بزرگ‌ترین حمله بدون نیاز به گذرواژه

چگونه هکرهای روسی بدون گذرواژه به میلیون‌ها حساب کاربری یاهو دسترسی پیدا کردند

وزارت دادگستری ایالات متحده روز شنبه اعلام کرد، جاسوسان و هکرهای روسی در قالب یک تیم گردهم آمدند تا به هزاران حساب کاربری یاهو نفوذ کنند. این هکرها به واسطه یک نقص داده‌ای موفق شدند بیش از 500 میلیون حساب کاربری یاهو را به سرقت ببرند. بزرگ‌ترین حمله هکری که تا به امروز انجام شده است.

هکرهای روسی چگونه موفق به انجام چنین کاری شدند؟

به طور کلی، هکرها حمله خود را به شکلی برنامه‌ریزی کرده بودند تا به یک پوشه مخفی متشکل از گذرواژه‌های رمزنگاری شده، نام‌های کاربری و اطلاعات دیگر دست پیدا کنند. در ادامه هکرها از این اطلاعات برای فریب یاهو استفاده کردند. به شکلی که یاهو این‌گونه تصور کند که این اطلاعات درون مرورگر کاربران و در زمان لاگین کردن به سرویس‌های آنلاین یاهو ذخیره‌سازی شده است. یک تکنیک هوشمندانه که به آن‌ها اجازه داد بدون آن‌که به رمزگشایی گذرواژه‌ها نیازی داشته باشند به حساب‌ها وارد شوند.

البته هکرها در این حمله کمی شیرین‌کاری نیز از خود نشان دادند. به طوری که یکسری حساب‌های کاربری خاص و جعلی را همراه با گواهی‌نامه‌های جعلی ایجاد کردند تا کاربران را فریب دهند که افراد برجسته و شناخته شده جامعه هستند. در دنیای زیرزمینی هکرها این روش حمله رایج و مرسوم بود و تاثیرگذاری بالایی دارد.

مطلب پیشنهادی

باز هم هک یاهو؛ نفوذ بدون نیاز به گذرواژه
وقت خداحافظی با یاهومیل فرا رسیده است!

صفحات زرد یاهو و کوکی‌های جعلی

وزارت دادگستری ایالات متحده گفته است، آلکسی آلکسیویچ بلان هکر روسی موفق شده است به حساب‌های

کاربری نفوذ کرده و حداقل یک کپی از بخش‌های مهم بانک اطلاعاتی کاربران یاهو را به دست آورد. به نظر می‌رسد هکرها به بانک اطلاعاتی یاهو که درون یک پوشه مرکزی یا صفحات زرد یاهو بوده و اطلاعات همه کاربران یاهو را در خود جای داده بود دست پیدا کرده بودند. این بانک‌اطلاعاتی داده‌های مربوط به نام کاربری، گذرواژه‌های رمزنگاری شده و دیگر اطلاعات حساس را در خود جای داده بودند. یک بانک اطلاعاتی کاملا محرمانه که به شکل عمومی در دسترس نیست. در کیفرخواست صادر شده هکرهای روسی با سه اتهام وارد کردن اطلاعات کلیدی به شکل دستی، انجام احراز هویت جعلی مبتنی بر کوکی‌ها و جعل کردن اطلاعات روبرو هستند.

هکرها چگونه از کوکی‌ها استفاده کرده‌اند؟

هر زمان از سایتی بازدید می‌کنید، سایت بازدید شده فایل کوچکی روی کامپیوتر شما قرار می‌دهد که به نام کوکی از آن نام برده می‌شود. این کوکی اطلاعات خاصی در ارتباط با جزییات حساب‌کاربری شما را نگه‌داری می‌کند. اطلاعات مربوط به لاگین، و هر گونه اطلاعاتی که در ارتباط با حساب کاربری شما است درون این فایل ذخیره‌سازی می‌شود. زمانی که سایت را مجددا مورد بازدید قرار می‌دهید، سایت بررسی می‌کند آیا شما یک کوکی معتبر و قابل استناد در اختیار دارید و آیا تاریخ مصرف این کوکی تمامی شده یا هنوز معتبر است. اکثر سایت‌ها به کاربران اجازه می‌دهند پیش از پایان یافتن تاریخ اعتبار کوکی‌ها به مدت 30 روز وضعیت لاگین به سایت را حفظ کنند. مادامی که تاریخ انقضای کوکی کاربر به پایان نرسیده باشد، کاربران برای ورود به سایت احتیاجی ندارند اطلاعات هویتی خود را وارد کنند. به دلیل این‌که سایت‌ها فرض را بر این موضوع می‌گذارند که کاربر از کامپیوتر و مرورگر یکسانی برای ورود به سایت استفاده می‌کند. سایت کوکی را خوانده و تصور می‌کند کاربر در گذشته فرآیند لاگین را انجام داده است.

در این حمله هکرها موفق شدند دستورالعمل کوکی‌های یاهو و اطلاعات مربوط به پوشه محرمانه را به سرقت ببرند. این به معنای آن است که هکرها موفق شدند کوکی‌های جعلی را برای حساب‌هایی که به دنبال آن‌ها بودند ایجاد کنند. کوکی‌های جعلی به شکلی زیرساختی قادر هستند سایت‌هایی شبیه به یاهو میل را فریب داده تا تصور کنند کاربر قبلا به سایت وارد شده است. این مکانیزم حمله به آن‌ها اجازه داد دسترسی کاملی به حساب‌های خاص داشته باشند. بدون آن‌که به گذرواژه نیازی باشد.

وزارت دادگستری ایالات متحده گفته است: «بر مبنای این رویکرد هکرها موفق شدند حداقل به 6500 حساب کاربری دست پیدا کنند. از جمله حساب‌های مهمی که مورد حمله قرار گرفتند به حساب‌های روزنامه‌نگاران و سیاستمداران روسی می‌توان اشاره کرد. هکرها همچنین به 30 میلیون حساب کاربری دست پیدا کردند و از طریق آن‌ها کمپینی برای ارسال هرزنامه‌ها ایجاد کردند. به احتمال زیاد این کمپین به آن‌ها اجازه داده است مبالغ زیادی را به دست آورند.»

این حمله به ما نشان داد همه چیز در یک چشم برهم زدن و بر مبنای یک رخنه داده‌ای به سادگی دگرگون می‌شود. حتا اگر هکرها هی‌چگونه اطلاعاتی درباره گذرواژه‌ها نداشته باشد.

تاریخ انتشار:
30 اسفند 1395

نشانی منبع: https://www.shabakeh-mag.com/security/7275