Malvertising

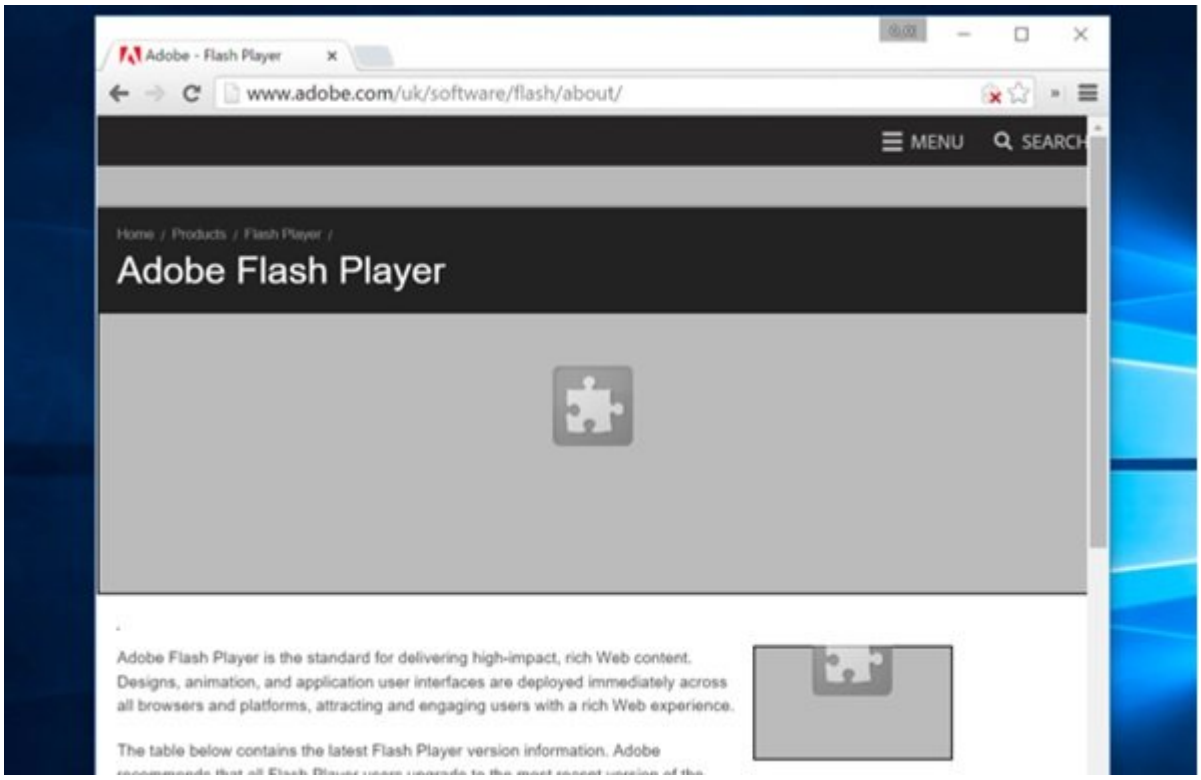
تبلیغ آلوده‌کننده چیست و چگونه از دست آن خلاص شویم؟

هکرها سعی می‌کنند مرورگر وب و افزونه‌هایی که مورد استفاده قرار می‌دهید را سرقت کنند. امروزه Malvertising یا به عبارت دقیق‌تر تبلیغات آنلاینی که با هدف گسترس بدافزارها مورد استفاده قرار گرفته و با استفاده از شبکه‌های تبلیغاتی قرار گرفته درون سایت‌های معتبر گسترش می‌یابند، بسیار محبوب شده‌اند. یاهو یکی از شناخته‌شده‌ترین قربانیان این مدل از حملات است. اما سؤال این است که چگونه می‌توانیم از دست این نوع بدافزارها خلاص شویم.

