گزارش

مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

شهریور ۱۴۰۰

امنیت سایبری


بسم الله الرحمن الرحیم

فهرست

Iranian Council For
Defending The Truth

پیشگفتار

۱

پیشگفتار

مجمع ایران 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 سوءتفاهم ها 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

خروج نیروهای نظامی امریکا از افغانستان نه تنها دارای ابعاد سیاسی، اقتصادی و بین المللی بود، بلکه از نگاه کارشناسان امنیت اطلاعات نیز حائز اهمیت است. حضور بیست‌ساله امریکا در این کشور سبب گردآوری حجم بیشماری از اطلاعات در پایگاه‌های این کشور شده است که برای رقبای ایالات متحده مهم هستند. بی شک خروج عجولانه امریکاییان موجب شده تا بخشی از این اطلاعات در افغانستان باقی بماند و در صورت دسترسی طالبان به آنها، عواقب آن غیرقابل پیش‌بینی است. از سوی دیگر موضع‌گیری که پلتفرم‌های اجتماعی در شرایط کنونی نسبت به مردم افغانستان و طالبان خواهد گرفت، بسیار تاثیرگذار است.

Iranian Council For
Defending The Truth

اخبار

۳


Data Breach
Cyber Attack

چالش افغانستان

داده‌های حساس دولتی آمریکا، یکی دیگر از قربانیان خروج از افغانستان است

در زمره هزینه‌های فراوان سقوط سریع دولت افغانستان و خروج سریع پرسنل دیپلماتیک و نظامی ایالات متحده، این مورد را نیز باید در نظر گرفت که بخش قابل‌توجهی از داده‌های حساس دولت ایالات متحده مطمئناً در کشور تحت کنترل طالبان باقی مانده است.

اکثریت قریب به اتفاق اطلاعات طبقه‌بندی شده که در رایانه‌های سفارت آمریکا موجود بودند، تقریباً از افغانستان خارج شده یا نابود شده‌اند. بسیاری از داده‌های بسیار مهم دولت نیز به جای دیسک‌های سخت در ابرهای رایانه‌ای ذخیره می‌گردید و با چندین کنترل امنیتی نیز محافظت می‌شوند؛ بنابراین به نظر نمی‌رسد خطری آنها را تهدید کند.

اما مطالب طبقه‌بندی نشده ولی حساس احتمالاً در افغانستان باقی خواهند ماند؛ چه به صورت دیجیتال و چه روی کاغذ. این اتفاقات به این دلیل رخ داده که این اطلاعات یا با دولت افغانستان ،یا با سازمان های غیردولتی و یا با سایر شرکای امریکا در این کشور به اشتراک گذاشته شده‌اند. حداقل برخی از دیگر از این اطلاعات نیز احتمالاً در هنگام خروج سریعتر از حد انتظار، در لپ‌تاپ‌های قدیمی و تلفن‌ها و رسانه‌های سیار نادیده گرفته شده هستند.

برخی از داده‌های نسبتاً بی ضرر باقی مانده در افغانستان را می‌توان با سایر داده‌ها ترکیب کرد تا اطلاعاتی را که واقعاً برای امنیت ایالات متحده مضر است آشکار شود- فرایندی که مقامات اطلاعاتی از آن با عنوان اثر موزاییکی یاد می‌کنند.

مطمئناً دشمنان ایالات متحده در خارج از افغانستان ، مانند روسیه و چین ، به دنبال چنین اطلاعاتی می‌باشند و مایل به پرداخت پول بابت هرگونه اطلاعاتی که طالبان بتواند برای آنها تهیه کند، هستند.

چالش جدید فیسبوک، توییتر و یوتیوب: آیا طالبان را به رسمیت بشناسند یا خیر؟

شرکت‌های رسانه‌های اجتماعی در طول این سال‌ها مجبور بوده اند تصمیمات بحرانی متعددی در مورد تغییرات بحث برانگیز و حتی خشونت آمیز دولت‌ها داشته باشند ، از جمله در مورد کودتای نظامی میانمار و انتخابات ریاست جمهوری ۲۰۲۰ آمریکا. آنها تا کنون این کار را با تکیه بر تصمیمات مقامات جهانی مانند سازمان ملل انجام داده اند.

