Terror EK via Malvertising delivers Tofsee Spambot

Published: 2017-03-24 · Archived: 2026-04-05 20:15:41 UTC

Summary:

This was a great find, Terror EK in the wild from malvertising. The landing page appeared to be in the compromised site itself and was not loaded from an iframe, etc. The site just displayed jibberish (Lorem Ipsum). The EK used three Flash files, attempted a Silverlight exploit and triggered several interesting ET signatures. There was also almost no obfuscation of the code as well.

The payload was Tofsee and a thanks goes to @Antelox for confirming it. Tofsee is a spambot known to send spam emails. It has been dropped by Rig EK in the past. I did not see much email traffic however I was using a proxy which may have caused some traffic to not be logged.

Anyway this is a great find and I hope you can gain a lot of information from it.

Background Information:

A few articles and samples on Terror exploit kit:

https://www.trustwave.com/Resources/SpiderLabs-Blog/Terror-Exploit-Kit–More-like-Error-Exploit-Kit/

http://www.broadanalysis.com/2016/06/13/rig-exploit-kit-from-5-200-55-156-sends-tofsee-spambot/

Article on Tofsee:

https://www.cert.pl/en/news/single/tofsee-en/

Downloads

- 230317TerrorTofsee-> Contains pcapng, payloads and flash files in password protected zip.

Notable Details:

- 52.29.235.194 – eu4.echo-ice.com- Part of a malvertising chain
- 173.208.245.114 – paydayloanservice.net – Part of a malvertising chain
- 128.199.233.119 – Terror EK Traffic
- 103.48.6.14– Tofsee Post Infection
- 111.121.193.242 – Tofsee Post Infection
- Payload was Tofsee Spambot (rad6AC11.tmp.exe created kxuepssx.exe)

Details of infection chain:

(click to enlarge!)

Full Details:

Source: https://zerophagemalware.com/2017/03/24/terror-ek-delivers-tofsee-spambot/