مشکل واقعی بدافزارهای تبلیغی در تبلیغاتی نبودن آن‌ها قرار دارد، در حقیقت یک آسیب‌پذیری نرم‌افزاری روی سیستم کاربر باعث می‌شود تنها با یک کلیک ساده به سایت مخرب وارد شود. حتی اگر همه آگهی‌های سایت‌ها یک شبه ناپدید شوند، باز هم مشکل اصلی به قوت خود باقی می‌ماند. هر چند کاربران با استفاده از ابزارهایی همچون AdBlock توانایی کم کردن خطرات مربوط به این‌گونه بدافزارها را دارند، اما توانایی دفع کامل حمله را ندارند. به‌طور مثال سایت جیم اولیور تاکنون سه بار توسط یک کیت مخرب مورد حمله قرار گرفت. سایتی که میلیون‌ها بازدید کننده دارد. سایت‌ها هر روزه هک می‌شوند، فرض کنید کاربران با این تصور که ابزارهای مسدود کننده تبلیغات از آن‌ها در برابر حملات محافظت به عمل می‌آورند استفاده کنند، اما اگر این نرم‌افزارها تمهیدات امنیتی را به درستی پیاده‌سازی نکرده باشند، و از سیستمی آسیب‌پذیر استفاده کنند، آن‌گاه تنها با یک کلیک ساده سیستم‌شان آلوده می‌شود.

مرورگرهای وب و افزونه‌هایی که آماج حملات قرار گرفته‌اند

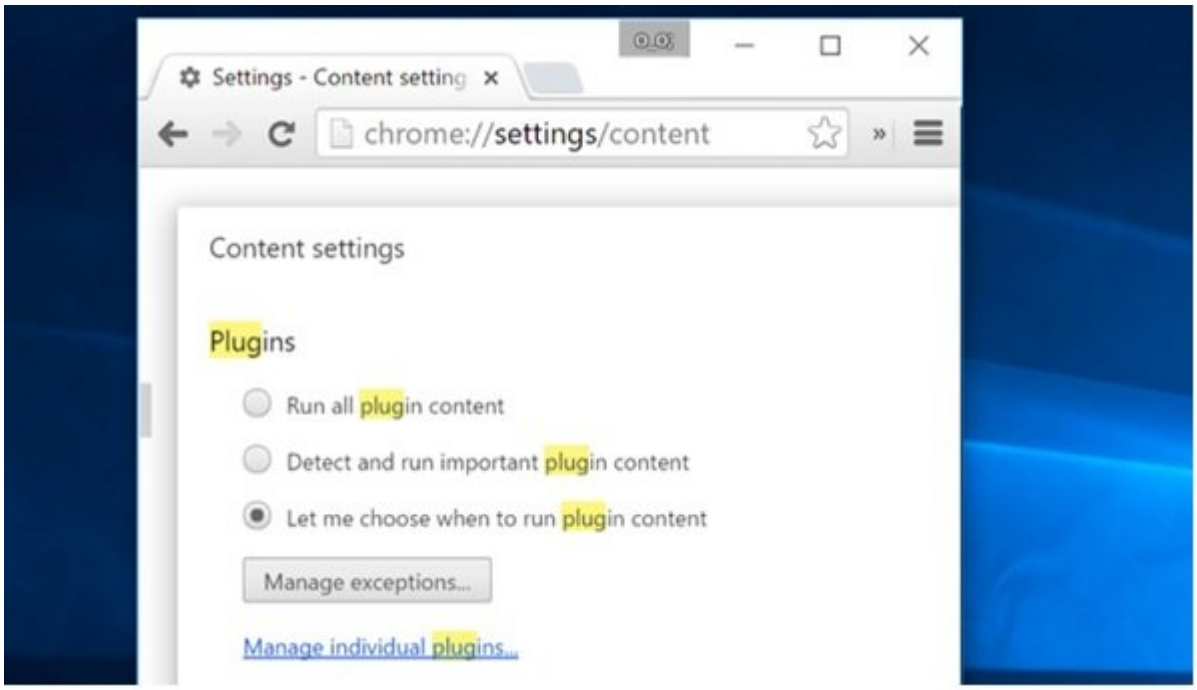
هکرها از دو راه اصلی برای تهدید یک سیستم کامپیوتری استفاده می‌کنند. در روش اول هکرها سعی می‌کنند با استفاده از روش‌های مهندسی اجتماعی کاربر را فریب داده تا کدهای مخرب را دانلود کرده و آن‌ها را اجرا کند. در روش دوم هکرها به‌طور مستقیم به مرورگر و نرم‌افزار جانبی وابسته شبیه به افزونه‌های فلش ادوبی، افزونه‌های جاوا اوراکل و Adobe Reader حمله می‌کنند. این حملات از رخنه‌های امنیتی موجود در نرم‌افزارها برای وادار ساختن کامپیوتر به دانلود و اجرای نرم‌افزارهای مخرب استفاده می‌کنند. اگر سیستم شما رخنه‌پذیر باشد، برای هکر فرقی نمی‌کند که از آسیب‌پذیری روز صفر با خبر باشد، یا شما وصله‌های امنیتی لازم را نصب نکرده باشید، اگر به مشاهده سایتی که دارای کدهای مخرب است بپردازید، هکر به راحتی توانایی آلوده‌سازی سیستم شما را دارد. این‌گونه آلوده‌سازی‌ها عمدتا بر مبنای مؤلفه‌های فلش یا اپلت جاوا پیاده‌سازی می‌شود. کلیک کردن روی لینکی در یک سایت مشکوک می‌تواند باعث آلودگی سیستم شما شود، حتی اگر در ظاهر این سایت برای اهداف مخرب طراحی نشده باشد، اما در باطن در گوشه و کنار سایت مؤلفه‌های مخرب در انتظار شما هستند.



