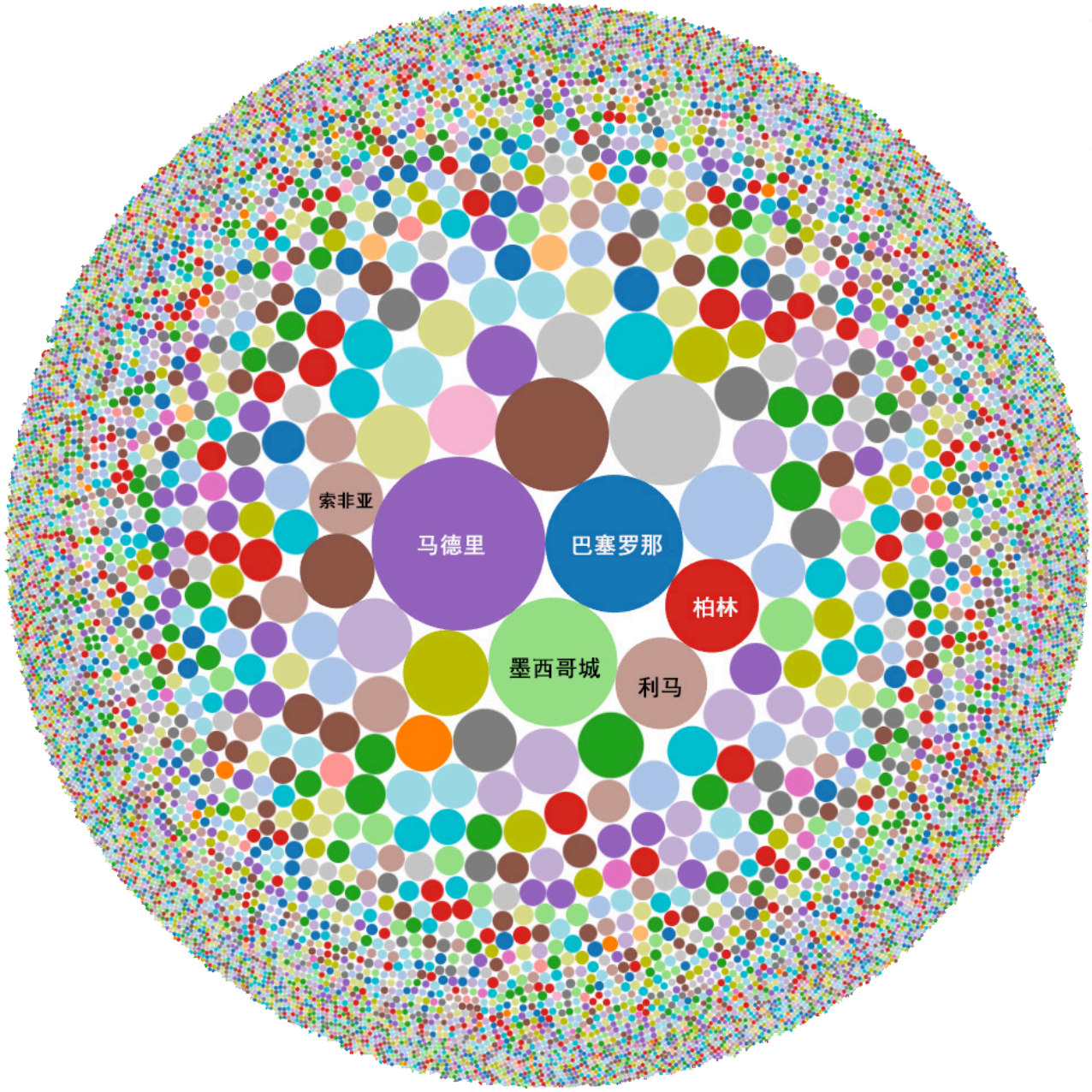
威胁聚焦：漏洞攻击包跨国攻击 150 多个国家/地区



Nuclear 在 150 多个国家/地区 1 万多个城市的活动

作者：Nick Biasini

概述

Talos 以持续关注威胁形势为己任，而谈到威胁形势，就需要警惕不断演变的漏洞攻击包。Talos 的当前目标之一是对这些攻击包进行曝光和瓦解，以保护成为其目标并受到其侵害的普通互联网用户。 我们曾经对 Angler 漏洞攻击包提出前所未有的深刻见解，并揭露了这个以前不为人知的活动的具体细节。 现在，我们将注意力放到具有类似影响的 Nuclear 漏洞攻击包上。

