری


بسم الله الرحمن الرحیم

فهرست

Iranian Council For
Defending The Truth

مقدمه

۱

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 از طرفی، به اعتراف مسئولین امریکایی بخش سایبری ایران از این توانایی برخوردار است که در تقابل با ایالات متحده از همین ضعف‌ها بهره‌برداری کند و به دشمن ضربه بزند. در نتیجه ما می‌توانیم زمین بازی را به نفع خود تغییر داده 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 این حوزه از مسائل بتوانند نسبت به وضعیت ایالات متحده از نگاهی جامع، کلان و به‌روز برخوردار شوند.

دیدکلی

رشد روزافزون عملیات‌های باج‌افزاری در جهان، نگرانی‌های قابل توجهی را در خصوص نحوه مقابله با آنها در میان کارشناسان و مقامات امنیتی بر انگیخته است. مقامات و مسئولین امریکایی که کشورشان را آماج اصلی این حملات یافته اند، تنظیم و اصلاح مقررات و گسترش نیروی انسانی متخصص را در اولویت قرار داده اند. نظارت و کنترل بیشتر بر پلتفرم‌های اینترنتی مهم‌ترین دغدغه این روزهای امنیت-سایبر است.

Iranian Council For
Defending The Truth

اخبار

۲

سایبر ایالات متحده

ایمن‌سازی خطوط لوله در برابر هک

در هفته‌های گذشته، حمله باج‌افزاری به Colonial Pipeline سبب کمبود گاز و افزایش قیمتی که در جنوب شرقی آمریکا ایجاد نمود منجر به آشفتگی در بخش انرژی و هرج و مرج در میان مصرف‌کنندگان امریکایی گردید. این اتفاق آسیب‌پذیری زیرساخت‌های حیاتی ایالات متحده را آشکار نمود. به همین خاطر بلافاصله قانون‌گذاران و مقامات فدرال در این کشور تلاش نمودند تا با وضع قوانین و مقررات جدید از وقوع چنین حوادثی در آینده پیش‌گیری نمایند.

نماینده جیم لانگوین ، بنیانگذار کمیسیون امنیت سایبری کنگره در این رابطه اظهار داشت: هک Colonial Pipeline به ما یاد داد که زیرساختهای حیاتی ما فوق العاده در برابر حمله سایبری آسیب پذیر است.

در اولین قدم از تلاش‌های چندجانبه برای جلوگیری از تکرار باج‌افزار خط لوله Colonial، وزارت امنیت داخلی شرایط سخت‌گیرانه جدید امنیت سایبری را برای شرکت‌های خط لوله صادر نمود. مطابق پیش‌نویس این قوانین ، در گام نخست، شرکت‌های خط لوله ملزم می‌شوند در صورت مواجه شدن با هرگونه اختلال در عملکردشان از طریق حملات سایبری یا حتی تهدید شدن به اختلال، ظرف ۱۲ ساعت به "آژانس امنیت سایبری و امنیت زیرساخت" اطلاع دهند. این شرکت‌ها همچنین باید یک مسئول هماهنگ‌کنند امنیت سایبری را استخدام نمایند که به طور شبانه‌روزی با مقامات DHS در ارتباط باشد. او باید در صورت عدم رعایت قوانین امنیت سایبری موجود "اداره امنیت حمل و نقل "، ظرف ۳۰ روز به CISA و TSA۲ گزارش دهد. در صورت کوتاهی در این حفاظت‌های سایبری ، شرکت ها با مجازات های مالی روبرو می شوند.

پیش از این انجام مقررات حفاظتی TSA به صورت داوطلبانه اجرایی می‌شده است. برخی از کارشناسان امنیت سایبری تردید دارند که قانون‌گذاری بتواند موثر باشد. موریس ترنر ، عضو امنیت سایبری در نهاد "اتحاد برای دموکراسی ایمن" ، معتقد است که شرکتها قوانین را دور خواهند زد.

یکی از ایراداتی که از سوی برخی کارشناسان مطرح شده آنست که سایر بخش‌های مهم زیرساختی

از جمله مدارس، امور مالی و بخش کشاورزی نیز باید ذیل چنین قوانینی قرار گیرند زیرا یک حمله باج‌افزاری بزرگ می‌تواند به همان در این بخش‌ها نیز پرهزینه و مخل‌کننده باشد.