Malvertising چیست؟

صرف‌نظر از تلاش برای فریب دادن کاربر برای بازدید از سایت‌های مخرب، بدافزارهای تبلیغی آنلاین از شبکه‌های تبلیغاتی برای انتشار محلقات مخرب فلش یا کدهای مخرب استفاده می‌کنند. هکرها اشیا مخرب فلش و دیگر کدهای مخرب را به درون شبکه‌های تبلیغاتی تزریق کرده و شبکه را وادار می‌کنند تا آن‌ها را شبیه به تبلیغات واقعی منتشر کند. فرض کنید به بازدید از سایت متعلق به یک روزنامه که یک اسکریپت تبلیغی را میزبانی کرده و اقدام به دانلود یک تبلیغ از یک شبکه تبلیغی می‌کند بپردازید. این دقیقا مکانی است که موج جدید حملات روی آن متمرکز شده‌اند. شبکه تبلیغی یاهو جدیدترین قربانی این مدل از حملات بوده است. هکرها با استفاده از آسیب‌پذیری موجود روی شبکه تبلیغی یاهو باعث شدند تا تبلیغات مخرب فلش روی شبکه منتشر شده و کاربران از همه جا بی خبر را آلوده سازد. ساختار و هسته بدافزارهای تبلیغی روی رخنه‌های نرم‌افزاری مستقر شده است. بدافزارهای تبلیغاتی با استفاده از رخنه‌های موجود سعی در آلوده‌سازی سایت‌های قانونی که کاربران به‌طور روزانه به بازدید از آن‌ها می‌پردازند، اقدام می‌کنند. تبلیغات مخرب به‌گونه‌ای طراحی می‌شوند که با ترفندهای زیرکانه‌ای شما را مجبور کنند، به بازدید از سایت‌های مخرب به پردازید. اما عدم وجود تبلیغات مخرب به معنای امنیت نیست. اگر روی لینک موجود در صفحه یک روزنامه کلیک کنید، باز هم احتمال آلودگی وجود دارد. رخنه‌های امنیتی ریشه در بسیاری از مشکلات دارند.