许多年来，Nuclear 漏洞攻击包一直在持续不断地侵害用户，并且一直在有效地发展进化，扩充其漏洞库。但是，与目前活跃的其他更盛行的漏洞攻击包相比，它的大部分活动都没有受到监控。我们之所以要对该漏洞攻击包的活动进行深入研究，其中一个理由就是因为缺乏对它的深入了解。我们发现，这是一个非常复杂的威胁，它成功入侵的用户遍布 150 多个国家/地区的 1 万多个城市。

通过利用我们的数据不断挖掘，我们获得了令人兴奋的结果：我们得到了托管 Nuclear 漏洞攻击包的 10-15 个 IP 地址的列表。这使我们可以重点关注托管该攻击活动的运营商。目前，我们确定了第一个关键感染源：DigitalOcean。我们能够确定，我们追踪的所有 Nuclear 活动几乎都是由 DigitalOcean 托管的。Talos 已与 DigitalOcean 建立联系，并将 Nuclear 的活动以及与该威胁相关的详细信息通知他们。DigitalOcean 的安全团队确认了主机的恶意性质，并与 Talos 合作，为摧毁该攻击包提供重要情报，以揭示该攻击包的运作方式。

运营商帐户详细信息

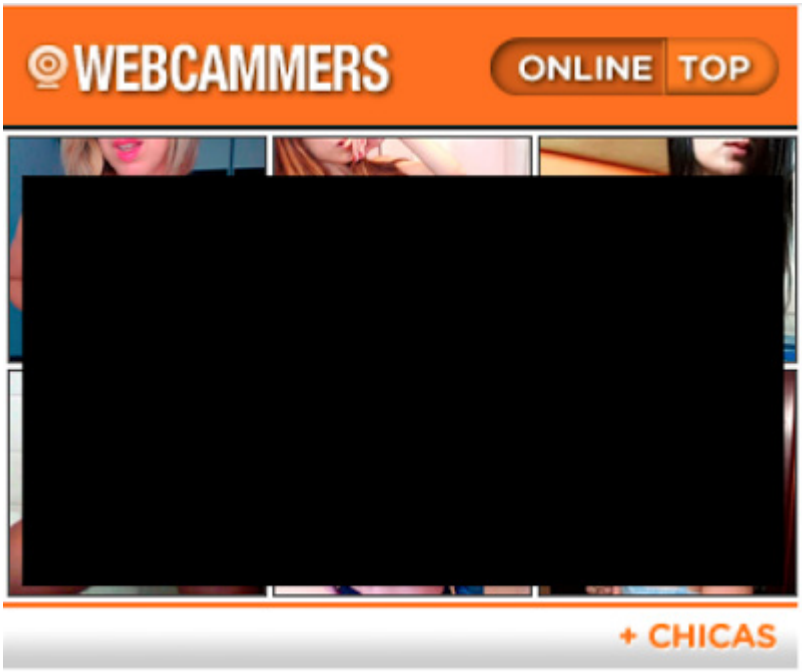
首先我们来快速比较一下 Nuclear 和 Angler 背后的攻击者所使用的策略。Angler 的活动与跨多个运营商的多个用户帐户相关，他们拥有大量服务器，并且利用被盗的信用卡来支付他们的帐单。Nuclear 则完全不同。托管 Nuclear 的帐户利用优惠券码来避免以传统方式进行支付，而且他们十分谨慎，仅注册一个主机。在调查的前几周，我们向 DigitalOcean 通知了一个新的 Nuclear 服务器实例，DigitalOcean 随即将其关闭，但是立即就出现了另一台主机。

