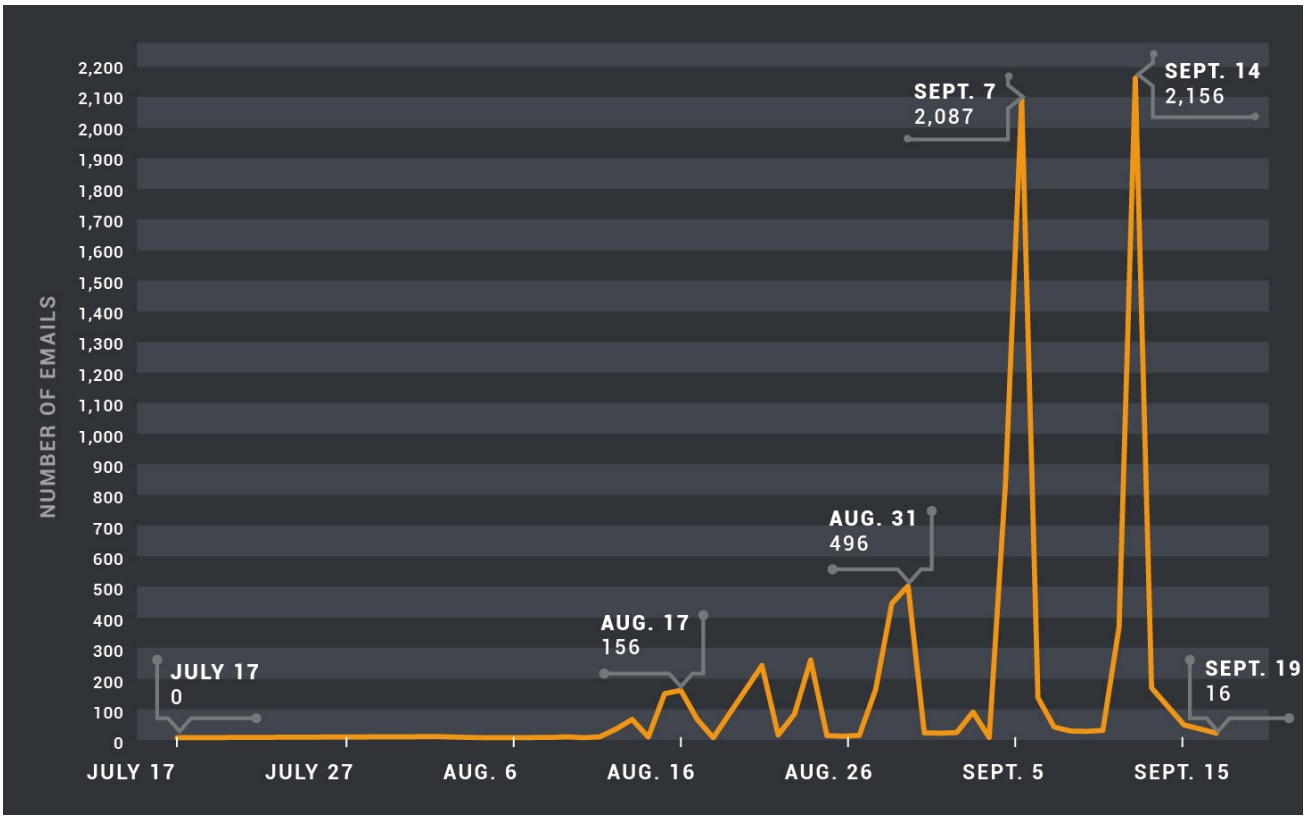
Want Tofsee My Pictures? A Botnet Gets Aggressive

blog.talosintelligence.com/tofsee-spam/

Edmund Brumaghin September 29, 2016



By Edmund Brumaghin

Thursday, September 29, 2016 11:09

This post was authored by Edmund Brumaghin

Summary

Tofsee is multi-purpose malware that has been in existence for several years, operating since at least 2013. It features a number of modules that are used to carry out various activities such as sending spam messages, conducting click fraud, mining cryptocurrency, and more. Once infected, systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control.