چگونه در برابر Malvertising از خود محافظت به عمل آوریم؟



حتی اگر مرورگر شما هیچ‌گاه تبلیغات را بارگذاری نکند، و راهی برای فریب دادن آن وجود نداشته باشد، باز هم انواع مختلفی از حملات آنلاین وجود دارند که شما را در معرض تهدید قرار می‌دهند. برای این منظور می‌توان از چند راهکار ساده استفاده کرد: این راه‌کارها عبارتند از:

گزینه click-to Play Plug-ins را فعال کنید

زمانی‌که صفحه وبی که در برگیرنده اشیا مربوط به جاوا یا فلش است را مورد بازدید قرار می‌دهید، تا وقتی که روی این اشیا کلیک نکنید، آن‌ها به‌طور خودکار توانایی اجرا شدن را ندارد. تقریبا همه تبلیغات مخرب از این افزونه‌ها استفاده می‌کنند، در نتیجه این گزینه از شما در برابر هر چیزی محافظت به عمل می‌آورد و اجازه نمی‌دهد محتوای مخرب به‌طور خودکار اجرا شود.

از کیت ضداکسپلویت MalwareBytes استفاده کنید

این ابزار با بهره‌مندی از رابط کاربری دوستانه و پیشنهاداتی که مبتنی بر راه‌حل‌های مایکروسافت است، راهکاری جامع و مناسب برای محافظت از سازمان‌ها به شمار می‌رود. گزینه دیگری که برای کاربردهای خانگی مورد استفاده قرار می‌گیرد، نرم‌افزار EMET مایکروسافت است. اما توصیه می‌کنیم، MalwareBytes را به عنوان یک برنامه ضد اکسپلویت مورد استفاده قرار دهید. البته لازم به توضیح است این برنامه را نباید به عنوان جایگزینی برای آنتی‌ویروس‌ها مورد استفاده قرار دهید. این ضد اکسپلویت، مرورگر شما را در ارتباط با فناوری‌هایی که ممکن است مورد اکسپلویت قرار گیرند، بررسی می‌کند. اگر MalwareBytes در خصوص چنین فناوری‌هایی به شما هشدار دهد، به‌طور خودکار آن‌ها را متوقف خواهد کرد. این ابزار رایگان بوده و می‌تواند همراه با نرم‌افزارهای ضدویروس مورد استفاده قرار گیرد و از مرورگر شما و افزونه‌های نصب شده در برابر حملات روز صفر محافظت به عمل آورد. نصب این ابزار برای هر کاربر سیستم‌عامل ویندوز ضروری و مهم است.

لینک دانلود MalwareBytes

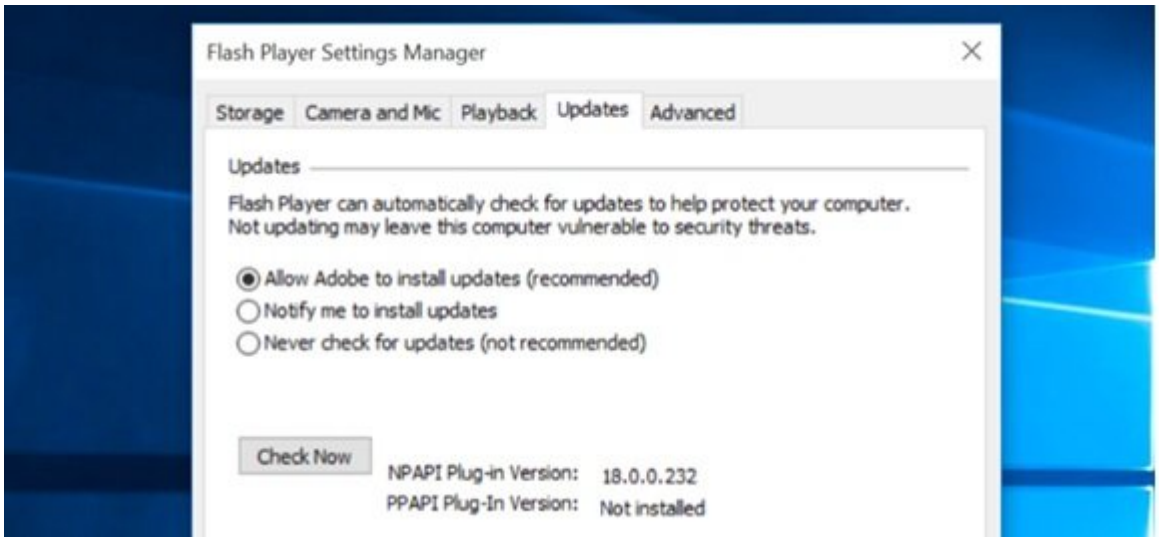
افزونه‌هایی که به ندرت از آن‌ها استفاده می‌کنید را پاک کرده یا غیرفعال کنید

