مبارزات دولت ترکیه با فعالیت‌های تروریستی برخط

روز شنبه وزارت کشور ترکیه خبر داد که در حال بازجویی از 10 هزار نفر مظنون است. این افراد مرتبط با فعالیت‌های تروریسی در سطح اینترنت هستند و در شبکه‌های اجتماعی نظراتی با محتوای توهین‌آمیز به مقامات ارسال می‌کنند.

این وزارتخانه در بیانیه‌ای گفت: «این فعالیت‌ها بخشی از برنامه‌ی مبارزه با تروریسم است که با عزم و اراده در همه‌جا دنبال می‌شود از جمله در شبکه‌های اجتماعی»

پس از کودتایی که مرداد ماه در ترکیه انجام شد، این دولت در وضعیت اضطراری قرار گرفت و پاکسازی کشور از مخالفان را آغاز کرد. در پی این عملیات، گروه‌های حقوق بشر از این سرکوب‌ها توسط دولت ترکیه اظهار نگرانی کردند.

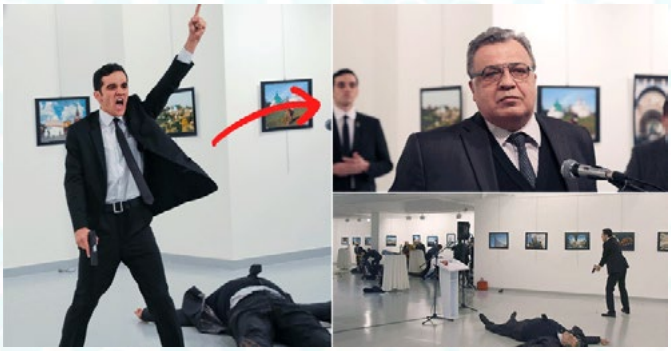
با توجه به گزارش‌های وزارت دادگستری ترکیه، در شش ماه گذشته 1600 نفر به اتهام شرکت در فعالیت‌های تروریستی یا توهین به مقامات دولتی دستگیر شده‌اند.

مقامات ترکیه در پی حوادث جدی که در این کشور رخ داد، دسترسی به شبکه‌های اجتماعی را محدود کردند تا از گردش اطلاعات جلوگیری کنند. گردش اطلاعات در شبکه‌های اجتماعی می‌تواند امنیت ملی ترکیه را تضعیف کند. دسترسی به شبکه‌های اجتماعی از روز دوشنبه هفته قبل، پس از ترور سفیر روسیه در ترکیه، به شدت مختل شده است.

دسترسی به شبکه‌های توییتر و یوتیوب نیز از روز پنج‌شنبه بسیار کُند شده است چرا که در این شبکه‌ها ویدئویی منتشر شده که گروه‌های داعشی دو سرباز تُرک را زنده‌زنده می‌سوزانند.

نهاد نظارت بر اینترنت ترکیه گزارش داده محدودیت‌هایی در دسترسی به شبکه‌های خصوصی مجازی (VPN) نیز ایجاد شده است. از این شبکه‌ها معمولاً برای دور زدن محدودیتِ دسترسی به شبکه‌های اجتماعی و وب‌گاه‌ها استفاده می‌شود.

درخواست روسیه از اپل: باز کردن قفلِ آیفون قاتل سفیر روسیه



احتمالاً شما نیز ویدئوی مربوط به ترور سفیر روسیه در ترکیه را دیده‌اید که به سرعت در اینترنت منتشر شده است. سفیر روسیه، آندری کارلو توسط یک افسر پلیس خارج از وظیفه‌ی آنکارا در 29 آذر ماه مورد شلیک قرار گرفت و کشته شد. سفیر روسیه در حالی مورد اصابت قرار گرفت که در یک نمایشگاه هنری مشغول سخنرانی بود. این فرد موفق شد خود را به‌عنوان محافظ رسمی سفیر جا بزند و در ادامه به ضرب گلوله، سفیر روسیه را بکشد.

