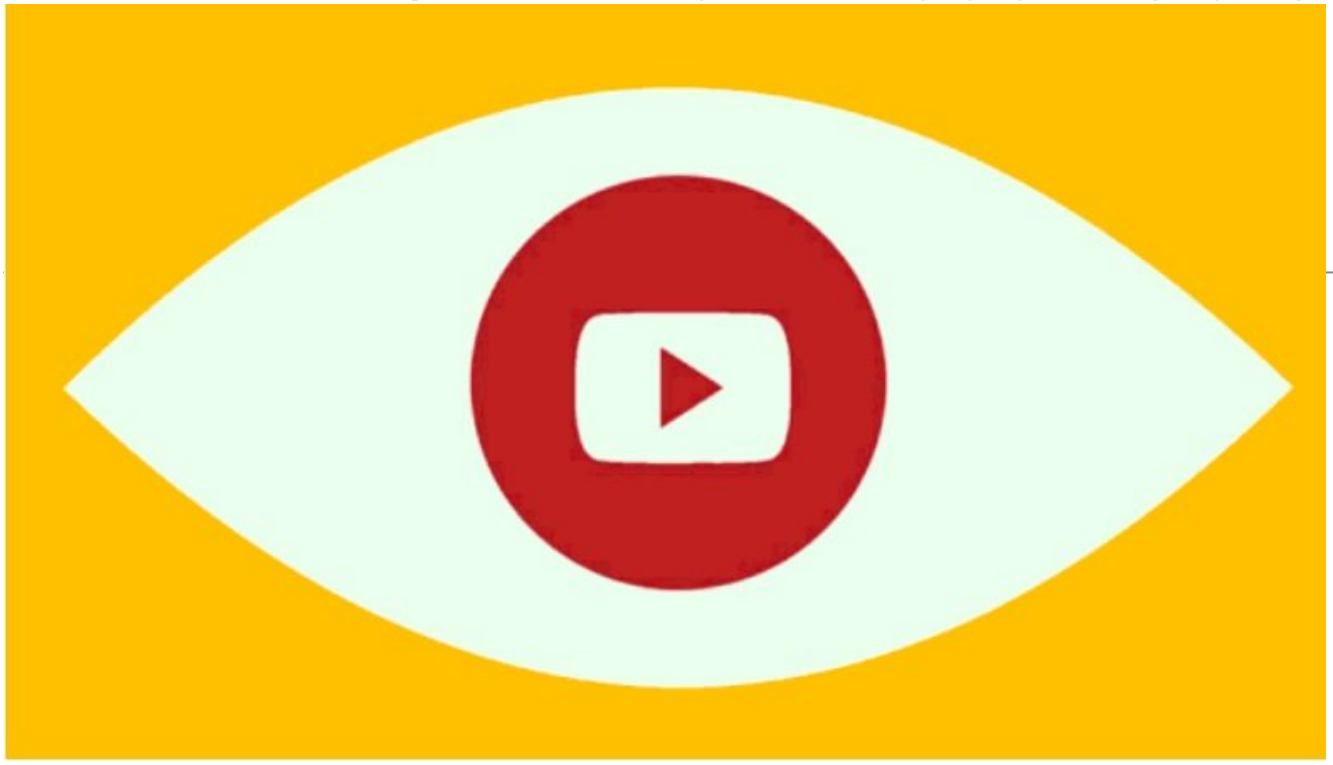
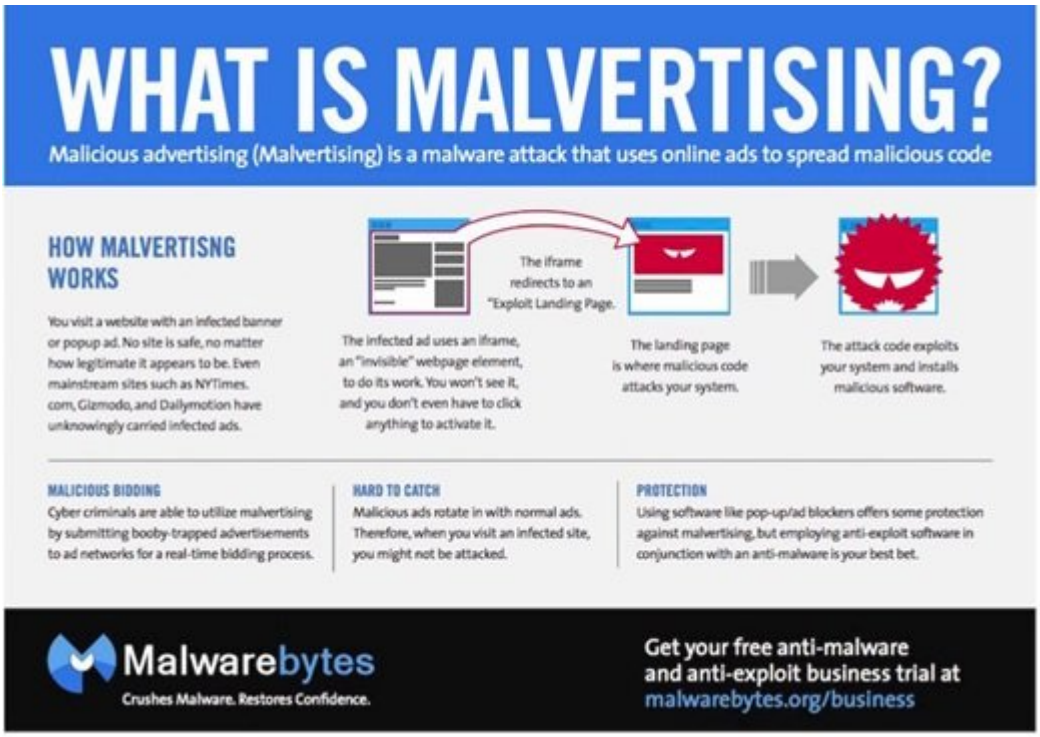
Malvertising و راه مقابله در برابر آن

