Category:

Web

Name:

Combat bogus EC sites – 2.

Message:

Now we believe you can get the contacted server address in the previous challenge “Combat bogus EC sites – 1”. This malware is used in attack campaigns known as “Japanese Keyword Hack” or “Blackhat SEO Spamming”. You can access the server to get the flag. We need your cooperation to make the blocklist!

Warning: DO NOT exploit vulnerabilities of the C2 server because this is not a PWN challenge.

Objective:

You can learn how you monitor malware C2 server.

Instructions:

The last sentence of the challenge message implies you need to collect malicious sites from the malware C2 server. You need to analyze the decoded PHP malware to get necessary parameters for talking with the C2 server as listed below:

- The c2-domain “service.myshop.trend”, encoded in $xmlname
- “web” : defaced website FQDN
- “zz”: 0 or 1 to express the access is from search engine bots
- “uri” : requested uri with URL-encoded such as “%2Fsitemap%2Exml”
- “urlshang”: URL-encoded referrer such as “https%3A%2F%2Fwww%2Egoogle%2Ecom%2F”
- “http”: “http” or “https”
- “lang”: URL-encoded HTTP_ACCEPT_LANGUAGE

If you know “Japanese Keyword Hack” very well, you can notice you should get sitemap and the contents.

You need to access /indexnew.php with necessary parameters to get sitemap as follows:

- “zz” = 1
- “uri” = “%2Fsitemap%2Exml”

Then you will get “sitemap.xml” which has around 2000 URLs. You need to check the URLs by calling

the server with the parameters.

- “zz” = 0
- “uri” = a URI (path only, starting with “/”) taken from sitemap, with URL-encode.
- “lang” must include “ja”, as this is targeting Japanese.
- “urlshang” must include google, bing or yahoo

You will get many htmls to transfer “bogusec.example.com”, but this is dummy page so please ignore with patience. When you access to get “/200095etidm62z.htm”, you will get flag “CSG_FLAG{H4ck3dCMS}”.

References:

Documents

https://web.dev/articles/fix-the-japanese-keyword-hack

https://blog.sucuri.net/2020/11/code-comments-reveal-scp-173-malware.html

https://www.trendmicro.com/ja_jp/research/22/j/seo-poisoning.html (In Japanese)

Tools