پس از این حادثه‌ی تکان‌هنده مقامات روسیه از اپل می‌خواهند قفل آیفون 4S این تیرانداز را باز کند و به احتمال زیاد بحثی شبیه به بحث اپل و FBI که اوایل امسال وجود داشت، مجدداً پیش بیاید. مقامات ترکیه و روسیه از اپل می‌خواهند در دور زدن پین کد آیفون 4S به آن‌ها کمک کند و معتقدند با این کار اپل می‌تواند به بررسی روابط این قاتل با گروه‌های تروریستی دیگر کمک کند. انتظار می‌رود اپل این درخواست را رد کند ولی به گزارش MacReports و رسانه‌های محلی، مقامات روسی گروهی از کارشناسان را به ترکیه اعزام کرده‌اند تا در باز کردن قفلِ آیفون به مقامات کمک کنند.

در بحث بین اپل و FBI، اپل از کمک به باز کردن قفل آیفون تیرانداز سان‌برنادیو سر باز زد و گفت که هر دربِ پشتی که در داخل دستگاه وجود داشته باشد، روزی ممکن است به دست افزار نابکار بیفتد و از آن سوءاستفاده شود.

زمانی‌که FBI از کمک اپل ناامید شد، با پرداخت 1.3 میلیون دلار به یک گروه نفوذ توانست قفلِ آیفون را باز کند اما اطلاعاتی در این تلفن همراه پیدا نکرد که در بررسی‌ها بتواند کمکی بکند.

مردی که سفیر روسیه را به قتل رسانده یک جوان 22 ساله به نام مولوت مرت آلتینتاس، یک افسر پلیس خارج از وظیفه‌ی آنکارا است که با استفاده از شناسه‌ی پلیس خود، زمانی که سفیر در حال سخنرانی بوده، توانسته به نمایشگاه هنری وارد شود.

در طول ترور، تیرانداز فریاد می‌زد: «حلب را فراموش نکنید!» مقامات روسیه و ترکیه معتقدند این ترور برای بی‌ثبات کردن روابط بین دو کشور طراحی شده است.

قرار دادن دربِ پشتی در رمزنگاری‌ها در تضاد با منافع ملی است

کارگروه رمزنگاری در آمریکا، در جلسه‌ی پایان سال خود گزارشی را ارائه کرد که یک پیروزی برای فناوری و حریم خصوصی به حساب می‌آید. در این گزارش به 4 نکته‌ی اصلی اشاره شده که در ادامه مشاهده می‌کنید. در ضمن می‌توانید متن کامل گزارش را از اینجا مطالعه کنید.

• هر اقدامی که رمزنگاری را تضعیف کند، در تضاد با منافع ملی است.

• فناوری رمزنگاری یک فناوری جهانی است که به‌طور گسترده در سراسر دنیا در دسترس همگان قرار گرفته است.

• ذی‌نفعان، فناوری‌ها و عوامل مختلف در حوزه‌ی رمزنگاری، چالش‌های مختلفی را ایجاد می‌کنند؛ بنابراین راه‌حل یک شکل و یکسانی برای تمامی این چالش‌ها وجود ندارد.

• کنگره آمریکا باید همکاری بین شرکت‌های فناوری و مراجع اجرای قانون را تقویت کند.

نکته‌ی اول که در این گزارش به آن اشاره شده، اساس رمزنگاری و حریم خصوصی را مطرح می‌کند که برای مدت‌های طولانی موضوع بحثِ شرکت‌های فناوری و دولت‌ها و نهادهای قانونی بوده است. این کمیته در بررسی‌های خود شاهد بوده بسیاری از نهادهای دولتی، شرکت‌های فناوری بخش خصوص را مجبور می‌کنند در رمزنگاری‌های خود از دربِ پشتی استفاده کنند. در گزارش این کارگروه آمده است: «کنگره نباید این فناوری حیاتی را تضعیف کند چرا که با این کار علیه منافع ملی عمل می‌کند. هرچند نباید نگرانی‌های نهادهای دولتی و اجرایی را نیز که گاهاً بجا نیز هست، نادیده بگیریم.»

