FBI چگونه یکی از بزرگترین مجرمان دارک وب را شکار کرد؟ - دیجیاتو

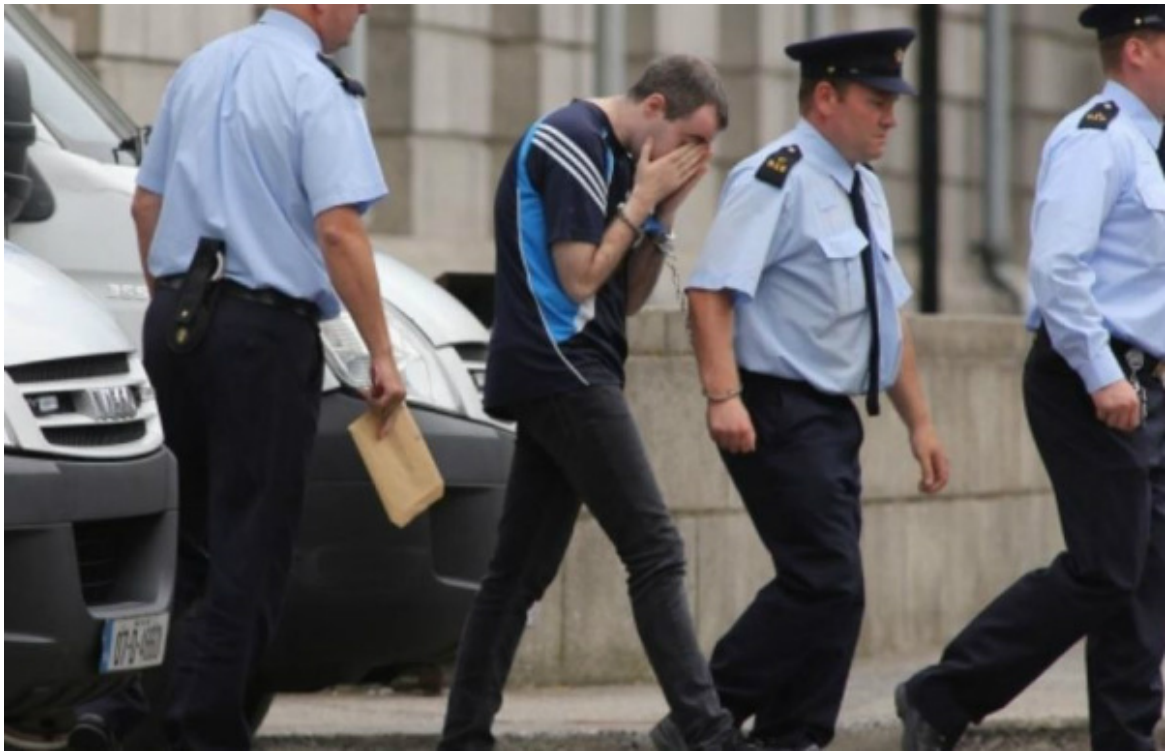
یونس مرادی | شنبه، ۱۹ بهمن ۱۳۹۸

پلیس فدرال آمریکا با در هکم شکستن لایه های امنیتی سرویس TOR موفق به دستگیری یکی از معروفترین خلافکاران دارک وب شد اما آنچه فعالان و حقوقدان ها را نگران کرده این است که سازمان های امنیتی نه تنها حاضر به افشای آسیب پذیری ها نیستند بلکه از آن به عنوان یک سلاح استفاده می کنند؛ سیاستی که امنیت کاربران عادی، روزنامه نگاران و دیگر فعلان را به خطر می اندازد.

«اریک مارکوس» یکی از معروف ترین تبهکاران دنیای دارک وب بود که با راه اندازی Freedom Hosting محفلی برای فروش مواد مخدر، پولشویی، رد و بدل کردن اطلاعات هک و میزبانی از تصاویر سوءاستفاده از کودکان ایجاد کرده بود.

این بازار سیاه اینترنتی از دسترس موتورهای جستجو خارج بوده و وبگردی در آن مستلزم استفاده از مرورگری به نام تور (Tor) بود که به لطف مسیریابی پیازی هویت، مکان و آدرس پروتکل کاربر را پنهان می سازد. این مرورگر به منظور مخفی سازی هویت کاربر داده ها را رمزنگاری کرده و بین رله های مختلف شبکه جابجا می کند.

