**تقریبا ۶۰٪ تبلیغات مخرب از سه ارائه‌دهنده تبلیغاتی ارائه می‌شود.**

طبق گزارش اخیر "Demand Quality Report for Q3 2019"، شرکت‌های امنیت و بررسی کلاهبرداری در تبلیغات، تأثیرات ۱۲۰ میلیارد آگهی را بین ۱ ژانویه و ۲۰ سپتامبر مورد بررسی قرار داده‌اند که از طریق سیستم‌ها، از فعالیت‌های تبلیغاتی مخرب مختلف استفاده شده است.

همچنین در این گزارش در مورد تبلیغات با کیفیت پایین و تبلیغات بنری که در اسلات‌های ویدیویی ظاهر می شود، بحث شده است و بر روی تبلیغات مخرب شناسایی شده و کمپین‌هایی که از آنها استفاده می‌کنند تمرکز شده است.

یک تبلیغ مخرب توسط Confiant اینگونه تعریف می‌شود که رفتارهای ناخواسته‌ای مانند هدایت اجباری برای مسیر موردنظر کلاهبرداری، cryptojacking و یا آلوده کردن سیستم بازدیدکننده‌ها توسط تبلیغات را، شامل می‌شود. گاهی یک تغییر مسیر اجباری ایجاد شده یا یک فایل مخرب برای اهداف خاص بارگذاری می‌شود. همچنین گمراه کردن کاربران از طریق فیشینگ نیز مدنظر است، البته اجبار برای دریافت فایل‌هایی که می‌تواند شامل باج‌افزارها نیز باشد یا اجرای بدافزارهایی برای الحاق سیستم قربانی به بات‌نت‌ها نیز در این موارد اتفاق افتاده است.

