

## آمریکا یک نفوذگر ترکیه‌ای را به جرم نفوذ به بانک‌ها زندانی کرد



یک شهروند ترکیه‌ای با نام ارکان فیندیک‌اوغلو، 35 ساله توسط دادگاهی در نیویورک دستگیر و به 8 سال زندان محکوم شد. او به رهبری یک پوشش سایبری در حمله به بانک‌هایی در سطح دنیا محکوم شده است. این فرد به جرم‌هایی همچون نفوذ به سامانه‌های بانک‌ها، تقلب، کلاه‌برداری و دسترسی و دست کاری غیرمجاز تراکنش‌های بانکی اعتراف کرده است.

مقامات قضایی می‌گویند در بازه‌ی سال‌های 2011 تا 2013 سه پوشش به رهبری این فرد راه‌اندازی و زبانی بالغ بر 55 میلیون دلار به بانک‌ها وارد شده است. این گروه‌های نفوذ به سامانه‌های پردازش کارت‌های بانکی نفوذ کرده و اطلاعات کارت‌ها را به سرقت می‌بردند. داده‌های سرقتی به اعضای دیگر ارسال می‌شد و آن‌ها نیز این اطلاعات را بر روی کارت‌های خالی چاپ و جعل می‌کردند. با استفاده از این کارت‌ها و پین‌ها در سراسر جهان، در دستگاه‌های خودپرداز می‌توان برداشت‌های جعلی انجام داد.

در اولین عملیات که در سال 2011 انجام شد، 15 هزار برداشت از 180 کشور انجام شده و 10 میلیون دلار به سرقت رفته بود. در عملیات بعدی، در سال 2012، تقریباً 5 میلیون دلار از 5 هزار دستگاه خودپرداز در 20 کشور به سرقت رفت. سومین و آخرین عملیات که در سال 2013 انجام شد، کلاه‌برداران توانستند در 24 کشور نزدیک به 40 میلیون دلار را از 36 هزار دستگاه خودپرداز بدزدند. تنها در نیویورک با 3 هزار برداشت، 2.4 میلیون دلار به سرقت رفته بود.

فیندیک‌اوغلو در سال 2103 در آلمان دستگیر و در سال 2015 به آمریکا تحویل داده شد. او پس از سپری کردن محکومیت خود در آمریکا به ترکیه فرستاده خواهد شد. محکومیت او برای جعل و کلاه‌برداری کارت‌های اعتباری 20 سال است.

دادگاه آمریکا که روز جمعه فیندیک‌اوغلو را محاکمه کرد، دستور داد تا مبلغی بالغ بر 55 میلیون دلار را به‌عنوان خسارت پرداخت کند ولی خیرگزارای‌ها اعلام کردند دولت ترکیه تمامی دارایی‌های او را تصرف کرده و دارایی فعلی او برابر با 150 هزار دلار است. هنگامی که فیندیک‌اوغلو به جرائم خود اعتراف کرد، دولت آمریکا گفت چندین نفر از اعضای این گروه نفوذ را نیز دستگیر کرده است.

## سناتورهای آمریکایی یاهو را برای ارائه‌ی اطلاعات بیشتر در مورد نقض‌های اطلاعاتی تحت فشار قرار دادند



چندین تن از سناتورهای آمریکایی یاهو را به عدم هم‌کاری در فرآیند بررسی بزرگ‌ترین نقض‌های داده‌ی تاریخ متهم کرده‌اند. با توجه به نامه‌ی امضاء شده توسط جان تون، سناتور ایالت داکوتای جنوبی در سنای ایالات متحده‌ی آمریکا در تجارت و علوم و حمل و نقل، و جری موران، رئیس کمیته‌ی فرعی حمایت از مصرف‌کنندگان، ایمنی محصولات، بیمه و امنیت داده‌ها، بسیاری از سؤالاتی که از یاهو پرسیده شده بی‌پاسخ مانده‌اند، این در حالی است که یاهو قول داده بود توضیحات لازم را به تفصیل بیان کند.

علاوه بر این، یاهو در آخرین لحظات یکی از جلسات برنامه‌ریزی شده کنگره برای کارکنان خود را که در اصل برای ۳۱ ژانویه‌ی ۲۰۱۷ تدارک دیده شده بود لغو کرد، این موضوع نشان‌دهنده‌ی عدم تمایل این شرکت مطرح به ارتباط با این کنگره بوده و موجب افزایش نگرانی‌ها شده است.

به نظر می‌رسد که یاهو با این کمیته تماس برقرار کرده و قصد بیان نقش خود را در رابطه با کشف نقض‌های داده‌ی ۲۰۱۳ در تاریخ ۱۴ دسامبر داشته است. اما این دیدار چند روز قبل از برگزاری لغو شده است و این موضوع باعث ناراحت شدن سناتورهای آمریکایی شده است.

آن‌ها گفته‌اند: «ما مدت‌ها تلاش کردیم تا اطلاعات بیشتری را در رابطه با این رخدادها کسب کنیم. هدف ما این بود که متوجه شویم یاهو قصد دارد چه گام‌هایی را در راستای بررسی این رخداد بردارد، و این‌که یاهو برای بازیابی و حفظ یکپارچگی سامانه‌های خود، و نیز شناسایی و کاهش آسیب‌های احتمالی چه فکری در سر دارد.»

