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

# اخبار فناوری اطلاعات و ارتباطات

۸۶

هفته نامه | سال دوم | شماره هشتاد و ششم | ۴ دی ۱۳۹۵

## دولت ترکیه مجدداً دسترسی به Tor را مسدود کرد

دولت ترکیه برای استفاده از شبکه‌ی گمنامی Tor محدودیت‌هایی اعمال کرد. این محدودیت‌ها توسط سازمان نظارت و سانسور اینترنت در ترکیه موسوم به Turkey Blocks ایجاد شده است. در پستی که توسط Turkey Blocks منتشر شده، آمده است: «مطالعات ما نشان می‌دهد ارائه‌دهندگان سرویس از دستورات دولتی مبنی بر ممنوعیت استفاده از سرویس VPN پیروی می‌کنند.»

همزمان با این گزارش، کاربران اشکالاتی را در اتصالات خود گزارش می‌کردند و این موضوع نشان می‌دهد که اقدامات جدیدی برای کنترل دسترسی بر روی اینترنت در حال اجرا بوده است. به دلیل افزایش سانسورها توسط مقامات محلی ترکیه، محبوبیت Tor در این کشور رو به افزایش است.

دولت ترکیه اقدامات مسدودسازی پیچیده‌ای را اعمال کرده که از کار افتادن شبکه‌های اجتماعی را متوقف نخواهد کرد. دولت ترکیه در بخشی از برنامه‌ی سانسور اینترنت، Tor و تمامی سرویس‌های VPN را مسدود کرده است.

دولت آنکارا به تازگی به ISP ها دستور داده هرگونه دسترسی به شبکه‌ی Tor و سرویس VPN را مسدود کنند. پیش از ماه دسامبر نیز در یک برنامه با نام «اینترنت تُرک» تمامی ISP های کشور توسط دولت تحت فشار قرار گرفتند تا به مسدودسازی‌ها ادامه دهند و آن را تکمیل کنند. دولت به ISP ها دستور داد در عرض یک هفته پس از اعمال محدودیت‌ها، وضعیت خود را به‌روزرسانی کنند.

در سال‌های اخیر دولت ترکیه چندین بار در پی ناآرامی‌ها و تظاهرات مردمی در خیابان‌ها، تعدادی از شبکه‌های اجتماعی را مسدود کرده است. در نمودار شکل زیر تعداد اتصالات مستقیم کاربران به Tor را مشاهده می‌کنید. به راحتی می‌توان دریافت محبوبیت این ابزار از سال گذشته در این کشور افزایش یافته است.

## فروش اطلاعات ۱ میلیارد کاربر یاهو در وب تاریک


اخیراً شرکت یاهو یک نقض داده‌ی عظیم در حساب‌های کاربری خود را افشا کرده است. در اثر این نقض داده، اطلاعات 1 میلیارد کاربر افشاء شده و گفته می‌شود این بزرگ‌ترین نقض داده در بین شرکت‌های مختلف بوده است.

اتفاق جدیدی که افتاده، این است که به گزارش اندرو کوماروف، از شرکت InfoArmor، نفوذگران پایگاه داده‌ی مربوط به اطلاعات 1 میلیارد کاربر را در مرداد ماه به قیمت 300 هزار دلار در وب تاریک به فروش رسانده‌اند.

کوماروف به نیویورک‌تایمز گفته است، به نظر می‌رسد 3 خریدار که 2 نفر از ارسال‌کنندگان برجسته‌ی هزرنامه بودند و یکی دیگر مربوط به پویش‌های جاسوسی، با پرداخت 300 هزار دلار به کل پایگاه داده دسترسی یافته‌اند.

به نظر می‌رسد این گروه نفوذ که اطلاعات کاربران یاهو را به سرقت برده و به فروش رسانده، در شرق اروپا مستقر هستند ولی با این‌حال یاهو مطمئن نیست که این اطلاعات دقیق است یا خیر.

در این پایگاه داده علاوه بر نام، گذرواژه، تاریخ تولد و شماره تلفن 1 میلیارد کاربر، اطلاعاتی همچون آدرس رایانامه‌های پشتیبان و در برخی موارد سؤال و جواب‌های امنیتی به‌صورت رمزنگاری‌شده و یا رمزنگاری‌نشده وجود دارد. با استفاده از این اطلاعات نفوذگران می‌توانند از طریق گرینه‌ی بازنشانی گذرواژه، هرچه سریع‌تر به حساب‌های کاربری یاهو دست یابند.

در حال حاضر نیز این پایگاه داده در وب تاریک به فروش می‌رسد ولی قیمت آن به‌طور چشمگیری کاهش یافته است چرا که یاهو اخیراً این نقض داده را به‌طور عمومی اعلام کرد و بسیاری از کاربران گذرواژه‌های خود را تغییر دادند. خریدارانی که علاقه‌مند هستند می‌توانند برای دریافت کامل این پایگاه داده 20 هزار دلار پرداخت کنند.کوماروف گفت که شرکت او، اوایل امسال از این پایگاه داده، رونویسی تهیه کرده و با مقامات قانونی و قضایی آمریکا و سایر کشورها در اتحادیه اروپا، کانادا و استرالیا در تماس است. او گفت مستقیماً به سراغ یاهو نرفته است چرا که یاهو به بررسی‌های این شرکت امنیتی اعتنایی نمی‌کند و همچنین مسئولان این شرکت نیز به بررسی‌های یاهو در خصوص این نقض داده، اعتماد ندارند.

