

[REVS] Web Server Botnets and Server Farms as Attack Platforms

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00030.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 12 Feb 2007 17:05:02 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Web Server Botnets and Server Farms as Attack Platforms

SUMMARY

This is an article on cross platform web server malware and their massive use as botnets, spam bots and generally as attack platforms.

DETAILS

In the February edition of the <<http://www.virusbtn.com/>> Virus Bulletin magazine Kfir Damari, Noam Rathaus and Gadi Evron of <<http://www.beyondsecurity.com/>> Beyond Security) wrote an article on cross platform web server malware and their massive use as botnets, spam bots and generally as attack platforms.

Web security papers deal mostly with secure coding and application security. In this paper they describe how these are taken to the next level with live attacks and operational problems service providers deal with daily.

They discuss how these attacks work using (mainly) file inclusion vulnerabilities (RFI) and (mainly) PHP shells. Further, they discuss how ISPs and hosting farms suffer tremendously from

this, and what can be done to combat the threat.

Malware is often built to operate within a certain OS environment. Web server malware is completely cross-platform (as long as a web daemon which supports scripting can be found such as IIS, Apache, etc.). These malware attack the web application first, and only then further compromise takes place platform by platform, using the web server's privileges.

Most web servers are being compromised by these attacks as a result of an insecure web application written in PHP, although attacks for other scripting languages such as Perl and ASP are also in-the-wild.

The main reason for this is that many different PHP applications are available online, and often freely as open source, which makes them a popular selection for use on many web sites. Another reason for the popularity of attacks against PHP applications is that writing securely in PHP is very difficult, which makes most of these PHP applications vulnerable to multiple attacks, with hundreds of new vulnerabilities released publicly every month.

While in the past botnets used to be composed of mainly broadband end users running Windows, today we can see more and more server botnets we can refer to as "IIS botnets" or "Linux botnets" as a direct result of these attacks.

One of the conclusions they reached was that although the technologies used are not new (RFI, PHP shells, etc.) the sheer scale of the problem is what's interesting.

In their research as detailed in the Virus Bulletin article they recognize that vulnerabilities such as file inclusion, as simple as they may be, are equivalent to remote code execution in effect.

Although escalation wars, which are reactive in nature, are a solution the industry hates and is stuck with on botnets, spam, fraud and many other fronts, this front of web server attacks stands completely unopposed and controlled by the bad guys. In their research they detail how over-time, when aggregated, most attacks come from the same IP addresses without these ever getting blocked.

ISPs and hosting farms selling low-cost hosting services can not cope with this threat, especially where an attack against one user running such an application can compromise a server running 3000 other sites.

Another issue discussed was <http://blogs.securiteam.com/index.php/archives/792> the formation of the <http://www.webhoneynet.net/> Web Honeynet Task Force (renamed from the Web Honeynet Project to avoid confusion with the honeynet project).

The paper can be found here: http://www.beyondsecurity.com/whitepapers/GadiEvron_VBFeb07.pdf Web

[REVS] Web Server Botnets and Server Farms as Attack Platforms

Server Botnets and Server Farms as Attack Platforms (
<<http://www.virusbtn.com/>> all rights reserved to Virus Bulletin)

ADDITIONAL INFORMATION

The information has been provided by <<http://www.beyondsecurity.com/>>
Beyond Security.

The original paper can be found at:
<http://www.beyondsecurity.com/whitepapers/GadiEvron_VBFeb07.pdf>
http://www.beyondsecurity.com/whitepapers/GadiEvron_VBFeb07.pdf

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential,
loss of business profits or special damages.