这显示出 Angler 和 Nuclear 托管恶意活动方式的有趣对比，并展现了攻击者如何发展并改变手段来继续他们的非法活动。网络攻击者使用众所周知的免费电子邮件服务来建立自己的帐户，并且不断使用不同的电子邮件地址和主机。

活动量

通过对托管该恶意活动的一台服务器一天的活动进行分析，我们发现大约有 6 万个 IP 连接到该服务器。这个活动量远远超出我们基于先前的数据分析所做的预测。

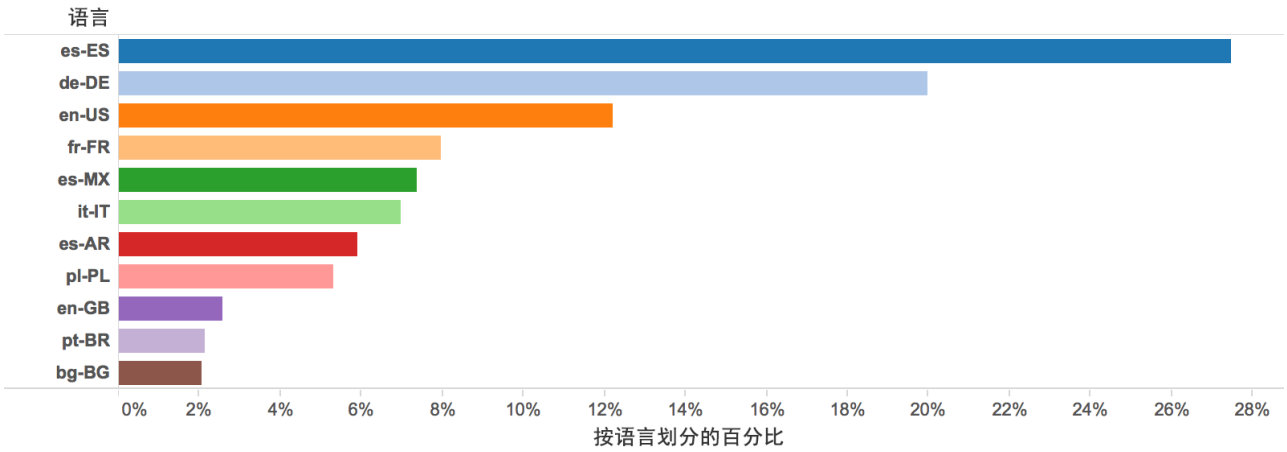
我们开始思考一个问题：“这种活动是如何避开视线，隐藏得如此巧妙？”而答案既显而易见又令人惊讶：那就是通过色情/成人娱乐网站。我们开始关注此流量的引用方，发现几乎有一半的 IP 地址都来自于一个色情网站上托管的一个网络摄像机广告，其删剪版本如下。



在一天内，我们就发现该摄像机广告将超过 25000 个 IP 地址重定向到 Nuclear。右下角显示的西班牙单词“chicas”让人推测该攻击包可能是针对母语非英语的国家/地区。

按语言划分的调查数据

我们对该攻击使用的语言进行了细分研究，并发现了一些支持上述假设的事实。在日志中捕获的 HTTP 报头包含“接受语言”(Accept-Language) 信息，我们利用该信息建立了一个语言细分统计表，如下所示：