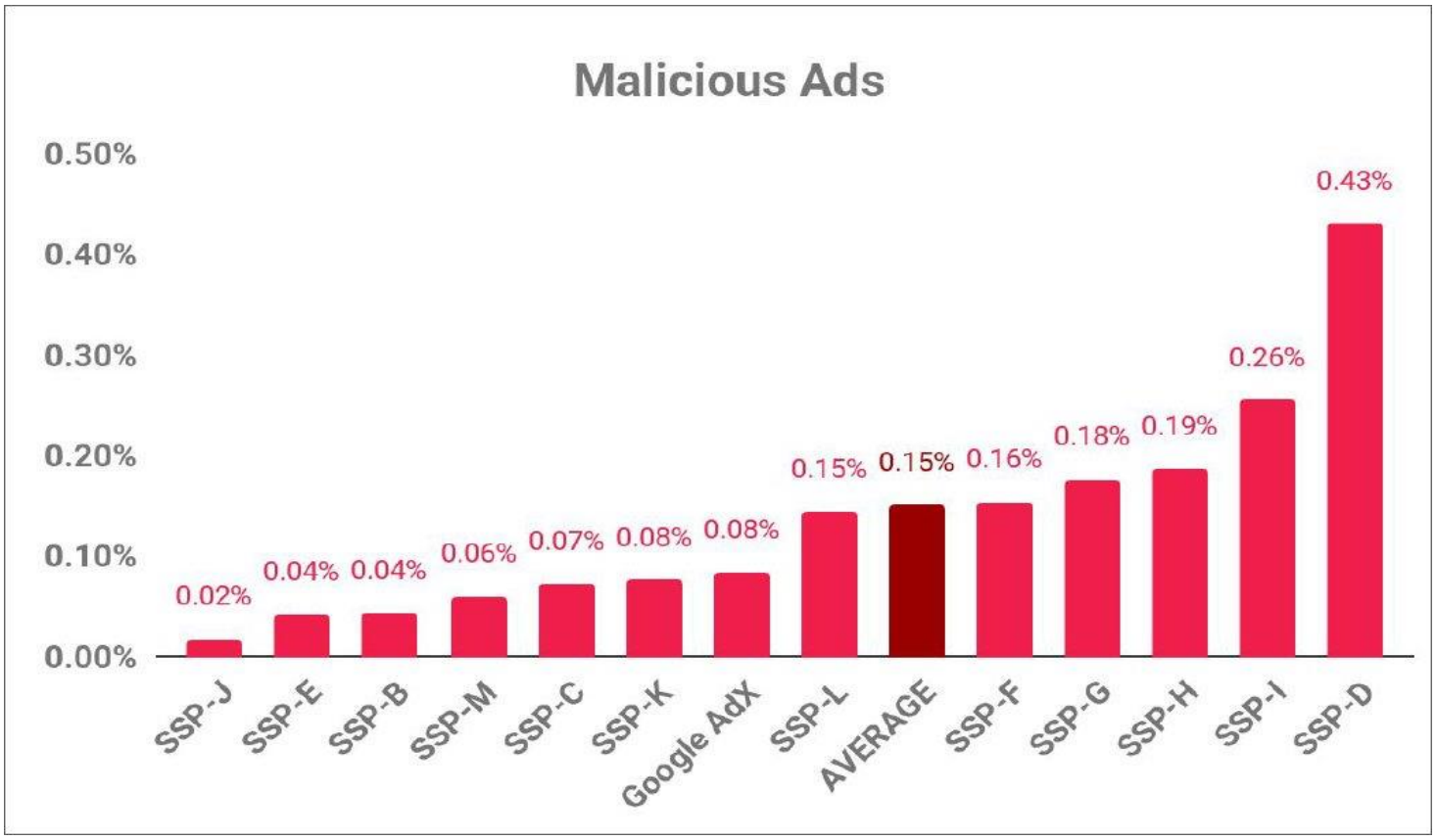
## از کار انداختن تبلیغات مخرب

بر اساس گزارش "Demand Quality Report for Q3 2019"، Confiant ۱۲۰ میلیارد اثر تبلیغات در برنامه‌ها را که توسط سیستم رسیدگی تبلیغاتی آنها رصد شده بود، تجزیه و تحلیل کرده است.

خبر خوب این است که به دلیل راه‌حل‌هایی مانند فیلتر بعضی از تبلیغات مخرب در مرورگر کاربر، این تعداد در حال کاهش است، همچنین صاحبان سایت‌ها درصدد هستند تا تصمیماتی