مارکوس به خیال خود پشت سد ایمن سرویس TOR پنهان شده بود و دست کسی به او نمی رسید. در سال ۲۰۱۳ اما سازمان های امنیتی با نفوذ به مرورگر TOR رد Freedom Hosting را در فرانسه زده و خود مارکوس را هم در ایرلند به دام انداختند تا در نهایت به ۳۰ سال حبس محکوم شود.



اریک مارکوس

وی آخرین کسی نبود که توسط سازمان های امنیتی از پشت لایه های پنهان TOR بیرون کشیده شد و همین مساله ثابت می کند که آژانس های دولتی توانایی رهگیری کاربران در شبکه های به ظاهر نفوذ ناپذیر را دارند. خود مارکوس بر این باور است که هکرهای تراز اول NSA او را به دام انداخته اند اما FBI هم از ۲۰۰۲ سرگرم یافتن راه هایی برای نفوذ به سیستم افراد مظنون است.

به باور کارشناسان این سازمان ها جزییات کلیدی تحقیقاتشان را پنهان کرده و حتی در اختیار قضات هم نمی گذارند چه رسد به متهمان و وکلای آنها. Mark Rumold، از وکلای بنیاد مرزهای الکترونیک در این باره می گوید:

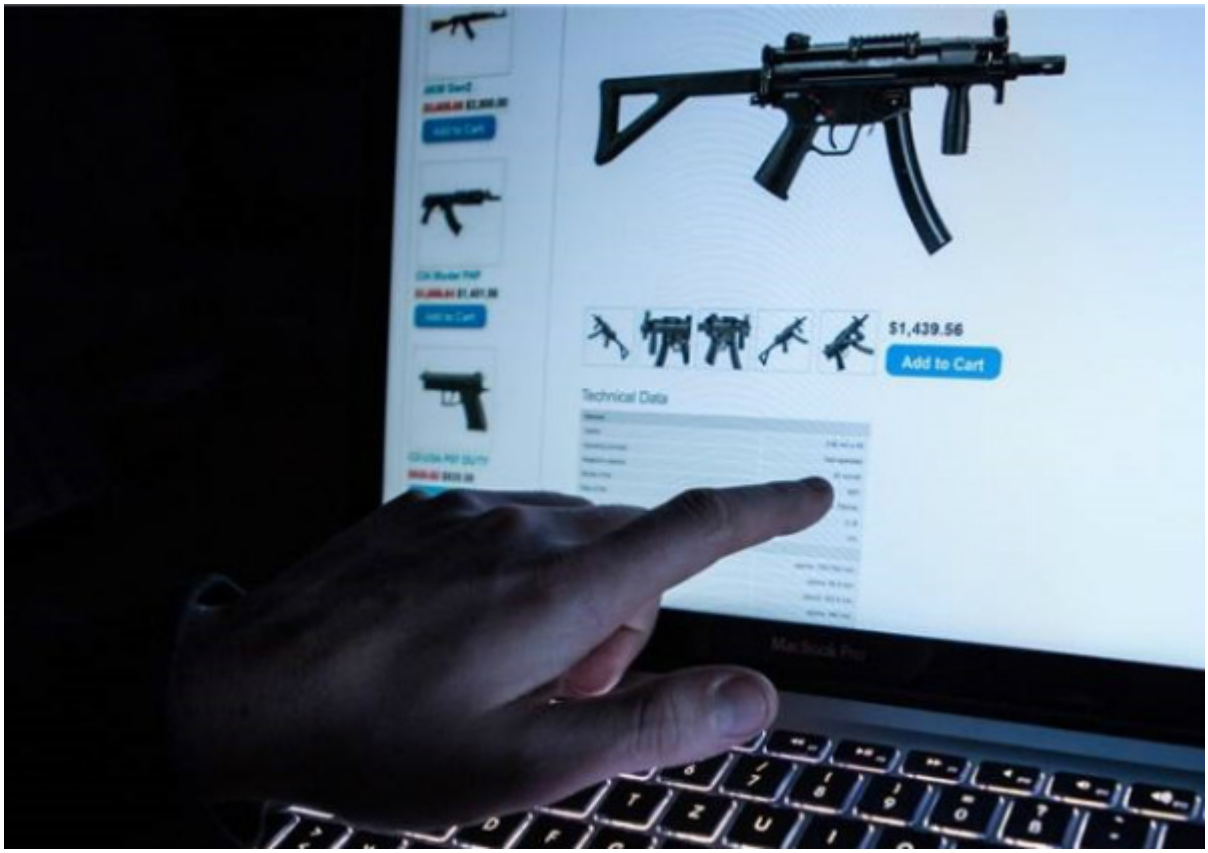
سوال همه این است که چه زمان اطلاعاتی در مورد نحوه رهگیری متهمان جرایم الکترونیکی در اختیار آنها قرار می گیرد. پنهان کردن روش های تحقیقاتی از عامه مردم و متهمان به سیستم قضایی ما ضربه می زند.