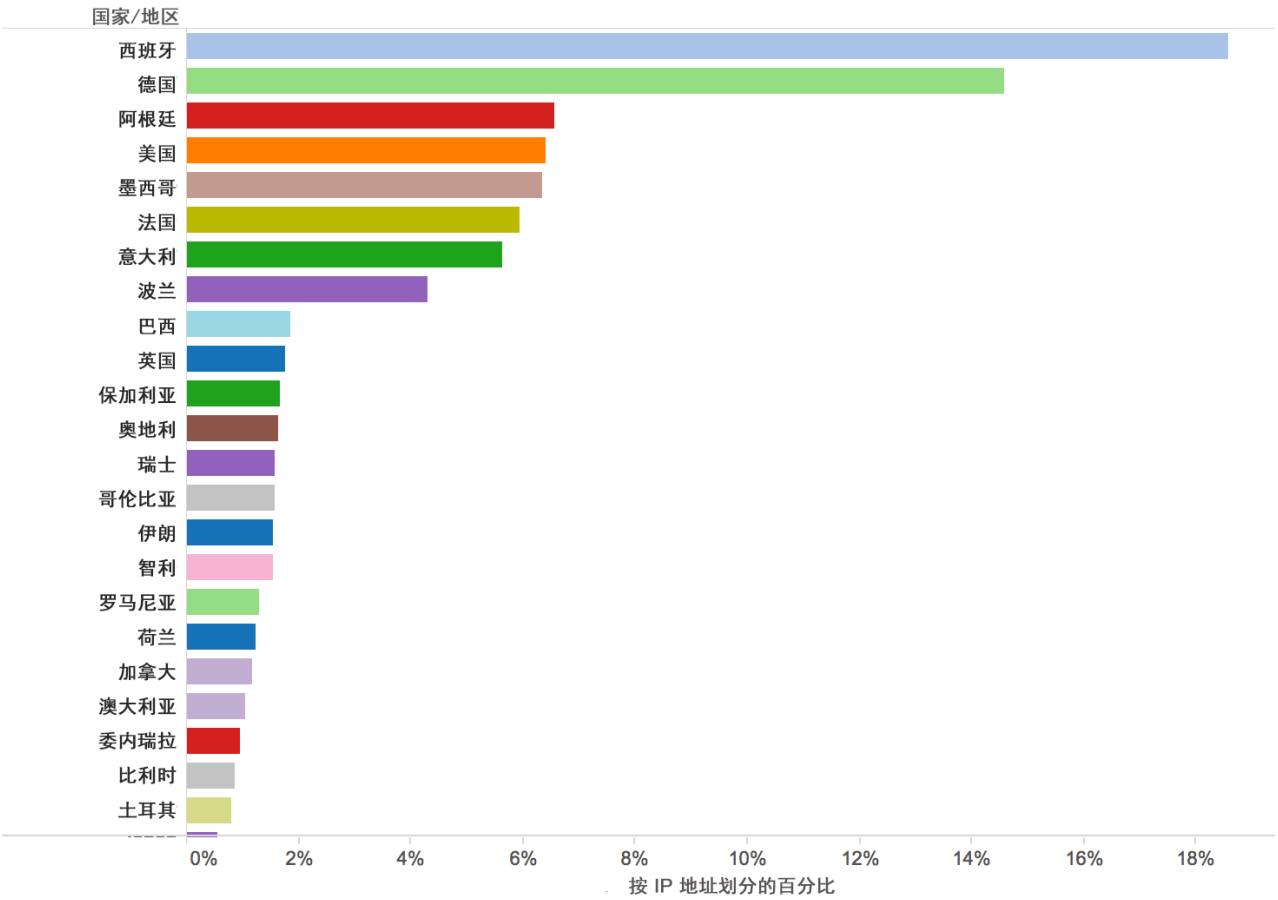


不出所料，英语并不是在数据中发现的最常用的语言报头。西班牙语和德语是排在英语之前的最常用语言，而法语、意大利语和波兰语也占有较大比例。

我们想查明这个结果与全球范围内相关语言母语者人数之间的联系。 我们发现从 2007 年以来的数据显示，世界上母语为英语 (5.52%) 和西班牙语 (5.85%) 的人口数量较为接近。 但是母语为德语的人口数量 (1.39%) 仅为母语为英语和西班牙语的人口数量的四分之一，而母语为法语、意大利语和波兰语的人口数量则明显低于其他语言（分别为 1.12%、0.90% 和 0.61%）。基于这些信息，我们决定围绕受影响的 IP 展开调查，并开始尝试确定这些流量的源头。

