قربانی جدید

هکرها به سیستم‌های تبلیغاتی یاهو نفوذ کردند

تبلیغات در بخش‌های مختلف سایت یاهو همچون ورزش، بازی‌ها، چهره‌ها و امور مالی به چشم می‌خورد. همین موضوع باعث شده است تا یک گروه از مجرمان اینترنتی از این ویژگی سوء استفاده کرده و اقدام به آلوده‌سازی کامپیوترهای کاربران کنند. شرکت امنیتی MalwareBytes بر همین اساس تحقیقی به عمل آورده است که نشان می‌دهد، مجرمان اینترنتی به شبکه تبلیغی یاهو نفوذ کرده‌اند.

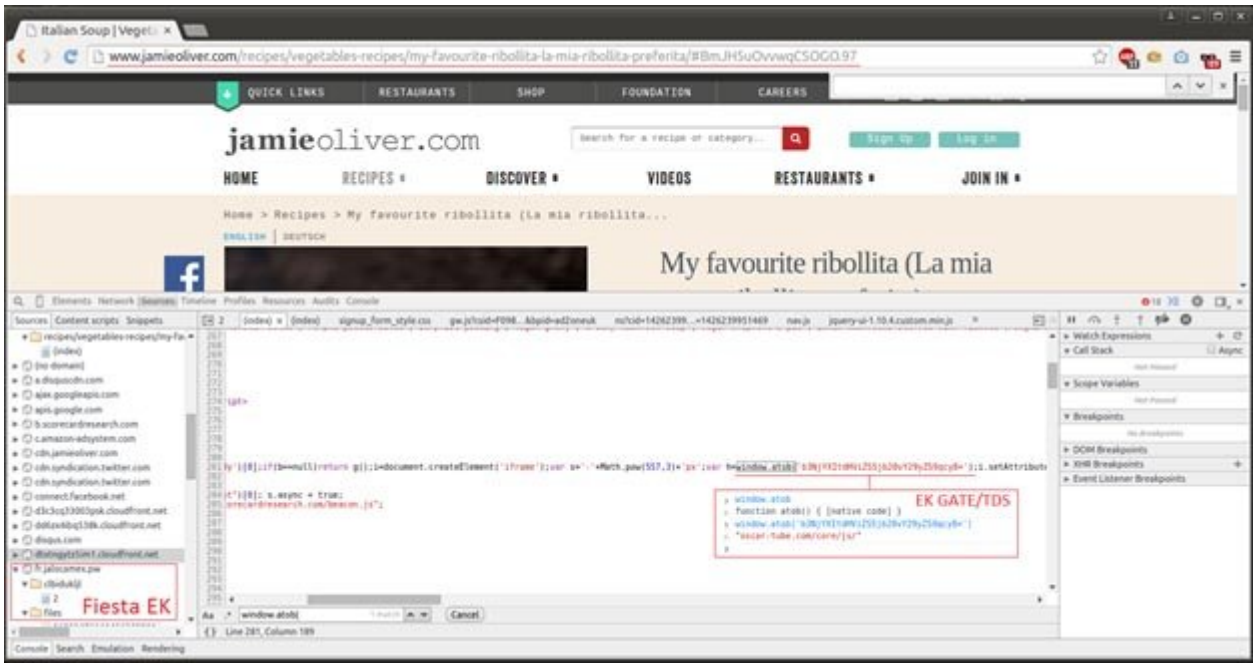
قربانیان یک گروه سازمان یافته

محققان شرکت امنیتی MalwareBytes می‌گویند یاهو قربانی همان گروهی شده است که تعداد زیادی کمپین را با هدف بهره‌برداری از آسیب‌پذیری‌ها در نرم‌افزار فلش ادوبی سازمان‌دهی کرده است. در ماه ژوئن کارشناسان اعلام کردند یک حفره امنیتی خطرناک را در فلش ادوبی شناسایی کرده‌اند. این آسیب‌پذیری از آن جهت به‌نام روز صفر نامیده شد که قبلا مورد شناسایی قرار نگرفته بود. هکرها با استفاده از این حفره اقدام به‌سرقت داده‌ها از ماشین‌های قربانیان کرده و در ادامه این داده‌ها را به شبکه‌های قانونی یک شرکت ارسال می‌کردند. وصله مربوط به این آسیب‌پذیری چند روز بعد همراه با Flash 18.0.0.194 و به‌نام CVE-2015-3113 منتشر شد. اما در آن زمان پیش‌بینی شد که این سبک از حملات راه را برای استفاده از کیت‌های بهره‌برداری هموار خواهد ساخت. پیش‌بینی ماه ژوئن اکنون به واقعیت تبدیل شده است.