تلاش سریع طالبان برای تسلط بر دولت افغانستان این پلتفرم ها را مجبور به اتخاذ تصمیمات پر ریسکی در قبال افغانستان کرده است: تعیین اینکه آیا انتقال قدرت و رژیم جدید به رسمیت شناخته شود یا خیر؟

تعیین مواضع در قبال حاکمیت طالبان یک چالش بزرگ برای این شرکت‌ها خواهد بود ، زیرا آنها نقش بسیار مهمی در رابطه با تصمیم گیری در خصوص این موضوع خواهند داشت که دولت افغانستان و طالبان چگونه می‌توانند به صورت آنلاین به مخاطبان دسترسی داشته باشند -و اینکه با این قدرت چه کاری می‌توانند انجام دهند.

در نهایت، این کمپانی‌های امریکایی خواهند بود که تعیین می‌کنند:

- چه کسی حساب های رسمی دولت افغانستان مانند دفتر رئیس جمهور افغانستان که نزدیک به یک میلیون دنبال کننده دارد را اداره کند
- و اینکه آیا صفحات خود طالبان با تأیید یا برچسب گذاری از طریق این سیستم عامل‌ها مشروعیت می یابد یا خیر.

این پلتفرم‌های اجتماعی به ویژه از سوی محافظه کاران امریکا و طرفداران رئیس‌جمهور سابق(ترامپ)، تحت فشار هستند تا رهبران طالبان را به طور کامل از خدمات خود بازدارند ، چرا که این گروه با تروریسم ارتباط دارد.

این بدان معناست که حساب‌هایی را که توسط خود طالبان یا از طرف آن حمایت می شود حذف می‌کنند و "ستایش ، حمایت و نمایندگی از آنها" به کلی ممنوع می‌گردد. (علیرغم وجود این ممنوعیت ، طالبان پیش از این از پلتفرم واتس‌اَپ فیس بوک - که در آن رمزگذاری از چت های خصوصی کاربران

محافظت می‌کند - برای جلب حمایت در کشور و انتشار پیام خود استفاده کرده است.)

مسئولین فیس‌بوک در این خصوص اعلان نمودند:« فیس‌بوک در مورد دولت به رسمیت شناخته شده در هیچ کشور خاصی تصمیم نمی‌گیرد بلکه در عوض به اقتدار جامعه بین المللی در انجام این تصمیمات احترام می‌گذارد.»

کتی رزبورو ، سخنگوی توییتر در بیانیه‌ای اظهار داشت که "وضعیت در افغانستان به سرعت در حال تغییر است" و "اولویت اصلی توییتر حفظ امنیت مردم است". سخنگویان YouTube متعلق به Google به درخواست اظهار نظر پاسخی نداده‌اند.

تاکنون رهبران جهانی هیچ موضع‌گیری تعیین‌کننده و جدی در قبال افغانستان نداشته اند. از یک طرف چین به برقراری روابط دوستانه با طالبان تمایل نشان داده اما رژیم جدید را هنوز به رسمیت نشناخته است. از طرف دیگر بوریس جانسون، نخست وزیر بریتانیا نیز خواستار عدم به رسمیت شناختن طالبان از سایر کشورها شد. وزارت امور خارجه امریکا نیز اعلان نموده که هنوز در حال بررسی وضعیت است.

در صورت عدم اشاره روشن از سوی رهبران جهانی، شرکت‌های فناوری مجبور می‌شوند، خودشان تصمیم بگیرند که چه کسی در رسانه‌های اجتماعی برای دولت افغانستان صحبت کند و چقدر طالبان را برای کسب مشروعیت جدی تلقی کنند. و برای انجام این کار ، آنها باید عوامل مهم دیگری از جمله ایمنی کاربرانی را که به شدت مایل به فرار از افغانستان هستند ، بسنجند.

