وب تاریک، بازار زیر زمینی هکر ها

AlphaBay یکی از بزرگ‌ترین بازارهای هکری در وب تاریک به شمار می‌رود. اما به تازگی رخنه بزرگی در آن شناسایی شد که به هکرها و البته کارشناسان امنیتی اجازه می‌داد به محاوره‌ها و گفت‌وگوهای خصوصی کاربران در این سایت دست پیدا کنند. اولین بار یک کارشناس امنیتی پس از آن‌که این سایت را مورد بررسی قرار داد موفق به شناسایی آسیب‌پذیری فوق شد.

به گزارش ایران هشدار – هکرها همانند کاربران عادی بازارهای خاص خود را دارند. بازارهایی که همواره زیرزمینی بوده و به نام وب تاریک از آن‌ها یاد می‌شود. این سایت‌ها مقررات سخت‌گیرانه و خاص خود را دارند. به طوری که سعی می‌کنند تا حد امکان هویت بدافزارنویسان و خریداران را از دید مقامات رسمی و پلیس سایبری پنهان نگاه دارند. اما زمانی که یک رخنه در چنین انجمن‌هایی پیدا می‌شود، تمامی معادلات بر هم می‌ریزد.

AlphaBay یکی از بزرگ‌ترین بازارهای هکری در وب تاریک به شمار می‌رود. اما به تازگی رخنه بزرگی در آن شناسایی شد که به هکرها و البته کارشناسان امنیتی اجازه می‌داد به محاوره‌ها و گفت‌وگوهای خصوصی کاربران در این سایت دست پیدا کنند. اولین بار یک کارشناس امنیتی پس از آن‌که این سایت را مورد بررسی قرار داد موفق به شناسایی آسیب‌پذیری فوق شد.

در ادامه رخنه فوق را مورد آزمایش قرار داد و مشاهده کرد که با استفاده از آن می‌توان به محتوای ۲۰۰ هزار پیام رمزنگاری نشده میان کاربران و فروشندگان دست پیدا کرد. AlphaBay پس از اطلاع از این آسیب‌پذیری وصله مربوطه را ارائه کرده و البته جایزه قابل توجهی را به این کارشناس امنیتی اهدا کرد. کاربری در سایت ردییت با نام کاربری ۰۰۰۷Cipher فردی بود که به مدیران این سایت گزارش کرد که رخنه‌ای وجود دارد. در مرتبه اول دست‌اندرکاران سایت نسبت به هشدار او بی توجه بودند. اما در ادامه جزییات بیشتری را از این کارشناس امنیتی دریافت کردند و موفق شدند وصله مربوطه را ارائه کنند.

آلفابای در این ارتباط گفته است: «تمامی پیام‌هایی که از طریق این رخنه قابل مشاهده و پیگیری بودند عمری کمتر از یک ماه داشتند. به واسطه آن‌که پیام‌های قدیمی این سایت به طور خودکار حذف می‌شوند. هکرها ممکن است تنها فهرستی از شناسه کاربری (ID) و نام کاربری را به دست آورده باشند اما اطلاعات دیگری همچون گذرواژه‌ها، آدرس‌های BTC یا اطلاعات قدیمی‌تر کاملا دست نخورده هستند.» اما به نظر می‌رسد دامنه افشای اطلاعات فراتر بوده است به دلیل این‌که عکس‌هایی که از سوی این کارشناس منتشر شده نام، نام خانوادگی، نام مستعار، آدرس ایمیل شماره ردیابی بسته‌ها و هر آن چیزی که با کلیدهای PGP محافظت نشده است را نشان می‌دهد. در نتیجه به نظر می‌رسد اطلاعات بیشتری لو رفته‌اند.

پیام‌های خود را رمزنگاری کنید

آلفابای می‌گوید: «تاکنون اتفاق بدی رخ نداده است، به واسطه آن‌که این کارشناس امنیتی پس از شناسایی این رخنه آن‌را به سرعت گزارش کرده است. اما به کاربران این سایت اعلام می‌داریم که همواره پیام‌های خود را رمزنگاری تا دچار مشکل نشوند. ما تمام تلاش خود را به کار می‌گیریم تا این سایت را ایمن کنیم اما طبیعی است به واسطه ماهیت سایت و پروفایل کاربران همواره هکرها و آزمایش کنندگان به دنبال نفوذ هستند.» آلفابای در سال ۲۰۱۴ کار خود را آغاز کرد و به سرعت نزد کاربران محبوب شد. کاربران در این سایت به انواع مختلفی از اطلاعات به سرقت رفته منجمله کارت‌های اعتباری و بانکی دسترسی دارند. مقامات رسمی همیشه به دنبال آن بوده‌اند تا کاربران این سایت وب تاریک را شکار کنند و در یک نمونه موفق شدند یکی از فروشندگان کارت‌های اعتباری را شناسایی کرده و حکم زندان را برای او بگیرند. گمنامی فاکتور مهمی برای پنهان ماندن کاربران اینگونه سایت‌ها است. اما به نظر می‌رسد اطلاعات ارائه شده از سوی ۰۰۰۷Cipher به پلیس در شناسایی این افراد کمک فراوانی خواهد کرد.

منبع: ایتنا

اداره حراست آموزشکده شهید یزدانپناه سنندج