بسمه‌تعالی

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر
مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

گزارش آسیب پذیری Changing 404 pages

گزارش فنی

نوع سند ..... گزارش فنی
شماره نگارش ۱
تاریخ نگارش ۱۴۰۲/۰۷/۱۸
طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷
(۰۲۱) ۸۸۱۱۵۷۲۴
(۰۲۱) ۸۸۱۱۵۷۲۴
cert.ir

فهرست مطالب

۱ شرح

یک کمپین جدید اسکیمینگ کارت Magecart صفحات خطای ۴۰۴ وب‌سایت‌های خرده‌فروشان آنلاین را ربوده و کدهای مخرب را برای سرقت اطلاعات کارت‌اعتباری مشتریان پنهان می کند.

این تکنیک یکی از سه نوع مشاهده شده توسط محققان گروه اطلاعات امنیتی Akamai است که دو روش دیگر کد را در ویژگی "onerror" تگ تصویر HTML و یک تصویر باینری پنهان می‌کنند تا به عنوان قطعه کد متا پیکسل به نظر برسد.

Akamai می‌گوید این کمپین بر روی سایت‌های مجنتو و ووکامرس متمرکز است و برخی از قربانیان با سازمان‌های مشهور در بخش‌های غذا و خرده‌فروشی مرتبط هستند.

۱-۱ دستکاری صفحه ۴۰۴

همه وب‌سایت‌ها دارای صفحه‌های خطای ۴۰۴ هستند که هنگام دسترسی به صفحه‌ای که وجود ندارد، منتقل شده یا دارای پیوند مرده یا شکسته است، به بازدیدکنندگان نمایش داده می‌شوند.

بازیگران Magecart از صفحه پیش‌فرض '۴۰۴ Not Found' برای پنهان کردن و بارگذاری کد سرقت کارت مخرب استفاده می‌کنند که قبلاً در کمپین‌های قبلی دیده نشده بود. در گزارش Akamai آمده است: "این تکنیک پنهان‌سازی بسیار نوآورانه است و چیزی که در کمپین‌های قبلی Magecart ندیده بودیم."

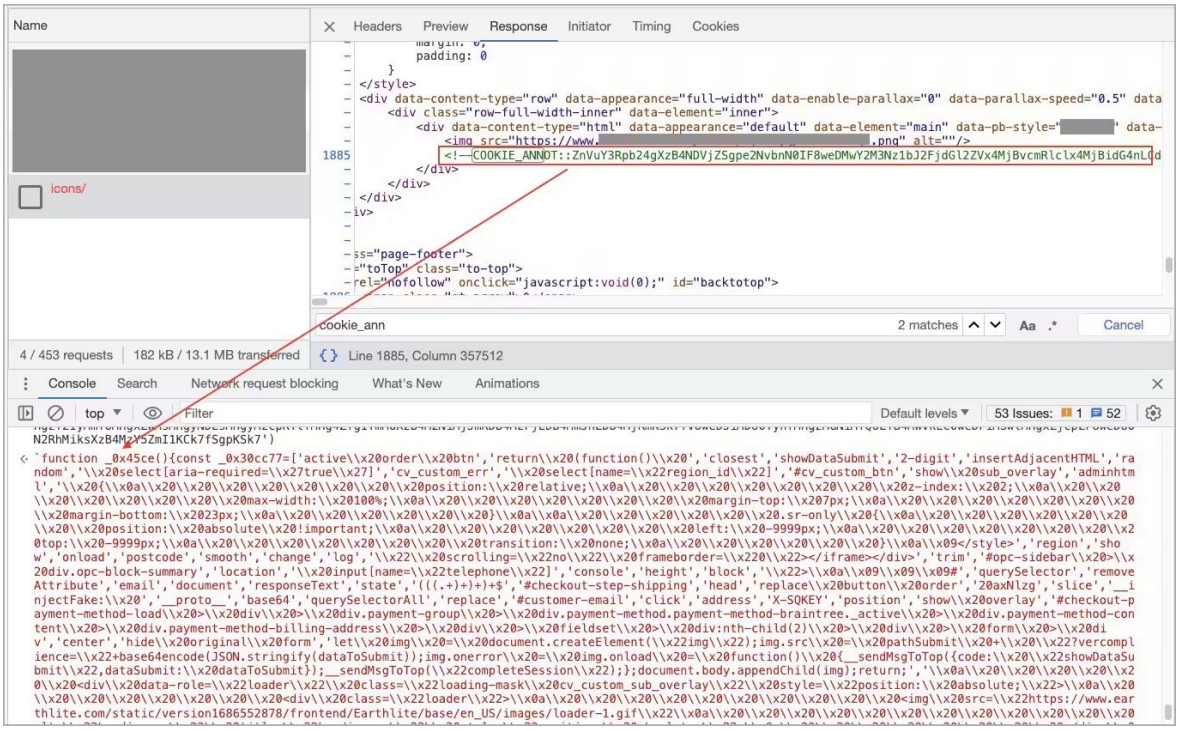
ایده دستکاری صفحه خطای پیش‌فرض ۴۰۴ یک وب‌سایت هدفمند می‌تواند گزینه‌های خلاقانه مختلفی را به بازیگران Magecart برای بهبود پنهان کردن و فرار ارائه دهد.