این موضوع حتی پیچیده‌تر هم می‌شود وقتی بدانیم که طالبانِ پاکستان از سوی وزارت خارجه امریکا به عنوان یک سازمان تروریستی خارجی تعیین شده اما در مورد طالبانِ افغانستان اینگونه نیست. اگر افغانستان تحت حاکمیت طالبان در سطح بین المللی به رسمیت شناخته شود ، می‌تواند با سیاست شرکت‌ها علیه ترویج تروریسم تضاد ایجاد کند.

کیفیت حضور طالبان در شبکه‌های اجتماعی

به گفته کارشناسان ، طالبان از تکنیک‌های پیشرفته برای دور زدن قوانین در شبکه‌های اجتماعی استفاده می‌کند. این یک تغییر عظیم نسبت به زمان حمله ایالات متحده به افغانستان در سال ۲۰۰۱ است. استراتژی‌های رسانه‌های اجتماعی این گروه بسیار ماهرانه است به طوری که برخی تحلیلگران می‌گویند حداقل یک گروهان روابط عمومی در طالبان وجود دارد که مانند کمپین‌های سیاسی نوین، پست‌های‌شان را وایرال می‌کنند.

شرکت‌های رسانه‌های اجتماعی مانند فیس‌بوک در روزهای پس از روی کار آمدن طالبان درباره حساب‌های مرتبط با طالبان اقداماتی را انجام داده اند. واتس‌اپ ، که متعلق به این شرکت است، خط تلفن شکایاتی را که طالبان برای شهروندان ایجاد کرده بود تا مشکلاتی مانند غارت را گزارش دهند، حذف نمود. فیس بوک اعلام کرد که شماره تلفن و "کانال های رسمی طالبان" را مسدود کرده است. این شرکت همچنین به طور فعال در تلاش است تا استفاده طالبان از پلتفرم‌های خود را مسدود کند. سخنگوی گروه طالبان در اولین کنفرانس مطبوعاتی خود در کابل ، فیس‌بوک را هدف قرار داد و وقتی از او درباره آزادی بیان سوال شد ، از این شرکت انتقاد نمود.

امنیت سایبری امریکا

هک سیستم‌های اداره سرشماری امریکا

یک ناظر دولتی خبر داد هکرها سیستم‌های اداره سرشماری ایالات متحده را نقض کرده‌اند. آنها برای نفوذ به سرورهای آژانس از یک روش هک راحت و در دسترس استفاده نموده‌اند. بازرس کل وزارت بازرگانی اعلان کرد: اداره سرشماری سیستم‌های آسیب پذیر را تعمیر نکرده بود ، حتی پس از اینکه شرکت تامین کننده تجهیزات رایانه‌ای به این آژانس هشدار داد که آنها ناامن هستند.

این سازمان هفته ها طول کشید تا درباره این هک تحقیق کند و به آژانس امنیت سایبری و امنیت زیرساخت‌ها از وقوع این رخنه سایبری اطلاع دهد.

به گفته این آژانس، سرورها به داده‌های مربوط به سرشماری ۲۰۲۰ متصل نبوده و هکرها نتوانسته‌اند داده‌های سرشماری ده ساله را تغییر دهند. هکرها همچنین نتوانستند راهی برای دسترسی طولانی مدت به سرورها ایجاد کنند.

شمار قربانیان نفوذ به T-MOBILE به بیش از ۵۰ میلیون نفر رسید

T-Mobile روز جمعه اعلام کرد در پی هک شدن داده‌های در حدود ۶ میلیون حساب دیگر، تعداد کل قربانیان این نقض به بیش از ۵۵ میلیون نفر رسیده است. این افشاگری‌ها در حالی صورت می‌گیرد که قانونگذاران نظارت بر این شرکت را تشدید کرده‌اند.

به گفته T-Mobile ، ۵.۳ میلیون از حساب‌های مشترکین دارای آدرس ، نام ، تاریخ تولد و شماره تلفن بودند. این شرکت همچنین متوجه شد که اطلاعات ۶۶۷،۰۰۰ حساب دیگر از مشتریان سابق T-Mobile ، شامل نام، شماره تلفن، آدرس و تاریخ تولد آنها نیز در دسترس هکرها قرار گرفته است.

