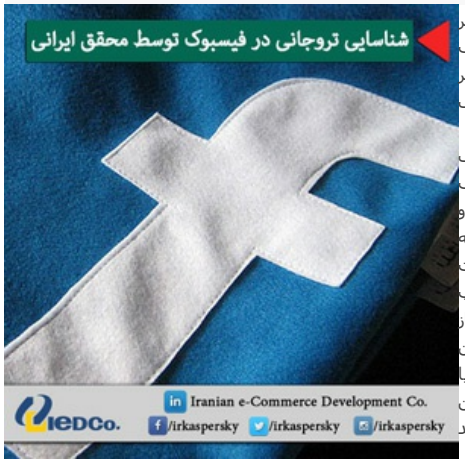
نویسنده : احمد گنجی | تعداد بازدید : 28 | تاریخ : ۱۳۹۳/۱۱/۱۲

شناسایی تروجانی در فیس بوک توسط محقق ایرانی

اخیراً محمدرضا فغانی، محقق امنیتی ایرانی، مطلبی مبنی بر شناسایی بدافزاری را منتشر نمود که با روشی جدید ضمن فعالیت از طریق محبوبترین شبکه اجتماعی یعنی فیسبوک سیستم بیش از 110 هزار کاربر از این شبکه را آلوده نموده است. در ادامه گزارش منتشر شده در بلاگ امنیتی کسپرسکی این خصوص اندیشیده است را بررسی می‌نماییم.



اخیراً محمدرضا فغانی، محقق امنیتی ایرانی، مطلبی مبنی بر شناسایی بدافزاری را منتشر نمود که با روشی جدید ضمن فعالیت از طریق محبوبترین شبکه اجتماعی یعنی فیسبوک سیستم بیش از 110 هزار کاربر از این شبکه را آلوده نموده است. در ادامه گزارش منتشر شده در بلاگ امنیتی کسپرسکی در مورد نحوه عملکرد و انتشار این بدافزار و همچنین تدابیری که فیس بوک در این خصوص اندیشیده است را بررسی می‌نماییم.

بنا بر گزارش کسپرسکی، روش کار این تروجان بدین صورت است که از طریق سیستم های قربانی و حسابهای کاربری کاربرانی که پیشتر مورد حمله قرار گرفته اند، اقدام به اشتراک گذاری کلیپ های ویدئویی که معمولاً هم حاوی عناوین و مضامین مستهجن است مینمایند و حدود 20 نفر از دوستان آن پروفایل را در همان پست تگ مینماید. این امر باعث میشود که کاربرانی که تگ شدند و سایر افراد که میتوانند آن پست را مشاهده کنند از انتشار آن پست بویژه متعجب شده و ترغیب به نمایش این کلیپ شوند. این آغاز کار این بدافزار است. کلیپ منتشر شده برای چند ثانیه به نمایش در می‌آید و پس از آن کاربر با پیغامی مبنی بر نیاز سیستم به بروزرسانی فلش پلیر (افزونه ی Flash Player) روبرو میشود. لینک دانلود آخرین نسخه از فلش پلیر جعلی بوده و فایل نصب مربوطه حاوی بدافزاری است که تروجان ها یا بدافزارهای دیگر را دانلود و روی سیستم آلوده اجرا مینماید (Trojan downloader) و این بدافزار اصلی که بعداً بصورت برنامه ریزی شده روی سیستم نصب میگردد هر بدافزاری میتواند باشد. بدین ترتیب از طریق کاربران دیگر نیز منتشر میشود.

خبر ابتدایی مربوط به شناسایی این بدافزار ابتدا از سوی یک محقق امنیتی ایرانی به نام محمدرضا فغانی منتشر گردید که طی آن فغانی همچنین گفته بود که این بدافزار همچنین قدرت کنترل و ثبت فعالیتهای کاربر نظیر ثبت کلیدهای صفحه کلید یا حرکات ماوس وی را دارد. یکی از نشانه‌های ابتدایی مبنی بر فعالیت این بدافزار مشاهده نام مرورگر گوگل کروم در بین برنامه‌های در حال پردازش (Processes) در پنجره Task Manager از ویندوز میباشد.

