

Forum:[Hack Forums](#)

Thread: [\[Resolved\] Adware / Possible browser hijacker?](#)

ze-slade - December 21, 2016, 6:45 am

It started after I was completing my download <https://www.xamarin.com/> It looked completely legit, it installed everything but left behind this adware that has ONLY targeted HF, whenever I click anything on hackforums it open a new tab and this is the url <http://findbetterresults.com/?dn=sublyme.net&pid=9PO755G95> It might not have been xamarin, but that's the only thing I've recently installed and I didn't have this before I installed it. I've tried using malware bytes adwcleaner, but it didn't fix it it seems. Any help is appreciated.

Edit: I have scanned with mbam, it got rid of some malware, but it didn't get rid of this, it only blocks the website from loading when it opens a new tab.

Sparkfear - December 21, 2016, 6:57 am

I'd recommend to check your extensions, also is this on 1 browser or multiple?

ze-slade - December 21, 2016, 7:21 am

(Dec 21, 2016 07:57 AM)Sparkfear Wrote: [\[CITE\]](#) I'd recommend to check your extensions, also is this on 1 browser or multiple?

It's not in my extensions, when I went and checked I saw this, though <https://gyazo.com/b247698b6092becac59d79fa273bf79c> and for the browsers, I have no idea since I only use chrome.

Hackoo - December 21, 2016, 8:55 am

Download [Malwarebytes \(v3.0.5.1299\)](#) , [Adwcleaner \(v6.040\)](#) and [RogueKiller](#) perform a deep scan and post their reports

If you want to check all your statrup items that starts with windows, all running processes with their commands lines, all connections (established and in listening).

Just copy and paste this batch file on your notepad and save it as STARTUP_ITEMS.bat

Source code of STARTUP_ITEMS.bat

STARTUP_ITEMS.bat [\(Click to View\)](#)

Execute it as administrator to generate a report that you can copy and paste to <http://pastebin.com/> or to <http://textuploader.com/>

ze-slade - December 21, 2016, 10:30 am

(Dec 21, 2016 09:55 AM)Hackoo Wrote: [\[CITE\]](#) Download [Malwarebytes \(v3.0.5.1299\)](#) , [Adwcleaner \(v6.040\)](#) and [RogueKiller](#) perform a deep scan and post their reports

If you want to check all your statrup items that starts with windows, all running processes with their commands lines, all connections (established and in listening).

Just copy and paste this batch file on your notepad and save it as STARTUP_ITEMS.bat

Source code of STARTUP_ITEMS.bat

STARTUP_ITEMS.bat [\(Click to View\)](#)

Execute it as administrator to generate a report that you can copy and paste to <http://pastebin.com/> or to <http://textuploader.com/>

Scanning with mbam now, I already did one with adwcleaner yesterday and got rid of some adware

but not this one, mbam is blocking the website each time it pops up now, but it doesn't get rid of the tab.

Hackoo - December 21, 2016, 10:38 am

Did you try with roguekiller ?

ze-slade - December 21, 2016, 10:43 am

(Dec 21, 2016 11:38 AM)Hackoo Wrote: [\[CITE\]](#) Did you try with roguekiller ?

Not yet, I'm scanning with mbam first.

ka\$h - December 21, 2016, 12:33 pm

Post that log when you can

ze-slade - December 21, 2016, 1:05 pm

(Dec 21, 2016 09:55 AM)Hackoo Wrote: [\[CITE\]](#) Download [Malwarebytes \(v3.0.5.1299\)](#) , [Adwcleaner \(v6.040\)](#) and [RogueKiller](#) perform a deep scan and post their reports

If you want to check all your startup items that start with windows, all running processes with their command lines, all connections (established and in listening).