بر خلاف اولین مجموعه ای از مشتریان که توسط T-Mobile در روز چهارشنبه شناسایی شد ، هیچ یک از این حساب های اضافی شماره تامین اجتماعی یا اطلاعات شناسایی آنها به خطر نیفتاده است.

یافته‌های جدید همچنین نشان می‌دهد که داده‌های IMEI و IMSI تلفن‌ها نیز در دسترس قرار گرفته است. IMEI ، که اغلب برای مقاصد تبلیغاتی استفاده می شود ، یک مشخصه منحصر به فرد برای دستگاه است که قابل تنظیم مجدد نیست.

این شرکت همچنین خاطرنشان کرد که ممکن است تا ۵۲۰۰۰ حساب پیش پرداخت متررو توسط T-Mobile نیز در این حمله گنجانده شده باشند. T-Mobile برای همه حساب‌های پیش پرداختی که هکرها به آنها دسترسی یافته‌اند ، پین‌های جدیدی را برای مشتریان، مجدداً ارسال نموده است.

روز دوشنبه گذشته گزارش‌هایی از دارک‌وب درز نمود که هکر این عملیات مدعی شده به اطلاعات ۱۰۰ میلیون اکانت دست یافته و قصد فروش آنها را دارد.

این پنجمین نفوذ سایبری به شرکت در چهار سال گذشته است. T-Mobile اطمینان داده است که این شرکت نقطه دسترسی هکر را برای ورود به سرورهای خود مسدود کرده است.

امنیت سایبر مرتبط با ایران

حمله سایبری به سیستم راه آهن ایران احتمالاً توسط هکرهای اپوزسیون ایران صورت گرفته است

این حمله نشان دهنده آسیب‌هایی است که گروه‌های هکری اپوزسیون در هر کشوری می‌توانند به دولت‌ها وارد کنند. به گفته شرکت امنیت سایبری Check Point ، ایندرا ، گروهی که ظاهراً پشت این حمله بوده ، سابقه هدف قرار دادن اشخاص مرتبط با ایران و ایجاد شرارت سایبری را دارد.

محقق ارشد CheckPoint ایتالی کوهن اظهار داشت:« بسیار محتمل است که ایندرا گروهی از هکرها ، متشکل از مخالفان رژیم ایران باشد که از داخل یا خارج از این کشور فعالیت می‌کنند و موفق شده‌اند ابزارهای هک منحصر به فرد خود را توسعه دهند و از آنها به نحو موثر استفاده کنند.»

طبق گزارش شرکت امنیت سایبری CLEARSKY، هکرهای دولتی برای تهاجم به اهداف اسرائیلی، هویت کارکنان منابع انسانی را جعل نموده‌اند

براساس گزارش این شرکت امنیت سایبری، هکرهای مرتبط با دولت ایران حملات خود را بر شرکت‌های فناوری اطلاعات و مخابراتی در اسرائیل متمرکز کرده اند تا از این طریق به اهداف اصلی خود وصل شوند.

این کمپین‌ها به گروه APT ایران معروف به Ly-Hexane ، ceum و Siamese Kitten نسبت داده شده است که حداقل از سال ۲۰۱۸ کمپین های جاسوسی را اجرا می‌کند.

در حملات متعددی که در ماه‌های مه و جولای شناسایی شد ، هکرها تکنیک‌های مهندسی اجتماعی را با یک بدافزار به روز شده ترکیب کردند که در نهایت به آنها امکان دسترسی از راه دور به دستگاه آلوده را می‌داد.

در یک مورد، هکرها از نام مدیر سابق منابع انسانی در شرکت فناوری ChipPC برای ایجاد نمایه (پروفایل) جعلی LinkedIn استفاده کردند؛ این نشان می‌دهد که مهاجمان قبل از شروع کمپین، سناریوی دقیقی داشته اند.