چگونه از خودمان در برابر تبلیغات مخرب محافظت کنیم؟



در دنیای فناوری اطلاعات نبرد بی پایانی در برابر تهدیدات امنیتی در جریان است. اما به نظر می‌رسد یک دشمن جدید به سرعت در حال گسترش است. Malvertising تبلیغات مخرب اینترنتی هستند که یک بدافزار را دانلود کرده و آن‌را به درون کامپیوتر کاربر وارد می‌کنند. این فرآیند زمانی انجام می‌شود که کاربر در حال تماشای یک تبلیغ است. در این شیوه حمله حتی اگر کاربر از یک مسدود کننده تبلیغات استفاده کرده باشد، باز هم امکان ورود بدافزار به سیستم او وجود دارد. اما دو سؤال اصلی در زمینه تبلیغات وجود دارد. در حالی که تبلیغات در فرم اصلی خود مشکل‌ساز نیستند چرا این پدیده تبدیل به یک معضل شده و چگونه می‌توان در برابر این تهدید از خود محافظت به عمل آورد؟

Malvertising یک ترفند موزیانه بوده که به سادگی در مقیاس وسیع گسترش یافته و تبلیغاتی را روی یک صفحه وب نمایش می‌دهد. در این روش تبلیغات بدافزاری بدون اطلاع سایت میزبانی کننده تبلیغات و بدون اطلاع شبکه تبلیغی از شیوع بدافزار گسترش می‌یابند. این بدان معناست که ایمیلی به مالک وبلاگ با این مضموم ارسال می‌شود: «تبلیغات شما کامپیوتر من را با یک ویروس آلوده ساخته است.» به همین ترتیب ایمیل‌هایی از سوی مالکان سایت‌ها برای شرکت‌های آگهی‌دهنده ارسال شده و واکنش‌های مشابهی بوجود خواهد آمد. اما به دلیل این‌که فرآیند ارجاع تبلیغات چند مرحله‌ای است به درستی نمی‌توان منشأ دقیق آن‌را پیدا کرد.