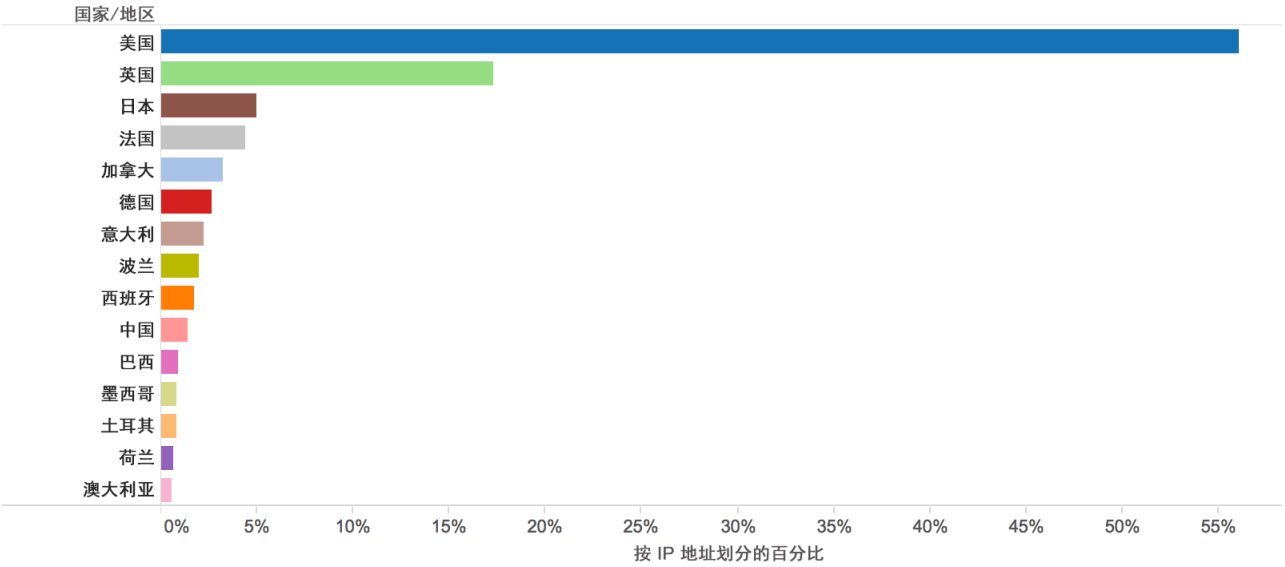
按地理 IP 划分的调查数据

Talos 选择了大约 6 万个 IP 地址，根据基本地理信息（例如源头城市和国家/地区）对它们进行追踪。结果显示，正如前面我们对 HTTP 报头的分析一样，西班牙语国家/地区构成了该活动的重要组成部分。



西班牙是最大的目标，在与此特定服务器交互的主机中占有近 20% 的比例。同样，德国的潜在受害者比例大约为 15%。需要注意的是，美国实际上是排名第四的受害国家，交互主机比例与墨西哥几乎相同。这是从地理分布数据得出的最显著差别之一，因为墨西哥的网民数量要比美国少很多。 另外，美国境内有 4100 万母语为西班牙语的人口，这也占美国境内受害者的一部分。

