2016 年 9 月 29 日，星期四

以美女照片作为诱饵的 Tofsee 恶意软件—个气焰嚣张的僵尸网络

作者：Edmund Brumaghin

摘要

Tofsee 是一种多用途恶意软件，已经存在多年，至少从 2013 年就已开始活动。它采用了大量模块来执行各种活动，例如发送垃圾邮件、实施点击欺诈、挖掘加密货币，等等。系统一旦感染这种恶意软件，就会成为 Tofsee 垃圾邮件僵尸网络的一部分，然后被攻击者用于发送大量垃圾邮件，以图感染更多系统并扩大受攻击者控制的僵尸网络的整体规模。

今年初，Talos 发布了一篇博文，论述了 RIG 漏洞攻击包如何利用恶意广告活动将此恶意软件传输到受危害的终端。恶意广告是一种漏洞攻击包常用的技术，以图感染那些浏览含有危害性广告的网站的用户电脑。6 月份这种活动似乎消失了，但最近 Talos 发现包含用于分发 Tofsee 的恶意附件的垃圾邮件活动在数量和速度上又有明显增长。

Tofsee 垃圾邮件活动

2016 年 6 月，在 Angler 漏洞攻击包从威胁格局中消失之后，其他主要漏洞攻击包纷纷开始转向其他负载。RIG 漏洞攻击包已从分发 Tofsee 转为分发其他负载，这可能是因为从牟利的角度来看，分发其他负载对于网络犯罪者更有吸引力，也可能只是因为不同的攻击者也已开始使用这种漏洞攻击包作为其恶意软件的分发机制。

鉴于受感染主机尝试分发的垃圾邮件数量之大，基于 DNS 的黑洞列表 (DNSBL) 迅速增加了很多新的节点，而且发生这种情况后，大多数主要邮件服务运营商都不再接受新邮件传输方式。为了保持垃圾邮件数量稳定不变，必须不断增加新节点。当 RIG 停止分发 Tofsee 负载时，负责 Tofsee 的攻击者开始转向其他分发方法。

众所周知，Tofsee 僵尸网络通常发送垃圾邮件，但最初这些邮件包含的都是成人交友约会网站和医药网站的链接。从 8 月份开始，Talos 发现这个僵尸网络发送的垃圾邮件性质开始有所变化。Tofsee 垃圾邮件僵尸网络开始利用恶意附件作为恶意软件下载程序。这种活动在速度和数量方面已经有所增长。

