Fireball [illegible]

[illegible]

[illegible] Fireball [illegible] 250 5 [illegible] Fireball [illegible]

[illegible] Fireball [illegible] fireball [illegible] (Home Page) [illegible]

هنگامی که مرورگر کاربر به سمت موتور جستوجوگر جعلی هدایت میشود در ادامه از طریق تکنیک ردیابی پیکسلهای صفحهنمایش اطلاعات حساس متعلق به قربانیان را جمعآوری میکند . بدافزار فوق در سال گذشته میلادی در قالب برنامههای معتبر و قانونی موفق شد بیش از 250 میلیون سامانه کامپیوتری را در سراسر جهان آلوده کند . این گزارش نشان میدهد بخش عمدهای از سامانههای قربانیان در کشورهای هندوستان، برزیل، مکزیک و اندونزی قرار داشتند . همچنین تعداد 5.5 میلیون سامانه کامپیوتری نیز در ایالات متحده قربانی این بدافزار شدند . تحلیل انجام شده در خصوص بدافزار fireball نشان میدهد نزدیک به 20 درصد از شرکتها نیز به بدافزار فوق آلوده شدند .

بدافزار fireball این پتانسیل را دارد تا پس از دستکاری تنظیمات مرورگر، مرورگر قربانی را به سمت سایتهای مخرب هدایت کرده و ابزارهای استراق سمع را روی دستگاه قربانی نصب کند . همچنین از تکنیکهای مختلفی برای گذر از تکنیکهای جعبه شن (sandbox) و عبور از لایههای امنیتی چندگانه استفاده کرده تا به شکل دقیقی به سرور کنترل و فرماندهی خود متصل شود . این بدافزار همچنین اقدام به نصب یک درب پشتی روی سیستم کاربر میکند تا در آینده بتواند از آن استفاده کند . با توجه به آنکه بدافزار فوق از گواهینامههای دیجیتالی استفاده میکند در نتیجه به شکل کاملا قانونی قادر است به درون سیستمهای کامپیوتری وارد شود . تحلیلهای بیشتر نشان میدهند که این بدافزار قادر است با یکسری محصولات دیگر ادغام شود تا توزیع آن به شکل دقیقتر و کاملتری انجام شود .

توجه داشته باشید، زمانی که تصمیم میگیرد یک نرمافزار رایگان را روی سامانه خود نصب کنید باید به این نکته دقت کنید که در ابتدا ممکن است هیچگونه بدافزاری روی سامانه شما نصب نشود . اما این اتفاق به معنای آن نیست که در پشت پرده هیچ اتفاقی رخ نداده است.

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
09:50 - 13/01/1398

برچسب:
Fireball - بدافزار - کنترل مرورگر کاربران - حریم خصوصی - محافظت از اطلاعات شخصی

نشانی
□□□□:https://www.shabakeh-mag.com/security/14191/%D8%B3%D8%B1%D9%82%D8%AA-%D9%86%D8%B4%D8%B3%D8%AA%E2%80%8C%D9%87%D8%A7-%D9%88-%DA%A9%D9%86%D8%AA%D8%B1%D9%84-%D9%85%D8%B1%D9%88%D8%B1%DA%AF%D8%B1-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86-%D8%AF%D8%B1-%D9%82%D8%A7%D9%84%D8%A8-%DB%8C%DA%A9-%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D9%87-%D9%85%D8%B9%D8%AA%D8%A8%D8%B1