## نفوذ به کمیسیون معاونت انتخابات آمریکا


محققان امنیتی سرویس‌های اطلاعاتی کشف کردند که یک نفوذگر روسی به سامانه‌ی کمیسیون معاونت انتخابات آمریکا نفوذ کرده و اطلاعاتی از جمله گواهی‌نامه‌های سطح مدیریتی را به سرقت برده و در ادامه این داده‌ها را در وب تاریک به فروش رسانده است.

در 11 آذر ماه محققان از شرکت امنیتی Recorded Future نشانه‌هایی در اینترنت کشف کردند که به نظر می‌رسید مربوط به نقض داده‌ی کمیسیون معاونت انتخابات باشد. این نفوذگر با نام راسپوتین، بیش از 100 گواهی‌نامه‌ی دسترسی به کارگزارهای دولت خاورمیانه را فروخته است. به نظر می‌رسد این مهاجم از آسیب‌پذیری SQLi برای دسترسی به سامانه استفاده کرده است. این آسیب‌پذیری در حال حاضر وصله شده است.

کمیسیون معاونت انتخابات، براساس قانون کمک به انتخابات آمریکا مربوط به سال 2002 تأسیس شده است. مسئولیت این کمیسیون نظارت و بررسی گواهی‌نامه‌های دیجیتال در انتخابات الکترونیکی است.

مهر ماه دولت آمریکا رسماً اعلام کرد که روسیه در نفوذ به سازمان‌های سیاسی آمریکا بویژه انتخابات ریاست جمهوری، نقش داشته است. ولی هنوز هم شواهدی مبنی بر این وجود ندارد که نقض رخ داده در کمیسیون معاونت انتخابات نیز در ادامه‌ی این نفوذها بوده باشد و ارتباط مستقیمی بین این نقض داده و نفوذگران دولت روسیه وجود ندارد. به احتمال زیاد این نقض داده یک نفوذ استاندارد بوده و در ادامه مهاجمان، داده‌ها را به سرقت برده و فروخته‌اند.

با این حال هنوز مشخص نیست که آیا گروه‌های نفوذ دیگری نیز قبلاً این آسیب‌پذیری را کشف و از آن بهره‌برداری کرده باشند. از آنجایی هم که این نقض توسط کمیسیون معاونت انتخابات کشف نشده و یک شرکت امنیتی دیگر آن را کشف کرده، این احتمال وجود دارد که نقض داده‌ی دیگری نیز رخ داده و هنوز کشف نشده باشد.

سخنگوی این کمیسیون گفت: «اینکه نفوذگران خارجی این قابلیت را داشته‌اند که نتایج نهایی انتخابات را تغییر دهند، بسیار اغراق‌آمیز است. نفوذگران رئیس جمهور بعدی ما را انتخاب نکرده‌اند و این انتخاب توسط مردم انجام شده است.»

## نفوذگران روسی بانک‌های اوکراین را هدف قرار داده‌اند

نفوذگران گروه BlackEnergy که با موفقیت بسیاری از حملات را علیه سامانه‌های انرژی انجام دادند و برق تعدادی از نیروگاه‌های اوکراین را قطع کردند، به نظر می‌رسد عامل احتمالی حمله به بانک‌های اوکراینی باشند.

شرکت امنیتی ESET یک گروه نفوذ با نام TeleBots را کشف کرد که شیوه‌ی عملکردی بسیار مشابهی به گروه BlackEnergy دارد. این گروه نفوذ جدید، در وهله‌ی اول بانک‌های اوکراینی را هدف قرار داده است و از حملات فیشینگ استفاده می‌کند. رایانامه‌های فیشینگ حاوی اسناد مخرب اکسل هستند که باعث آلوده شدن رایانه‌های کاربران می‌شود.

اسناد اکسل حاوی ماکروهای مخرب هستند که به محض فعال شدن، به‌طور خودکار بر روی ماشین قربانی بدافزاری را بارگیری و اجرا می‌کنند. در ادامه این بدافزار سامانه را آلوده می‌کند، به کل شبکه نفوذ می‌کند، اسناد و گذرواژه‌ها را به سرقت می‌برد و هر اطلاعاتی را که مهاجم بخواهد، از رایانه‌ی قربانی استخراج می‌کند.

ESET توضیح داد: «هدف اصلی ماکروی مخرب قرار دادن باینری مخرب با نام explorer.exe در رایانه‌ی قربانی است. بدافزار بارگیری‌شده متعلق به خانواده‌ی تروجان‌های بارگیری‌کننده است که برای بارگیری بدافزارهای بیشتر مورد استفاده قرار می‌گیرد. این بدافزار با زبان برنامه‌نویسی Rust نوشته شده است.»

سامانه‌ها با یک دربِ پشتیِ نشانه‌گذاری‌شده با Python/TeleBot. AA آلوده شده‌اند که بسیار شبیه به تروجانی است که در حملات قبلی گروه BlackEnergy علیه اوکراین استفاده شده بود. در نهایت نیز مهاجمان از KillDisk استفاده می‌کنند که یک بدافزار مخرب برای غیرقابل بوت کردن سامانه عامل است. این بدافزار نیز شبیه به بدافزاری است که در حمله به نیروگاه‌های برق اوکراین استفاده شده بود.

شرکت ESET اشاره کرد: «جالب است که بدافزار KillDisk این تصویر را هیچ جایی ذخیره نمی‌کند و با استفاده از GDI ویندوز به‌طور بلادرنگ این تصویر را رسم می‌کند. به نظر می‌رسد مهاجمان برای رسم این تصویر و نوشتن کد آن بسیار تلاش کرده‌اند.»

در حال حاضر مشخص نیست چه تعداد از حملات موفقیت‌آمیز بوده است.