محققان شرکت امنیت سایبری ClearSky در گزارش خود می‌گویند که بازیگران Siamesekitten از پروفایل جعلی برای انتقال بدافزار به سیستم قربانیان به بهانه پیشنهاد کار استفاده کرده‌اند:

۱. شناسایی قربانی احتمالی (کارمند)

۲. شناسایی کارمند بخش منابع انسانی برای جعل هو یت

۳. ایجاد یک وب سایت فیشینگ که به عنوان جایگزین سازمان هدف عمل می‌کند

۴. ایجاد فایل‌های فریبنده سازگار با سازمان جعل هویت شده

۵. راه اندازی یک پروفایل جعلی در LinkedIn به نام کارمند منابع انسانی

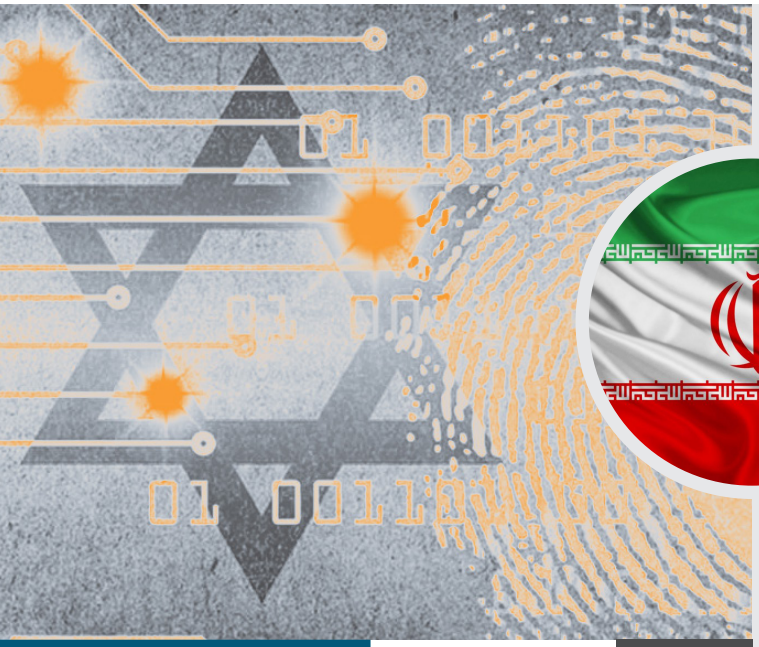
۶. تماس با قربانیان احتمالی با پیشنهاد شغلی "فریبنده" ، تشریح جزئیات یک موقعیت شغلی در سازمان جعل هویت شده

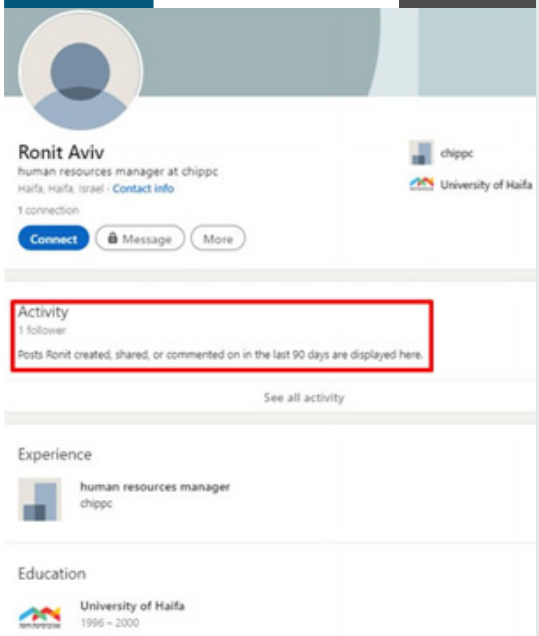
۷. ارسال قربانی به یک وب سایت فیشینگ با فایل فریبنده

۸. یک در پشتی سیستم را آلوده کرده و از طریق DNS و HTTPS به سرور C&C متصل می‌شود

۹. DanBot RAT در سیستم آلوده بارگیری می شود

۱۰. هکرها اطلاعاتی را برای مقاصد جاسوسی





دریافت می‌کنند و سعی می‌کنند در شبکه پخش شوند

در این گزارش آمده است: در حالی که به نظر می‌رسد علاقه بازیگران تهدید کننده نسبت به سازمان‌های خاورمیانه و آفریقا تغییر کرده است ، محققان می‌گویند که شرکت‌های فناوری اطلاعات و ارتباطات در اسرائیل تنها وسیله‌ای برای رسیدن به اهداف واقعی هستند.