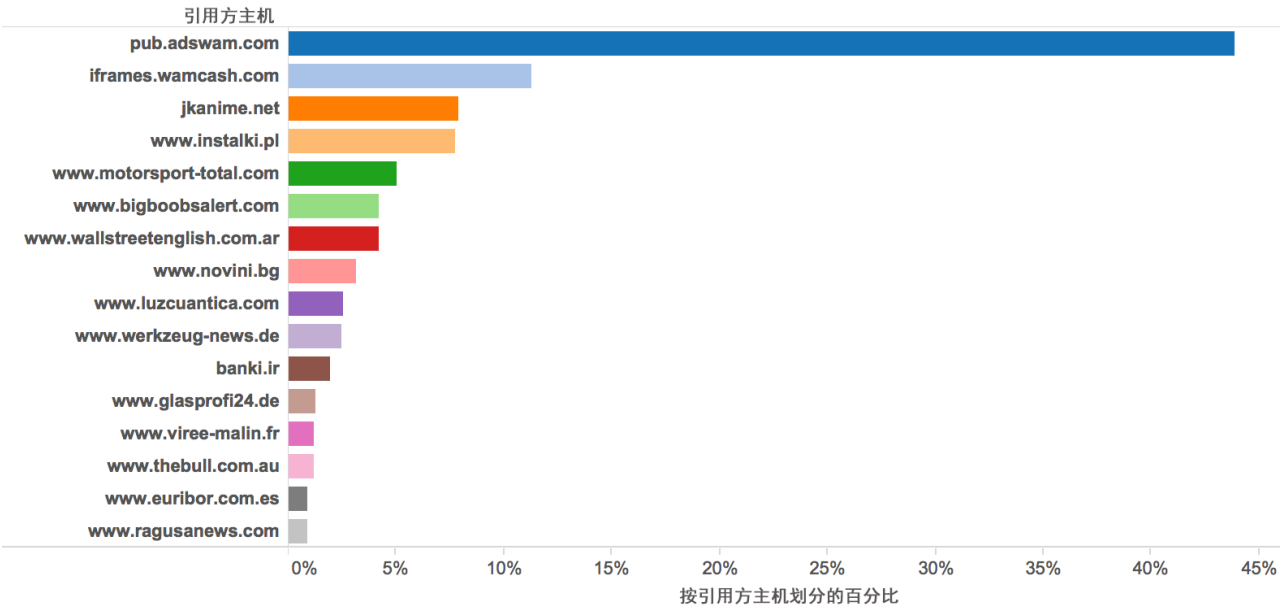
因为我们在之前对 Angler 的研究中得到了相似的数据集，我们可以得出这两者之间的一些明显差异。从下图可以看出，Angler 的绝大多数潜在受害者来自英语国家。



近 75% 的 Angler 受害者来自美国和英国。这也说明只有为数不多的国家/地区受到波及。Angler 的受害者仅来自 15 个不同的国家/地区。Nuclear 的影响范围则大得多，我们发现有超过 100 个国家/地区向 Nuclear 服务器发送流量，包括来自伊朗和委内瑞拉等国家/地区的出人意料的流量。Nuclear 似乎在试图避开美国和英国，将重点放在世界其他国家/地区的用户。和我们以前观察到的一样，Nuclear 以外的漏洞攻击包（如 Angler）主要以英语国家/地区为目标。有可能 Nuclear 是为了避免与他们争抢用户。

按引用方和用户代理划分的调查数据

接下来，我们又以流量的引用方为对象进行了研究，而结果再一次证明了我们在地理分布分析中得出的结论。从数据上看，我们发现了超过 7500 个唯一引用方，其中上述色情广告引起的重定向占有很大比例（约占 45%）。另外，在数据中发现的不同顶级域名 (TLD) 也很值得注意。我们发现许多 TLD 都与欧洲和美国/英国之外的其他地区的非英语国家相关。



这可能是利用受入侵的网站和恶意广告造成的结果。基于我们看到的趋势，这两种途径都在不同的时间得到利用，并且该活动看起来主要以恶意广告为主。

用户代理数据揭示了恶意广告对其针对的特定用户的效果。根据这个数据，我们可以确定 65% 的用户使用的是运行在 Windows 7 或 Windows 8 上的 Internet Explorer 11。基于网络浏览器的过滤是与网上广告相关的一项常见功能，并且至少在这个案例中，似乎非常有效。