کیت‌های بهره‌برداری Exploit Kits ابزارهایی هستند که به‌طور معمول در حملات مورد استفاده قرار گرفته و در شبکه‌های زیرزمینی آنلاین و بازار سیاه به فروش می‌رسند. این ابزارها به مجرمان سایبری این توانایی را می‌دهد تا بدون داشتن مهارت‌های کامپیوتری حملات سایبری خود را پیاده‌سازی کرده و به معامله به‌پردازند.

سایت جیمی الیور

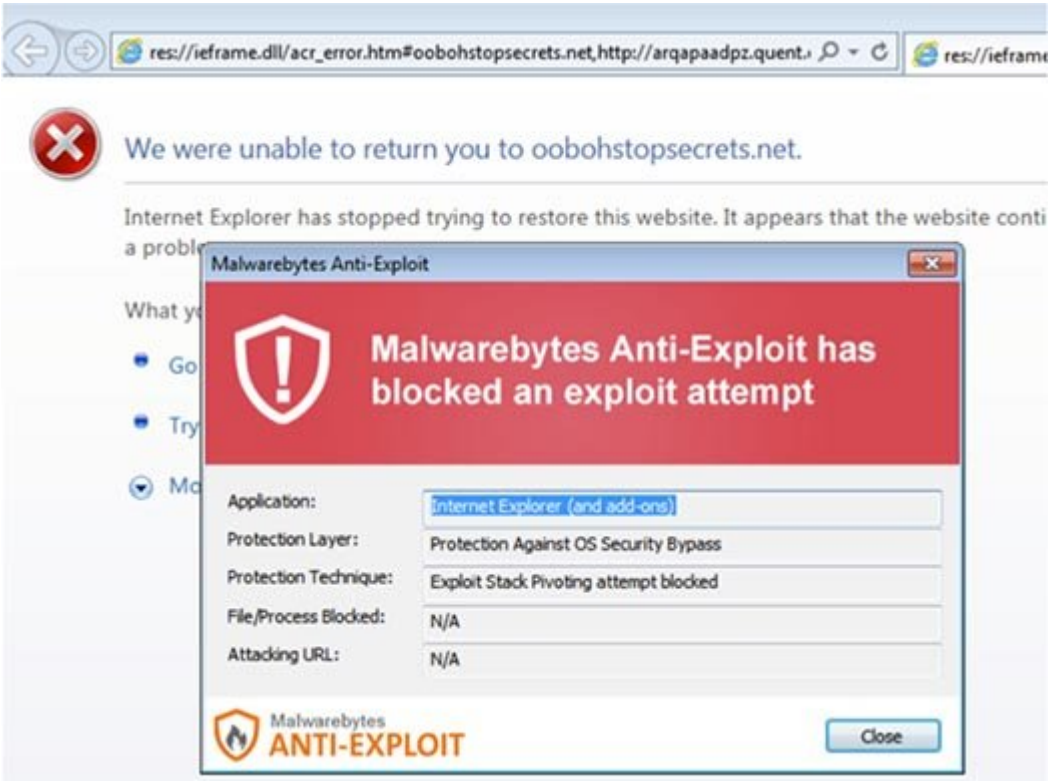
به‌تازگی سایت جیمی الیور برای دومین بار در ماه‌های گذشته قربانی حملات هکری شده است که به اعتقاد کارشناسان این حملات توسط یک گروه هکری مشخص انجام شده است. محققان شرکت امنیتی Fox It اعلام کردند در صفحه اصلی این سایت کدهای مخربی را شناسایی کرده‌اند. Fox It در همین رابطه اعلام کرد که اولین بار سایت جیمی الیور در تاریخ 5 مارس بازدیدکنندگان خود را به سمت یک کیت بهره‌برداری هدایت می‌کرد که نشان می‌داد این سایت حداقل از هشت روز قبل از این تاریخ مورد حمله قرار گرفته بود. در آن تاریخ شرکت Fox It تصویری از بدافزارهای قرار گرفته درون این سایت را برای سایت بیزنس اینسایدر ارسال کرده بود.