نگهداری اسناد حساس تهدیدات سایبری در منزل توسط یکی از تحلیل‌گران FBI

به گفته دادستان‌های این پرونده ، کندرا کینگزبری، تحلیلگر اف‌بی‌آی بیش از یک دهه اسناد امنیتی مربوط به تهدیدات سایبری و سایر تهدیدات را به خانه برده و در آنجا نگهداری می‌نموده است. این اسناد شامل مطالبی مربوط به القاعده و اسامه بن لادن نیز می‌شده است.

دستیار مدیر بخش ضد جاسوسی FBI ، در بیانیه ای گفت: "وسعت و عمق اطلاعات طبقه بندی شده امنیت ملی که توسط متهم برای بیش از یک دهه نگهداری شده است ، بسیار حیرت انگیز است." کنگزبری به افشای اسناد ملی متهم نشده و جرم وی سوء حفاظت از اسناد طبقه بندی شده اعلان شده است. رای قضایی او در تاریخ ۱ ژوئن صادر خواهد شد.

توسعه برنامه ردیابی جرم CITIZEN از طریق پاداش برای ارائه اطلاعات

مدیرعامل Andrew Frame ، Citizen ، آتش سوزی اخیر کالیفرنیا را فرصتی برای شکار فرد مظنون به ایجاد آتش سوزی، به صورت آنلاین و اثبات سودآوری شرکت خود برای کاربران دانست. در همین راستا این شرکت بابت ارائه اطلاعات در مورد عامل حریق پاداش ۳۰۰۰۰ دلاری تعیین کرد. در نهایت پس از تعقیب گسترده در سطح شهر، یک فرد بی‌گناه توسط پلیس بازداشت شد. سرانجام پلیس او را بازجویی و آزاد کرد و فرد دیگری را متهم نمود.

کارشناسان می‌گویند این حادثه به خوبی نشان داد که خطر گزارش های اشتباه ،حفظ حریم خصوصی و هدف گزاری نادرست و نامتناسب روی اقلیت ها از اشکالات اساسی این نرم‌افزار است و چگونه منافع تجاری این شرکت در تضاد با منافع و خدمات عمومی است.

این شرکت کاهش تعداد حوادث ناگوار و جرایم را بد می‌داند و با ارسال نامه‌های الکترونیکی به تحلیلگران آنها را تشویق می‌کند که حوادث بیشتری را گزارش دهند.

این اپلیکیشن بیش از ۷ میلیون کاربر در ۳۰ شهر دارد و در حال تست ویژگی ای است که می تواند به درخواست کاربران ، یک نیروی امنیتی خصوصی را در هر محلی مستقر سازد، هم چنین شهروندان می‌توانند با شرکت‌های خصوصی امنیتی در حل حوادث مشارکت نمایند.

آیا عدم اطلاع‌رسانی عمومی از رفع باگ‌های باج‌افزاری می توانست از حمله COLONIAL PIPELINE جلوگیری کند؟

شرکت امنیت سایبری رومانی BitDefenderدر گذشته ابزاری دیجیتال را به بازار ارائه کرده بود که برای گشودن قفل کامپیوترهایی که توسط باند باج‌افزار DarkSide هک شده بودند، استفاده شد. شرکت BitDefender برای تبلیغ خدمات خود این ابزار را به صورت رایگان به تمام قربانیان DarkSide ارائه می‌داد.

