# Terror EK via Malvertising delivers Tofsee Spambot


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

zerophage March 24, 2017

## 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.

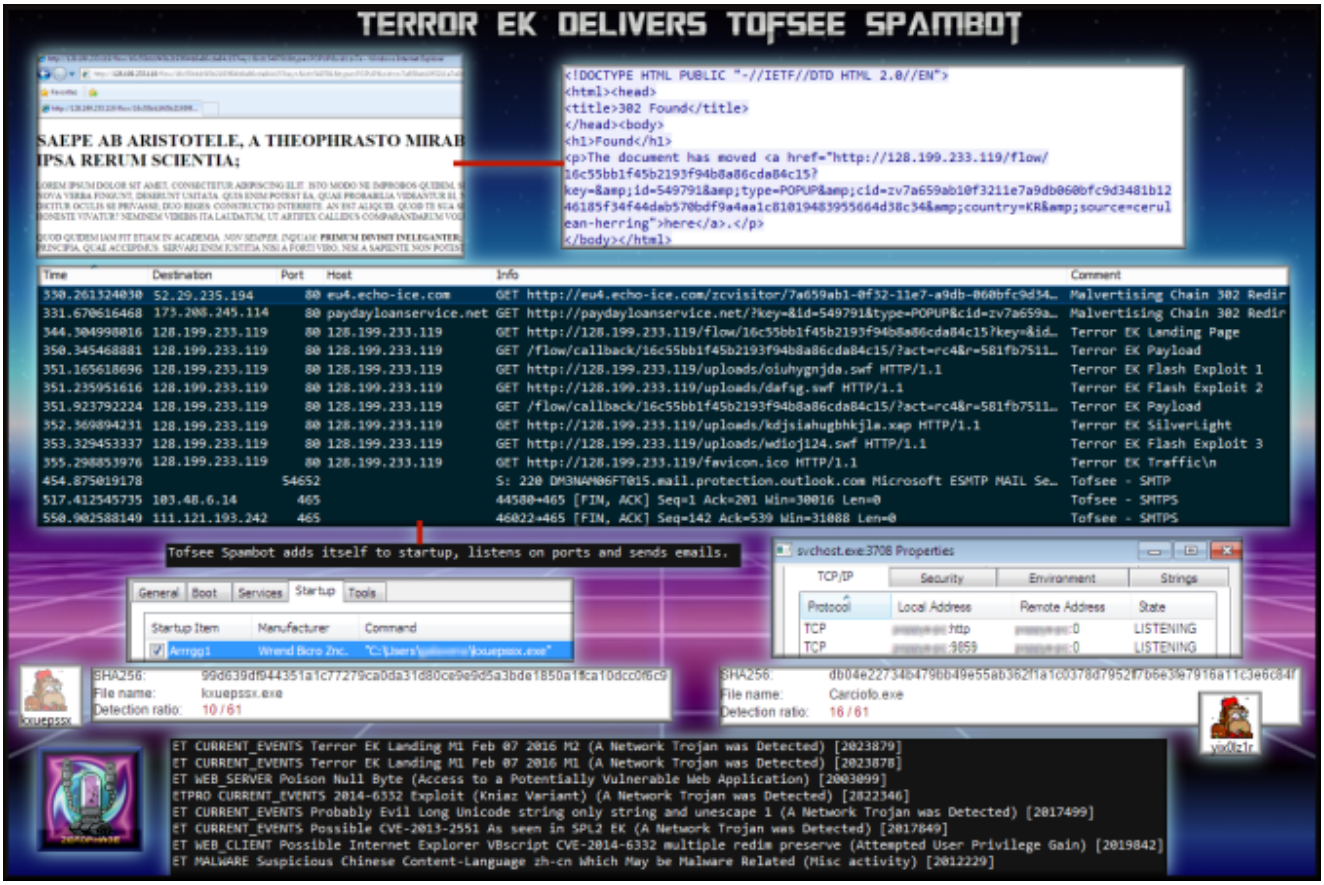
## Notable Details:

- 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!)



Terror EK via malvertising drops Tofsee spambot. I have added the IP addresses in here manually. The PCAP uses a proxy IP.

## Full Details:

- The malvertising chain let to a website that contained jibberish but also hosted the entire landing page with little to no attempt to obfuscate it. Below is a snippet:

```
<P>CUR, NISI QUOD TURPIS ORATIO EST? PHILOSOPHI AUTEM IN SUIS LECTULIS PLERUMQUE MORIUNTUR. NAM QUIBUS REBUS EFFICIUNTUR VOLUPTATES, EA
NON SUNT IN POTESTATE SAPIENTIS. AN HOC USQUE QUAQUE, ALITER IN VITA? PRAETEREO MULTOS, IN BIS DOCTUM HOMINEM ET SUAVEM, HIERONYMUM, QU
IAM CUR PERIPATETICUM APPELLEM NESCIO. QUAE DILIGENTISSIME CONTRA ARISTONEM DICUNTUR A CHRYIPPO. <B>QUALEM IGITUR HOMINEM NATURA
INCHOAVIT?</B> SUMMUS DOLOR PLURES DIES MANERE NON POTEST? SED QUID MINUS PROBANDUM QUAM ESSE ALIQUEM BEATUM NEC SATIS BEATUM? ERGO ILL
INTELLEGUNT QUID EPICURUS DICAT, EGO NON INTELLEGO? </P>

<DL>
          <DT><DFN>SI LONGUS, LEVIS.</DFN></DT>
          <DD>MIHI, INQUAM, QUI TE ID IPSUM ROGAVI?</DD>
          <DT><DFN>MAGNA LAUS.</DFN></DT>
          <DD>VERBA TU FINGAS ET EA DICAS, QUAE NON SENTIAS?</DD>
          <DT><DFN>MEMINI VERO, INQUAM;</DFN></DT>
          <DD>ILLE VERO, SI INSIPIENS-QUO CERTE, QUONIAM TYRANNUS -, NUMQUAM BEATUS;</DD>
</DL>

                    <html dir='ltr' lang='en'><head><meta http-equiv='content-type' content='text/html;charset=UTF-8'>
                    </head><body>
                    <script type="text/javascript"><!--
document.write( '<head>\n' );
document.write( '<meta http-equiv=\"X-UA-Compatible\" content=\"IE=EmulateIE8\">\n' );
document.write( '<script language=\"VBScript\">\n' );
document.write( 'dim   gYpp0()\n' );
document.write( 'dim   vti()\n' );
document.write( 'dim   a0\n' );
document.write( 'dim   a1\n' );
document.write( 'dim   info\n' );
document.write( 'dim   a2\n' );
document.write( 'dim   a3\n' );
document.write( 'dim   herrop\n' );
document.write( 'Begin()\n' );
```