Earlier this year, Talos published a blog post discussing how the RIG exploit kit was delivering this malware to compromised endpoints using malvertising. Malvertising is a technique commonly used by exploit kits to infect users that browse web sites that are serving compromised advertisements. This activity seemed to disappear in June, however Talos has recently observed a marked increase in the volume and velocity of spam email campaigns containing malicious attachments that are being used to distribute Tofsee.

Tofsee Spam Campaigns

In June 2016, following the disappearance of the Angler exploit kit from the threat landscape, other major exploit kits began to shift to different payloads. The RIG exploit kit moved from distributing Tofsee to other payloads, possibly because distributing them was more attractive to cybercriminals from a monetization standpoint or simply because different actors began using this exploit kit as a distribution mechanism for their malware.

Given the volume of spam messages that infected hosts attempt to distribute, new nodes are quickly added to DNS-based Blackhole Lists (DNSBL) and most of the major email service providers will not accept new message transmissions once this occurs. In order to keep spam levels consistent new nodes must be added constantly. When RIG stopped distributing Tofsee payloads, those responsible for Tofsee switched to alternative distribution methods.

While the Tofsee botnet has been known for sending spam messages, the messages have historically contained links to adult dating and pharmaceutical websites. Starting in August, Talos began to observe a change in the nature of the spam messages being sent by this botnet. The Tofsee spam botnet has begun utilizing malicious attachments that function as malware downloaders. This activity has increased in velocity and volume.