اکنون این سایت یک‌بار دیگر مورد حمله هکری قرار گرفته، به‌طوری‌که سایت مذکور مملو از بدافزارهای مختلف شده است. فریزر هاوارد از محققان SophosLabs در این‌باره می‌گوید: « Angler Exploit Kit که در آخرین حمله از آن استفاده شده است، اکنون در بازارهای زیرزمینی به‌شدت مورد توجه قرار دارد. به‌طوری‌که سهم آن در این بازارها نزدیک به یک سوم رشد داشته و به مرز 83 درصد رسیده است. »

بیشتر حملات بدافزاری، از کیت‌های اکسپلویت در تلاش برای تغییر مسیر قربانیان به سایتی که میزبان نرم‌افزارهای مخرب است، استفاده می‌کنند. در اغلب موارد سایت آلوده کامپیوتر قربانی را با یک باج‌افزار آلوده می‌سازد، به‌طوری‌که دستگاه مورد استفاده قربانی تا وقتی که پول لازم از طرف قربانی به هکرها پرداخت نشود، در دسترس و استفاده دوباره او قرار نمی‌گیرد. کریس بوید، تحلیل‌گر اطلاعاتی نرم‌افزارهای مخرب در MalwareBytes به سایت بزینس اینسایدر گفته است: «از تروجان‌های بانکی گرفته تا تبلیغات کلاهبرداری موجود در نرم‌افزارها همگی می‌توانند در این حملات مورد استفاده قرار گیرد.» بنابر اعلام مؤسسه Solve Media تبلیغات کلاهبردارانه تاکنون بیش از 11 میلیارد دلار برای تبلیغ کنندگان سود به‌همراه داشته است. برای کاربران، این تبلیغات باعث کم شدن سرعت ماشین‌های مورد استفاده آن‌ها شده و قدرت اجرایی آن‌ها را کاهش می‌دهد. بنابر گزارش شرکت امنیتی MalwareBytes هکرها حمله‌ای را از تاریخ 28 جولای روی شبکه تبلیغات سایت یاهو آغاز کرده‌اند. این حملات تا تاریخ 3 آگوست همچنان ادامه داشته است. شرکت امنیتی MalwareBytes می‌گوید، یاهو از روز دوشنبه از این مسئله آگاه شده و تدابیر امنیتی لازم را اتخاذ کرده است.

در تصویر زیر پیام ترسناک آنتی اکسپلویت MalwareBytes را زمانی‌که کاربری سعی می‌کند روی یک تبلیغ آلوده کلیک کند مشاهده می‌کنید.