漏洞攻击包分解

下面几节内容将着重讨论我们发现的 Nuclear 漏洞攻击包的运作方式。和我们过去对 Angler 的研究结果相似，Nuclear 使用代理服务器直接与用户进行交互。在本案例中，我们发现此系统连接到地址为 144.76.82.55 的漏洞攻击服务器。对于每个发送到代理服务器的 GET 请求，我们都看到有一个相应的 GET 请求向外发送给攻击服务器。该活动使用端口 80，而不是我们以前见过的非标准端口。另外，该攻击包似乎还向 HTTP 报头加入一些信息，包括受害者的 IP 地址和语言，示例如下所示。

```
GET /discuss-progressing.jsp?squishes=v7v4qt44cnqf4g3&29v4v6=genre HTTP/1.0
Host: eu.fabrikakids.com.br
X-Real-IP: [redacted]
X-Forwarded-For: [redacted]
Connection: close
Accept: */*
Referer: http://eu.fabrikakids.com.br/v9k1n-benighted/opinions_impanel/porticoes?
ugvrzd8v=corning&taste-litany=200k8i41o9up0ong&fatherly=6797
Accept-Language: es-AR
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; MANMJS; rv:11.0) like Gecko
DNT: 1

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 28 Mar 2016 22:34:59 GMT
Content-Type: application/x-shockwave-flash
Content-Length: 95632
Connection: close
Accept-Ranges: bytes
```


```
CWS.....x.\....\...%U.A
..!.,%.90...T./...v....}...I]..n.!c.-0b.]$..**..t.h......k=
+..._.._..._./....................?...?.i.........C?n..>.w.W.... x].?\.?Lk..4M..."...#.~..
{r.............[.6..L....<I.c.w..w.q.<.O......u.<.....q.@...w.<..rZ.d.K2.}.
%........S.].Y.}.'[.O....s...}..&...o.......[._..u........_6....c&....l..y..#{.T.K.u..>..
%.#........c?N..........l-.}....._...>..#....._..O....d/..'..".........a....O......+.
.............../....9......................_...y....o....+.........?...o...2Dp.]..F}.'.uw
+..|]......~....1g...|...A..>.yS .g...`.P7. ..b.&.....}.=..........?...#.U..
......1.    ......T x<\....9z.i&=..../d.....S.qg.~.....j/}..B.0..l.......R.K=.K.....4.../x{........VW
\"...~..
s...q....yH..W.......z...{..1.
..."'.,....X...Kse......uZ}0....z..u...*..w.$!.m..i.Z..JF.Wo.......]R...h.....H...j.$..
8..z.A.",E.W..A.......SS.....l...<[.....$0.m73..o..+g"...Z..$...Qg.-..!QO.r.....{.!1q......K...&/
```


这可能与代理服务器本身相对缺乏日志记录相关。该代理服务器在系统中几乎禁用了所有日志记录，并且使用的 NGINX 配置与我们在 Angler 看到的非常相似。以下是我们在 Nuclear 服务器上发现的 NGINX 配置的副本。

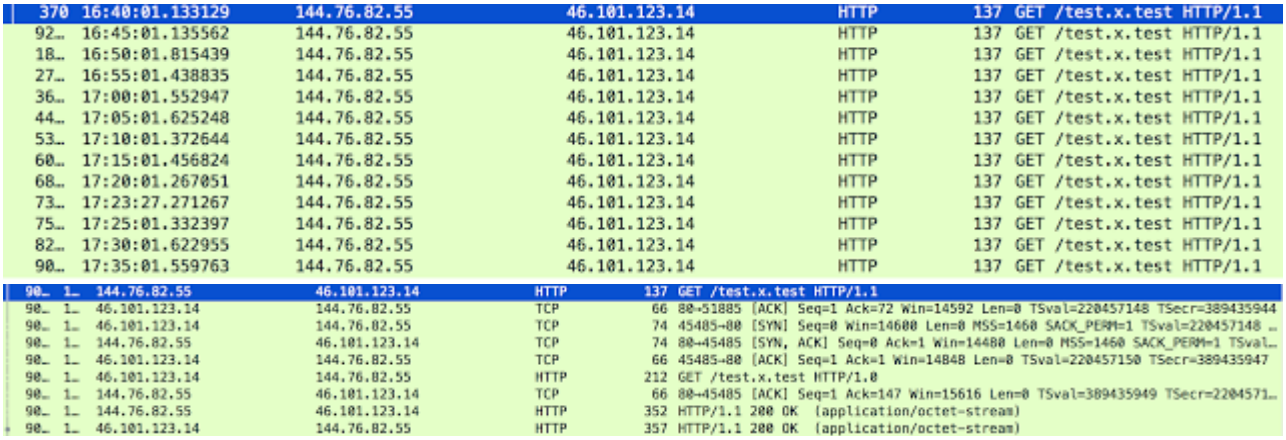
```
worker_processes 2;
    pid /var/run/nginx.pid;
    worker_rlimit_nofile 200000;
    events {
    worker_connections 100000;
    }
    http {
    sendfile on;
    tcp_nopush on;
    tcp_nodelay on;
    keepalive_timeout 10;
    types_hash_max_size 2048;
    server_tokens off;
    access_log off;
    include /etc/nginx/mime.types;
    default_type application/octet-stream;
    server {
    if ($http_user_agent ~
(MRSPUTNIK|LSSRocketCrawler|CPython|SeaMonkey|NetcraftSurveyAgent|McAfee|masscan|Bada|Playstation|Nintendo|Xbox|Screenshoot|Screenshot|Genieo|
Crawler|facebookexternalhit|BIDUBrowser|fMcAfee))
{
    return 404;
    }
    location / {
    proxy_pass http://144.76.82.55/;
    proxy_redirect off;
    proxy_buffering off;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }
    gzip off;
    }
    }
```