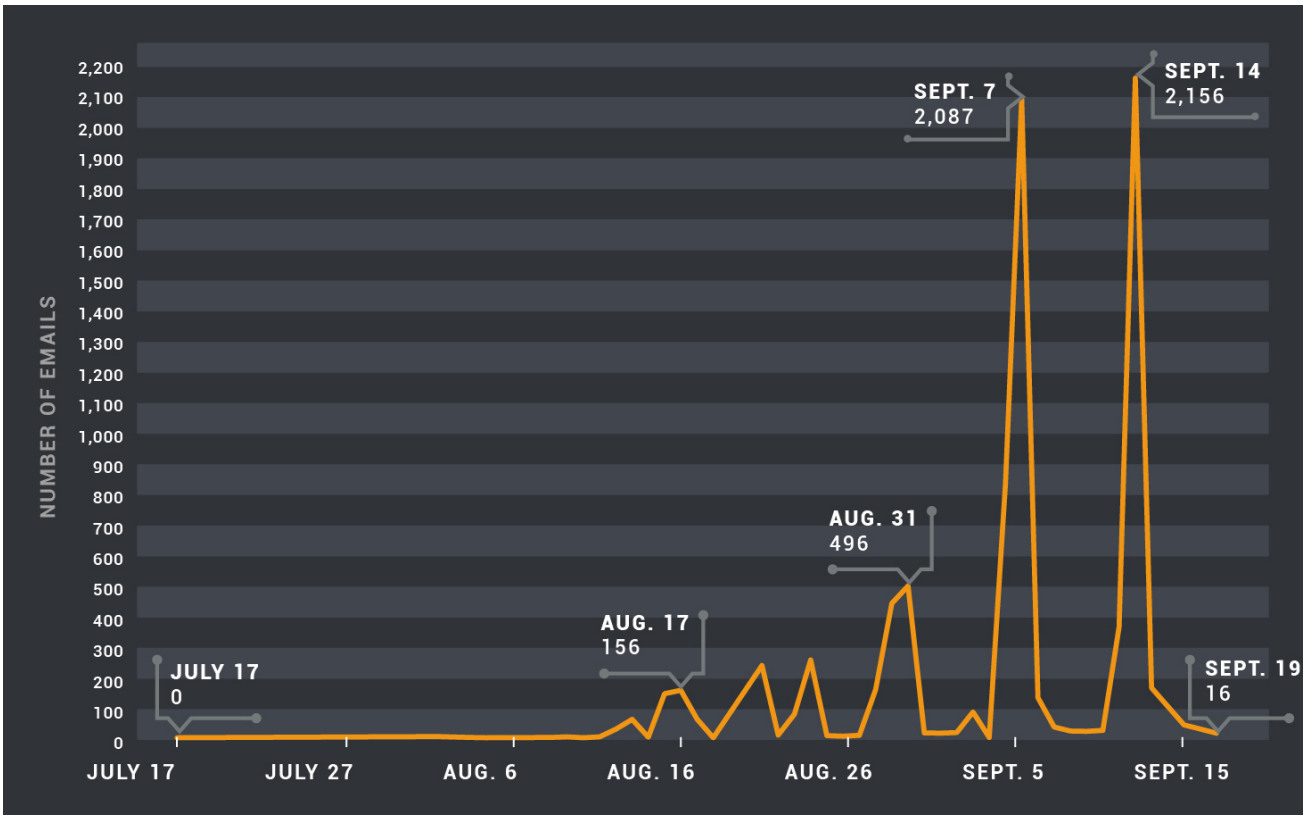


Figure 1: Number of Emails Containing Malware Downloaders

Initial Infection Vector

The initial infection for this variant of Tofsee appears to be accomplished by convincing users to open malicious attachments that are delivered via phishing emails. The phishing emails purport to be from women in Eastern Europe (namely Russia and Ukraine) and the theme of the emails is adult dating. Each email contains slightly different text, however the same format is used across all of the messages Talos analyzed. The messages purport to contain an attached zip archive with pictures of the sender as well as links to a Russian adult dating website. Here is an example of a Tofsee message body:

Excuse me dear = =3D]
Would = you mind to finding a young = and nice girl?
My name = is Dierdre. I am = from Ukraine = !
Have you ever = heard that the = loveliest = girls in the = world live in my = country? Don't even = doubt!
The page is over = there: http://igamrzdh.datingsd&#= 12290;ru

It's my = photo-
3D"Dierdre95"=
I have = much more sexy pics for = you, my love :-) Welcome!

Figure 2: Sample Tofsee Spam Message

Javascript Downloader

The attachment is a zip archive named [Sender First Name]-photos.zip that contains a Javascript file. In all cases analyzed, the filename of the javascript file is a woman's first name. The filename and hash changes across groups of emails with several being sent on any given day. The code in javascript attachment is obfuscated in an attempt to make analysis more difficult.

```
var ubulagsagq5 = new Array("phammage", "13732", "10473", "ing");
var fjotyfevhy = new Array("19473", "te");
var rqehavsy = new Array('us', "12595");
var omefatar2 = new Array("mlugegudynk", "fihabitdun", 599, "20164", "lbasoqnespu");
var ycighanr4 = new Array("Write", "zlomxervoz");

function uxagky() {
    var xzohoqu1 = [];
    xzohoqu1["fcopqavim"] = "zubze";
    xzohoqu1["ecwulwyw"] = "e /";
    return xzohoqu1["ecwulwyw"];
}
var ycwekjokwul3 = new Array("em0", "sqivyndyguw", "18978", "24328", "tyvotelr");
var lubkormow = new Array("MS", "yfofaj");
var nbekyxwak = new Array("13048", "now", "22055");

function waqexo2() {
    var wxutul0 = new Array("ame", "15265", "11240");
    return wxutul0[0];
}
function epyvsajo() {
    var rvyxymre = new Array("el", "uqullutijm", "ufoqjez", "20847");
    return rvyxymre[0];
}
var nbykcodo = new Array("uzysyl", "21746", "ipt", "opribijpif", "14953");

function rpuhhijexf8() {
    var ksittyqi1 = new Array("21685", "16180", "20986", "ltG", "hfewzoram");
    return ksittyqi1[3];
}
var oladgufb0 = new Array("ifmucuryv", "20050", "B.St");
var yjkorgelr = new Array("pisryxnapgyp", "10282", 218);
var ujgadleco = new Array("ydebkeju", "ipt", "19944", "12696", "14924");
var derurmafg1 = new Array("17765", "23278", "TP", "14275");
var ofexypbo = new Array("21070", "ti", "20459");
var punidaqh = new Array("23911", "pwupxabti", "14763", "Adu", "16917");
```

Figure 3: Sample Obfuscated Javascript Downloader

The above Javascript obfuscates a WScript downloader, which is used to retrieve and execute a malicious PE32 executable from an attacker controlled web server. When executed, the downloader retrieves a malicious executable and runs it, infecting the system with Tofsee.

