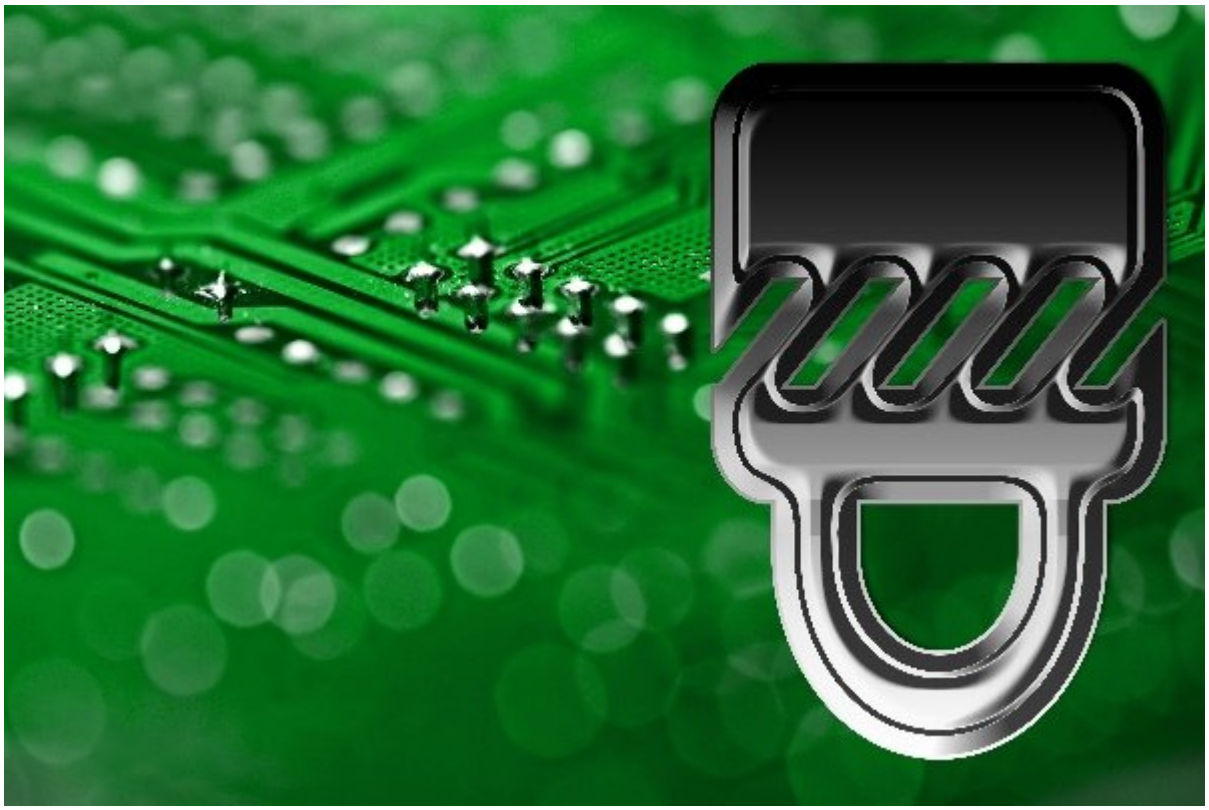

禪

بدافزارهایی مستتر در تبلیغات

کدهای پیچیده موجود در تبلیغات ویدیویی مانع از شناسایی بدافزارها میشود

مجرمان سایبری، سالهاست با استفاده از تبلیغات آنلاین، اقدام به انتشار بدافزارها میکنند. شناسایی بدافزارهای مستتر در شبکه تبلیغاتی یاهو، جدیدترین مورد شناسایی شده در این زمینه بود. بدافزارهای پنهان در شبکه تبلیغاتی یاهو موفق شدند، هزاران کاربر این شبکه تبلیغاتی را قربانی خود سازند؛ اما به نظر میرسد که مجرمان سایبری، روشهای تازهای برای انتشار بدافزارها پیدا کردهاند. ویدیوهای تبلیغاتی، راهکار جدید هکرها در این زمینه است.