اگر از افزونه‌ای استفاده نمی‌کنید، آن‌را غیر فعال کنید. این‌کار باعث می‌شود تا کمتر در معرض حمله قرار بگیرید. همچنین شانس کمتری را به هکرها می‌دهید که از آسیب‌پذیری‌های موجود در نرم‌افزارهای شما استفاده کنند. کاربران این روزها کمتر به افزونه‌ها نیاز دارند. به‌طور مثال سیلورلایت مدت‌ها است توسط Netflix مورد استفاده قرار نمی‌گیرد، در نتیجه حذف کردن آن پیامد خاصی را به‌همراه نخواهد داشت. البته راهکار جامع‌تری در این زمینه وجود دارد. همه افزونه‌های مرورگر خود را غیر فعال کرده و در ادامه مرورگر جدیدی نصب کرده و افزونه‌هایی که مورد استفاده سایت‌های خاصی هستند را روی مرورگر دوم نصب کنید. البته این‌کار کمی زمان‌بر است اما ارزش به کارگیری را دارد. اگر فلش ادوبی و جاوا به‌طور کامل از وب حذف شوند، آن‌گاه کار برای بدافزارهای تبلیغی بسیار مشکل می‌شود.

[illegible]: [illegible]

افزونه‌های خود را به‌روز نگه دارید

هر زمان افزونه‌های مورد نیاز خود را نصب کردید باید اطمینان حاصل کنید که آن‌ها همواره به‌روز بوده و جدیدترین وصله‌های امنیتی را دریافت کرده باشند. کروم به‌طور خودکار اقدام به به‌روزرسانی فلش ادوبی می‌کند، مایکروسافت ایج نیز به همین منوال عمل می‌کند. اینترنت اکسپلورر در سیستم‌عامل‌های خانواده ویندوز 8 و ویندوز 10 نیز به‌طور خودکار به‌روزرسانی می‌شوند. اما اگر از اینترنت اکسپلورر نسخه 7، فایرفاکس، اپرا یا سافاری استفاده می‌کنید، اطمینان حاصل کنید گزینه به‌روزرسانی خودکار روی این مرورگرها فعال باشد.در سیستم مک این گزینه در پنجره System Preferences قرار دارد.