- Terror EK uses a variety of exploits and has three different Flash files. The Flash files had not been uploaded to VT before for over a year.

- SHA256: d7919a2c2a03e96200858fe2c8a405af1ae40f0590937f9a1a8b076f1d341c27

| | |
|---|---|
| File name: | dafsg.swf |
| Detection ratio: | 34 / 56 |

- SHA256: 55eea72f4fdf639987fc80789040dc1e98091c4adf8f30aebaba86d15f3aae06

| | |
|---|---|
| File name: | oiuhygnjda.swf |
| Detection ratio: | 27 / 56 |

- SHA256: 6e16ddfcf4c5f557f0f64ee8a4f16741e79dbe29acb43eccab87329116e88b9e

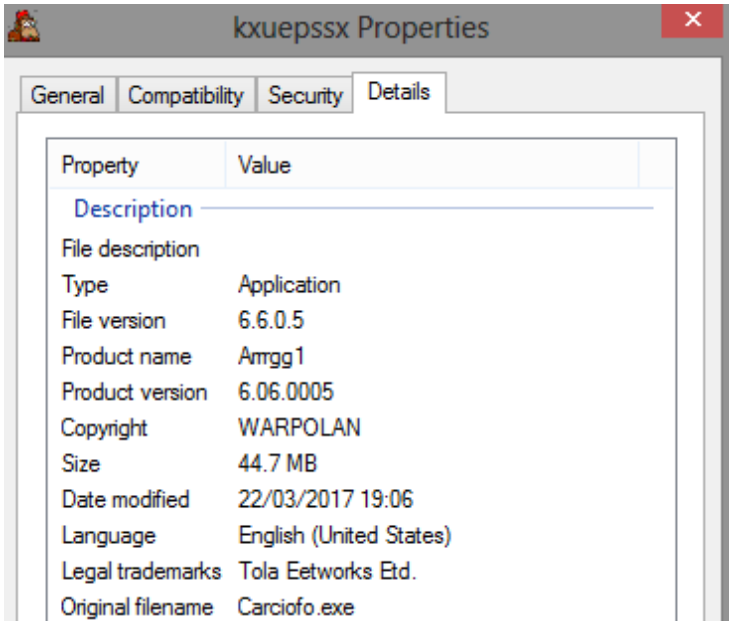
| | |
|---|---|
| File name: | wdioj124.swf |
| Detection ratio: | 21 / 56 |

- The payload was Tofsee, thanks to @Antelox for confirming this. It actually dropped two payloads but they both had the same hash despite one having the old style “rad” naming.

| | |
|---|---|
| SHA256: | db04e22734b479bb49e55ab362f1a1c0378d7952ff7b6e3fe7916a11c3e6c84f |
| File name: | Carciofo.exe |
| Detection ratio: | 16 / 61 |
| Invincea | backdoor.win32.tofsee.f |

- 

| | |
|---|---|
| SHA256: | 99d639df944351a1c77279ca0da31d80ce9e9d5a3bde1850a1ffca10dcc0f6c9 |
| File name: | kxuepssx.exe |
| Detection ratio: | 10 / 61 |
| Invincea | backdoor.win32.tofsee.f |

- Tofsee added itself to startup, listened on random ports and began to send emails.
- 

- ET Signatures

```
ET CURRENT_EVENTS Terror EK Landing M1 Feb 07 2016 M2 (A Network Trojan was Detected) [2023879]
ET CURRENT_EVENTS Terror EK Landing M1 Feb 07 2016 M1 (A Network Trojan was Detected) [2023878]
ET WEB_SERVER Poison Null Byte (Access to a Potentially Vulnerable Web Application) [2003099]
ETPRO CURRENT_EVENTS 2014-6332 Exploit (Kniaz Variant) (A Network Trojan was Detected) [2822346]
ET CURRENT_EVENTS Probably Evil Long Unicode string only string and unescape 1 (A Network Trojan was Detected) [2017499]
ET CURRENT_EVENTS Possible CVE-2013-2551 As seen in SPL2 EK (A Network Trojan was Detected) [2017849]
ET WEB_CLIENT Possible Internet Explorer VBscript CVE-2014-6332 multiple redim preserve (Attempted User Privilege Gain) [2019842]
ET MALWARE Suspicious Chinese Content-Language zh-cn Which May be Malware Related (Misc activity) [2012229]
```