From: **Mary Geddry** mary@geddry.com
Subject: Re: website
Date: March 7, 2018 at 8:11 PM
To: Darlene Elliott daeelliott1@gmail.com
Cc: Dr Gene Landrum quantumcafecoos97420@gmail.com, Travis Hayer travhayer@gmail.com, Knute Nemeth knute.nemeth@gmail.com, Octavia Shafer octavia.shafer@gmail.com, Deborah Hamill hamil3az@aol.com, onave5555@gmail.com

It's coming from the radio stream. When I remove the embedded player it goes away again.

Mary

filter log entries | 1000

			http://kjaj.org/wp-content/uploads/2018/02/KJAJlogo.jpg
			http://kjaj.org/wp-content/uploads/2018/02/KJAJlogo.jpg
22:59:13		xhr	http://myradiostream.com/embed/json.php?s=KJAJ
22:59:12		font	https://fonts.gstatic.com/s/mavenpro/v11/7Au9p_AqnyWWAxW2Wk3GzWQI.woff2
22:59:12		font	http://myradiostream.com/embed/assets/fonts/fontawesome-webfont.woff2?v=4.7.0
22:59:12		css	https://fonts.googleapis.com/css?family=Maven+Pro:400,500,700,900
22:59:12		css	http://myradiostream.com/embed/assets/css/font-awesome.min.css
22:59:12		script	http://myradiostream.com/embed/assets/js/buzz.min.js
22:59:12		script	http://myradiostream.com/embed/assets/js/jquery.min.js
22:59:12		css	http://myradiostream.com/embed/assets/css/style.css
22:59:12		inline-script	http://myradiostream.com/embed/free.php?s=KJAJ&btnstyle=default
22:59:12		font	http://fonts.gstatic.com/s/opensans/v15/mem5YaGs126MiZpBA-UN_r8OUuhp.woff2
22:59:12		font	http://fonts.gstatic.com/s/opensans/v15/mem5YaGs126MiZpBA-UN7rgOUuhp.woff2
22:59:12		font	http://kjaj.org/wp-content/themes/Extra/fonts/ET-Extra.woff
22:59:12		font	http://fonts.gstatic.com/s/opensans/v15/mem8YaGs126MiZpBA-UFVZ0b.woff2
22:59:12		font	http://fonts.gstatic.com/s/opensans/v15/mem5YaGs126MiZpBA-UNirkOUuhp.woff2
22:59:12		frame	http://myradiostream.com/embed/free.php?s=KJAJ&btnstyle=default
22:59:12	lljsecoin.com^	script	https://load.**jsecoin.com/**load/12060/myradiostream.com/optional5uIID/0/
22:59:11		script	http://kjaj.org/wp-includes/js/mediaelement/wp-mediaelement.min.js?ver=4.9.4
22:59:11		script	http://kjaj.org/wp-includes/js/mediaelement/mediaelement-migrate.min.js?ver=4.9.4
22:59:11		script	http://kjaj.org/wp-includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.6-78496d1
22:59:11		script	http://kjaj.org/wp-includes/js/wp-embed.min.js?ver=4.9.4
22:59:11		script	http://maps.googleapis.com/maps/api/js?key&ver=2.0.104#038;callback=initMap
22:59:11		script	http://kjaj.org/wp-content/plugins/divi-builder/core/admin/js/common.js?ver=3.0.105
22:59:11		script	http://kjaj.org/wp-includes/js/masonry.min.js?ver=3.3.2
22:59:11		script	http://kjaj.org/wp-content/themes/Extra/scripts/scripts.min.js?ver=2.0.104
22:59:11		css	http://kjaj.org/wp-includes/js/mediaelement/wp-mediaelement.min.css?ver=4.9.4
22:59:11		css	http://kjaj.org/wp-includes/js/mediaelement/mediaelementplayer-legacy.min.css?ver=4.2.6-78496d1
22:59:11		image	http://kjaj.org/wp-content/themes/Extra/images/pagination-loading.gif
22:59:11		image	http://kjaj.org/wp-content/uploads/2017/02/IMG_1745.jpg
22:59:11		image	http://kjaj.org/wp-content/uploads/2017/03/Solar-Garden-Shed.jpg
22:59:11		image	http://kjaj.org/wp-content/uploads/2017/03/Science.jpg
22:59:11		image	http://kjaj.org/wp-content/uploads/2017/05/AdobeStock_47382753-e1494110129850.jpeg
22:59:11		image	http://kjaj.org/wp-content/uploads/2017/03/Global-warming-infographic-shows-key-metrics-that-are-effecting-global-climate-change-and-becoming-a-high-risk-alert-for-the-life-on-the-Earth-1.jpg
22:59:11		image	http://kjaj.org/wp-content/uploads/2017/03/Screen-Shot-2017-03-06-at-9.48.10-AM.png
22:59:11		script	http://myradiostream.com/embed/KJAJ
22:59:11		image	http://kjaj.org/wp-content/uploads/2018/02/591-s-main-closeup.jpg