را اتخاذ کنند تا جلوی تبلیغات غیرمجاز در سایت‌های خود را بگیرند و کنترل‌های حساس‌تر و محکم‌تری در بین Supply Side Platforms (SSP) داشته باشند.

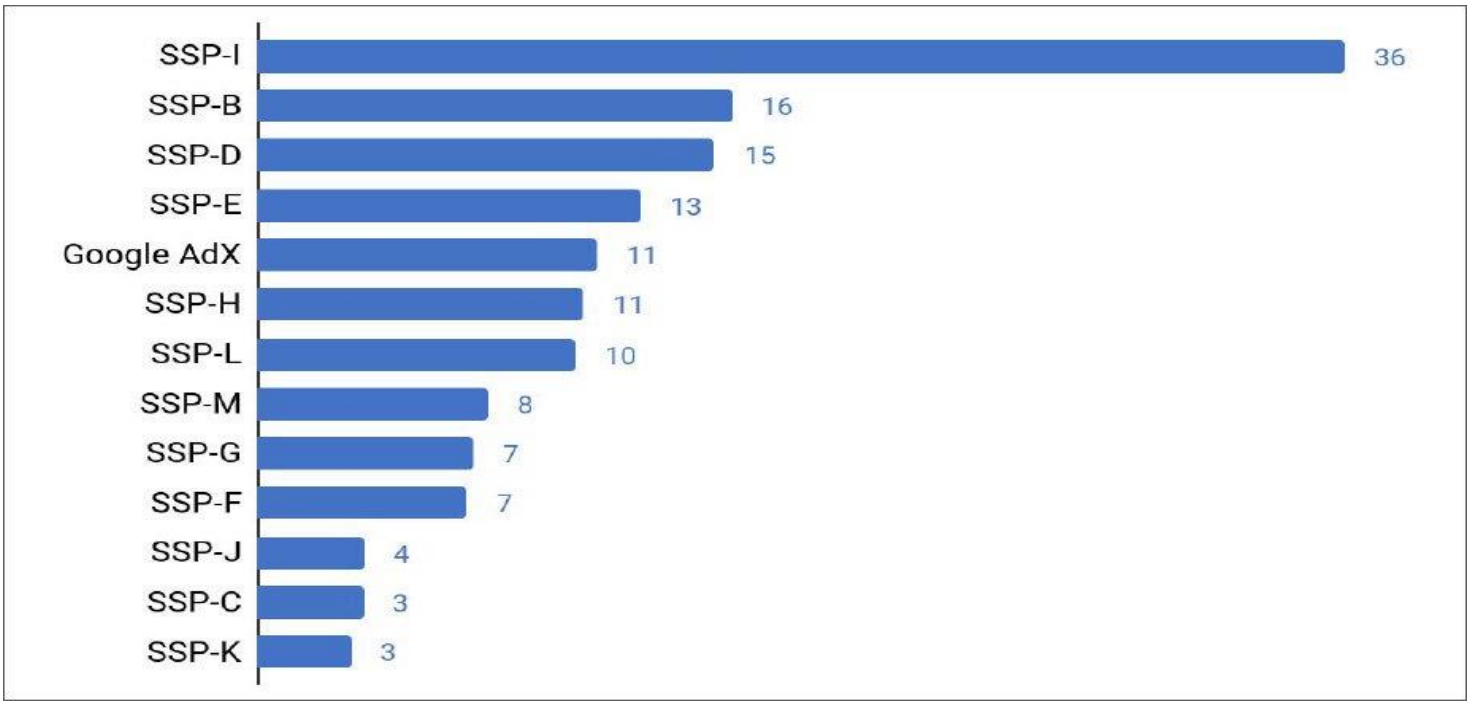
روند کنونی به‌نظر می‌رسد در جهت صحیح و مناسبی باشد ونرخ میزان تبلیغات مخرب از ۲۵٪ به ۱۵٪ کاهش یافته است اما طبق این گزارش هنوز تبلیغات ناخواسته زیادی وجود دارد که اکثراً از طریق سه ارائه‌کننده تبلیغ‌کننده عمده بوده است.