گروه سیاست امنیت سایبری اتحادیه‌ی اروپا گفت قرار دادن دربِ پستی در رمزنگاری‌ها بیش از اینکه مزیت داشته باشد، خطرساز است. این کار باعث می‌شود تلاش‌های انجام‌شده برای حفظ محرمانگی و حریم خصوصی کاربران به هدر رفته و دربِ پشتی به سلاحی برای مهاجمان تبدیل شود تا بتوانند عملیات مخرب خود را اجرایی کنند.

مشابه همین گزارش، اوایل امسال لایحه‌ای در مجلس آمریکا به توصیب رسید مبنی بر اینکه دولت‌ها باید درخواست قرار دادن دربِ پشتی در رمزنگاری را متوقف کنند.

مقامات تایلند منتقدان دولت در فضای مجازی را دستگیر می‌کنند

یک مقام ارشد نظامی روز دوشنبه اعلام کرد مقامات تایلندی دست‌کم 9 نفر مظنون به نفوذ سایبری را دستگیر کردند. این دستگیری‌ها پس از آن رخ داد که تعدادی از نفوذگران به وب‌گاه نهادهای دولتی این کشور در اعتراض به قانون بحث‌برانگیز سانسور، نفوذ کردند.

در اوایل ماه جاری مجلس تایلند به اتفاق آرا قانونی را تصویب کرد. براساس این قانون تمامی مقامات ارشد نظامی می‌توانند وب‌گاه‌هایی که محتوایی بر ضد آن‌ها منتشر کرده را دست‌کاری کرده و از کار بیندازند.

در این لایحه که به‌طور گسترده عملیاتی شده است، کاربران از بارگذاری هرگونه محتوا که اخلاق خوب را نقض می‌کند، منع شده‌اند و کمیته‌ای نیز تشکیل شده تا وب‌گاه‌های دارای چنین محتواهایی را از کار بیندازد. به‌دنبال تصویب این لایحه، نفوذگران وب‌گاه‌های دولتی تایلند را هدف قرار دادند.

در حملات علیه وب‌گاه‌های دولتی تایلند، برخی از آن‌ها در اثر منع سرویس به‌طور موقت غیرفعال شده‌اند. در برخی موارد نیز نفوذگران عنوان کردند که توانستند به پایگاه داده‌ی وب‌گاه‌ها دست یافته و اطلاعات مهم کاربران آن را بدست آوردند.

شایعاتی مبنی بر بازداشت چندین نفر توسط ارتش این کشور در چند روز گذشته وجود داشت. اما مقامات این موضوع را روز دوشنبه به‌طور رسمی تأیید کردند. معاون نخست وزیر این کشور به خبرنگاران گفت: «ما تعدادی از نفوذگران را دستگیر کردیم. تعداد آن‌ها 9 نفر است و در چند روز آینده تعداد بیشتری از آن‌ها را بازداشت خواهیم کرد.»

روز دوشنبه پلیس بانکوک اعلام کرد یک جوان 19 ساله را به اتهام نفوذ سایبری دستگیر کرده و چند روز مورد بازجویی قرار داده است. مقامات پلیس اعلام کردند این جوان اعتراف کرده با جعل هویت توانسته است به سامانه‌های پلیس دسترسی پیدا کند. گروه‌های حقوقی و فعالان حوزه‌ی سایبری در تلاش هستند این قانون را در دادگاه به چالش بکشانند.

در حال حاضر در کشور تایلند مجموعه‌ای از قوانین به تصویب رسیده که مخالفان می‌گویند مناظرات را محدود می‌کند. در یکی از این قوانین عنوان شده که انتقاد از سلطنت و نظام حاکمیتی یک جرم محسوب می‌شود.