Infection Details

The malware drops a randomly named PE32 executable into the %USERPROFILE% directory.

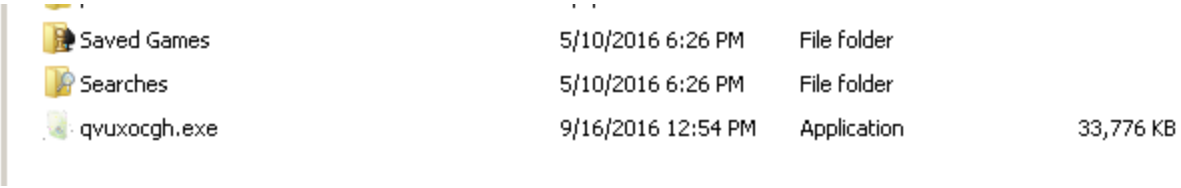


Figure 4: Dropped Tofsee Binary

The dropped executable is registered to start whenever the infected user logs onto the system. This is performed by adding an entry to HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

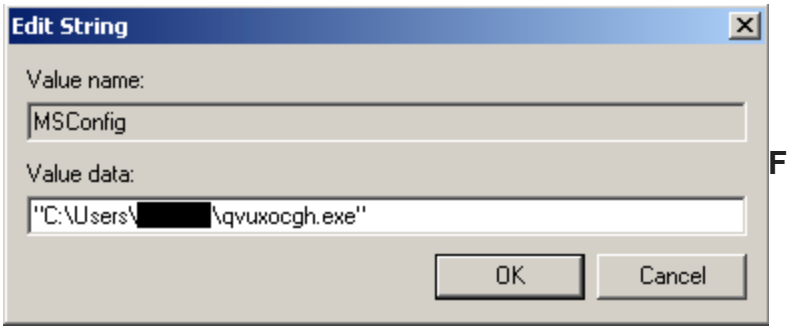


Figure 5: Persistence Mechanism

It also deletes the initial binary using a batch file that is temporarily stored inside the %TEMP% directory.

```
1  @echo off
2  :next_try
3  del "C:\Users\[redacted]\Desktop\tofsee.exe">nul
4  if exist "C:\Users\[redacted]\Desktop\tofsee.exe" (
5  ping 127.0.0.1 >nul
6  goto next_try
7  )
8  del "%0"
```

Figure 6: Batch File Stored in Temp

Once infected, systems will begin connecting to various SMTP relays and sending spam email messages.

Waiting connections	[redacted]	2583	65.55.37.88	25	TCP	Time wait
Waiting connections		2584	144.160.159.21	25	TCP	Time wait
Waiting connections		2585	98.138.112.33	25	TCP	Time wait
Waiting connections		2586	mtain-a-mtc-a.mx.aol.com	25	TCP	Time wait
Waiting connections		2587	64.233.160.27	25	TCP	Time wait
Waiting connections		2589	98.138.112.33	25	TCP	Time wait
Waiting connections		2590	65.54.188.94	25	TCP	Time wait
Waiting connections		2591	65.55.92.136	25	TCP	Time wait
Waiting connections		2592	144.160.159.21	25	TCP	Time wait
Waiting connections		2593	98.138.112.32	25	TCP	Time wait
Waiting connections		2595	98.138.112.32	25	TCP	Time wait
Waiting connections		2596	65.54.188.126	25	TCP	Time wait
Waiting connections		2597	vq-in-f27.1e100.net	25	TCP	Time wait
Waiting connections		2598	65.55.37.88	25	TCP	Time wait
Waiting connections		2599	144.160.159.21	25	TCP	Time wait
Waiting connections		2601	173.194.219.27	25	TCP	Time wait
Waiting connections		2602	152.163.0.99	25	TCP	Time wait
Waiting connections		2604	98.138.112.32	25	TCP	Time wait
Waiting connections		2605	64.233.160.27	25	TCP	Time wait
Waiting connections		2606	65.54.188.94	25	TCP	Time wait
Waiting connections		2607	144.160.159.21	25	TCP	Time wait
Waiting connections		2608	98.138.112.33	25	TCP	Time wait