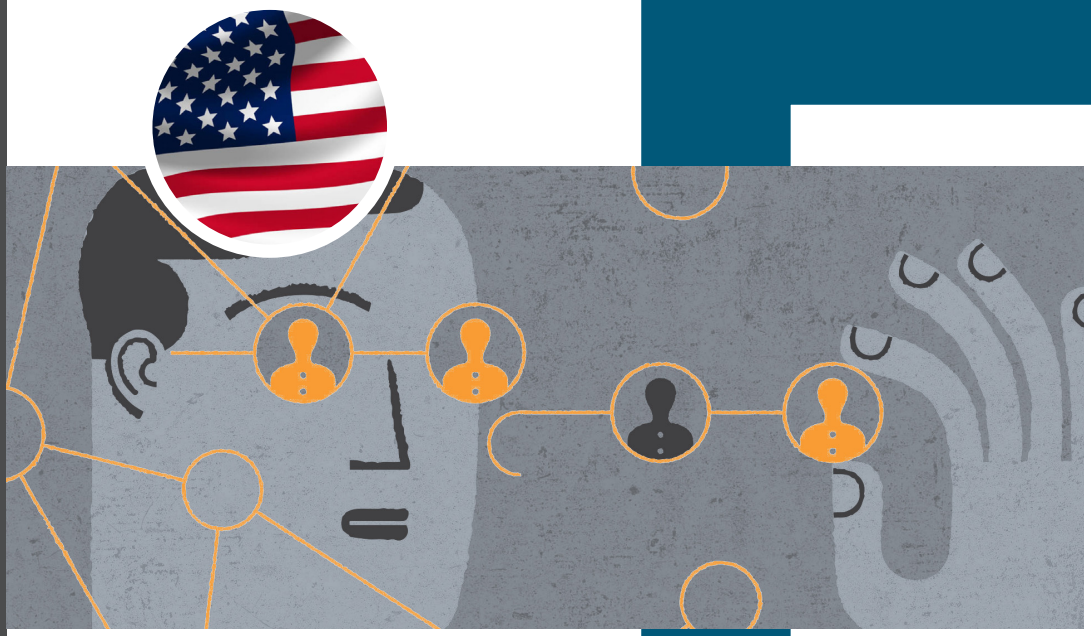
انتشار این خبر به بسیاری از قربانیان DarkSide کمک نمود؛ اما به این باند نیز فرصت داد تا با استفاده از آن روشهایی که BitDefender در نرم‌افزار خود به کار بسته بود، باج افزار خود را دوباره مهندسی کند و درنهایت قفل‌گشای این شرکت را بی اثر کند.

چند ماه بعد ، وقتی باج افزار DarkSide به Colonial Pipeline حمله سایبری نمود، هیچ راه حل ساده‌ای وجود نداشت. سرانجام ، ۴.۴ Colonial میلیون دلار باج پرداخت تا دوباره به سیستم‌های رایانه‌ای خود دسترسی پیدا کند.

گروهی از کارشناسان می‌گویند اگر شرکت BitDefender به جای انتشار آنلاین قفل‌گشای خود، آنرا بی سر و صدا با قربانیان DarkSide به اشتراک گذاشته بود ، ممکن بود در زمان هک خط لوله سوخت شرق امریکا مورد استفاده قرار می‌گرفت. این حادثه نشان می‌دهد که چگونه اشتیاق شرکت‌های ضد ویروس برای دست و پا کردن اسم و رسم برای خود، یکی از قوانین اصلی جنگ سایبری را نقض می‌کنند؛ اولین قانون مسدود کردن حملات باج افزار این است: در مورد چگونگی انسداد حملات باج افزار صحبت نکنید.

اما مسئولان BitDefender متفاوت به این قضیه نگاه می کند. بوگدان بوتزاتو ، مدیر تحقیقات تهدیدات این شرکت گفت ، ما با تبلیغ ابزار خود ، بیشتر از آنچه که می توانستیم به قربانیان DarkSide کمک کردیم. حتی اگر این ما سکوت کرده بودیم ، DarkSide ممکن بود به تنهایی متوجه نقص در باج افزار خود شود.


COLONIAL PIPELINE CO
213
NO SMOKING



معرفی قانون ممانعت از تبعیض الگوریتمیک توسط دموکرات‌ها

دموکراتهای کنگره فشار فزاینده‌ای را ایجاد نموده اند تا قانونی را تدوین نمایند که شبکه‌های اجتماعی و سایر وبسایت‌ها از ترویج الگوریتمیک منع می‌شوند.

این لایحه ، قانون "شفافیت بسترهای نرم افزاری آنلاین و عدالت الگوریتمی" نامیده می‌شود و توسط سناتور اِد مارکی و نماینده دوریس ماتسوی معرفی شده است. این قانون ، الگوریتم‌های آنلاین را از مبانی تبعیض آمیز نظیر نژاد ، جنسیت ، سن ، توانایی(سلامت/معلولیت) و... منع می‌کند.