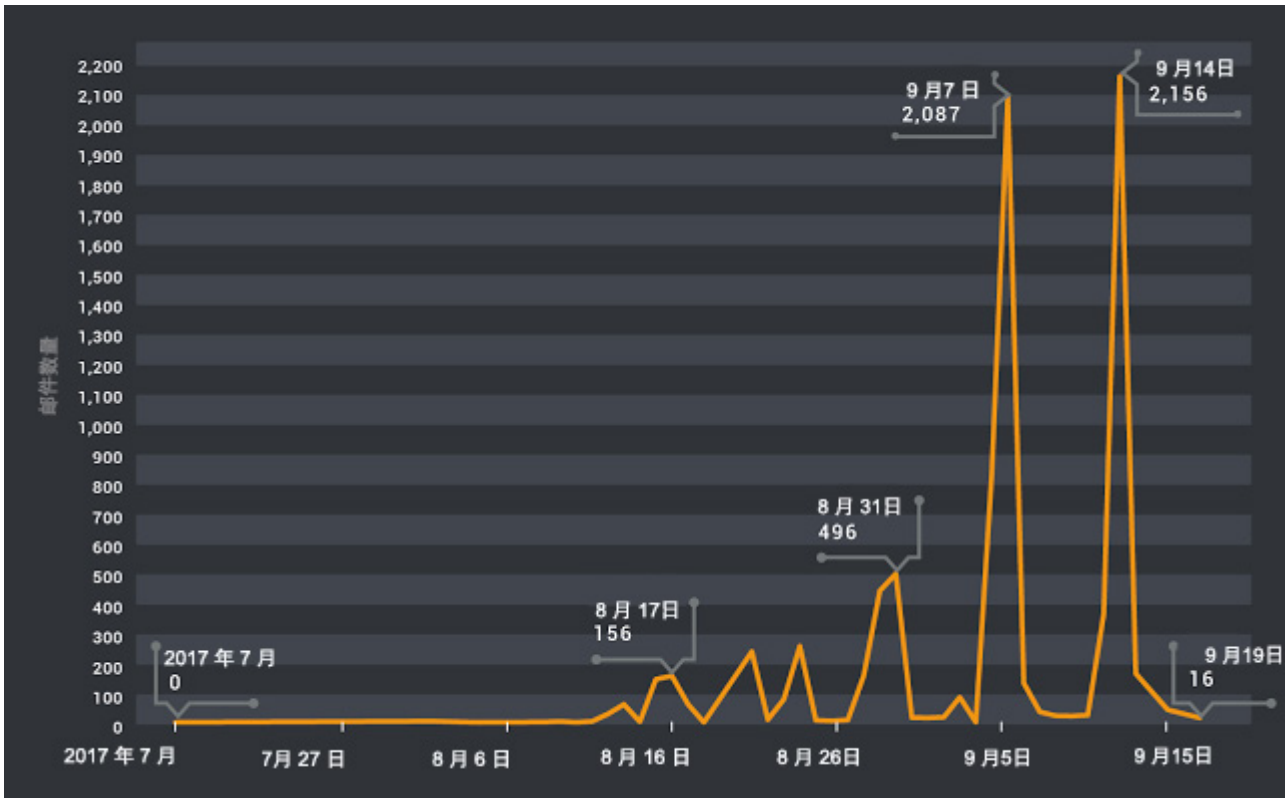

图 1：包含恶意软件下载程序的邮件的数量

初始感染媒介

一开始感染这种 Tofsee 变体的方式似乎是通过诱使用户打开由网络钓鱼邮件发送的恶意附件完成的。这种网络钓鱼邮件声称来自东欧（即俄罗斯和乌克兰）的女性，而且邮件主题是成人交友约会。每封邮件包含的文本略有差异，但是经 Talos 分析的所有邮件均采用相同的格式。这些邮件声称包含 zip 存档附件，内含发件人的照片以及某个俄罗斯成人交友约会网站的链接。下面是 Tofsee 邮件正文的示例：

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!

图 2：Tofsee 垃圾邮件示例

Javascript 下载程序

此附件是一个名称为 [发送者名字]-photos.zip 的 zip 存档文件，其中包含一个 Javascript 文件。在我们分析的所有案例中，此 Javascript 文件的文件名都是某位女性的名字。各组邮件的文件名和散列各不相同，其中有些邮件是在任意特定日期发送的。Javascript 附件中的代码经过混淆处理，以图增加分析难度。

```
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");
```

图 3：经过混淆处理的 Javascript 下载程序示例

上面的 Javascript 对 WScript 下载程序进行了混淆处理，此下载程序用于从攻击者控制的网站检索和执行恶意 PE32 可执行文件。此下载程序在执行时会检索恶意可执行文件并运行该文件，从而使系统感染 Tofsee。

感染详情

此恶意软件将一个随机命名的 PE32 可执行文件投放到 %USERPROFILE% 目录中。

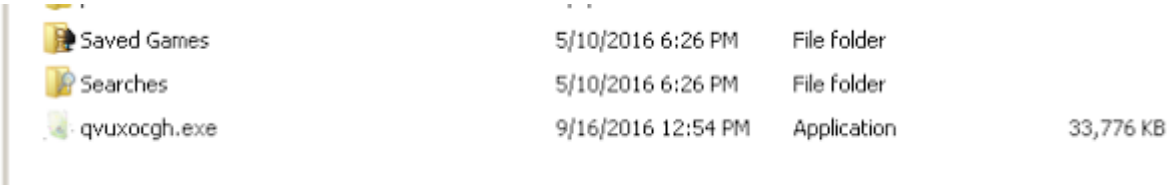

图 4：所投放的 Tofsee 二进制文件

所投放的可执行文件已注册，只要受感染的用户登录系统就会启动。此过程是通过向 HKCU\Software\Microsoft\Windows\CurrentVersion\Run 添加一个条目来执行的。