برخلاف این بدافزار، بدافزارهای فیسبوکی قبلی معمولاً از طریق ارسال پیغام شخصی به لیست دوستان کاربر هک شده اقدام به تکثیر و انتشار می‌نمودند و این بدافزار جدید از روشی استفاده میکند که محقق فغانی آن را روش مغناطیس (Magnet) می‌نامد. با این روش انتشار نه تنها کاربران تگ شده بلکه بسیاری دیگر از دوستان کاربر اصلی و کاربران تگ شده نیز ممکن است این پست را مشاهده نموده و سیستم آنها به این بدافزار آلوده شود که در نتیجه این امر منجر به تکثیر فوق العاده سریعتر این بدافزار میگردد.

فغانی همچنین اشاره کرده بود این موضوع همچنان در دست بررسی از سوی کارشناسان شبکه فیس بوک است. بلاگ امنیتی کسپرسکی‌نیز ضمن تماس مجدد با کارشناسان امنیتی فیسبوک خاطرنشان کرد این کارشناسان از وجود این بدافزار مطلع بوده و در حال انجام اقدامات بعدی بمنظور مسدودیت فعالیت غیر مستقیم این بدافزار از جانب کاربر میباشند.

کارشناسان فیس بوک در پاسخ خود به شرکت کسپرسکی اظهار داشتند که فیس بوک به سیستم های خودکاری بمنظور بررسی و کنترل فعالیت های مشکوکی که مستقیماً یا غیر مستقیم از جانب کاربران صورت میگیرد میباشد. این کارشناسان همچنین نتیجه بررسی های خود را تاکنون اینگونه گزارش دادند که این بدافزارهای فیس بوکی غالباً از طریق افزونه های مرورگرها و یا لینکهایی در شبکه های اجتماعی نظیر این مورد آخر منتشر میگردند و اطمینان دادند که تیم امنیتی فیسبوک همواره سعی دارد تا در اولین فرصت ممکن اقدام به مسدودیت لینک به صفحات جعلی، فیشینگ و در کل صفحات کلاهبرداری (scams) یا مخرب نمایند تا محیط این شبکه اجتماعی محبوب را همواره برای کاربرانش ایمن نگاه دارد.

منبع: کسپرسکی آنلاین

*کسپرسکی اسم یکی از بزرگترین شرکتهای امنیتی و سازنده آنتی ویروس است که برخی از کاربران اشتباهاً این شرکت و محصولات آنتی ویروس آن را با عناوینی نظیر کسپرسکای،کاسپرسکی، کسپراسکی، کسپراسکای، و یا کاسپراسکای نیز میشناسد. همچنین لازم به ذکر است مدیرعامل این شرکت نیز یوجین کسپرسکي نام دارد.

اشتراک گذاری مطلب

0 دیدگاه در مورد شناسایی تروجانی در فیس بوک توسط محقق ایرانی بیان شده است

دیدگاه خود را بیان نمایید

نام *

ایمیل (منتشر نمی شود) *

پر بازدید ترین پستها

- آنالیز بدافزار (Online SandBox)
- تجربه خوش آنلاین
- این admin,admin های مرگبار
- چند نکته برای مذاکره
- ابزار Riprep - آماده کردن سیستم ها برای نصب از راه دور
- مهم ترین قابلیت های ورژن 10 کسپرسکی - KES و KSC
- سازگاری Kaspersky Endpoint Security 10 با Windows Server 2012 R2 و Windows 8.1
- چگونگی ناتوان سازی فایل autorun.inf در فلش ها با استفاده از KES 10
- اولین گام در امنیت اطلاعات
- تکنولوژی امنیتی PKI

یادداشت *

ارسال دیدگاه

شرکت گسترش خدمات
تجارت الکترونیک ایرانیان
Iranian e-Commerce Development Co.

هم اکنون شرکت تجارت الکترونیک ایرانیان افتخار دارد در زمینه ارائه راهکارهای امنیت اطلاعات و ارتباطات بیش از 750 سازمان و شرکت دولتی و خصوصی را در کنار خود داشته باشد. مهمترین هدف شرکت در کلیه فعالیت های خود، استفاده از آخرین دستاوردهای علمی و ایجاد رضایتمندی مشتریان است...

ادامه ...

آخرین مطالب

- شناسایی باگ امنیتی در مودم روترهای D-Link ...
- شناسایی باگ امنیتی در مودم روترهای D-Link ...
- معرفی ابزار رایگان ضدتروجان رکتور (RectorDecr..
- CTB-Locker خطرناکتر از قبل

عضویت در خبرنامه

Enter your e-mail ...