از ۷۵ SSP یا ارائه‌دهنده تبلیغات، تحت نظارت Confiant، بیش از ۶۰٪ اثرات تبلیغاتی مخرب از ۳ مورد تحت عنوان SSP-H، SSP-I و SSP-D گرفته شده‌اند. حتی نکته نگران‌کننده‌تر این است که یک SSP مسئول بیش از ۳۰٪ تبلیغات مخرب است که توسط Confiant گزارش شده است. در عکس زیر این آمار نشان داده شده است.



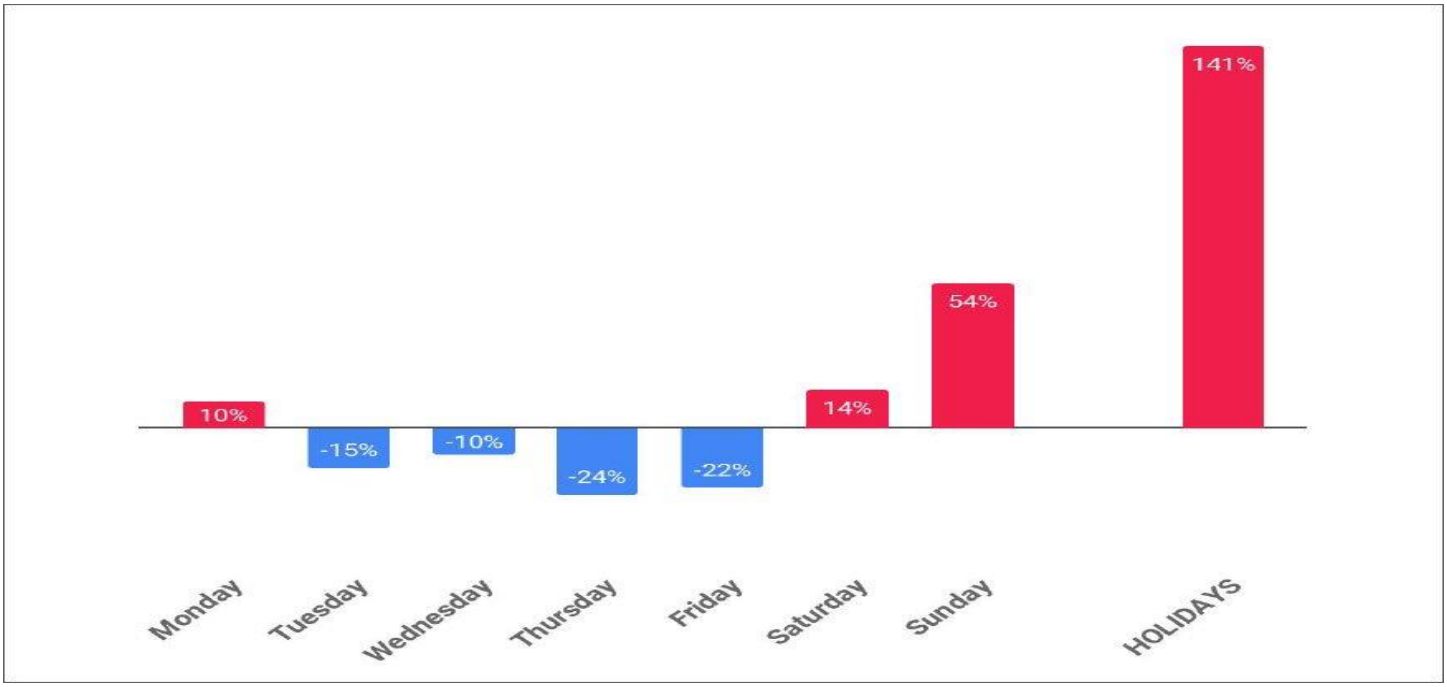

*میزان اثرات مخرب SSPهای برتر*

نکته قابل تامل دیگر این است که SSP هایی که مسئول مخرب‌ترین تبلیغات هستند، نسبت به پاسخ دادن به حملات، کندتر عمل می‌کنند. در شکل زیر این آمار نشان داده شده است.




*زمان پاسخ به حملات توسط SSPها*

همچنین تبلیغ‌کنندگان مخرب تمایل دارند کمپین‌های تبلیغاتی خود را در زمان‌هایی انجام دهند که پرسنل فعال کمتری بر شبکه‌های تبلیغاتی نظارت داشته باشند و از این رو ممکن است نسبت به حملات کندتر باشند. در نمودار زیر نمایان است که اکثر کمپین‌ها در طول آخر هفته انجام می‌شود و بیشترین کمپین‌ها در طول تعطیلات برگزار می‌شوند.