همچنین هدف از این قانون ایجاد شفافیت بیشتر در مورد عملکرد پلتفرم های دیجیتال از طریق الزام شرکت ها به توضیح روش کار الگوریتم های خود و نوع اطلاعاتی که جمع آوری می کنند به زبان ساده است. علاوه بر این ، یک گروه ویژه از آژانس های مختلف فدرال ، از جمله کمیسیون تجارت فدرال و وزارت مسکن و شهرسازی ایجاد می کند تا موارد احتمالی سوگیری در الگوریتم ها را بررسی کند.

مدافعان حقوق مدنی پس از سالها تلاش برای ایجاد تغییر در سیاست‌های غول‌های فناوری به منظور اینکه تضمین نمایند محصولاتشان به مردم رنگین پوست آسیب نمی‌رساند ، کنگره را برای تنظیم مقررات علیه شرکتهای فناوری تحت فشار قرار داده اند. آنها به ویژه در تحت فشار قرار دادن شرکت‌ها برای انجام اقدامات بیشتر جهت مقابله با سخنان نفرت انگیز و اطلاعات نادرست در مورد انتخابات فعال بودند.

در پی انتخابات ۲۰۱۶ ، محققان دریافتند که عملیات نفوذ روسیه به طور خاص تلاش نمود تا میزان مشارکت دهندگان سیاه پوست را کاهش دهد . هم چنین کارشناسان متوجه شدند که جماعت سیاهپوستان بیش از هر گروه دیگری با تبلیغات فیس بوک هدف قرار گرفته اند.

این قانون جدید به طور خاص فرآیندهای الگوریتمی را که در حق رأی افراد مداخله دارند ، ممنوع می کند. همچنین طرح سناتور مارکی و نماینده ماتسوی شرکت‌های فناوری را مجبور می کند گزارش‌های سالانه‌ای را با جزئیات شیوه‌های تعدیل محتوای خود منتشر کنند ؛ کاری که برخی از شرکتهای بزرگ ، از جمله فیس بوک ، پیش از این انجام می دادند.


ELECTION
ELECTION DATE
CITY OF
WARD and PRECINCT
NUMBER OF BALLOTS
ELECTION
ELECTION DATE
CITY OF
WARD and PRECINCT
NUMBER OF BALLOTS
ELECTION

ضعف‌های امنیتی بازرسی از فرایند انتخاباتی شهر "ماری‌کوپا"

به دنبال دخالت روسیه در رقابت انتخاباتی سال ۲۰۱۶ ، یک تلاش سراسری برای بهبود دستور العمل‌های حفاظتی امنیت سایبری در انتخابات امریکا صورت گرفت.

این تلاش‌ها شامل خرید ماشین‌های رای گیری جدید و ایمن‌تر با امکان بررسی کاغذی آرا و هم‌چنین ایجاد شبکه گسترده ای از حسگرهای امنیت سایبری وزارت امنیت داخلی در دفاتر انتخابات سراسر کشور بود. با وجود این بهبودها ، اعتماد رای دهندگان به امنیت انتخابات در سال ۲۰۲۰ خدشه‌دار شد.

سنای ایالت آریزونا که تحت کنترل حزب جمهوریخواه است، علی رغم اعتراض مقامات ارشد شهرستان Maricopa ، بازرسی از انتخابات را به راه انداختند و شرکت Cyber Ninjas را برای انجام این کار استخدام نمودند. این شرکت هیچ تجربه بازرسی انتخاباتی را ندارد و مدیر عامل آن نیز ادعای دزدیده شدن انتخابات سال ۲۰۲۰ را تکرار کرده بود.

از زمان آغاز بازرسی‌ها، خطاهای امنیتی ساده‌ای رخ داده است. از جمله لپ تاپ‌های حاوی اطلاعات انتخابات و روترهای WiFi متصل به لپ تاپ های که حاوی اطلاعات انتخابات بودند بدون نظارت رها شدند. هم چنین برگه‌های رأی گیری در مراکز نگهداری با امنیت ضعیف بدون مراقبت رها شده و تصویربرداری از فرایند رأی گیری با دوربین‌هایی صورت گرفته که ظاهراً تحت بررسی امنیتی نبوده‌اند یا توسط یک نهاد دولتی تأیید نشده اند.