از نظر Rumold ریشه این مخفی کاری به استفاده از روش های غیرقانونی یا راهکارهایی برمی گردد که سوال های را در مورد نیات واقعی FBI در ذهن مردم ایجاد می کند.

استفاده سازمان های دولتی از بدافزار و اکسپلویت

Freedom Hosting یک سازمان رایانش ابری غیرقانونی بود که در ۲۰۱۳ حدود نیمی از کل محتوای دارک وب را به دوش می کشید. جرایم این شرکت از پشتیبانی فوروم HackBB تا موسسه پولشویی Onion Bank و سرویس ایمیل غیرقانونی Tor Mail را شامل می شد اما آنچه بیش از

همه خشم مقامات را برانگیخته بود، میزبانی حجم عظیمی از تصاویر سوءاستفاده از کودکان بود.



اوایل آگوست سال ۲۰۱۳ برخی از کاربران متوجه اجرای کدهای جاوا اسکریپت مشکوکی در سایت های متکی بر Freedom Hosting شدند. چند ساعت بعد تمامی این سایت ها به شکل همزمان از دسترس خارج شدند. در پشت پرده این حمله سایبری FBI از کدی استفاده کرده بود که از طریق یک آسیب پذیری در فایرفاکس، کاربران Tor را شناسایی می کرد.

پلیس فدرال پس از در اختیار گرفتن کنترل Freedom Hosting از بدافزاری استفاده کرده بود که احتمالا هزاران کامپیوتر را آلوده کرده است. پس از این ماجرا «اتحادیه آزادی های مدنی آمریکا» FBI را به خاطر استفاده از کد مذکور مثل یک نارنجک و پرتاب آن به هر سو به باد انتقاد گرفت.