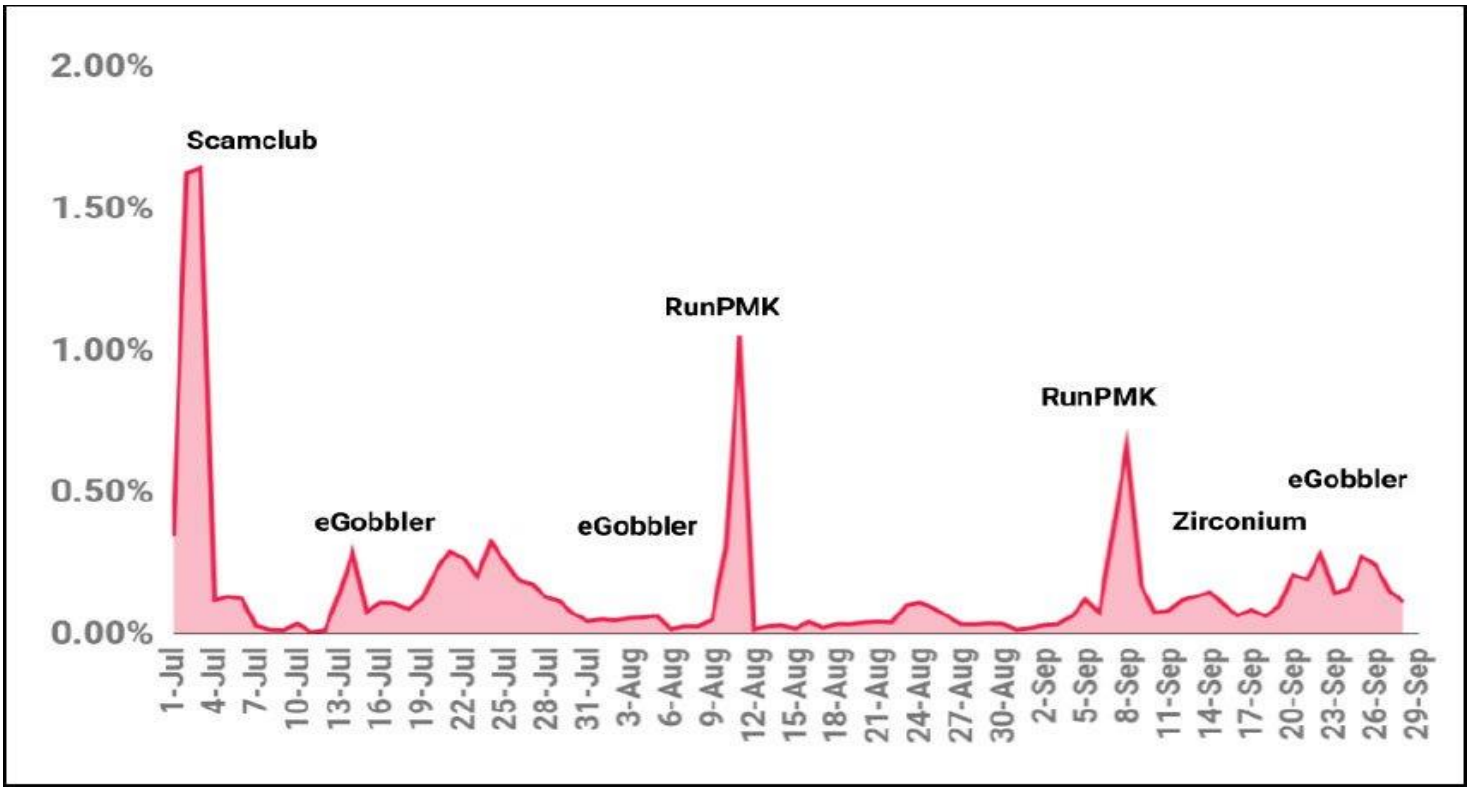

*نرخ نمایش حملات تبلیغات مخرب در طول روزهای هفته*

## گروه‌های تهدید آمیز اصلی

در فصل سوم سال ۲۰۱۹، چهار عامل تهدید کننده مسئول توزیع اکثر تبلیغات مخرب از طریق شبکه‌های تبلیغاتی بوده‌اند.

این گروه‌های تهدیدآمیز دارای نام‌های Scamclub، eGobbler، RunPMK و Zirconium بوده‌اند. نکته جالب این است که این کمپین‌ها ممکن است در طول سال از نظر تبلیغات جریان ثابتی داشته باشند اما در مواقع خاص فعالیت‌های قابل توجه خود را شروع کرده و نشان‌دهنده یک فشار تبلیغاتی سنگین توسط یک عامل خاص است.

در شکل زیر کمپین‌های مختلف تبلیغاتی را که توسط عاملان مختلف در زمان‌های متفاوت طی سه ماهه سوم سال ۲۰۱۹ انجام شده، قابل مشاهده است.




*فعالیت مخرب تبلیغات برای ۴ گروه اصلی تهدیدآمیز*

هر گروه تهدیدآمیز تمایل دارد به نوع متفاوتی بر روی تبلیغات مخرب و نحوه تزریق آن‌ها به ترافیک تبلیغاتی مشروع، همانطور که در ادامه توضیح داده می‌شود، تمرکز کند.