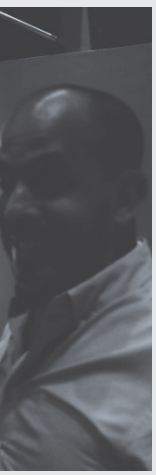
به گفته منتقدان، بازرسی Maricopa حتی اگر هیچ سندی از تقلب را هم پیدا نکند، می‌تواند اعتماد رای‌دهندگان را بیش از پیش تضعیف نماید.

شرکت های فناوری

بنا به گفته فیس‌بوک، هکرهای روس عامل حمله سایبری SOLARWINDS فعالیت خود را از سرگفته‌اند

طبق گفته فیس‌بوک ، هکرها تلاش نمودند تا ۳۰۰۰ نفر را در ۱۵۰ سازمان هدف قرار دهند. حداقل یک چهارم از سازمان‌های مورد هدف مربوط به بخش های بشردوستانه ، حقوق بشر و توسعه بین الملل بوده‌اند. بر اساس اعلان فیس‌بوک، روش هکرها در این عملیات ارسال ایمیل بوده است که توسط آژانس توسعه بین المللی ایالات متحده (USAID) شناسایی شده و توسط نرم‌افزار به صورت خودکار مسدود شده‌اند.

تام برت ، معاون رئیس مایکروسافت در یک پست وبلاگ گفت ، این گروه پس از دسترسی به حساب ایمیلی مرکز تجارت آژانس USAID توانست این حمله را آغاز کند.



فیس‌بوک: روسیه بزرگترین تولید کننده اطلاعات نادرست(MISINFORMATION) در جهان است

به گفته فیس‌بوک گروه‌های سایر کشورها نیز از برنامه‌های روسیه آموخته اند که چگونه عملکردهای محتوا و پردازش اطلاعات در پلتفرم‌های فیس‌بوک را هماهنگ ساخته و سپس دستکاری نمایند و از آن برای ایجاد کمپین‌های ضد اطلاعات در کشورهایشان استفاده کنند.

فیس‌بوک اعلام کرد ایران ، میانمار ، ایالات متحده و اوکراین اصلی‌ترین عوامل (مبتکرین) ایجاد اطلاعات غلط (ضداطلاعات) در امور خارجی و داخلی هستند. هم چنین بیشترین هدف در این زمینه ایالات متحده ، اوکراین ، انگلیس ، لیبی و سودان می‌باشند.

