به‌کارگیری یک الگوریتم ناکارآمد

متخصصان امنیتی رمزنگاری توانستند 320 میلیون رمزعبور را بشکنند

متخصصان امنیتی گروه CynoSure که نزدیک به دو سال پیش موفق شده بودند رمزعبور مربوط به 11 میلیون حساب کاربری را رمزگشایی کنند، یکبار دیگر موفق شدند دست به کار بزرگ‌تری زده و این بار به بازیابی 320 میلیون رمزعبور بپردازند.

بسیاری از سایت‌ها برای آن‌که از حساب‌های کاربردی خود در برابر حملات هکری محافظت به عمل آورند، گذرواژه مربوط به حساب‌های کاربری را به‌طور مستقیم در بانک اطلاعاتی خود ذخیره‌سازی نمی‌کنند، بلکه در ابتدا این گذرواژه‌ها را درهم شکسته (که در اصلاح رمزنگاری به آن Hash گفته می‌شود) و پس از انجام این‌کار گذرواژه‌ها را در بانک‌های اطلاعاتی ذخیره‌سازی می‌کنند.

مطلب پیشنهادی

یک ویژگی امنیتی در اختیار توسعه‌دهندگان
تا چه اندازه با دیوارآتش سرویس App Engine گوگل آشنا هستید؟

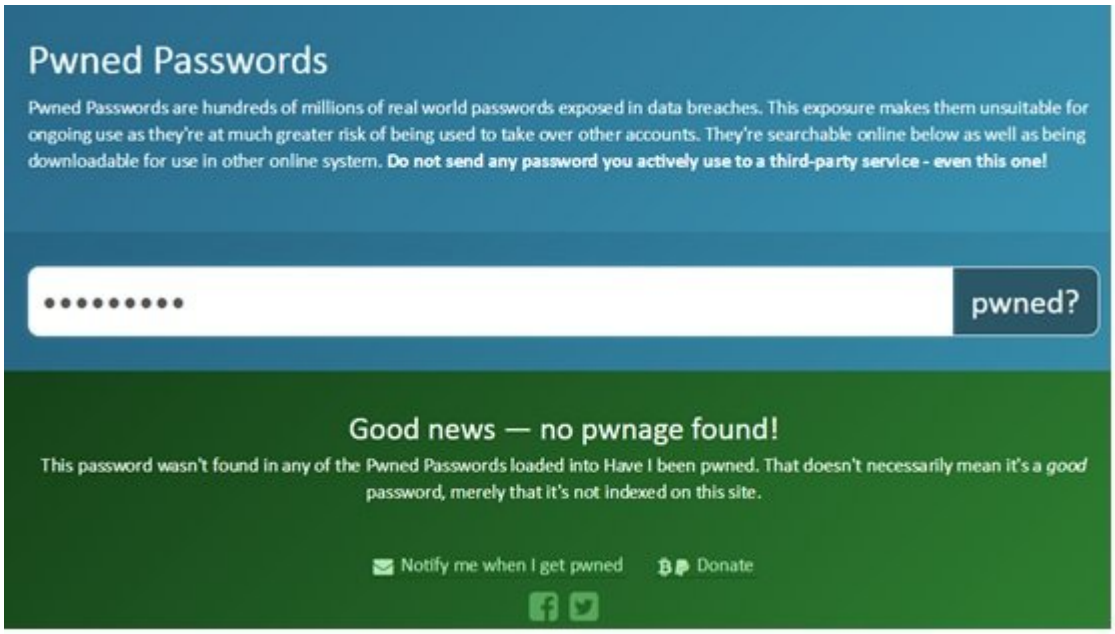
همین موضوع باعث می‌شود تا فرآیند بازیابی گذرواژه‌های درهم شکسته شده برای هکرها کار ساده‌ای نباشد. اما اوایل ماه جاری میلادی سایت HaveIBeenPwned گزارشی از میلیون‌ها گذرواژه و آدرس ایمیلی را منتشر کرده که مورد نفوذ قرار گرفته‌اند. مسئولان این سایت هدف از انجام این‌کار را این‌گونه تشریح کردند: «کاربران باید بدانند به‌کارگیری گذرواژه‌های یکسان برای حساب‌های کاربری مختلف کار عاقلانه‌ای نیست. همچنین مدیران سایت‌ها هم نباید گذرواژه‌های تکراری و ساده را قبول کرده و باید این موضوع را به کاربران اطلاع دهند.»

رویس ویلیامس و یک دانشجوی آلمانی مقطع دکترای امنیت اطلاعات که عضو گروه CynoSure Prime هستند به همراه دیگر اعضا این گروه تصمیم گرفتند چالش پیشنهاد شده از سوی تونی هانت را قبول کرده و به بازیابی 320 میلیون گذرواژه‌ای بپردازند. تروی هانت به واسطه کلاس‌هایی که در زمینه امنیت اطلاعات بزگزار می‌کند و همچنین بانک‌اطلاعاتی مربوط به رخنه‌هایی که Have I been Pwned راه‌اندازی کرده شهرت دارد.

مطلب پیشنهادی

نشت اطلاعات پورت USB به پورت‌های مجاور

کته جالب توجهی که در این ارتباط وجود دارد این است که بخش عمده‌ای از شرکت‌های نرم‌افزارهای از الگوریتم درهمساز SHA1 برای غیرقابل دسترس کردن گذرواژه‌های خود استفاده کرده بودند.



الگوریتمی که به هیچ عنوان ایمن نبوده و حتا گوگل نیز راهکار جالبی را برای شکستن این الگوریتم پیشنهاد داده بود. این گروه از طریق ابزار MDXfind موفق شدند 15 الگوریتمی که برای درهم‌سازی گذرواژه‌ها به کار رفته بود را شناسایی کنند. اگر کنجکاو شده‌اید که بدانید گذرواژه‌ای که برای حساب‌های خود استفاده می‌کنید ایمن است یا خیر پیشنهاد می‌کنیم به آدرس https://haveibeenpwned.com/Passwords مراجعه کنید. اگر گذرواژه شما قبلا شکسته شده باشد این سایت موضوع را به شما اطلاع می‌دهد. این گروه اعلام داشته‌اند تنها 116 گذرواژه‌ای که از الگوریتم SHA1 استفاده کرده‌اند را با موفقیت بازیابی نکرده‌اند. به عبارت دقیق‌تر این گروه 99.99 درصد گذرواژه‌ها را با موفقیت بازیابی کرده‌اند.

تاریخ انتشار:
20 شهریور 1396

نشانی منبع:
https://www.shabakeh-mag.com/news/world/9604/%D9%85%D8%AA%D8%AE%D8%B5%D8%B5%D8%A7%D9%86-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%B1%D9%85%D8%B2%D9%86%DA%AF%D8%A7%D8%B1%DB%8C-%D8%AA%D9%88%D8%A7%D9%86%D8%B3%D8%AA%D9%86%D8%AF-320-%D9%85%DB%8C%D9%84%DB%8C%D9%88%D9%86-%D8%B1%D9%85%D8%B2%D8%B9%D8%A8%D9%88%D8%B1-%D8%B1%D8%A7-%D8%A8%D8%B4%DA%A9%D9%86%D9%86%D8%AF