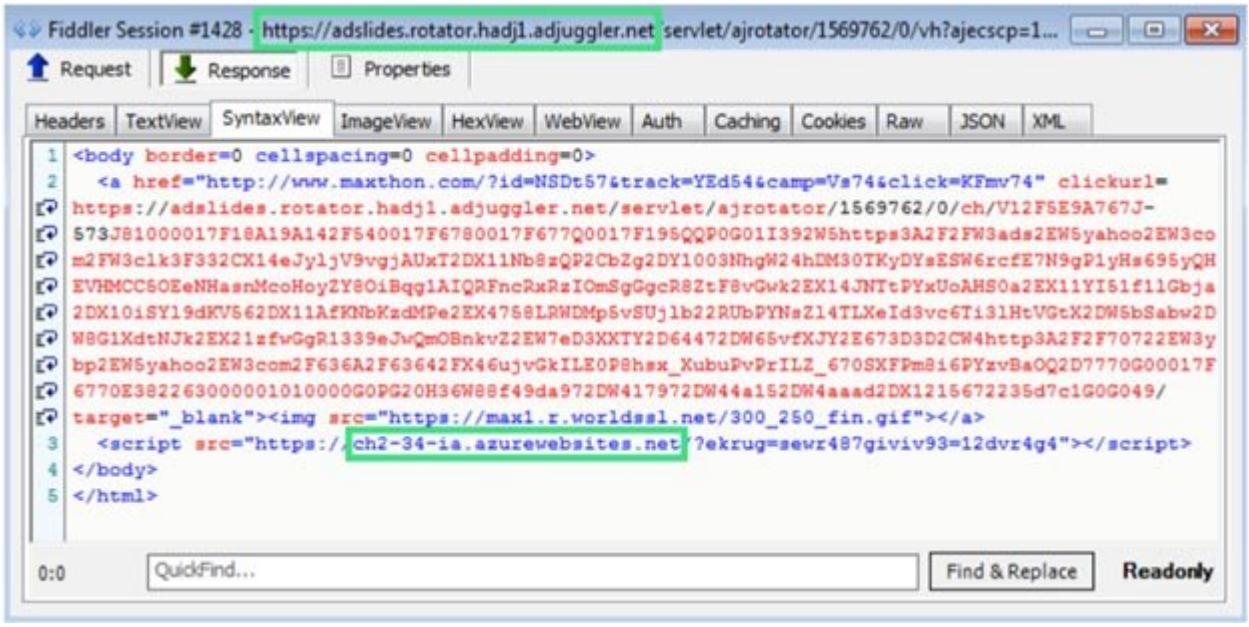


MalwareBytes موفق شده است بخشی از کدهای بومی که در شبکه تبلیغی یاهو قرار داشته‌اند را شناسایی کند.

```
ads.yahoo.com
 -> adslides.rotator.hadj1.adjuggler.net
  -> ch2-34-ia.azurewebsites.net/?ekrug=sewr487giviv93=12dvr4g4
   -> basestyle.org/?id=1423150231&JHRufu346&camp=URhfn67458&click=UEjd856
    -> siege.nohzuespoluprace.net/forums/viewforum.php?f=2sb49&sid=y1yki0
```

این کد نشان می‌دهد، آدرس URL شبکه تبلیغی یاهو به‌عنوان بخشی از این حمله بوده که باعث آلوده شدن تعدادی از سایت‌های Microsoft Azure شده است. بنابر اعلام کریس بوید بیشتر سایت‌های آژر به احتمال زیاد قربانی این حمله شده‌اند و بیشتر حساب‌ها و هویت‌ها به‌سرقت رفته‌اند. سایت‌های Microsoft Azure به‌عنوان یکی از گزینه‌های اصلی طراحان به‌شمار رفته به‌طوری‌که امکان ساخت یک سایت فردی را فراهم می‌آورند.

اطلاعاتی که MalwareBytes از سایت‌های مایکروسافت آژر به‌دست آورده است را در تصویر زیر مشاهده می‌کنید.



بنابر اعلام SimilarWeb سایت‌های یاهو بیش از 6.9 میلیارد بازدید کننده را در ماه به سمت خود جذب می‌کنند. همین موضوع باعث شده است تا این حمله در مقیاس وسیعی صورت پذیرد.

کریس بوید در همین رابطه به سایت بیزینس اینسایدر گفته است: «در حالی‌که هیچ راهی برای اطلاع یافتن از این‌که چه کسی این تبلیغات آلوده کننده را قرار داده است وجود ندارد، با این حال تعداد زیادی حالت‌های ویژه در صفحات یاهو وجود دارد که باعث می‌شوند، نرخ آلودگی‌ها افزایش یابد. »

در ماه ژوئن، کارشناسان امنیتی به کاربران فلش ادوبی اعلام کردند که وصله امنیتی مهمی را که برای پیشگیری از کلاه‌برداری و باج‌خواهی هکرها عرضه شده است در سریع‌ترین زمان ممکن نصب کنند. همچنین؛ سایت یاهو اعلام کرده است تمامی تبلیغاتی که باعث به خطر افتادن کاربران شده‌اند اکنون از روی سایت یاهو برداشته شده‌اند. تبلیغات آلوده بدون اطلاع کاربر اقدام به بارگذاری بدافزارها روی کامپیوتر او می‌کردند.

تاریخ انتشار:
18 مرداد 1394

نشانی منبع: https://www.shabakeh-mag.com/security/1200