فضای سایبر بین‌الملل


Data Breach
Cyber Attack
System Safety Compromised

کارزار هک چینی‌ها علیه شرکت‌های حمل و نقل و مخابرات امریکا

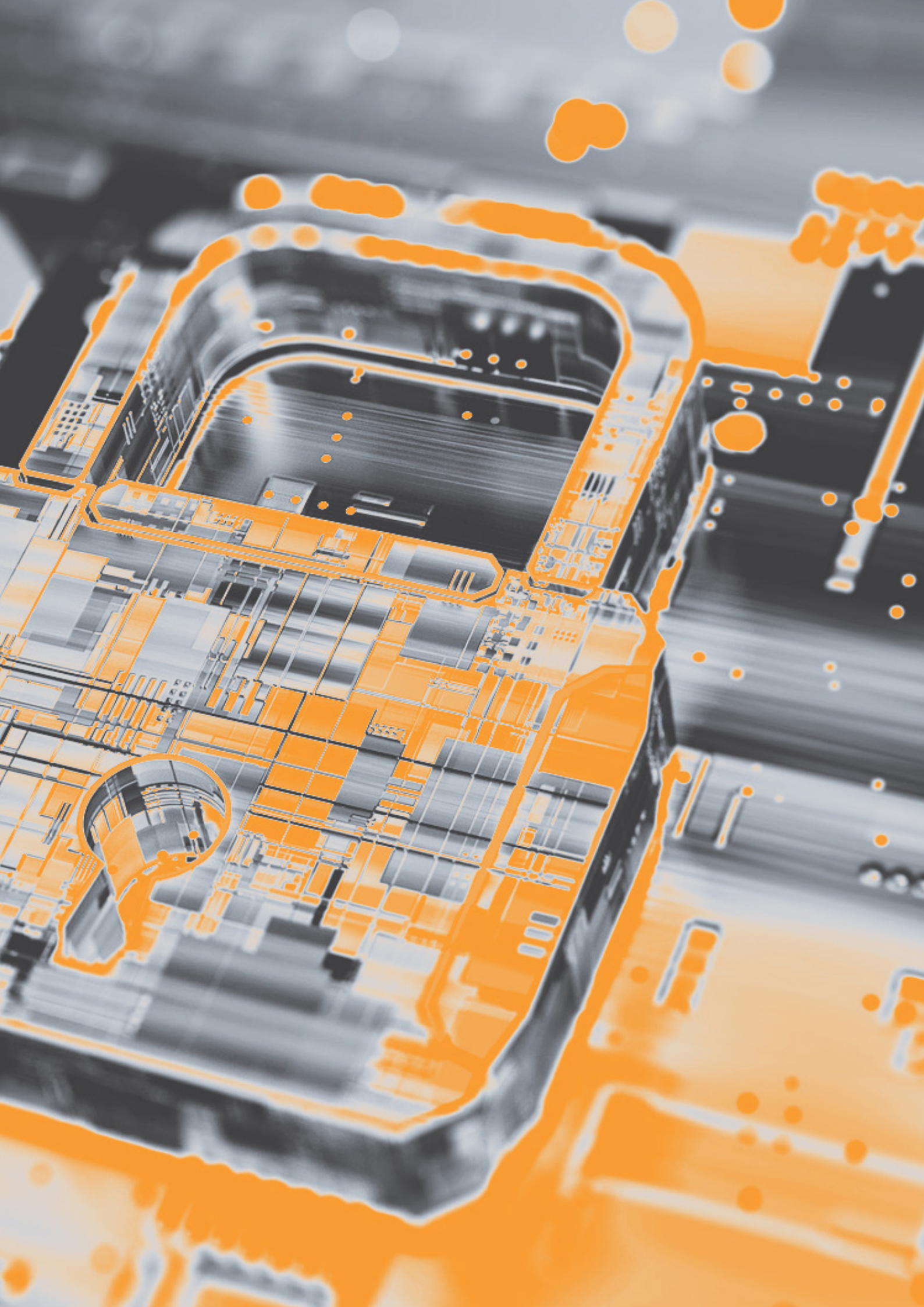
شرکت امنیت سایبر FireEye گفت دو گروه هک مرتبط با چین از آسیب پذیری‌های نرم‌افزار Pulse Secure VPN برای سرقت اطلاعات از سازمان هایی که "در صنایع همسو با مقاصد استراتژیک پکن فعالیت می کنند" استفاده کرده اند.