دو نفوذ جداگانه به وب‌گاه اتاق صنعت و بازرگانی ترکیه

وب‌گاه اتاق صنعت و بازرگانی ترکیه واقع در انگلستان در چند روز گذشته توسط دو گروه نفوذ جداگانه مورد حمله قرار گرفته است. اولین و مهم‌ترین این نفوذها توسط یک گروه کردی با نام مزوپتامیا انجام شده است. در این نفوذ پیامی در وب‌گاه به نمایش گذاشته شده که نشان می‌دهد نفوذگران در اعتراض به حمله‌ی هوایی ترکیه که منجر به کشته شدن 34 کرد روستانشین شد، این وب‌گاه را هدف قرار داده‌اند.

باوجود اینکه انگیزه‌ی حمله‌ی این گروه کاملاً روشن است، هنوز مشخص نشده آیا این نفوذگران توانسته‌اند اطلاعاتی را به سرقت ببرند و یا سایر صفحات وب‌گاه را نیز آلوده کنند یا خیر.

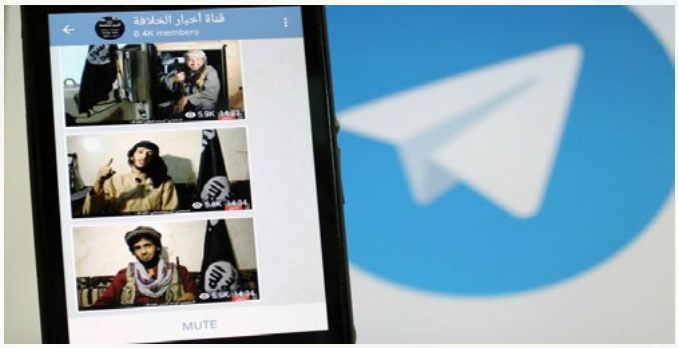
در یک نفوذ جداگانه، کاپوست‌کی که روش نفوذ به وب‌گاه‌های اتاق صنعت و بازرگانی را یاد گرفته، تلاش کرد تا به این وب‌گاه نیز نفوذ کند. در این حمله کاپوست‌کی توانسته به اطلاعات کاربران از جمله نام، آدرس رایانامه، شماره تلفن و آدرس‌های تعدادی از اعضای وب‌گاه دست یابد.

در نمونه داده‌هایی که بدست سافت‌پدیا رسیده، معلوم شده این پایگاه داده حاوی اطلاعات شخصی افراد از جمله نام، شماره تلفن و آدرس است. در این پایگاه داده یک حساب کاربری مدیریتی نیز به چشم می‌خورد که به نظر نمی‌رسد گذرواژه‌ی آن درهم‌سازی شده باشد.

کاپوست‌کی اعلام کرد با مدیران این وب‌گاه تماس گرفته و این مسئله را اطلاع داده ولی هنوز پاسخی از طرف آن‌ها دریافت نکرده است. به همین منظور بخشی از اطلاعات را افشاء کرده تا نشان دهد که واقعاً به پایگاه داده‌ی این وب‌گاه دست یافته است.

در زمان نگارش این خبر این وب‌گاه در حالت نفوذشده قرار دارد و پیغام گروه مزوپتامیا در آن در حال نمایش است. همچین این احتمال نیز وجود دارد که آسیب‌پذیری کشف‌شده توسط کاپوست‌کی هنوز وصله نشده باشد. به عبارت دیگر اطلاعات صدها نفر در معرض خطر قرار دارد.

تلگرام، اولین انتخاب داعش به‌عنوان بستر ارتباطی



برنامه‌ی پیام‌رسان تلگرام به اولین انتخاب اعضای داعش تبدیل شده و استفاده از آن به‌طور عجیبی از سایر رسانه‌های اجتماعی همچون توییتر پیشی گرفته است.