### پرسشی که همه‌ی ما به دنبال جواب آن هستیم

این دو سناتور دو سؤال را مطرح کردند که احتمالاً همه‌ی ما در ماه‌های گذشته به آن فکر کرده‌ایم. برای مثال آن‌ها قصد دارند بدانند که دقیقاً چه تعداد کاربر از این ماجرا آسیب دیده‌اند، و این‌که یاهو برای شناسایی و اطلاع‌رسانی به این کاربران چه کاری انجام داده است، همچنین چه داده‌هایی به عقیده‌ی یاهو مورد نفوذ قرار گرفته‌اند.

## درخواست دو سناتور آمریکایی برای بررسی تلفن همراه دونالد ترامپ



دو تن از سناتورهای آمریکایی خواستار بررسی امنیت تلفن همراه دونالد ترامپ شدند. این سناتورها اعلام کردند اگر ترامپ از تلفن همراه قدیمی خود استفاده کند، ممکن است اسرار ملی آمریکا در معرض خطر قرار بگیرد.

یکی از این سناتورها روز سه‌شنبه در توییتی گفت: «آیا دونالد ترامپ برای استفاده‌های شخصی خود از یک دستگاه ایمن و رمزنگاری شده استفاده می‌کند؟ ترامپ اینک باید با پروتکل‌های امن و مناسبی در راستای امن نگه داشتن اسرار ملی آمریکا آشنا شود.» او در ادامه همچنین از دولت جزئیاتی در خصوص دستگاه تلفن همراه ترامپ درخواست کرد.

این درخواست از طرف این دو سناتور در تاریخ 21 بهمن برای رئیس امنیت داخلی آمریکا، مدیر آژانس ملی آمریکا و همچنین وزارت دفاع ارسال شده است. این درخواست دوشنبه‌ی گذشته توسط این سناتورها منتشر شده است. آن‌ها اعلام کردند در خصوص استفاده‌ی ترامپ از یک دستگاه اندرویدی قدیمی بسیار نگران هستند. در این نامه آمده است: «در حالی که بسیار مهم است که رئیس جمهور توانایی استفاده از ارتباطات الکترونیکی را داشته باشد، همان‌قدر هم مهم است که به امنیت آن توجه کرده و سوابق ریاست جمهوری خود را حفظ کند. خطراتی که استفاده از دستگاه اندرویدی توسط رئیس جمهور برای امنیت ملی این کشور دارد بسیار قابل توجه است.»

نیویورک‌تایمز ماه گذشته اعلام کرد باتوجه به اینکه ترامپ پس از تحلیف، یک دستگاه امن و رمزنگاری شده دریافت کرده است ولی همچنان از دستگاه اندرویدی خود استفاده می‌کند. این گزارش باعث نگرانی تعداد زیادی از کارشناسان امنیتی در این کشور شده است. روز سه‌شنبه یک محقق امنیتی مستقل اعلام کرد که تلفن همراه دونالد ترامپ یک منبع باارزش برای نفوذگران در سطح اینترنت است و آژانس‌های اطلاعاتی در سراسر دنیا می‌توانند به آن نفوذ کنند.

## حمله‌ی نفوذگران روسی به سامانه‌های وزارت امور خارجه‌ی ایتالیا



یک منبع دیپلماتیک روز جمعه به خبرگزاری‌ها اعلام کرد سال گذشته به سامانه‌های وزارت امور خارجه‌ی ایتالیا حمله شده و این کشور نفوذگران روسی را متهم اصلی این ماجرا می‌داند. وزارت امور خارجه‌ی روسیه نیز بیان کرد هیچ مدرکی مبنی بر انجام این حمله توسط نفوذگران روسی وجود ندارد.

این منبع دیپلماتیک که روابط نزدیکی با وزارت امور خارجه‌ی ایتالیا دارد اعلام کرد این حمله، سامانه‌های رمزنگاری شده‌ی ایتالیا را تحت تأثیر قرار نداده است. از این سامانه‌های رمزنگاری شده برای تبادل و نگهداری اطلاعات حساس در این وزارت‌خانه استفاده می‌شود. اما این نفوذ حساب‌های رایانامه‌ی کارکنان وزارت‌خانه را در معرض خطر قرار داده است.

گاردین اعلام کرد این حملات به مدت چهار ماه ادامه داشته ولی حساب‌های وزیر امور خارجه‌ی ایتالیا تحت تأثیر قرار نگرفته است چرا که او در دوران خدمت خود از این سرویس‌های رایانامه‌ای استفاده‌ای نکرده است. هر داده‌ای که از طریق رایانامه‌های وزارت امور خارجه ارسال شده در امنیت کامل بوده است چرا که داده‌ها رمزنگاری می‌شوند.

کشورهای اروپایی از جمله آلمان، فرانسه، نروژ و هلند از اینکه هدف حملات سایبری روسیه قرار بگیرند بسیار نگران هستند. این کشورها معتقدند روسیه پویس‌های سایبری زیادی را برای حمله به این کشورهای اروپایی راه‌اندازی کرده است.

چند ماه قبل شاهد بودیم که آمریکا مدعی شده بود روسیه در انتخابات ریاست جمهوری این کشور دخالت کرده و نفوذگران روسی به کارگزارهای حزب دموکرات حمله کرده و اطلاعاتی را راجع به ارتباطات شرم‌آور کاندیدای این حزب منتشر کرده‌اند. این ادعا باعث شده کشورهای اروپایی نیز برای انتخابات آتی خود، نگران حملات سایبری روسیه باشند.