> On Mar 7, 2018, at 7:27 PM, Mary Geddry <mary@geddry.com> wrote:
>
> Thanks Darlene,
>
> You may be pulling it up from cache. My degree may only be in economics I was a beta tester for Microsoft for almost a decade and have been running my own linux server for several years. Since I suspect the virus originated from the two IP's I mentioned I will work with my own tech guys. None of my other websites have been infected and I would like to keep it that way.
>
> Mary
>
> > On Mar 7, 2018, at 5:51 PM, Darlene Elliott <daeelliott1@gmail.com> wrote:
> >
> > Mary I just visited our website and the banner is still on it.
> >
> > I read the article that you sent also and found this:
> >
> > One thing is clear – the release of JavaScript coin miners for websites was not unnoticed by the bad guys. They immediately began looking for ways to abuse it, and **we expect to see mass infections** switching their attention to crypto-miners instead of traditional types of malicious payloads, and not just on WordPress and Magento.
> >
> > While the cryptocurrency miners for websites is a very new thing, there is nothing new in approaches that hackers use to abuse it. If something can be installed on a web site and monetized, hackers will do it on websites

they compromise. Thus one of the best security practices for webmasters is to monitor integrity of their sites.

For WordPress infections like this, you can use our step-by-step guide on how to identify hack and clean a compromised WordPress site. We also have a similar guide that will help owners of Magento sites.

Travis could be helping you with this since he has a degree in computer programing and understands the language and the operations.

From what I can see what you did to the website did not remove that banner. Is this malware removed from your server.

It just amazes me that we cannot seem to get an organization or cooperation amongst ourselves.

On Wed, Mar 7, 2018 at 8:08 AM, Mary Geddry <mary@geddry.com> wrote:

> Please, Geno, I am not trying to poke at anyone. My server alerted me to excessive cpu usage and I discovered the crypto overlay which, if anyone read the article I forwarded, is known to embed itself and exploit wordpress theme files. Only people with access to the admin panel can infect those files (without even knowing they are doing it), thus I was trying to determine has access because I must isolate the source. Upon review of the log files only two users were on when the usage began to go up.
>
> 1) An android user coming in from Verizon Wireless Network IP number.
> 2) A Window NT user on a Charter IP number (given almost no one uses NT anymore I am guessing this is the station computer).
>
> One or both of these users is very likely infected with this crypto virus. I'm not accusing anyone of anything or poking at anybody. Just trying to solve the problem and keep the board informed.
>
> Mary
>
>> On Mar 6, 2018, at 8:34 PM, Dr Gene Landrum <quantumcafecoos97420@gmail.com> wrote:
>>
>> In my opinion, yes I have one: Reading e-mails between Mary and Travis is very interesting especially when they seem, in a somewhat polite way, poke each other! I refuse to take sides, however, if other BOD Member's want to take a stance I'm willing to review your opinions on the subjects being discussed between these two BOD members. 2018 Geno.
>>
>> On Tue, Mar 6, 2018 at 12:12 PM, Mary Geddry <mary@geddry.com> wrote:
>>> If you login with your KJAJweb account you will see that you can still edit the programming page.
>>>
>>> Mary
>>>
>>>> On Mar 6, 2018, at 12:06 PM, Travis Hayer <travhayer@gmail.com> wrote:
>>>>
>>>> I created the user KJAJweb so I wouldn't have to keep asking you for your password every time I forgot/mislpaced it.
>>>>
>>>> If, as you say, it has always been your responsibility to maintain the website, then when had you planned to start doing that? ...why did you keep giving me your password? ...and why would you tell me I needed to learn Wordpress?
>>>>
>>>> The website was more user-friendly than it had ever been and certainly more user friendly than it is now.
>>>>
>>>> I understand what it's like to have several other projects in progress and small measured amounts of time to dedicate to KJAJ, but in the few instances that you found time to become involved with technical operations, you have

repeatedly cost me more of my time.