محققان دو وب سایت را شناسایی کردند که بخشی از شالوده کمپین‌های جاسوسی سایبری Siamesekitten هستند. یکی از آن دو، سایت کمپانی نرم افزاری موسسه آلمان AG را مشابه سازی نموده و دیگری وب سایت ChipPc را جعل کرده است. در هر دو مورد ، از قربانی احتمالی خواسته می شود که یک فایل XLS (Excel) را که ظاهراً حاوی جزئیات مربوط به یک پیشنهاد کاری یا قالب رزومه است ، بارگیری کند.

این دو فایل شامل یک سلسله دستورات مخرب رمزگذاری شده است که با فعالسازی در پشتی به نام MsNpENg ، فرایند آلوده‌سازی دستگاه را آغاز می کند.


You
Tube

پلتفرم‌ها و رسانه‌های اجتماعی

کوشش توئیتر برای مقابله با نشر MISINFORMATION (اطلاعات غلط و گمراه‌کننده)

از این به بعد، کاربران توئیتر قادر خواهند بود توییت‌های گمراه کننده سیاسی و مرتبط با سلامت را گزارش دهند ؛ اگرچه هیچ تضمینی وجود ندارد که هر گزارشی مورد بازبینی قرار گیرد. این ویژگی سیستم اطلاع رسانی برای جلوگیری از انتشار گسترده‌تر چنین اخبار و اطلاعاتی در روند پردازشی توئیتر برای اکثر کاربران ایالات متحده و دو کشور دیگر طراحی شده است.

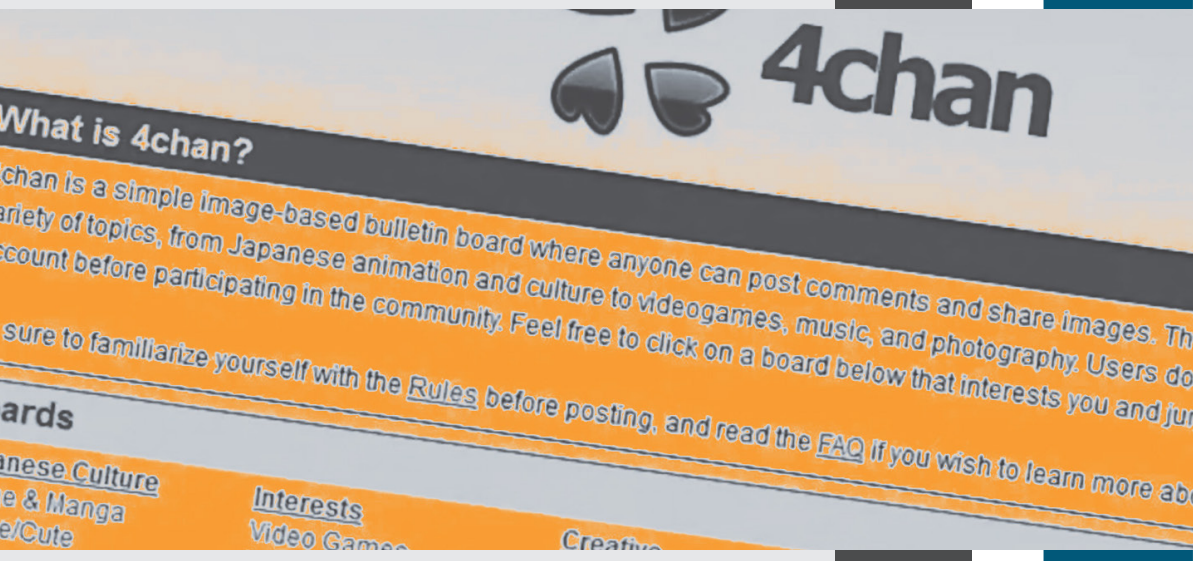
ویژگی جدید گزارش گیری توییتر پس از آن مطرح گردیده که کاخ سفید شرکت‌های رسانه‌های اجتماعی را به دلیل عدم انجام اقدام کافی برای جلوگیری از گسترش ادعاهای بی اساس و گمراه کننده در مورد ویروس کرونا و واکسن‌ها در پلتفرم‌های خود مورد انتقاد قرار داد.

