

هر گردی گردو نیست: بازار داغ فیلترشکن های خطرناک در ایران - دیجیاتو

آرش پارساپور | یکشنبه، ۱۷ دی ۱۳۹۶

کاربران اینترنت در ایران با موضوع فیلترشکن آشنایی دیرینه دارند چرا که برای دسترسی به بسیاری از سایت‌های علمی و معتبر دنیا احتیاج به چنین ابزارهایی است. امروز حتی برخی معاملات بانکی و تجاری در خارج از بستر فیلترشکن‌ها شدنی نیست ولی اکنون این موضوع حالتی فراگیرتر پیدا کرده به طوری که بسیاری از جامعه‌شناسان معتقدند ضررهای استفاده از این ابزارها می‌تواند برای نوجوانان بیشتر از صرفا استفاده از برنامه‌هایی چون تلگرام باشد. اما خارج از این موضوع و از دید فنی چگونه؟ آیا می‌توان به این فیلترشکن‌ها اعتماد کرد؟

فیلترشکن حالا به زندگی بیشتر مردم رخنه کرده و می‌تواند عواقب بدی را به همراه داشته باشد

این روزها در بیشتر مکان‌های عمومی مثل تاکسی، مترو، اتوبوس و حتی داخل فروشگاه‌ها مردمی را از سنین مختلف می‌بینیم که با یکدیگر درباره اینکه کدام فیلترشکن کار می‌کند صحبت می‌کنند و مشغول تبادل برنامه‌های این چنینی با یکدیگر هستند.

جوانی که به نظر می‌رسد واردتر از دیگر افراد حاضر در واگن مترو است، تک تک موبایل مردم را می‌گیرد و فیلترشکن‌هایی که به قول خودش همه‌جوره کار می‌کند را برای آنها می‌ریزد، وقتی از روی کنجکاوی از او می‌خواهم برای من هم این کار را بکند تازه متوجه می‌شوم که قصد ریختن تلگرامی بدون فیلتر را روی موبایلم دارد، برنامه‌ای که به گفته کارشناسان وجود خارجی ندارد و صد در صد یک بد افزار به شمار می‌رود.



مرکز ماهر درباره بدافزارهایی که در قالب فیلترشکن بین مردم می‌چرخند هشدار داده است

سودجویان فعال در فضای مجازی همواره با بهره‌گیری از فرصت، در تلاش هستند تا ویروس‌ها و بدافزارها را از طریق نرم‌افزارهای فیلترشکن وارد سیستم کاربران کنند تا بتوانند به اطلاعات شخصی آنها دست پیدا کنند، اطلاعاتی که در موارد گوناگونی برای آنها به کار می‌آید و کاربران ناوارد ناخواسته آنها را تقدیم سودجویان می‌کنند. حالا با اوضاع فیلترینگ در کشور به نظر می‌رسد تعداد این بدافزارهای در ظاهر نرم افزار، بیشتر و بیشتر شده و دست به دست بین کاربران می‌چرخد.

مرکز ماهر (مدیریت امداد و هماهنگی رخدادهای رایانه‌ای) نیز ضمن تایید این موضوع هشدارهایی را به تمام کاربران ایرانی داده است:

«تحلیل‌های فنی روی کد این بدافزارها نشان می‌دهند که آغاز حمله آنها با دریافت یک پیامک فریبنده که مدعی ارایه فیلترشکن از طریق یک آدرس وب است، آغاز می‌شود. با کلیک کردن کاربر روی لینک مذکور، بدافزار روی تلفن قربانی دانلود می‌شود. از کاربر در زمان نصب، مجوز دسترسی به مواردی از جمله فهرست مخاطبان و خدمات پیامک اخذ می‌شود. در ادامه بدافزار لینک انتشار خود را برای تمام افراد موجود در فهرست مخاطبان از طریق پیامک ارسال می‌کند. پس از آن فهرست مخاطبان حذف می‌شود.»

نسخه نصبی تلگرام بدون فیلتر وجود خارجی ندارد!

«مهدی واعظی»، کارشناس امنیت اطلاعات در گفتگو با [دیجیاتو](#) به شایع شدن استفاده از این نرم افزارها اشاره می‌کند که منجر شده تا هرکاربر ناواردی هم درگیر آنها شود: «بسیاری از افراد کم سن و سال و یا پدر مادرها و حتی کاربران جوان ولی نابلد به استفاده از این فیلترشکن‌ها رو آورده‌اند که در قالب‌های مختلف من جمله فایل‌های نصبی APK در کنار جملات گول زننده‌ای همچون: **تلگرام بدون فیلتر** و... به دست آنها می‌رسد.»



محدودیت دسترسی به برخی شبکه‌های مجازی، استفاده از راهکارهای عبور از فیلترینگ توسط کاربران نهایی را ۷ برابر کرده است

این کارشناس امنیت اطلاعات باور دارد که هیچ کدام از ابزارهای فیلترشکن رایگان خدمات خود را بی‌دلیل برای کاربران عرضه نمی‌کنند و باید هوشمندانه‌تر با آنها برخورد کرد:

«هر فیلترشکن به محض اجرا روی سیستم، چندین پورت را برای اجرای دستورات باز می‌کند. هیچ شرکت امنیتی در هیچ کجای دنیا، امنیت استفاده از VPN و دیگر فیلترشکن‌ها را تأیید نکرده است. اکثر این نرم افزارهای VPN، دارای درب پشتی و آسیب پذیری‌های فراوانی هستند که می‌توانند توسط نفوذگران و حتی خود تولید کننده آن نرم افزار VPN هم مورد سوءاستفاده قرار بگیرند.»