اگر از کاربران قدیمی وب باشید، روزگاری که شبکه‌های تبلیغی فریبنده از بنرهای تبلیغاتی و پنجره‌های pop-up برای متقاعد ساختن شما به دانلود بدافزارها، نصب نوارابزارها یا تغییر homepage استفاده می‌کردند را به خاطر می‌آورید. در آن روزگار ما به مردم می‌گفتیم از سایت‌های فریبنده دوری کنید تا در امان باشید. اما اکنون آن روزگار سپری شده و Malvertising رفتاری متفاوت‌تر از گذشته از خود نشان می‌دهد. به‌طوری که به درون شبکه‌های تبلیغی سالم از طریق ضعف‌های امنیتی یا به درون فناوری‌های روز از طریق ضعف‌های امنیتی نفوذ می‌کند. نتیجه آن می‌شود که یک تبلیغ دیگر به شما نمی‌گوید چه چیزی را دانلود کنید، بلکه به‌طور خودکار بدافزارها را به سمت سیستم شما روانه می‌کند. جالب آن‌که به‌کارگیری یک مسدود کننده تبلیغات به صورت فعال یا در پس زمینه در بعضی موارد راه‌گشا نبوده و تبلیغ‌افزار مخرب باز هم به کار خود ادامه می‌دهد. حتی بدتر آن‌که تبلیغات مخرب ممکن است سیستم‌های خاصی را نشانه بروند. ماهیت شبکه‌های تبلیغی به گونه‌ای است که داده‌هایی را از مرورگر، سیستم‌عامل و حتی مکان فیزیکی کاربر دریافت می‌کنند. (همه این داده‌ها به منظور ارائه تبلیغات هدف‌مند بر اساس موقعیت جغرافیایی کاربر دریافت می‌شوند.) یک مهاجم نیز می‌تواند از داده‌های شبکه تبلیغی برای ارسال و ساخت بدافزارهای ویژه استفاده کند.

□□□□□□□□ □□□□: □□□ □□□□□□□□ □□□ □□□□□ □□□□□□□ □□□□□ **20** □□□□□□□□ □□□ □□□□□□□ □□□ □□ □ □□□□□ □□□□□□□ □□□□□ □□□ □□□□□□□

به‌طور مثال بدافزار تنها برای کاربرانی که از سیستم‌عامل اکس‌پی در امریکای شمالی استفاده می‌کنند ارسال شود. آلوده‌سازی آژانس‌های دولتی با هدایت تبلیغات آلوده برای کارمندان یک دولت که هنوز از سیستم‌عامل اکس‌پی استفاده می‌کنند نمونه‌ای از این موارد به شمار می‌رود. روش دیگر، در ارتباط با فلش است. به‌طوری که بدافزار تنها برای کاربرانی که فلش روی سیستم آن‌ها فعال است یا کاربرانی که از اینترنت اکسپلورر استفاده می‌کنند یا هر چیزی که شانس آلوده شدن را داشته باشد، ارسال شود. اما خبرهای خوبی نیز وجود دارد. شبکه‌های تبلیغی برای اعتبار خودشان هم که شده، فرآیندی را برای ثبت تبلیغات در نظر گرفته‌اند تا اگر یک مرتبه بدافزاری شناسایی شد، شانس حضور دوباره را نداشته باشد. به دلیل این‌که تجارت نمایش تبلیغات باید همواره بر پایه اعتمادسازی در جریان باشد، شرکت‌ها سعی می‌کنند تبلیغات مفیدی را به کاربران‌شان نشان دهند. آن‌ها اگر مورد مشکوکی شناسایی کنند به سرعت دست به کار می‌شوند. به عنوان کلام آخر این قسمت، بدافزارها همواره بر اساس آسیب‌پذیری‌هایی که شناسایی کرده‌اند، سعی می‌کنند به درون فناوری‌ها وارد شوند. فناوری‌هایی شبیه به ادوبی فلش، آکروبات و جاوا نمونه‌ای از این موارد به شمار می‌روند.