Figure 7: SMTP Connections

Additionally, HTTP GET requests are generated periodically as the malware attempts to simulate clicking on ads as part of its click fraud routine:

```
GET http://ticketsnow.com/InventoryBrowse/Hamilton-Tickets-at-Richard-Rodgers-Theatre-NY-in-New-York-9-13-2016?
PID=1816075&ts=1472670103 HTTP/1.1
Proxy-Authorization: Basic Og==
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109
Safari/537.36
Connection: close
Host: www.ticketsnow.com
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://www.ticketsnow.com/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
```

Figure 8: HTTP Connections

Conclusion

Threats are constantly evolving as attackers change the way in which they attempt to distribute malware and attack systems. Threat actors also constantly strive to expand their presence by taking advantage of the ever increasing number of Internet users and devices. By leveraging our vast visibility into the threat landscape, Talos is able to effectively monitor these threats and quickly detect changes in the tactics, techniques, and procedures attackers are using so that we can continually protect our customer's networks and data.

Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CWS	✔
ESA	✔
Network Security	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

The Network Security protection of IPS and NGFW have up-to-date signatures to detect malicious network activity by threat actors. ESA can block malicious emails sent by threat actors as part of their campaign.

Indicators of Compromise

URLs:

hXXp://franny.goadultgame[.]ru:80/js/boxun4.exe
hXXp://getfile.myadultgame[.]ru:80/js/boxun4.exe
hXXp://gsbooz.goadultgame[.]ru:80/js/boxun4.exe
hXXp://ibvl.theadultgame[.]ru:80/js/boxun4.exe
hXXp://oajwwh.goadultgame[.]ru:80/js/boxun4.exe
hXXp://picshare.adultgamemedia[.]ru:80/js/boxun4.exe
hXXp://pics.theadultgame[.]ru:80/js/boxun4.exe
hXXp://reworder.adultgamesite[.]ru:80/js/boxun4.exe
hXXp://rkeujctg.adultgamemedia[.]ru:80/js/boxun4.exe
hXXp://video.theadultgame[.]ru:80/js/boxun4.exe
hXXp://view.webadultgame[.]ru:80/js/boxun4.exe

Domains:

myadultgame[.]ru
theadultgame[.]ru
webadultgame[.]ru
adultgamesite[.]ru
goadultgame[.]ru

adultgamemedia[.]ru
datingst[.]ru
globalhotstore[.]ru
datingrg[.]ru
datingsd[.]ru
datingds[.]ru
datinghq[.]ru
datingfr[.]ru
datinghl[.]ru
dategh[.]ru

IP Addresses:

184[.]18[.]26[.]30
103[.]232[.]222[.]57
111[.]121[.]193[.]242

Downloader Filenames:

Sandi.js
Tessa.js
Dori.js
Debbie.js
Lira.js
Griselda.js
Chere.js
Jess.js
Bettie.js
Katerine.js
Karena.js
Birdie.js
Blondelle.js
Pansy.js
Thomasina.js
Nananne.js
Abigail.js
Adelaida.js

Downloader Hashes:

fe6290253a02c231c07e8604c6b2a1b298520e112e0c0ba08f76c26724b3c820
f706c9c0982c358a165c5d31b218140461e110662332c6c508a9a66305311b17
7e3e4d33b9477f4d38934fdafa2203815950bef6d3b5b1011cd433035f9c0975