بارگذار اسکیمر یا خود را به عنوان یک قطعه کد Meta Pixel پنهان می‌کند یا در اسکریپت های تصادفی درون‌خطی که قبلاً در صفحه وب تسویه حساب در معرض خطر وجود دارد پنهان می‌شود. لودر یک

درخواست واکشی را به یک مسیر نسبی به نام "icons" آغاز می‌کند، اما از آنجایی که این مسیر در وب سایت وجود ندارد، درخواست منجر به خطای "Not Found ۴۰۴" می شود.

محققین Akamai در ابتدا تصور کردند که دیگر فعال نیست یا گروه Magecart یک اشتباه در پیکربندی مرتکب شده است. با این حال، پس از بررسی دقیق‌تر، آنها دریافتند که لودر حاوی یک عبارت منظم مطابق با جستجوی یک رشته خاص در HTML برگشتی صفحه ۴۰۴ است.

به محض یافتن رشته در صفحه، Akamai یک رشته به هم پیوسته رمزگذاری شده با base64 را پیدا کرد که در یک نظر پنهان شده بود. رمزگشایی آن رشته اسکیمر جاوا اسکریپت را نشان داد که در تمام ۴۰۴ صفحه پنهان می‌شود.



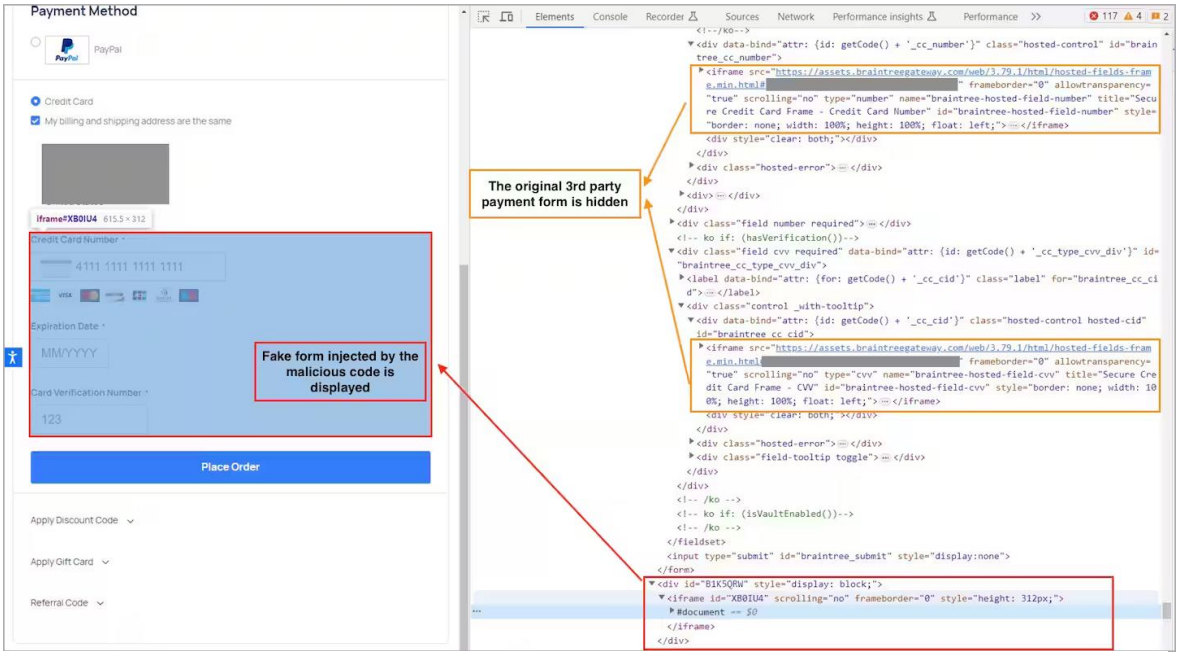
رشته ای که لودر به دنبال آن در HTML است

Akamai توضیح می دهد: "ما درخواست های اضافی را به مسیرهای موجود شبیه سازی کردیم، و همه آنها همان صفحه خطای ۴۰۴ حاوی نظر را با کد مخرب رمزگذاری شده برگرداندند." این بررسی ها تایید می‌کند که مهاجم با موفقیت صفحه خطای پیش‌فرض را برای کل وب‌سایت تغییر داده

و کد مخرب را در آن پنهان کرده است.از آنجا که درخواست به یک مسیر شخص اول ارسال می شود، اکثر ابزارهای امنیتی که درخواست های مشکوک شبکه را در صفحه پرداخت نظارت می‌کنند، آن را نادیده می‌گیرند.