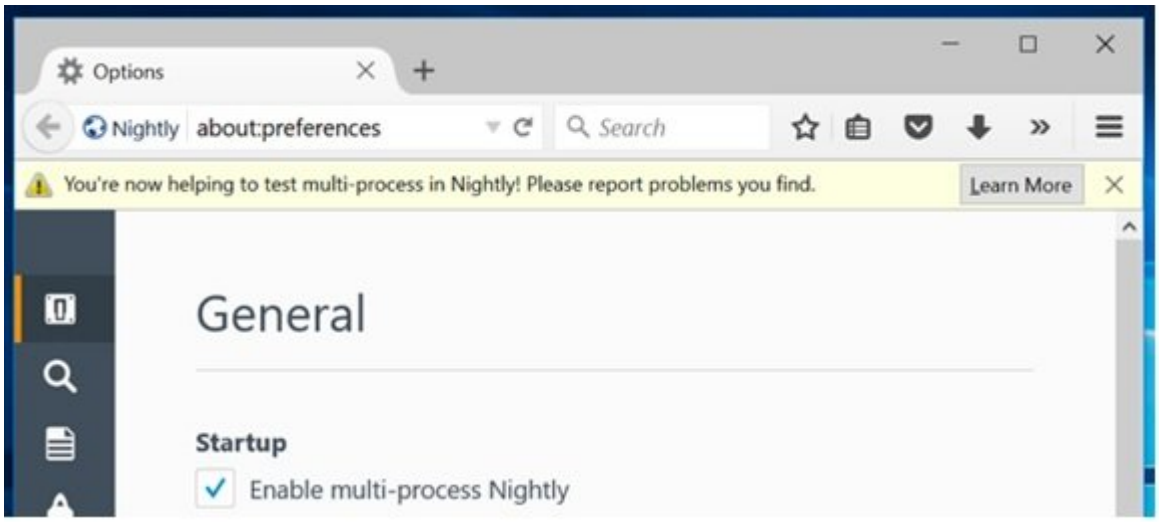
مرورگر خود را به‌روز نگه دارید

سعی کنید همواره مرورگر خود را به‌روز نگه دارید. مرورگرهای وب باید به‌طور خودکار توانایی دریافت به‌روزرسانی‌ها را داشته باشند. در نتیجه هیچ‌گاه گزینه به‌روزرسانی خودکار مرورگر خود را غیر فعال نکنید. اگر از اینترنت اکسپلورر استفاده می‌کنید، اطمینان حاصل کنید گزینه Windows Update فعال بوده و به‌روزرسانی‌ها در بازه زمانی مشخص دریافت می‌شوند. در حالی‌که بیشتر حملات بدافزارهای تبلیغی روی افزونه‌ها رخ می‌دهد، اما تعداد کمی از آن‌ها از حفره‌های موجود در خود مرورگرها استفاده می‌کنند.

سعی کنید از فایرفاکس کمتر استفاده کنید

حرف و حدیث‌های بسیاری در خصوص استفاده کردن یا کنار گذاشتن مرورگر فایرفاکس در میان است. هر چند این مرورگر از محبوب‌ترین مرورگرها نزد کاربران به شمار می‌رود، اما در خصوص به‌کارگیری یک اصل مهم هنوز هم در پشت سر بسیاری از مرورگرهای مطرح قرار دارد. در حالی‌که مرورگرهایی همچون کروم، اپرا، اینترنت اکسپلورر و مایکروسافت اچ همگی از فناوری سندباکس برای پیشگیری از اکسپلویت‌هایی که مرورگر را دور زده و سیستم کاربر را در معرض تهدید قرار می‌دهند استفاده می‌کنند، فایرفاکس هنوز به فناوری سندباکس مجهز نیست. بدافزارهای تبلیغاتی که هدفشان مرورگر فایرفاکس است با استفاده از یک حمله روز صفر می‌توانند به اهداف خود دست یابد. فناوری‌های سندباکس باعث می‌شوند از بروز چنین حملاتی روی فایرفاکس ممانعت به عمل آید. اگر از فایرفاکس استفاده می‌کنید، از کیت ضد بدافزاری MAlwareBytes برای محافظت از خود استفاده کنید.

اما فناوری سندباکس بعد از سال‌ها به عنوان بخشی از پروژه Electrolysis به فایرفاکس افزوده خواهد شد. این فناوری قرار است در قالب تکنیک چند فرآیندی به فایرفاکس افزوده شود. ویژگی چند فرآیندی به عنوان بخشی از نسخه پایدار فایرفاکس در پایان سال جاری میلادی عرضه خواهد شد. تا آن زمان که فایرفاکس موزیلا تبدیل به مرورگری ایمن شود، بهتر است از مرورگرهایی استفاده کنید که از فناوری سندباکس استفاده می‌کنند.



هر چند بسیاری از حملات بر پایه سیستم‌عامل ویندوز انجام می‌شوند، اما کاربران پلتفرم‌های دیگر نباید خود را در ساحل امنی تصور کنند که از این حملات به دور هستند. حملاتی که به تازگی فایرفاکس را نشانه رفته بودند، روی پلتفرم‌های لینوکس، مک و ویندوز پایه‌ریزی شده بودند. حملات این مدت به افسانه شکست ناپذیری مک پایان دادند.

منبع:
howtogeek
تاریخ انتشار:
28 شهریور 1394

نشانی منبع: https://www.shabakeh-mag.com/security/1569