83a5e5e319169ec0de90a3ffa3513bbfdcb169fcda57ee671b9c4d08893f5d86
762be900fa19aff05fe6459da36b407b81cf08d2e95c8aa7b23870c2fe4178cc
40f039b9bfedbe5829c9301b0f2b1f322191694961f54a34853d5b4ae5627355
91e57da11ec889574aebd03f9a213d7154d899d2cf137ec7275e90201e62a170
f524ed3077caf65891d8b2c56c0fd32a5f58bba53ff09ad805fef8e7818a9b71
d9fa2cd39e8dd741a95bb83576e4f7a1e766e8e1ba6580676a5aad145b2ac56d
0274427bae4e479c28e9f8f21460cd03947c4878038458aeca406b7564563dc0
0931fc405a4bc660dc695f5da8f9e6c027832530e7ee48a5385ea6b43587ff52
0d98ad52e4db0085fbcf7d87465a14883e64038923e164d27e23983d4bde290c
f6d17a1034a08de4048ba3b5f3adea7aa7d11180277c74c3ea09e3826520f768
979ca79de2e3f3bdfa2a202824b3d6070aca61908f1413413777efeee224869f
e8072ee6e6007ba44071bee91bd25f88c3e9d5db8c49c59975946d8f421b7ab7
23a37772ff69c0da4294f858ee1b50ef8f261c007fc5ae0a1216757d0a1a4148
5d005f26295b05b7a9e8bf317c1452a616c362594e787d3bac5ecb2709059f2e

Binary Hashes:

3100af215a1dbe16be91fa5ee4fd8def2c58623e5c7b3751e2a4c4df1263c5bc
08eb7d50f070f84227ba9a7f55149bcd775d700636417c917a317248acd2f57d
0904af6c04c349dddc1cdb1e76a7c0782dd750e36c3e2e9e84ea8e40f41905c6
0aaea185e269923b4181951b3761a33a745f1ff8671f9a17ee69798c605b7aff
25fae47b7959cfb5be90cffc9a33d0875a0f5cb8dc7f6bd1bfb926ca26e24ea3
4529bc3de5ac1e5807d91dbe9883aca563dc845ef80cbddd835fd04a4b2d7ab8
4cb9925bcc4d8e8e74f8a1288595b3775bc8a8e7cac3e2e05f4fe6fefceb8af2
5ba6eb7748f1e01c8302f8a97c264e82256f5b7c796b5a893550673c5ca0e134
5d06f55a5fb94d5717dfa798e670c3cdacbaa57a798fe917e0c69ee0e42cfcb8
6c6b60b62b1090fee62336852ecf2e9999050de32ec7a9114a0fce54fe9fb177
785c9f48829d0ac2958a403976346833d630e8eba24bf5fa4024d36e37d8f77d
7c41a29a697dab21b7303baf75bf931bdc06123b339349268e5de0f124818364
8204b8590b916268dd683a5d040225d1ec3836a473e79fda5463031da9cce632
906cbae96a9d21d0dd692b858f11c7515d515773da854add7dc695e8b0f973d1
9a7e3fda688862acbad677f62f99ac449c3df6b884408c80a34938dd18d5284f
9e0550c4a5dbbb19c30fa82ff05d28971d8934f1a954b24a6335ed19aeba72d5
a77355c3dd7f65957aab46a586463762e02cbfc981817fdb95c44b144dea1842
acb5bd713f0077725d754e98961eb4c691e1d68d45678597c5dbf1ff667e27ca
b1f96a761338ec65ecfb385486c583f8677fb865735b8d839a4a7ff094cc9744
b86c1f59060c6607f8da882ac45c9e4e82a899dbb57a77f007b15f8460d32a71
bcf9256595fa8da550b479ccfd518a67a1fc53ff2bffe990c3789dda29cc5886
c1a1b521a365402ec82adff554be11e22cdedce7d50dc49d47609b1b6aed2d79
c4808689aaf69cee2db9783d9831abe568e0953f9f6f1e80e162e99fb9c664f0
ca8851bdb285c02fd1d5176cffc9cedafe8838610466df859b33e465f3a91572

d2085fd53064953de40f9735ec31c09b479612cfa13597c9a30df4ebf06dd85b
e522062d780fc38f89c463f0a2002b3646681a1582435276d2f81d75b9c7696b
ffc9744be0450e5ed8dd296798c2562f688d77c954ed976c9ccb723163fa7006