اگر می‌خواهید از فعالیت‌های داعش باخبر باشید، باید بدانید که امروزه تلگرام کانال ارتباطی اصلی داعش برای تبلیغات است. در چند وقت اخیر استفاده از پیام‌رسان‌های مبتنی بر رمزنگاری در بین گروه‌های تروریستی افزایش یافته و اینک داعش نیز بیش از پیش از تلگرام استفاده می‌کند. این موضوع استفاده از سایر شبکه‌های اجتماعی مانند توییتر را تحت‌الشعاع قرار داده است.

شبکه‌های اجتماعی تلاش می‌کنند تا محتوای ارسال شده توسط گروه‌های داعشی را مسدود کنند و می‌خواهند تبلیغات برخط این گروه را متوقف نمایند.

توییتر بستن صدها هزار حساب کاربری به دلیل نقض سیاست‌های خشونت افراطی را ادامه می‌دهد. در شهریور ماه توییتر یک پست وبلاگی را منتشر کرد که نشان می‌داد از سال گذشته این شرکت نزدیک به 360 هزار حساب کاربری با محتوای تروریستی را مسدود کرده است.

در هفته‌های قبل از حادثه‌ی برلین، تحلیلگران اطلاعاتی مشاهده کردند در کانال‌های تلگرام منتسب به گروه‌های داعشی، پیام‌هایی برای جذب داوطلبان و دعوت به قانون‌شکنی و کشتار به اشتراک گذاشته شده است.

یکی از دلایل استفاده‌ی گسترده‌ی داعش از تلگرام این است که این شرکت اقدامات سرکوب‌گرانه‌ی جدی را علیه فعالیت‌های داعش انجام نمی‌دهد. گروه‌های داعشی و القاعده در شبه جزیره‌ی عربستان چندین کانال تلگرامی را راه‌اندازی کردند و اعضای این گروه‌های تروریستی می‌توانند به‌طور امن با هم در ارتباط باشند.

کانال «ناشر» یکی از کانال‌های مربوط به داعش است که به چند زبان خبرهایی را در تلگرام منتشر می‌کند. به گزارش محققان برنامه‌ی تلگرام به عنوان یک بستر ارتباطی برای گروه‌های تروریستی گوی سبقت را از توییتر ربوده است. استفاده از تلگرام برای تروریست‌های داعشی آسان بوده و این برنامه گزینه‌های مختلفی برای ارتباطات عادی و رمزنگاری‌شده را ارائه می‌دهد.

نفوذ به توپخانه‌های اوکراین با استفاده از بدافزار اندرویدی

در تحقیقی که توسط محققان امنیتی شرکت CrowdStrike منتشر شد، نشان داده شده است که نفوذگران گروه Fancy Bear با استفاده از برنامه‌های اندرویدی مخرب، به سامانه‌های توپخانه‌ی اوکراین نفوذ کرده‌اند.

در این گزارش آمده است از این بدافزار برای ردیابی واحدهای مختلف توپخانه از جمله بخش خمپاره‌انداز D-30 ساخته‌شده توسط اتحادیه‌ی جماهیر شوروی در سال‌های 2014 تا 2016 استفاده شده است. این نفوذگران که با دولت روسیه مرتبط هستند، حدس زده می‌شود اطلاعات جمع‌آوری‌شده را برای ارتش نظامی روسیه ارسال کرده‌اند.

محققان امنیتی این شرکت کشف کردند که نفوذگران از یک برنامه‌ی اندرویدی آلوده به ابزار X-Agent برای دست یافتن به دستگاه‌های اندرویدی استفاده کرده‌اند. این دستگاه‌های اندرویدی در توپخانه‌های اوکراین برای عملیات خاصی مورد استفاده قرار می‌گرفت. این بدافزار در انجمن‌های نظامی اوکراین توزیع شده است و تقریباً 9 هزار نفر از افراد توپخانه، با استفاده از برنامه‌های قانونی به این انجمن دسترسی داشته‌اند.