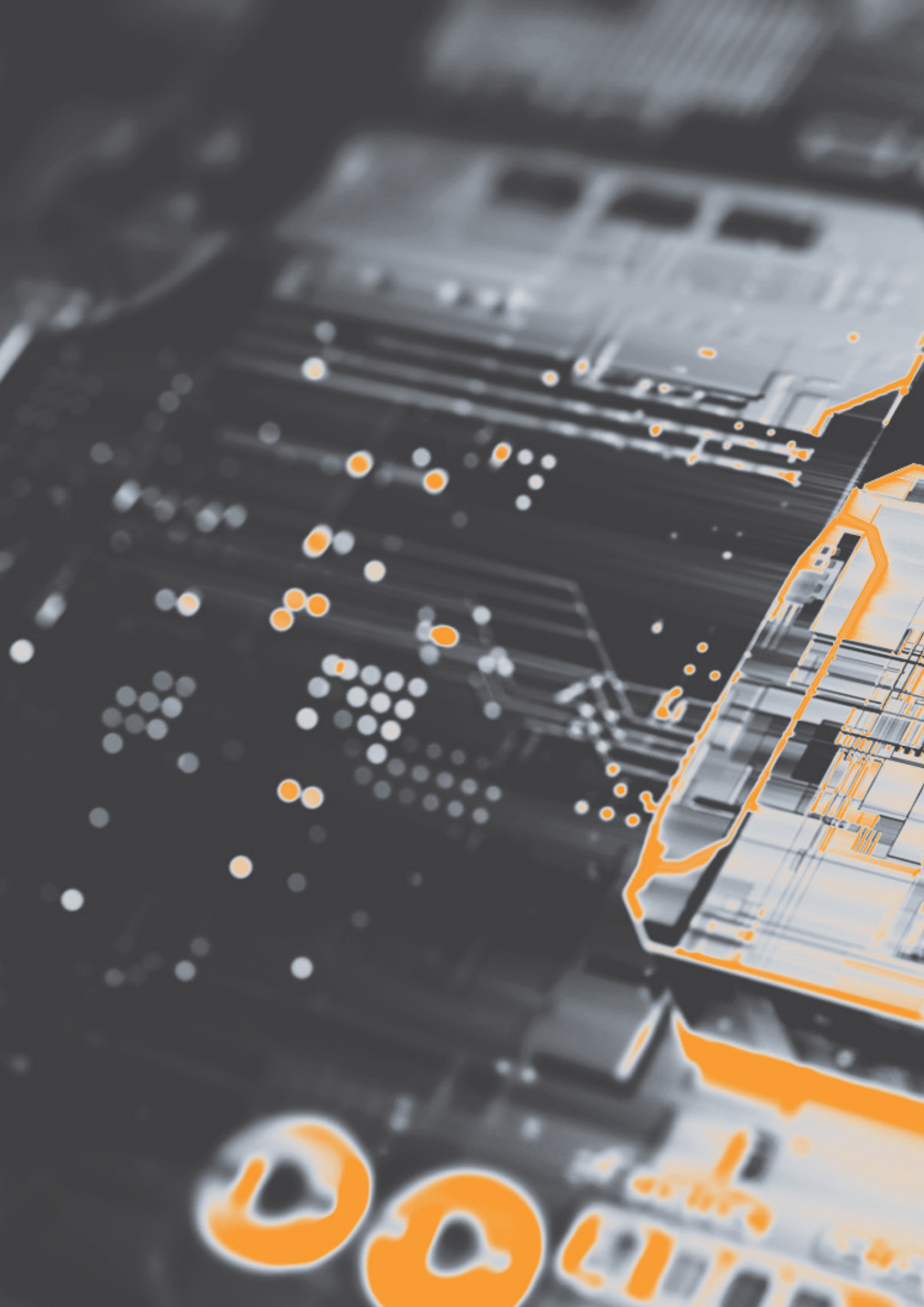
این شرکت در ابتدا گفت که شرکتهای دفاعی و مالی ، همراه با بخش دولتی ، مورد هدف قرار گرفته‌اند.

ارتباط بزرگترین سازنده فناوری نظارتی در جهان با ارتش چین

بر اساس گزارشی از شرکت تحقیقات نظارت IPVM ، شرکت "هایک‌ویژن" فناوری هواپیماهای بدون سرنشین را به نیروی هوایی چین فروخته و با کارشناسان تسلیحاتی چینی همکاری نموده است. مقامات امریکایی سالهاست ادعا می‌کنند این شرکت با ارتش چین ارتباطات عمیق دارد. شرکت هایک‌ویژن این ادعاها را رد نموده است.

سخنگوی هایک ویژن گفت: "نه اکنون ، و نه هیچ‌وقت دیگری ، کارهای تحقیق و توسعه را برای کاربردهای ارتش چین انجام نداده است" ، و اظهار داشت که "هر فعالیتی از این قبیل توسط هر یک از کارمندان ما به عنوان یک مقام شخصی انجام شده است و نه تحت مدیریت شرکت."





خرید تجهیزات نظارتی از چین توسط دولت‌های محلی امریکا

بیش از ۱۰۰ شهرداری ایالات متحده تجهیزات نظارتی چینی را خریداری کرده اند که دولت ایالات متحده می گوید برای سرکوب اویغورها استفاده شده است.

با وجود این که کنگره ، آژانس‌های فدرال را از خرید این تجهیزات منع کرده است، دولت‌های محلی همچنان به خرید این فناوری ادامه می‌دهند. دولت های محلی این دوربین‌ها را - که توسط شرکت‌های چینی Hikvision و Dahua ساخته شده اند - برای استفاده در مدارس دولتی ، بخش های آزمایشی و... خریداری کرده اند.