پکن بخشی از سهام مالکیتی شرکت مادر TIKTOK را به دست آورد.

به نظر می‌رسد این حرکت مستقیماً بر مالکیت TikTok تأثیر نمی گذارد ، اما نشان می‌دهد که دولت چین در تلاش است تا نفوذ بیشتری بر ByteDance (شرکت مادر تیک‌تاک) داشته باشد. این اقدام در راستای تلاش دولت چین برای کنترل بیشتر بر بخش فناوری این کشور رخ داده است. پیش از این نیز دولت چین دستور حذف برنامه‌های محبوب خارجی را از فروشگاه‌های برنامه داخلی داده بود.

ByteDance ، تیک‌تاک را در خارج از چین اداره می‌کند. این شرکت همچنین یک برنامه مشابه ، معروف به Douyin ، را در این کشور در اختیار دارد.

نفرت‌پراکنی عوامل پروپاگاندای روسی در پلتفرم ۴CHAN در میان افراطیان راست‌گرا امریکا



عوامل یک کمپین تبلیغاتی مسلماً روسی در تلاش برای تأثیرگذاری بر جناح راست افراطی آمریکا، اطلاعات غلط و گمراه‌کننده در رابطه با کروناویروس را در شبکه‌های مجازی اشتراک‌گذاری می‌کردند.

این یافته ها در گزارش جدیدی قرار گرفته است که به روشن شدن کمپین تبلیغاتی روسیه معروف به "عملیات عفونت ثانویه" می پردازد. این کمپین چندین ساله از وب سایت‌های منطقه اروپا، اسناد جعلی و اکانت‌های بی‌مصرف برای پیشبرد برنامه سیاسی روسیه در اروپا استفاده کرده است.

"عملیات عفونت ثانویه" اتفاقاً به دلیل انتشار اطلاعات نادرست از طریق وب سایت‌های کوچک محلی و سپس ترویج روایات ساختگی در رسانه‌های اجتماعی ، به خوبی شناخته شده است. عفونت ثانویه روایاتی را مطابق با دستور کار سیاسی روسیه در اروپا ترویج می‌کند و سبب شده تا محققان به این باور برسند که این گروه از سوی دستگاه اطلاعاتی روسیه حمایت می‌شود.

این گروه از سال ۲۰۱۴ چندین کمپین را راه اندازی کرده است؛ برای مثال از توییت‌های جعلی از حساب‌هایی متعلق به سناتور مارکو روبیو ، استفاده کرد تا روایتی دروغین مبنی بر اینکه شهروندان انگلیسی قصد ترور بوریس جانسون نخست وزیر را داشتند، نشر دهد.

محققان می‌گویند این گروه همچنان فعال باقی می‌ماند و عوامل آن همچنان به انتشار اطلاعات غلط با موضوع ویروس و احساسات ضد غربی ادامه می‌دهند ، هرچند که در ماه‌های اخیر فعالیت کمتری داشته اند.

در آخرین مورد از اقدامات شناسایی شده، این کمپین به دنبال ایجاد روایتی بود که برخی آمریکایی‌ها جامعه مسلمانان را مسئول COVID-۱۹ معرفی کرده بودند.

محققان مقاله‌ای را در یکی از سایتهای روسی با عنوان "جناح فوق افراطی آمریکا، مسلمانان را متهم به گسترش کرونا می کنند" پیدا کردند.

این مقاله به رشته توئیت هایی در ۴chan ارجاع می‌داد که به نظر می رسد مسلمانان را به انتشار ویروس در کشورهای غربی ترغیب می نمود. یک پاسخ به این پست نشان می‌دهد که اقدامات خشونت‌آمیزی علیه مسلمانان انجام می‌شود.