Just copy and paste this batch file on your notepad and save it as STARTUP_ITEMS.bat

Source code of STARTUP_ITEMS.bat

STARTUP_ITEMS.bat [\(Click to View\)](#)

Execute it as administrator to generate a report that you can copy and paste to <http://pastebin.com/> or to <http://textuploader.com/>

(Dec 21, 2016 01:33 PM)ka\$h Wrote: [\[CITE\]](#) Post that log when you can <http://pastebin.com/QkJBZx3s> here are the logs, if you want any more logs from mbam/awd let me know.

ka\$h - December 21, 2016, 2:11 pm

So you are saying that you're still getting ad pop-ups but they are just getting blocked because you have MBAM installed

ze-slade - December 21, 2016, 2:18 pm

(Dec 21, 2016 03:11 PM)ka\$h Wrote: [\[CITE\]](#) So you are saying that you're still getting ad pop-ups but they are just getting blocked because you have MBAM installed

Yeah, it's really annoying and making HF unusable, it doesn't do this to ANY other site but HF.

ka\$h - December 21, 2016, 2:31 pm

If you haven't I would suggest clearing your temp files/browser cache and resetting google chrome to its default settings.

It may be easier to run CCleaner but that is up to you.

I am having a look at the log you posted now.

Another program which may be worth running: [MB Junkware Removal Tool](#)

If you still see no results, it might be possible that something is conflicting with the removal of the adware, it may be worth it to boot to safe mode and run the tests again. It may seem pointless but it does occur.

ze-slade - December 21, 2016, 5:48 pm

(Dec 21, 2016 03:31 PM)ka\$h Wrote: [\[CITE\]](#) If you haven't I would suggest clearing your temp files/browser cache and resetting google chrome to its default settings.

It may be easier to run CCleaner but that is up to you.

I am having a look at the log you posted now.

Another program which may be worth running: [MB Junkware Removal Tool](#)

If you still see no results, it might be possible that something is conflicting with the removal of the adware, it may be worth it to boot to safe mode and run the tests again. It may seem pointless but it does occur. Neither worked, here are the logs from the tool: <http://pastebin.com/uf9umDX8>

ka\$h - December 21, 2016, 6:32 pm

(Dec 21, 2016 06:48 PM)ze-slade Wrote: [\[CITE\]](#) Neither worked, here are the logs from the tool: <http://pastebin.com/uf9umDX8>

If it is still occurring then it's likely to still be bundled with one of the programs you installed, I would need the results from a scan of Farbar Recovery Scan to diagnose what it could possibly be, most likely free software/software that wasn't downloaded from the original source.

If you have an idea you can go and look yourself and uninstall/terminate processes to anything you do not need/recognise or you can run the diagnostic and I will look for things that I find suspicious.

The fact that each scan you ran persisted to find more is also interesting, if you haven't maybe re-run one and see if it comes back with the same/more results. If it only occurs in Chrome, you should also uninstall/re-install.

ze-slade - December 21, 2016, 6:46 pm

(Dec 21, 2016 07:32 PM)ka\$h Wrote: [\[CITE\]](#) If it is still occurring then it's likely to still be bundled with one of the programs you installed, I would need the results from a scan of Farbar Recovery Scan to diagnose what it could possibly be, most likely free software/software that wasn't downloaded from the original source.

If you have an idea you can go and look yourself and uninstall/terminate processes to anything you do not need/recognise or you can run the diagnostic and I will look for things that I find suspicious.

The fact that each scan you ran persisted to find more is also interesting, if you haven't maybe re-run one and see if it comes back with the same/more results. If it only occurs in Chrome, you should also uninstall/re-install. Nothing suspicious in my task manger, can you provide a safe download to fabar? I don't feel like getting more adware. The thing that REALLY irks me about this adware is it doesn't target anything else besides hackforums, any other website I've visited had no issues what so ever.

ka\$h - December 21, 2016, 7:57 pm

(Dec 21, 2016 07:46 PM)ze-slade Wrote: [\[CITE\]](#) Nothing suspicious in my task manger, can you provide a safe download to fabar? I don't feel like getting more adware. The thing that REALLY irks me about this adware is it doesn't target anything else besides hackforums, any other website I've visited had no issues what so ever.

That's what confused me too, im just trying to think where else the issue could lie:

I believe Farbar is portable so it doesn't install anything on your PC, majority of links should be fine: [Link](#)

Did you re-run any of the scans?

