

Op EvilTraffic - Thousands of compromised sites involved in a malvertising campaign

By Pierluigi Paganini

Published: 2018-01-22 · Archived: 2026-04-02 12:03:01 UTC

Op EvilTraffic CSE CybSec ZLAB Malware Analysis Report – Exclusive, tens of thousands of compromised sites involved in a new massive malvertising campaign



Cyber Security Strategists

Malware experts at CSE Cybsec uncovered a massive malvertising campaign dubbed EvilTraffic leveraging tens of thousands compromised websites. Crooks exploited some CMS vulnerabilities to upload and execute arbitrary PHP pages used to generate revenues via advertising.

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 huge malvertising campaign was dubbed EvilTraffic

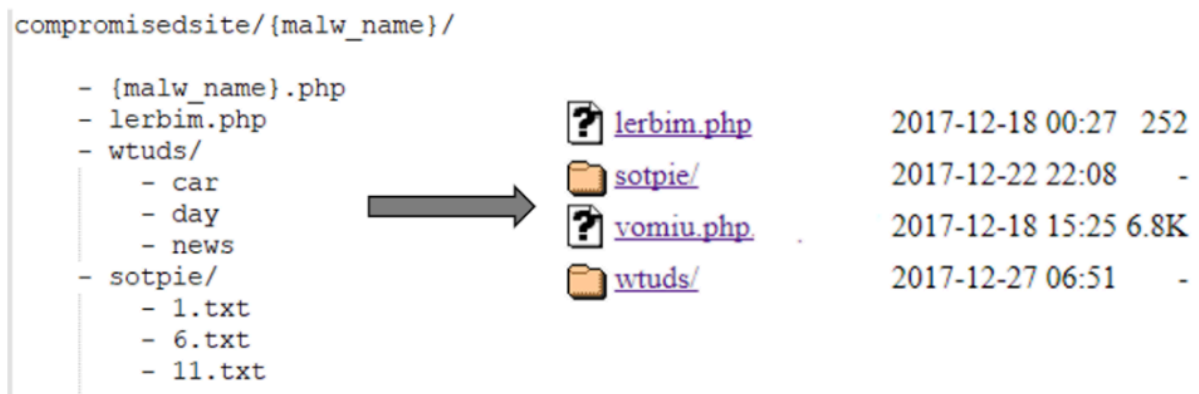
The compromised websites involved in the EvilTraffic campaign run various versions of the popular WordPress CMS. Once a website has been compromised, attackers will upload a “zip” file containing all the malicious files. Despite the “zip” file has different name for each infection, when it is uncompressed, 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”, “slvktly”).

Under this folder there are:

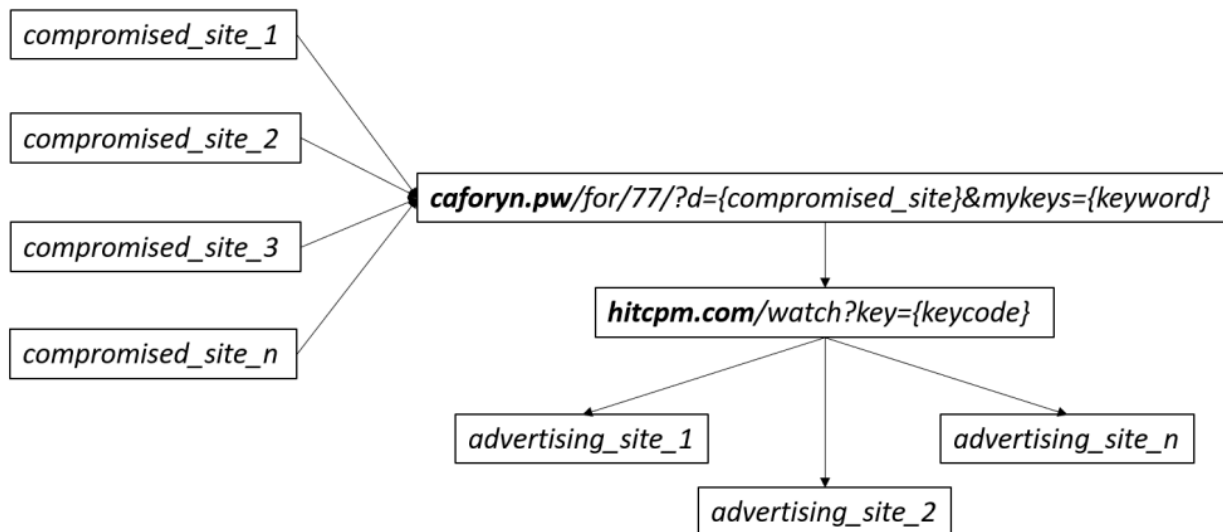
- a php file, called “lerbim.php”;
- a php file, that has the same name of the parent dir; it has initially “.suspected” extension and only in a second time, using “lerbim.php” file, it would be changed in “.php” file;
- two directories, called “wtuds” and “sotpie”, containing a series of files.

An example of this structure is shown in the following figure:



The main purpose of the “malware” used in the EvilTraffic campaign 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 a dispatcher to different sites registered to this revenue chain.



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).

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

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}”.

Researchers from CSE CybSec ZLab discovered roughly 18.100 compromised websites.

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

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

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

The analysis of the traffic shows an exponential increase in the traffic during October 2017.

Experts discovered that crooks behind the Operation EvilTraffic used a malicious software to hijack traffic, it acts as brows a browser hijacker. The malware 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.

Further technical details about this campaign, including IoCs, are available in the report titled:

[“Tens of thousands of compromised web sites involved in new massive malvertising campaign”](#)

You can download the full ZLAB Malware Analysis Report at the following URL:

http://csecybsec.com/download/zlab/20180121_CSE_Massive_Malvertising_Report.pdf



[adrotate banner="9"]

[adrotate banner="12"]

[Pierluigi Paganini](#)

([Security Affairs](#) – malvertising campaign, EvilTraffic)

[adrotate banner="5"]

[adrotate banner="13"]

Source: <http://securityaffairs.co/wordpress/68059/cyber-crime/eviltraffic-malvertising-campaign.html>