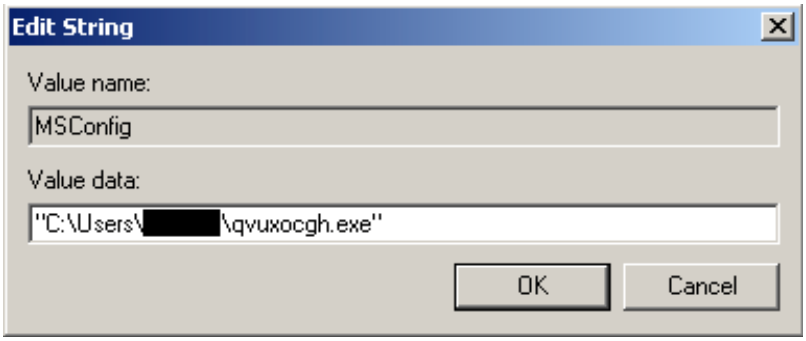

图 5：持续性机制

它还会使用一个批处理文件删除初始二进制文件，此批处理文件临时存储在 %TEMP% 目录中。

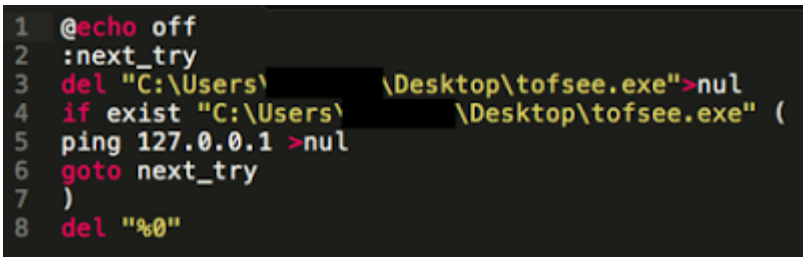

图 6：TEMP 目录中存储的批处理文件

系统一旦感染，就会开始连接各种 SMTP 中继并发送垃圾邮件。

图 7：SMTP 连接

此外，当恶意软件在点击欺诈程序中尝试模拟点击广告时，会定期生成 HTTP GET 请求。

```
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
```

图 8：HTTP 连接

结论

随着攻击者改变其尝试分发恶意软件和攻击系统的方式，威胁也在不断发展变化。威胁发起者还会利用数量日益增长的互联网用户和设备，不断努力扩大其影响范围。Talos 利用我们对威胁形势的全面可视性，能够有效地监控这些威胁并快速检测攻击者所使用的策略、技术和程序方面的变化，从而使我们能够持续保护客户的网络和数据。

覆盖范围

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	保护
AMP	✔
CWS	✔
ESA	N/A
网络安全	✔
WSA	✔

高级恶意软件防护（AMP）解决方案可以有效防止执行威胁发起者使用的恶意软件。
CWS 或 WSA 的 Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。
IPS 和 NGFW 的网络安全防护功能拥有最新的签名库，可以检测威胁发起者的恶意网络活动。
ESA 可以拦截威胁发起者在攻击活动中发出的恶意电子邮件。

危害表现

URL：

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

域：

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 地址：

184.18.26.30
103.232.222.57
111.121.193.242

下载程序文件名：

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

下载程序散列：

fe6290253a02c231c07e8604c6b2a1b298520e112e0c0ba08f76c26724b3c820
f706c9c0982c358a165c5d31b218140461e110662332c6c508a9a66305311b17
7e3e4d33b9477f4d38934fdafa2203815950bef6d3b5b1011cd433035f9c0975
83a5e5e319169ec0de90a3ffa3513bbfdcb169fcda57ee671b9c4d08893f5d86
762be900fa19aff05fe6459da36b407b81cf08d2e95c8aa7b23870c2fe4178cc
40f039b9bfedbe5829c9301b0f2b1f322191694961f54a34853d5b4ae5627355
91e57da11ec889574aebd03f9a213d7154d899d2cf137ec7275e90201e62a170
f524ed3077caf65891d8b2c56c0fd32a5f58bba53ff09ad805fef8e7818a9b71
d9fa2cd39e8dd741a95bb83576e4f7a1e766e8e1ba6580676a5aad145b2ac56d
0274427bae4e479c28e9f8f21460cd03947c4878038458aeca406b7564563dc0
0931fc405a4bc660dc695f5da8f9e6c027832530e7ee48a5385ea6b43587ff52
0d98ad52e4db0085fbcf7d87465a14883e64038923e164d27e23983d4bde290c
f6d17a1034a08de4048ba3b5f3adea7aa7d11180277c74c3ea09e3826520f768
979ca79de2e3f3bdfa2a202824b3d6070aca61908f1413413777efeee224869f
e8072ee6e6007ba44071bee91bd25f88c3e9d5db8c49c59975946d8f421b7ab7
23a37772ff69c0da4294f858ee1b50ef8f261c007fc5ae0a1216757d0a1a4148
5d005f26295b05b7a9e8bf317c1452a616c362594e787d3bac5ecb2709059f2e

二进制文件散列：

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

发布者：Edmund Brumaghin；发布时间：11:02
标签：僵尸网络、恶意软件、垃圾邮件、威胁研究、Tofsee