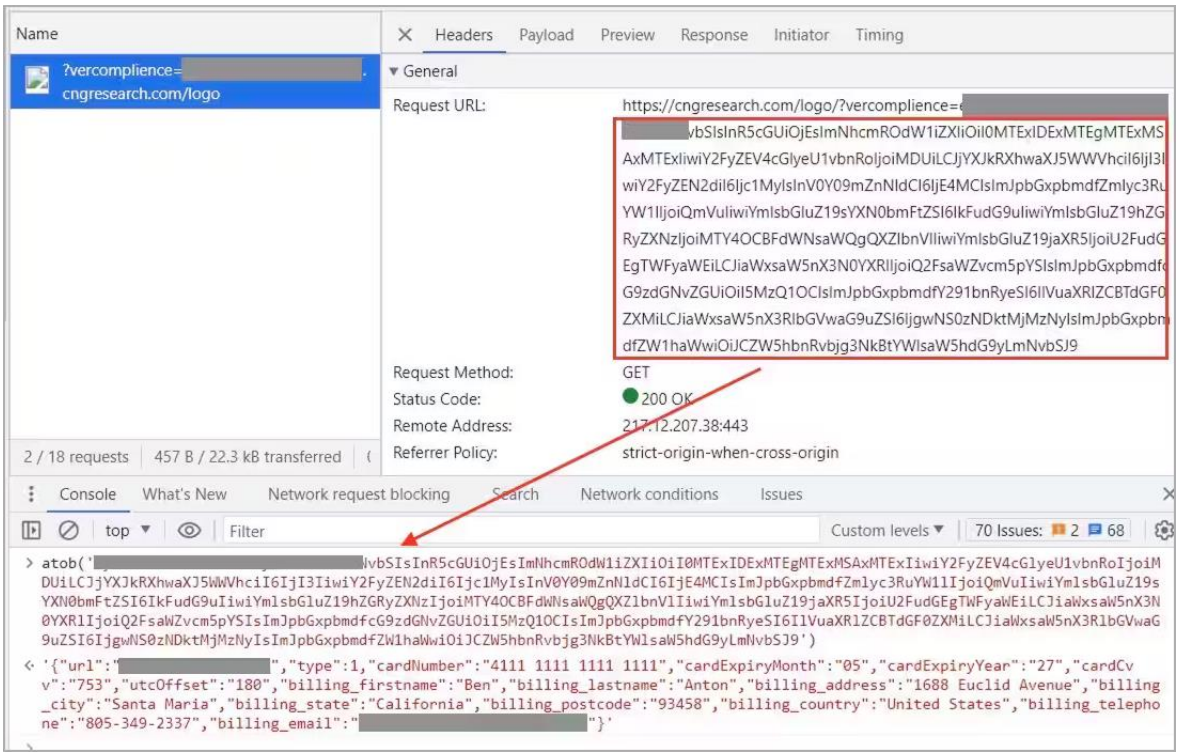
۲-۱ سرقت داده ها

کد اسکیمر فرم جعلی را نشان می‌دهد که بازدیدکنندگان وب‌سایت باید آن را با جزئیات حساس از جمله شماره‌کارت اعتباری، تاریخ انقضا و کد امنیتی خود پر کنند.



شکل ۱- فرم پرداخت جعلی

هنگامی که این داده ها در فرم جعلی وارد می‌شوند، قربانی یک خطای جعلی "زمان پایان جلسه" دریافت می‌کند. در پس‌زمینه، تمام اطلاعات با base64 کدگذاری می‌شوند و از طریق URL درخواست تصویر که رشته را به‌عنوان پارامتر پرس و جو حمل می‌کند، به مهاجم ارسال می‌شود.



شکل ۲- درخواست استخراج داده ها

این رویکرد به جلوگیری از تشخیص توسط ابزارهای نظارت بر ترافیک شبکه کمک می‌کند، زیرا درخواست شبیه یک رویداد واکشی تصویر خوش‌خیم است. با این حال، رمزگشایی رشته base64 اطلاعات شخصی و کارت اعتباری را نشان می‌دهد.

مورد دستکاری ۴۰۴ صفحه، تاکتیک های در حال تحول و تطبیق پذیری بازیگران Magecart را برجسته می‌کند، که به طور مداوم مکان‌یابی کدهای مخرب خود را در وب‌سایت های در معرض خطر و پاکسازی آنها را برای مدیر وب سخت‌تر می‌کند.

۲ مراجع

https://www.bleepingcomputer.com/news/security/hackers-modify-online-stores-404-pages-to-steal-credit-cards/