If you can't find time to help us with KJAJ, could you at least stop hindering us?

-Travis

On Tue, Mar 6, 2018 at 9:16 AM, Mary Geddry <mary@geddry.com> wrote:

> Excuse me, but my understanding is that the website has always been my responsibility to maintain. The site resides on my server along with several other websites that I host and leaving a virus on the front page is in itself very destructive. The virus may have originated from a user's own computer. There is a user account (KJAJweb) which I assume Travis created, if not, then who else has access to the site? The only person I gave admin privileges to is Travis. The KJAJweb account now has "editor" privileges which DO allow updates to the programming page and blog posts. KJAJweb has an email account linked to KJAJweb@gmail.com. If this is not an account setup by Travis then I will delete it and create a new account specifically for Travis.
>
> As I said below, the site will look a bit rough for a couple of days but then be fully functional again. Take a look at kbog.org for an example of what is more appropriate for a radio station.
>
> Thanks,
>
> Mary
>
>> On Mar 6, 2018, at 8:45 AM, Travis Hayer <travhayer@gmail.com> wrote:
>>
>> I spent several weeks learning Wordpress and making improvements to our website so it was easier for our listeners to use.
>>
>> When you chose Wordpress as our web design platform, I told you that I didn't have any experience with it. I asked that if I was going to be responsible for maintaining our website, that you choose something that I already knew how to use. You refused to take that into consideration and responded, "You'll just have to learn." Well I learned how to clean up the sample website that you set up and later abandoned. I found a free service to stream our audio to the internet. I replaced the picture of downtown coos bay with one of our own facility. I removed the videos of some other city that you left on there. I also removed outdated and unrelated information and found a way to organize the podcasts into groups so listeners could easily find what they were looking for. When you were upset that you couldn't tell when each show started, I created a schedule and I update it each week. I have received positive feedback about the changes I made, including a compliment from a former board member who remembers how confusing and awkward the website was before.
>>
>> I saw the pop-up ad for JSEcoin, and I thought it was some online fundraiser you were working with. But the pop-up was far less disruptive than what you have done to our website. The changes you made yesterday have destroyed countless hours of work, and left the website more confusing and less usable. There is now no way to listen to our station on our website. The paragaph about Rob Rioux is repeated 3 times, and he's not even on the air now. And I am not even able to update the program schedule.
>>
>> If you don't have time to research it right now, can you at least restore the website to what it was a couple days ago? We can find out how to remove the pop-up ad in a less destructive way.
>>
>> -Travis
>>
>> On Mon, Mar 5, 2018 at 8:07 PM, Mary Geddry <mary@geddry.com> wrote:
>>
>>> Good Evening,
>>>
>>> Does anyone know who else besides myself and Travis have access to our website? As you can see from the screenshot below our site has been compromised by an overlay for cryptocurrency which will not only draw traffic away from our site but is effectively a free advertisement on our non-commercial website.
>>>
>>> For sometime I have wanted to change the theme to something more suitable to our needs. The easiest way to eliminate this intrusion is to change the theme immediately but since I am in the middle of building two websites for paying customers we may look a little rough for a few days until I can really dig in. For security's sake I have downgraded the only other user account from admin to editor to prevent this happening. Any editor can still access pages or create blog posts but will have no access to the themes or plugins. This is the first time in 15 years I have had a wordpress site compromised this way. If anyone wants a user account let me know and I can create one but until I have time to check the log files the fewer users the better.
>>>
>>> Thanks,
>>>
>>> Mary
>>>
>>> <Screen Shot 2018-03-05 at 5.38.41 AM.png>

--
Darlene

"If you obey all the rules, you miss all the fun"
Katherine Hepburn