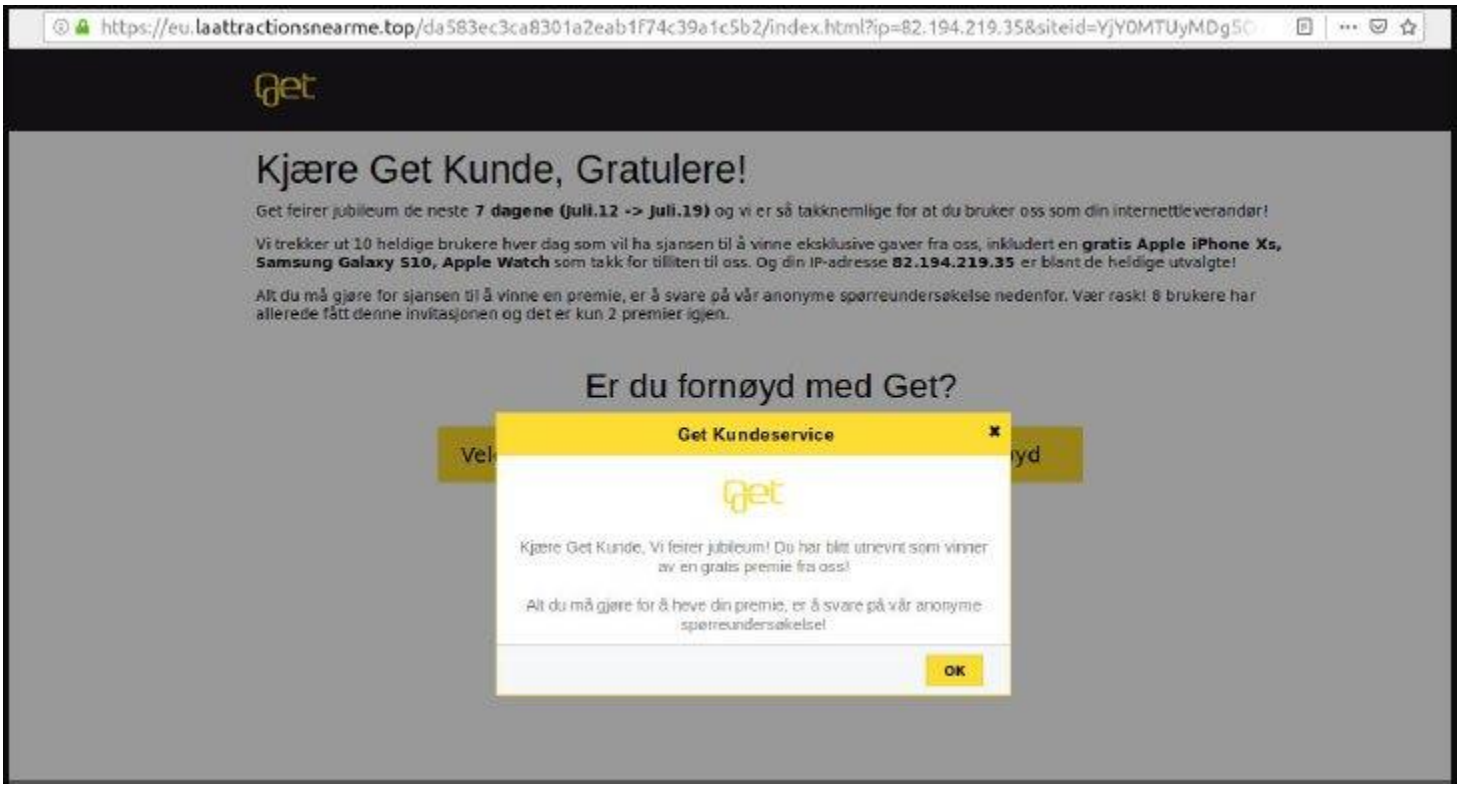
- **Scamclub**

Scamclub برخلاف سایر عاملین تبلیغات مخرب، این عامل تلاش زیادی برای جلوگیری از تشخیص توسط امضا و هدف‌گیری خاص، نمی‌کند. در عوض، Scamclub به منظور دور زدن سیستم شبکه تبلیغاتی مشروع و امنیت آن‌ها، به این

امید که برخی از این تبلیغات و اثرات آن‌ها به بازدیدکنندگان سایت‌های مشروع راه پیدا کنند، کمپین‌های بزرگی را با ده‌ها یا حتی صدها نفر از نیروهای خلاق برگزار می‌کند.