بدافزار 9 هزار دستگاه را هدف قرار داده است

نفوذگران گروه Fancy Bear این برنامه را با یک بسته‌ی آلوده به نام Monp-M30.apk هدف قرار داده‌اند. این بسته‌ی مخرب اطلاعات مکانی و ارتباطی را از دستگاه آلوده بازیابی خواهد کرد.

این اطلاعات به ارتش روسیه کمک می‌کند تا مکان جغرافیایی دقیق توپخانه‌های اوکراین را پیدا کرده و آن را نشانه برود. در گزارش‌ها آمده است که ارتش اوکراین در طول 2 سال درگیری، 50 درصد از سلاح‌ها و نزدیک به 80 درصد از خمپاره‌اندازهای D-30 را از دست داده است.

این برنامه‌ی اندرویدی مخرب در بسیاری از انجمن‌های نظامی توزیع شده ولی هنوز شواهدی مبنی بر این وجود ندارد که در بازار گوگل پلی نیز منتشر شده باشد. کاربران باید این پرونده‌ی APK را به‌طور دستی نصب کنند.

این شرکت امنیتی اشاره کرده است: «استفاده از ابزار X-Agent نشان می‌دهد گروه Fancy Bear علاوه بر بستر iOS بدافزارهایی را در حوزه‌ی اندروید نیز توسعه داده و به یک مولفه‌ی جدید در جنگ روسیه علیه اوکراین تبدیل شده است.

لیتوانی دولت روسیه را به جاسوسی سایبری متهم کرد

روسیه مجدداً بخاطر نفوذ به رایانه‌های دولت‌های خارجی متهم شده است. این بار نیز لیتوانی جاسوس‌افزاری را کشف کرده و ادعا می‌کند این بدافزار توسط کرملین بر روی رایانه‌های دولتی این کشور نصب شده است.

در بیانیه‌ی رویترز، رئیس مرکز امنیت سایبری لیتوانی اعلام کرده نفوذگران روسی اولین بار در سال 2015 تلاش کردند تا رایانه‌های این کشور را با جاسوس‌افزار آلوده کنند ولی فقط همین امسال 20 تلاش مجدد دیگر توسط این نفوذگران به ثبت رسیده است.

قضیه زمانی بدتر می‌شود که این جاسوس‌افزار 6 ماه پس از نصب بر روی رایانه‌ها کشف شده است و رئیس این مرکز مدعی است که بدافزار اسناد و گذرواژه‌های دولت لیتوانی را برای آژانس‌های جاسوسی روسیه ارسال کرده است.

هنوز مشخص نیست که آیا اسناد محرمانه یا دولتی به سرقت رفته است یا خیر ولی مقامات لیتوانی می‌گویند برخی از این رایانه‌های آلوده توسط مقامات دولتی رده متوسط تا رده پایین مورد استفاده قرار می‌گرفت و این افراد بر روی پیش‌نویس تصمیمات دولت کار می‌کردند.

سخنگوی رئیس جمهور روسیه این اتهامات را رد کرده و این مسئله را خنده‌دار توصیف کرده است. او در ادامه گفت: «آیا درون این بدافزارها نوشته که توسط روسیه نوشته شده است؟ ما این اتهامات بی‌پایه و اساس را رد می‌کنیم.» او عنوان کرد که کشور روسیه هدف حملات و جاسوسی‌های سایبری قرار گرفته ولی دولت این کشور هیچ دولت خارجی را متهم نکرده است.

رئیس مرکز امنیت سایبری لیتوانی اشاره کرد که روسیه در حوزه‌ی امنیت سایبری به تهدیدی بزرگ تبدیل شده و همه‌ی دولت‌ها برای مقابله با نفوذهای نفوذگران وابسته به کرملین باید آماده شوند.