سپس محققان تصویر صفحه (اسکرین‌شات) مربوط به یک پست واقعی در ۴chan را در یک انجمن آنلاین ناشناس مرتبط با محتوای افراطی و خشونت آمیز ، پیدا کردند. مقالاتی در مورد این پست بلافاصله پس از انتشار آن بر روی منابعی که معمولاً جزئی از عملیات عفونت ثانویه بودند ، منتشر گردیده بود و این نشان می‌داد که یکی از عوامل آن را پست کرده است. اکنون محققان بر اساس خطاهای ترجمه در یک تصویر جاگرفته در مقالات می‌گویند که احتمالاً آنها جعلی و ساختگی هستند.

انگیزه دوگانه تلاش برای برانگیختن نارضایتی در جناح راست آمریکا و ترسیم نگاه منفی از ایالات متحده از جمله نیات اصلی این کمپین عملیات روانی شمرده شده است.

برایان لیستون ، تحلیلگر ارشد این گزارش می گوید: "نکته نگران کننده این است که بازیگران نفوذی که ما معتقدیم با عفونت ثانویه مرتبط هستند نشان دادند که می‌توانند در پلتفرم‌هایی که با خشونت و افراط گرایی داخلی ارتباط دارند ، حضور داشته باشند." "آیا آنها به تحریک یا پیشبرد آن رفتارها در موارد دیگری که ما آنها را شناسایی نکرده‌ایم کمک می کنند یا نه ... باید دید."

برخلاف Reddit و سایر شبکه‌های اجتماعی که در تشخیص رفتارهای اطلاعاتی روسیه مهارت بیشتری پیدا کرده‌اند ، ۴chan عملاً کنترل نشده است و آن را به یک هدف عالی تبدیل می‌کند.

عملیات عفونت ثانویه در مقایسه با توفیق و مقیاس سایر عملیات‌های روسیه مانند کمپین آژانس تحقیقات اینترنتی GRU که در انتخابات ۲۰۱۶ اختلاف‌پراکنی می‌کرد و میلیون‌ها آمریکایی را هدف قرار داد ، نسبتاً کوچک و ساده است.


Cellebrite

توقف فروش محصولات شرکت جاسوسی اسرائیلی به بنگلادش

شرکت اسرائیلی Cellebrite که قفل تلفن‌ها را می‌شکند ، پس از انتقادات حقوق بشری ، کمیته ایجاد کرده و قصد دارد فروش فناوری‌هایش را به بنگلادش متوقف کند.

این تصمیمات احتمالاً ناشی از برنامه‌های Cellebrite برای فروش عمومی سهام خود در ایالات متحده است. این شرکت مدعی است، دستگاه‌هایی را که اطلاعات تلفن‌های قفل شده را استخراج می‌کند به مجریان قانون می فروشد. در بنگلادش ، سخت افزار Cellebrite توسط یک یگان شبه نظامی متهم به شکنجه مردم، مورد استفاده قرار گرفته است.

گروه‌های حقوق دیجیتال در ماه ژوئیه از تنظیم کننده‌ها و سرمایه گذاران خواستند تا برنامه "سلبرایت" را برای عمومی‌سازی سهامش تا زمانی که این سازمان در زمینه حقوق بشر پیشرفتی نداشته باشد، متوقف نمایند. به گفته بنیاد تامسون رویترز ، این شرکت سال گذشته فروش فناوری خود به هنگ کنگ و چین را متوقف کرد و امسال فروش خود را به روسیه و بلاروس متوقف نمود.

Iranian Council For
Defending The Truth

اخبار کوتاه

۴


CONNECTED
NETWORK
[PROCESSING
02
// HACK ATTE
CONNECTED
[PROCESSING]
USER S
//SCANN
NETWORK

- هکرهای باج افزار که به خط لوله Colonial حمله کردند ، اطلاعات شخصی نزدیک به ۶۰۰۰ نفر ، از جمله کارکنان و خانواده های آنها را سرقت کردند. شبکه CNN گزارش داد که هکرها اطلاعاتی از جمله شماره‌های تامین اجتماعی کارکنان را در جریان حمله‌ای که در ماه مه به شبکه‌های این شرکت رخ داد، سرقت کردند.

- وزارت امور خارجه ایالات متحده امریکا قصد دارد "ایده پرریسک" تقدیم پاداش به مخبران دارک وب جهت ارائه اطلاعات درباره حمله هکرها به ایالات متحده را عملی کند.

ICDT.IR