- **eGobbler**

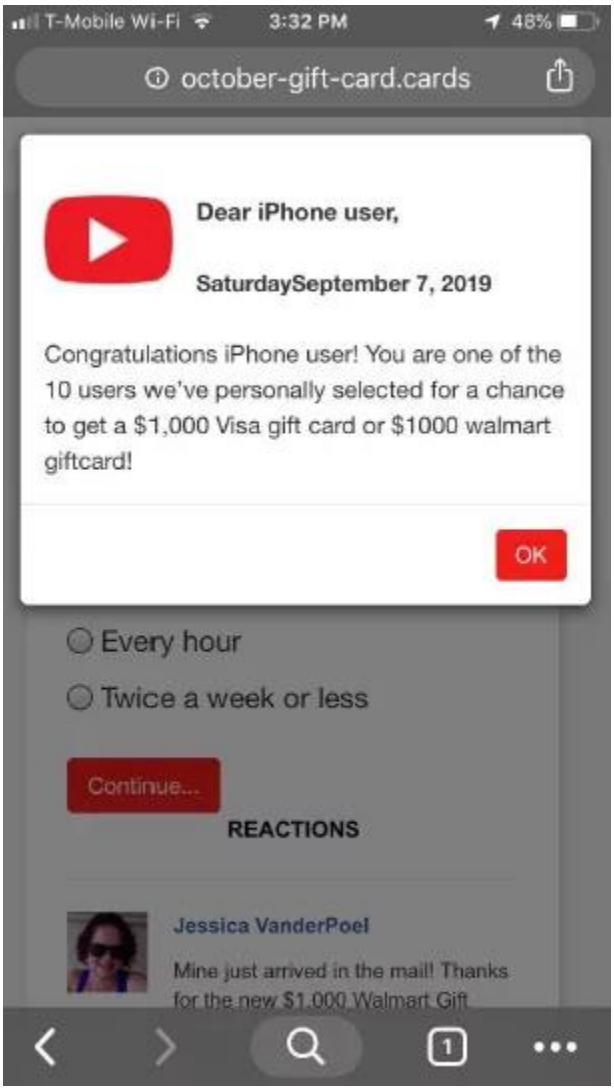
eGobbler بدافزار شناخته شده‌ای است که از اشکالات مرورگر به منظور هدایت کاربران به سایت‌های مخرب سوءاستفاده می‌کند. در یکی از عملیات‌های صورت گرفته در گذشته، eGobbler از یک باگ WebKit برای آلوده کردن بیش از ۱ میلیارد تبلیغات بهره‌برداری کرده است.




به گفته Confiant، eGobbler سیستم‌هایی را که معمولاً با سیستم‌عامل ویندوز کار می‌کنند، هدف قرار می‌دهد. گزارش‌ها حاکی از آن است که این عامل در کشورهای مختلف تبلیغات مخرب داشته است اما بیشتر کاربران کشورهای ایتالیا، اسپانیا و منطقه اسکاندیناوی را تحت تاثیر قرار داده است. Confiant این آسیب‌پذیری‌ها را در تاریخ ۷ آگوست به تیم Webkit گزارش داد و برطرف شد.

- **RunPMK**

RunPMK برای نمایش تبلیغات کلاهبرداری از قبیل مواردی که هدایایی به شکل صوری در قرعه‌کشی اهدا می‌شوند، استفاده شده و ترافیک تلفن‌همراه را در iOS و Android هدف قرار می دهد. طبق گزارش Confiant اجرای RunPMK در حدود ۲۱۲ کشور بوده است.




- **Zirconium**

گروه تهدیدات Zirconium به منظور هدف قرار دادن کاربران با تبلیغات خاص از روش‌های منحصر به فرد استفاده می کند. طبق گزارش Confiant، آنها از اسکریپت‌هایی پیشرفته برای تبلیغات مخرب استفاده کرده و معمولاً کلاهبرداری‌های خود را در قالب پشتیبانی فنی بر روی سیستم کاربران اعمال می‌کنند.

## پیشرفت تدریجی

در حالی که هنوز تبلیغات مخرب به عنوان یک مشکل به صورت آشکارا وجود دارد و کاربران باید همچنان به استفاده از نرم‌افزارهای امنیتی و انتی‌ویروس که سایت‌های مخرب یا سایت‌های دارای تبلیغات مخرب را مسدود می‌کنند، ادامه دهند اما طبق این گزارش با توجه به آمار و اطلاعات موجود، چشم‌انداز حذف تبلیغات مخرب در حال بهبود است. بر اساس خروجی این گزارش‌ها،

روش‌های موثری برای فیلتر کردن تبلیغات مخرب وجود دارد و اگر SSP هوشیار باقی بماند و شرکای مناسبی را انتخاب کند، کاهش بیشتری نیز در حوزه تبلیغات مخرب می‌تواند رخ دهد.

منبع:

https://www.bleepingcomputer.com/news/security/almost-60-percent-of-malicious-ads-come-from-three-ad-providers/