در هر دو روش حمله، بدافزارنویسان میتوانند تأثیر قابل توجهی بر صنعت تبلیغات بر جای گذارند؛ اگر تنها یک بدافزار بتواند خود را در تبلیغات مستتر کند و به درون سایتهای مختلفی که از ترافیک بالایی برخوردار هستند، تزریق شود، بهراحتی میتواند در مدت زمان کوتاهی، دهها هزار کامپیوتر را آلوده کند. تعدادی از شبکههای تبلیغی و همچنین یکسری از منتشرکنندگان تبلیغات، سعی میکنند تا با استفاده از فیلترهایی، این همجه آلودهسازی را کم کنند؛ اما هکرها بهطور مداوم در حال جستوجوی ضعفهای امنیتی جدید هستند.

```xml
<?xml version="1.0" encoding="utf-8"?>
<VAST version="2.0">
<Ad id="229">
    <InLine>
        <AdSystem version="4.9.0-10">LiveRail</AdSystem>
        <AdTitle><![CDATA[LiveRail creative 1]]></AdTitle>
        <Description><![CDATA[]]></Description>
        <Impression id="LR"><![CDATA [http://t4.liverail.com/?metric=impression&cofl=0&pos=0&coid=135&pid=1331&nid=1331&oid=229&olid=2291331&cid=331&tpcid=&
vid=&amid=&cc=default&pp=&vv=&tt=&sg=&tg=&pmu=0&pau=0&psz=0&ctx=&tctx=&coty=0&adt=0&scen=&url=http%3A%2F%2Fwww.longtailvideo.com%2Fsupport%2Fopen-video-
ads%2F23120%2Fwhat-is-vast%2F&cb=1259.192.118.68.5.0.690&ver=1&w=&wy=&x=121&y=121&xy=0b79&z2=0]]></Impression>
            .......
        <Creatives>
            <Creative sequence="1" id="331">
                <Linear>
                    <Duration>00:00:09</Duration>
                        <TrackingEvents>
                            <Tracking event="firstQuartile"><![CDATA [http://t4.liverail.com/?metric=view25&pos=0&coid=135&pid=1331&nid=1331&oid=229&
olid=2291331&cid=331&tpcid=&vid=&amid=&cc=default&pp=&vv=&tt=&sg=&tg=&pmu=0&pau=0&psz=0&ctx=&tctx=&coty=0&adt=0&scen=&url=http%3A%2F
%2Fwww.longtailvideo.com%2Fsupport%2Fopen-video-ads%2F23120%2Fwhat-is-vast%2F&cb=1259.192.118.68.5.0.690&ver=1&w=&wy=&x=&y=&xy=]]></Tracking>
                        <Tracking event="midpoint"><![CDATA [http://t4.liverail.com/?metric=view50&pos=0&coid=135&pid=1331&nid=1331&oid=229&olid=2291331&
cid=331&tpcid=&vid=&amid=&cc=default&pp=&vv=&tt=&sg=&tg=&pmu=0&pau=0&psz=0&ctx=&tctx=&coty=0&adt=0&scen=&url=http%3A%2F%2Fwww.longtailvideo.com%2Fsupport%2Fopen-
video-ads%2F23120%2Fwhat-is-vast%2F&cb=1259.192.118.68.5.0.690&ver=1&w=&wy=&x=&y=&xy=]]></Tracking>
                        .......
                    </TrackingEvents>
                    <VideoClicks>
                    <ClickThrough><![CDATA [http://t4.liverail.com/?metric=clickthru&pos=0&coid=135&pid=1331&nid=1331&oid=229&olid=2291331&cid=331&tpcid=&
vid=&amid=&cc=default&pp=&vv=&tt=&sg=&tg=&pmu=0&pau=0&psz=0&ctx=&tctx=&coty=0&adt=0&scen=&url=http%3A%2F%2Fwww.longtailvideo.com%2Fsupport%2Fopen-video-
ads%2F23120%2Fwhat-is-vast%2F&cb=1259.192.118.68.5.0.690&ver=1&w=&wy=&x=&y=&xy=&redirect=http%3A%2F%2Fliverail.com%2F]]></ClickThrough>
                </VideoClicks>
                    <MediaFiles>
                <MediaFile delivery="progressive" bitrate="256" width="480" height="352" type="video/x-flv"><![CDATA [http://cdn.liverail.com/adasset4
/1331/229/331/lo.flv]]></MediaFile>
                .......
            </MediaFiles>
            </Linear>
        </Creative>
        </Creatives>
    </InLine>
  </Ad>
</VAST>
```