فیلترشکن تنها مجوز اینترنت می‌خواهد و بس، دسترسی‌های بیشتر صرفاً برای سواستفاده خواهد بود

واعظی از مجوزهایی می‌گوید که این برنامه‌ها هنگام نصب از کاربر می‌گیرند و آنها را خیلی فراتر از عملکرد و نیازهای آن می‌داند. به گفته وی دسترسی‌ها تقریباً به تمام دستگاه موبایل کاربر، دسترسی کامل دارند و توانایی هر اقدام مخربی را در دستگاه‌های کاربر دارند:

«برخی از این برنامه‌ها به تمامی عکس‌های کاربر، لیست شماره‌های تماس، فایل‌های روی موبایل کاربر دسترسی دارند، آنها را سرقت کرده و حتی می‌توانند از طرف کاربر پیامی را به صورت عمومی (یا SMS یا از طریق پیام رسان‌ها) به مخاطبین فرد ارسال و آنها را ترغیب به دانلود فیلترشکن مذکور کنند.»



وی با اشاره به دو فیلترشکن بیشتر مورد استفاده قرار گرفته ایرانیان یعنی سایفون و لنترن، آنها را نیز نوعی بازی سیاسی برای شبکه‌های خارجی می‌نامد و خطراتشان را کمتر از دیگر برنامه‌ها نمی‌بیند:

«شاید این برنامه‌ها علی‌الظاهر دسترسی چندان خاصی به Storage موبایل نداشته باشند ولی در هر صورت در هنگام اتصال به آنها از بستر ارتباطی‌شان گذر می‌کنید و هر دیتایی که در حین اتصال در هر برنامه‌ای رد و بدل می‌شود توسط صاحبان آنها قابل ردیابی و شناسایی است، مگر در موارد خاص که نرم افزار از هر دو سو رمزنگاری شده باشد.»

فیلترینگ تلگرام باعث شده اطلاعات میلیون‌ها کاربر ایرانی در ناکجاآباد ذخیره شود

«میلاد نوری»، توسعه دهنده اپلیکیشن موبایل نیز اپلیکیشن‌های مطرح فیلترشکن را چندان ایمن نمی‌داند چرا که به نظر او در هر حال سرور این موارد دقیقاً مشخص نیست که کجاست و چه دیتاهایی را از کاربر ذخیره می‌کند:

«با فیلتر شدن تلگرام می‌توان این فرضیه را داشت که اطلاعات شخصی میلیون‌ها کاربر ایرانی اکنون در دست صاحبان این برنامه‌های فیلترشکن است و یا حتی در فرضیه‌هایی بدتر می‌توان متصور شد که اطلاعاتی همچون لوکیشن افراد دست دیگران است و آنها با توجه به دسترسی‌های دیگری چون دفترچه تلفن می‌توانند از سمت شما به مخاطبانتان پیام‌هایی تهییج آمیز بفرستند.»



به گفته میلاد نوری دسترسی‌هایی که برخی از فیلترشکن‌ها می‌خواهند فراتر از واقعیتی است که برای کارکرد خود نیاز دارند.

نوری معتقد است که VPN در همه جا برای امنیت بیشتر به کار می‌رود ولی در ایران بیشتر به جنبه دور زدن فیلترینگ به وسیله آن پرداخته شده و حالا با وجود اختلالات گسترده در شبکه VPN بسیاری از کاربران به دنبال یک جایگزین رایگان که فعال باشد می‌گردند که همین نکته باعث استفاده از برنامه‌هایی ناشناخته و ناایمن می‌شود: «دسترسی‌هایی که فیلترشکن برای کارکردن لازم دارد صرفاً مجوز اینترنت است و نه دیگر موارد، در اندروید 6 به بعد می‌توان تمام دسترسی‌های یک اپلیکیشن را با جزییات دید و آنها را غیرفعال کرد. در ضمن وارد شدن کاربران به هنگام اتصال به این فیلترشکن‌ها به سایت‌های مهم همچون پرداخت بانکی و ایمیل و... می‌تواند باعث لو رفتن اطلاعات آنها شود به همین دلیل استفاده از این قبیل برنامه‌ها توصیه نمی‌شود.»

داشتن آنتی ویروس‌ها شاید بتواند تا حدی در مقابله با این بدافزارها موثر واقع شود

این دو کارشناس به کاربران توصیه می‌کنند تا حد مقدور از این نرم افزارها استفاده نکنند و در صورت نیاز مبرم حتماً اطلاعات مهم خودشان را از موبایل پاک کرده و سپس با این فیلترشکن‌ها ارتباط برقرار کنند: «بکارگیری برنامه‌های ضد ویروس بر روی تلفن‌های همراه و تهیه پشتیبان از اطلاعات ارزشمند نیز به عنوان یک سیاست کلی در مقابله با بدافزارها توصیه می‌شود.»

بر اساس گفته‌های پلیس فتا در واقع 38 درصد از اپلیکیشن‌های فیلترشکن رایگان در فروشگاه گوگل‌پلی آلوده به بدافزار هستند و نمی‌توان به آنها اطمینان کامل داشت. این صحبت به این معناست که به فروشگاه‌های بزرگ و رسمی هم نمی‌توان چندان اعتماد کرد و باید قبل از استفاده از این فیلترشکن‌ها تمام جوانب را رعایت کرد. طبق گفته برخی از مسئولین فیلترینگ تلگرام به زودی برداشته خواهد شد و شاید لازم باشد تا آن زمان کمی صبر پیشه کرد.

[دیجیاتو](#)