راه چاره چیست؟

غیرفعال کردن افزونه‌ها و به کارگیری یک مسدود کننده تبلیغات اولین گام مؤثر در این زمینه به شمار می‌رود. (اما نه به عنوان یک درمان کامل). آیا راه حل این است که فلش و جاوا را غیر فعال کنیم؟ شاید واقعا نیازی به حضور آن‌ها نداشته باشید. اگر فلش و جاوا غیر فعال شوند، مرور وب بدون آن‌ها بسیار دلنشین‌تر خواهد شد.

آیا جاوا ایمن است؟ آیا باید از آن استفاده کنم؟ به نظر می‌رسد هر چه رو به جلو پیش می‌رویم حفره‌های جدیدی در جاوا شناسایی می‌شوند. غیرفعال کردن افزونه‌های جاوا و فلش اولین گام مثبت در این زمینه به شمار می‌رود. به‌طوری که شما را در امنیت قرار خواهند داد. در کنار غیر فعال کردن جاوا و فلش بهتر است افزونه‌هایی که به آن‌ها نیازی ندارید را غیر فعال کنید. این بهترین توصیه‌ای است که در این زمینه می‌توانیم داشته باشیم. شما ممکن است با خود این‌گونه فکر کنید که آیا مشکل تنها فلش است؟ در جواب باید گفت آسیب‌پذیری بعدی ممکن است به سادگی غیر فعال نشود یا مشکل ممکن است از درون خود مرورگری که از آن استفاده می‌کنید آغاز شود. بسیاری از بدافزارهای تزریق شده درون شبکه‌های تبلیغاتی از طریق جاوا و فلش به سمت کامپیوتر کاربران نهایی ارسال می‌شوند. اما همه این بدافزارهای تبلیغی به این شیوه کار نمی‌کنند. در بیشتر حالات آن‌ها از اکسپلویت‌های روز صفر در سایت‌هایی که در حال اجرای تبلیغات هستند (به شما اعلام می‌کنند بدافزار را دانلود کنید) یا سایت‌هایی که در حال تماشای آن‌ها هستید، استفاده کنند (که با دور زدن پیغامی سعی می‌کنند سیستم شما را به‌طور مستقیم آلوده کنند.) به‌طور مثال، زمانی که سایت جیمی الیور هک شد، بازدیدکنندگان هیچ‌گونه هشدار یا پیغامی دریافت نکردند. آن‌ها ده‌ها بدافزار که در پشت صحنه در حال اجرا بودند را در قالب یک پیغام تشکرآمیز و در قالب جاوااسکریپت دریافت کردند. حال سؤال دیگری پیش می‌آید؟ آیا هرگز نباید تبلیغات را مشاهده کنیم تا در برابر Malvertising در امان باشیم؟ در جواب باید گفت مسدود کنندگان تبلیغاتی و ابزارهای مشابه تا حدودی در این زمینه کمک‌کننده هستند. اما دو مشکل عمده در ارتباط با این ابزارها وجود دارد:

1. مسدود کنندگان تبلیغات بعضی از تبلیغات را اولویت‌بندی کرده و آن‌ها را نمایش می‌دهند. در نتیجه آسیب‌پذیری‌ها ممکن است همچنان به قوت خود باقی باشند. به‌طور خلاصه زمانی‌که تصور می‌کنید با نصب AdBlock Plus از شر تبلیغات نفوذی خلاص شده‌اید، همانند آن است که تیری به پای خود شلیک کرده باشید. در حقیقت شبکه‌های تبلیغی غالبا به عنوان یک منبع قابل اعتماد شناخته می‌شوند. همین موضوع باعث می‌شود آن‌ها به هدف بزرگی برای Malvertising تبدیل شوند. شبکه تبلیغی یاهو که اوایل سال جاری میلادی هک شد نمونه‌ای از این موارد به شمار می‌رود. این شبکه بعد از آن‌که هک شد اقدام به ارسال بدافزارهایی برای کاربران سایت Planet of Fish کرد. سایتی که روزانه سه میلیون کاربر از آن بازدید می‌کنند. گوگل نیز از شبکه تبلیغاتی خاص خود Double click