Dahua اتهامات دولت ایالات متحده مبنی بر کمک تجهیزاتش به جاسوسی از جمعیت مسلمان اویغور چین را رد کرد. این شرکت در بیانیه ای گفت: "برخلاف برخی گزارش ها در رسانه ها ، شرکت ما هرگز هیچ فناوری یا راه حلی را که بخواهد گروه قومی خاصی را هدف قرار دهد ، توسعه نداده است."

بر اساس حکم دادگاه عالی اروپا ، نظارت گسترده آژانس جاسوسی انگلیس از توده مردم نقض قانون است.

دادگاه نهایی تجدیدنظر دادگاه حقوق بشر اروپا حکم کرد، برنامه نظارت گسترده GCHQ آزادی بیان شهروندان را نقض نموده و از ابزار محرمانه مورد استفاده روزنامه نگاران حمایت کافی نکرده است. این دادگاه گفت، تصمیم برای اجرای یک برنامه نظارت گسترده به خودی خود نقض کنوانسیون حقوق بشر اروپا نبوده است.

به گفته یکی از شاکیان پرونده، به موجب این حکم ادوارد اسنودن ، پیمانکار سابق آژانس امنیت ملی ، فرد بی گناهی می‌باشد. اسنودن افشا نموده بود GCHQ مقدار زیادی اطلاعات را از طریق کابلهای فیبر نوری از مردم جمع می کند. برنامه‌ای که اسنودن افشا نمود ، در سال ۲۰۱۶ تا حد زیادی با قانون جدید نظارت انگلیس جایگزین شد.


SITA
B5

درز بایگانی ۱۰ ساله اطلاعات مسافران شرکت هواپیمایی ملی هند

در این نفوذ سایبری ، اطلاعاتی از جمله گذرنامه و جزئیات کارت اعتباری مسافران شرکت هواپیمایی SITA Passenger Service System به سرقت رفته است. هواپیمایی هند اعلام کرد ۴.۵ میلیون مسافر در سراسر جهان تحت تأثیر این نقض قرار گرفته اند؛ هرچند که تعداد دقیق مسافران آن را بیان نکرد. این شرکت هواپیمایی گفت هیچ گذرواژه مشتری سرقت نشده است.

Edna Ayme-Yahil ، رئیس ارتباطات جهانی SITA ، به تایمز آف هند گفت: هکرها ۲۲ روز در سیستم های SITA حضور داشتند. این شرکت در ابتدا گفت که سایر خطوط هوایی مهم ، از جمله خطوط هوایی سنگاپور و لوفت هانزا ، تحت تأثیر قرار گرفتند.

Iranian Council For
Defending The Truth

اخبار کوتاه

۳


mirror_mod.use_y = True
mirror_mod.use_z = False
elif operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the deselected mirror
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
mirror_ob.select = 0

- محققـان شـرکت امنیـت سـایبری SentinelOne اعـلان نمودنـد کـه یـک گـروه هکـری جدیـد کـه ممکـن اسـت بـه ایـران مرتبـط باشـد ، تاسیسـات سـایبری اسـرائیل و دیگـر سـازمان‌های خاورمیانـه را هـدف قـرار داده اسـت. ایـن گـروه هکـری عملیـات خـود در پشـت بـاج افـزار مخفـی می‌کننـد.

- بـازار عظیـم جرایـم رایانـه‌ای روسـیه توسـعه جهانـی خـود را بـه تعویـق انداختـه اسـت. معامـلات در بـازار دارک‌وب Hydra در سـال گذشـته بـه ۱.۳۷ میلیـارد دلار افزایـش یافـت. بـر اسـاس گـزارش جدیـد شـرکت امنیـت سـایبری Flashpoint و شـرکت تجزیـه و تحلیـل بـلاک چیـن Chainalysis ، ایـن بـازار برنامه‌هـای توسـعه خـود را بـه تعویـق انداختـه اسـت ، و مقصـر اصلـی مسـائل خارجـی و همـه گیـری ویـروس کرونـا اسـت.

- WhatsApp از دولت هند شکایت کرد تا قوانین جدید اینترنت را متوقف کند.

- بلژیک کمپین جاسوسی سایبری را که مشکوک به ارتباط با چین است ریشه کن نمود.

- هکرها اطلاعات سرقت شده بیماران از سیستم‌های بهداشتی نیوزلند را منتشر نمودند.

ICDT.IR