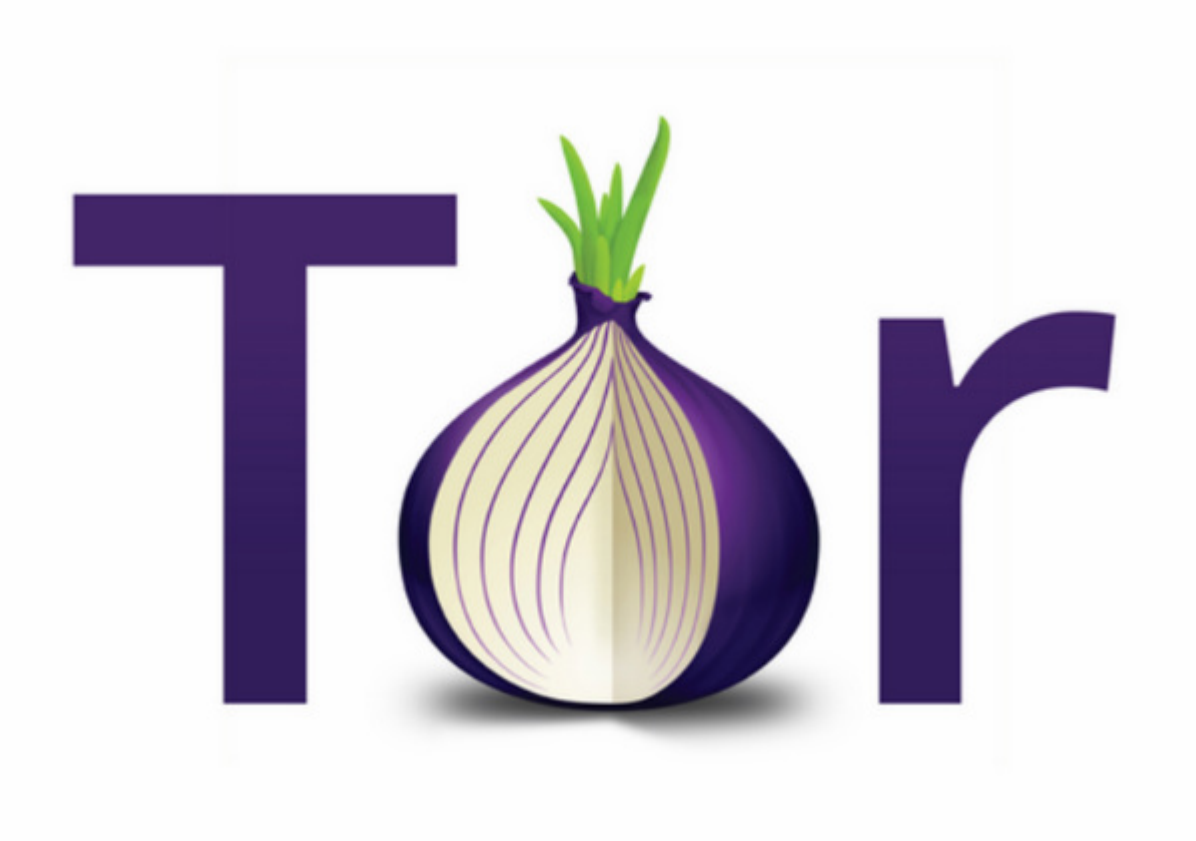
واضح است که FBI توانایی در هم شکستن معیارهای حفاظتی TOR را دارد اما در کیفرخواست ارائه شده تنها به ذکر «تحقیقاتی در ۲۰۱۳» که منجر به یافتن یک IP کلیدی مرتبط به Freedom Hosting شد، بسنده کردند. وکلای مارکوس مدعی شده اند که تنها داده های مبهم در اختیار آنهاست و به آنها گفته شده بخشی از پنهانکاری به خاطر این است که تکنیک های تحقیقاتی تا امروز طبقه بندی شده بوده اند.

خبری از افشای کامل نیست

سازمان های امنیتی آمریکا معمولا در جریان فعالیت های سایبری به وجود آسیب پذیری در نرم افزارها پی می برند. هرچند گاهی اوقات این مشکلات را به گوش شرکت های توسعه دهنده می

رسانند اما در برخی موارد آنها را پنهان کرده و بعدا به عنوان سلاح علیه افراد مظنون به کار می گیرند.

این در حالی است که بر اساس فرایند موسوم به VEP هر سازمان امنیتی که در پی پنهان کردن آسیب پذیری است باید مجوزهای لازم را کسب کند چون امکان سوءاستفاده از آن علیه افراد بی گناه وجود دارد. در چنین شرایطی اگر FBI بدون توجه به امنیت عمومی، ابزارهای هک TOR را برای نفوذ به Freedom Hosting کنار گذاشته، چه تضمینی وجود دارد که علیه افراد بی گناه نظیر کاربران عادی یا روزنامه نگارانی که به دنبال پنهان کردن هویتشان به TOR روی آورده اند از آن استفاده نکند؟



این مشکل تنها به سازمان های امنیتی ختم نمی شود و دولت آمریکا در ۲۰۱۷ نشان داد که محرمانه ماندن ابزارهای هک از همه چیز برایش مهمتر است. در آن سال وزارت دادگستری برای لو ندادن نحوه هک TOR اتهام سوءاستفاده جنسی از کودکان توسط یک مظنون را ملغی کرد.

به گفته Rumold نباید به دولت اجازه داشتن یک جعبه سیاه فناوری داده شود که با توسل به آن پرونده های کیفری به این مهمی را راه بیندازد. متهمان باید امکان مشاهده و بازبینی روش های مورد استفاده در پرونده های کیفری را داشته باشند.

علیرغم این ادعاها سازمان های امنیتی کماکان به استفاده از روش های پنهانی برای هک و نفوذ به سیستم های مظنونان استفاده می کنند. این موارد تنها شامل جرایم گسترده نظیر Freedom Hosting و Silk Road نیست و اخیرا گزارش هایی منتشر شده که نشان می دهد پلیس نیویورک

از مدت ها قبل فناوری یک کمپانی اسراییلی را برای باز کردن قفل آیفون متهمان خریداری کرده است.

دیجیاتو