استفاده می‌کند. شبکه‌ای که در سال 2014 میلادی میلیون‌ها بدافزار را روانه کامپیوتر کاربران کرد. بدافزارهایی که هدفشان کاربران ویندوز ایکس پی بود. زمانی که مسدود کنندگان تبلیغات کسب در آمد از شبکه‌های تبلیغی را آغاز کنند، آن‌گاه ورود شبکه‌های آگهی به فهرست سفید این ابزارها امری اجتناب‌ناپذیر خواهد بود.

2. مسدودکنندگان تبلیغات توانایی خوبی در مدیریت تبلیغاتی که به کاربران نشان داده می‌شود دارند. اما Malvertising اکنون مسیر خود را به سمت تبلیغات ویدویی تغییر داده است. جذاب بودن تبلیغات ویدویی و شناسایی سخت‌تر بدافزارهای قرار گرفته درون کدهای آن‌ها، باعث شده است هکرها به این سمت از صنعت تبلیغات گرایش پیدا کنند.

در نهایت

راه‌حل این نیست که یک مسدود کننده تبلیغات را نصب کنید، بلکه باید یک مسدودکننده تبلیغات که می‌دانید چگونه باید از آن استفاده کنید را نصب کرده و به‌طرز درستی از آن استفاده کنید. این بدان معناست که باید اسکرپیت‌های غیرضروری را غیرفعال کرده و همچنین فهرست سفید مسدودکنندگان تبلیغات را بررسی کرده تا ببنید چه چیزی در فهرست سفید قرار دارد و چه چیزی در آن نیست. uBlock Origin و Diconnect دو مسدودکننده تبلیغاتی هستند که در اغلب موارد توانایی مسدود کردن بدافزارهای تبلیغی روی دستگاه‌های همراه و دسکتاپ دارند. با این وجود فراموش نکنید، آنتی‌ویروس‌های خوب و ضدبدافزارها در محافظت از شما ارزشمند هستند. ابزارهایی شبیه به MalwareBytes توانایی متوقف کردن بدافزارهایی که آنتی‌ویروس‌ها ممکن است آن‌ها را تشخیص نداده باشند را دارند. این ابزارها همچنین به شما کمک می‌کنند از خودتان در برابر آسیب‌پذیری‌های ناشناخته محافظت به عمل آورید. در واقع برخی از کارشناسان امنیتی از آن‌ها به عنوان اولین ابزار در برابر بدافزارهای تبلیغاتی یاد می‌کنند. ترکیب ضدبدافزار با ابزارهای مرورگرمحور باید محافظت خوبی را برای شما به ارمغان آورند. اگر تنها AdBlock Plus، را نصب کرده‌اید و این ابزار تنها سایت‌های پیش‌فرض را کنترل می‌کند، اکنون زمان آن رسیده است که خود شخصا وارد عمل شوید. سعی کنید زمانی را صرف مدیریت سیستم خود کنید. در غیر این صورت در معرض تهدید قرار خواهید گرفت. نه فقط بدافزارها یا اکسپلویت‌ها پیرامون وب شناور هستند، بلکه ضعف‌های امنیتی در ابزارهایی که به آن‌ها اعتماد دارید و از آن‌ها برای محافظت از خود استفاده می‌کنید نیز پیرامون شما قرار دارند.

تاریخ انتشار:
03 دی 1394

نشانی منبع: https://www.shabakeh-mag.com/security/2408