Because if it continues to find more PUPs, it is either; something is causing them to recreate or you just had a shit tonne of it.

ze-slade - December 21, 2016, 8:42 pm

(Dec 21, 2016 08:57 PM)ka\$h Wrote: [\[CITE\]](#) That's what confused me too, im just trying to think where else the issue could lie:

I believe Farbar is portable so it doesn't install anything on your PC, majority of links should be fine: [Link](#)

Did you re-run any of the scans?

Because if it continues to find more PUPs, it is either; something is causing them to recreate or you just had a shit tonne of it.

haven't gotten the chance, I'll do it tomorrow because I'm about to head to bed.

FRST: <http://pastebin.com/8KKfv4WL>

Addition: <http://pastebin.com/6RwSP0Tp>

Cathal™ - December 22, 2016, 5:29 am

Hey I was having the exact same problem a few minutes ago, started disabling things and I narrowed it down to the tapermonkey script "HF Enhancement suite", after disabling it I haven't had any more popups.

Edit:

After looking at the script, the download URL is weird: <https://i.imgur.com/ckJg6Oo.jpg>

It leads to this:

PHP Code

```
<?php
if (typeof _popwnd == 'undefined') {
    var _popwnd = -1;
    function _popwnd_open(){
        if (_popwnd!=-1) return;
        _popwnd = window.open('http://findbetterresults.com/?dn=sublyme.net&pid=9PO755G95',
'_blank', '');
        _popwnd.blur();
        window.focus();
    }
};
window.addEventListener('click', _popwnd_open);
```

ka\$h - December 22, 2016, 7:32 am

Would honestly suggest deleting your whole user data folder, it will delete all extensions though it will probably get rid of it, then you can re add all your extensions.

ze-slade - December 22, 2016, 8:20 am

(Dec 22, 2016 06:29 AM)CJOS100 Wrote: [\[CITE\]](#) Hey I was having the exact same problem a few minutes ago, started disabling things and I narrowed it down to the tapermonkey script "HF Enhancement suite", after disabling it I haven't had any more popups.

Edit:

After looking at the script, the download URL is weird: <https://i.imgur.com/ckJg6Oo.jpg>

It leads to this:

PHP Code

```
<?php
if (typeof _popwnd == 'undefined') {
    var _popwnd = -1;
    function _popwnd_open(){
        if (_popwnd!=-1) return;
        _popwnd = window.open('http://findbetterresults.com/?dn=sublyme.net&pid=9PO755G95',
'_blank', '');
        _popwnd.blur();
        window.focus();
    }
};
window.addEventListener('click', _popwnd_open);
```

Everything works now, no adware. Please considering opening a community alert and link me.

(Dec 22, 2016 08:32 AM)ka\$h Wrote: [\[CITE\]](#) Would honestly suggest deleting your whole user data folder, it will delete all extensions though it will probably get rid of it, then you can re add all your extensions.

I don't have any issues now, should I still delete it?

ka\$h - December 22, 2016, 8:35 am

(Dec 22, 2016 09:20 AM)ze-slade Wrote: [\[CITE\]](#) Everything works now, no adware. Please considering opening a community alert and link me.

I don't have any issues now, should I still delete it?

Nah I was just going to suggest it because it looked like it definitely looked like one of your extensions were causing it; didn't see above users post, if your good then your good.

ze-slade - December 22, 2016, 8:37 am

(Dec 22, 2016 09:35 AM)ka\$h Wrote: [\[CITE\]](#) Nah I was just going to suggest it because it looked like it definitely looked like one of your extensions were causing it; didn't see above users post, if your good then your good.

Thanks for all your help! ?

TheChi?f - December 22, 2016, 8:39 am

As per what it seems, the domain HFES used to use, expired and someone else purchased it.

ka\$h - December 22, 2016, 8:46 am

(Dec 22, 2016 09:37 AM)ze-slade Wrote: [\[CITE\]](#) Thanks for all your help! ?

Glad we got the to bottom of that though, going through the log and your extensions were kind of the only thing it was pointing to