شکل 1

حملهای که نزدیک به دو هفته پیش از دامنه brtmedia.net شناسایی شد، نشان داد چگونه مجرمان سایبری میتوانند، ویدیوهای تبلیغاتی مخرب را به کاربران نشان دهند؛ هر چند قدمت حملاتی که بر پایه تبلیغات ویدویی کار میکنند، به گذشته باز میگردد؛ اما اینبار، حملات هکری سایتها را نشانه رفتهاند . در مکانیزم جدید، سایتهایی به عنوان هدف شناخته میشوند که در رتبهبندی الکسا، در بالای فهرست قرار دارند . اینکار باعث میشود تا سرعت انتشار بدافزارها، به راحتی افزایش پیدا کند . رشد روزافزون این مدل از حملات، باعث شد تا در اوایل ماه جاری میلادی شرکت امنیتی Media Trust، شرکتی که در زمینه عرضه ابزارهای امنیتی و ارائه سرویسهایی در ارتباط با شناسایی بدافزارها فعالیت میکند، تحقیقات مفصلی در این زمینه انجام دهد . تحقیقات انجام شده از سوی این مؤسسه، آمارهای وحشتناکی به جای گذاشته است. تنها در یک مورد از این تحقیقات، در تاریخ 29 اکتبر و تنها در مدت زمان 12 ساعت، نزدیک به 3000 سایت، میزبان تبلیغات ویدویی مخرب بودند . تبلیغاتی که در قالب پنجرههای تبلیغاتی موسوم به TripBox به نمایش درآمدهاند . در پنجره ظاهر شده، پیغامی در خصوص بهروزرسانی نرمافزارهای مرورگر، شبیه به سافاری اپل، به کاربر نشان داده شده و از کاربر درخواست شده است، مطابق با دستورالعملهای یاد شده رفتار کند؛ اگر کاربری فریب این تبلیغ را خورده و مطابق با دستورالعملهای رفتار کرده باشد، یک در پشتی روی کامپیوتر او ایجاد شده است . (شکل 2)

Step 1. Malicious file drop
Brtmedia.net drops a swf file imitating video player
Step 2. Obfuscation
File detects domain, avoiding certain large publishers
On list of excluded sites?
Step 3. Site Infection
NO. Injects malicious javascript into site page
YES. No site infection.
Step 4. Ad placement
Simulates ad bidding and places video into the 300x250 tag position
As flash video plays, injects 1x1 tracking iframe which triggers "Tripbox" popup
Step 5. Malware drop on user device
User clicks Tripbox and payload downloads
Security Update
Sample Tripbox popup on Apple desktop device
The Media Trust

شکل 2

کریس اولسون، مدیرعامل مدیا تراست، در اینباره میگوید : «تبلیغات ویدیویی، یک هدف جذاب برای هکرها به شمار میرود؛ به دلیل اینکه شناسایی این بدافزارها نسبت به تبلیغات تصویری، بسیار مشکلتر است و همچنین جذابیت بیشتری برای کاربران دارد .» این روزها، تبلیغات ویدیویی اغلب توسط VAST (سرنام Digital Video Ad Serving Template) که یک الگوی جاوااسکریپتمحور است، توزیع میشود؛ اما بیشتر عناصر، از قبیل برچسبهای ردیابی، میتوانند در قالب الگوهایی در کدها قرار بگیرند و درون یک بسته دیجیتالی، به شکل ساندویچ، بستهبندی و استفاده شوند . اولسون میگوید : «اضافه شدن این برچسبها دست و پاگیر است. یک قطعه کدی که به این شکل و در قالب یک الگو، آماده اجرا میشود، در اصل به عنوان یک کانتینر برای کدها رفتار میکند . همین موضوع باعث میشود به راحتی نتوان به این کدها و محتوایی که درون آنها قرار دارد، اطمینان کرد .»

هر چند خرید تبلیغات ویدویی نسبت به تبلیغات تصویری گرانتر هستند؛ اما به دلیل تأثیر قابل توجهی که بر جای میگذارند، هکرها حاضرند برای خرید آنها، پول اضافی پرداخت کنند . هکرها تا حد امکان، سعی میکنند بیشترین نرخ آلودهسازی را در اختیار داشته باشند . نزدیک به دو هفته پیش، محتوای مخربی همراه با دامنهای به نام brtmedia[.]net منتشر شد. هنوز به درستی مشخص نیست آیا این دامین، متعلق به شرکت BRT Media بوده است یا هیچ ارتباطی به این شرکت ندارد .

BRT Media یک شرکت فعال در زمینه تبلیغات آنلاین به شمار میرود . اولسون درباره این بدافزار میگوید : «هنوز نمیتوانیم آمار دقیقی از کامپیوترهای آلوده منتشر کنیم؛ اما یک موضوع کاملا روشن است؛ ما با مشکلی جدید و نوظهور در ارتباط با ویدیوها روبرو هستیم »؛ وی همچنین در این ارتباط میگوید : «شرکتها و ناشرانی که در زمینه سرویسدهی به تبلیغات ویدیویی فعالیت میکنند، باید به کانالهای ویدیویی و کدهای متعلق به نرمافزارهای ثالث که از طریق آنها اقدام به انتشار تبلیغات ویدیویی میکنند، توجه بیشتری داشته باشند .»

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
18:52 - 13/10/1394

برچسب:

بدافزار - تبلیغات مخرب - تبلیغات آلوده - یاهو

□□□□□ منبع: https://www.shabakeh-mag.com/security/2476