它明确显示了代理服务器配置将带有额外报头数据的流量传送给攻击服务器。但是，还有一个关键的信息，一些用户代理会执行检查。用户代理中有一个关键词清单，会导致漏洞攻击包返回 404。该工具包检查的的关键词如下：

- MRSPUTNIK
- LSSRocketCrawler
- CPython

- SeaMonkey
- NetcraftSurveyAgent
- McAfee
- masscan
- Bada
- Playstation
- Nintendo
- Xbox
- Screenshoot
- Screenshot
- Genieo
- Crawler
- facebookexternalhit
- BIDUBrowser
- fMcAfee

其中一些关键词显然与安全产品相关，其他则与电子游戏机、截屏工具和网络爬虫等技术相关。这是一个有趣而有效的方法，可以减少向他们无法入侵的系统发送登录页面的数量。在配置中未发现的一样东西是运行状况监控方法。这不是通过此配置进行的，但是确实存在。每五分钟我们就看到从攻击服务器向代理系统发出 GET 请求。



370	16:40:01.133129	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
92…	16:45:01.135562	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
18…	16:50:01.815439	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
27…	16:55:01.438835	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
36…	17:00:01.552947	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
44…	17:05:01.625248	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
53…	17:10:01.372644	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
60…	17:15:01.456824	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
68…	17:20:01.267051	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
73…	17:23:27.271267	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
75…	17:25:01.332397	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
82…	17:30:01.622955	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
90…	17:35:01.559763	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1

90…	1…	144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
90…	1…	46.101.123.14	144.76.82.55	TCP	66	80→51885 [ACK] Seq=1 Ack=72 Win=14592 Len=0 TSval=220457148 TSecr=389435944
90…	1…	46.101.123.14	144.76.82.55	TCP	74	45485→80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=220457148 …
90…	1…	144.76.82.55	46.101.123.14	TCP	74	80→45485 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval…
90…	1…	46.101.123.14	144.76.82.55	TCP	66	45485→80 [ACK] Seq=1 Ack=1 Win=14848 Len=0 TSval=220457150 TSecr=389435947
90…	1…	46.101.123.14	144.76.82.55	HTTP	212	GET /test.x.test HTTP/1.0
90…	1…	144.76.82.55	46.101.123.14	TCP	66	80→45485 [ACK] Seq=1 Ack=147 Win=15616 Len=0 TSval=389435949 TSecr=2204571…
90…	1…	144.76.82.55	46.101.123.14	HTTP	352	HTTP/1.1 200 OK (application/octet-stream)
90…	1…	46.101.123.14	144.76.82.55	HTTP	357	HTTP/1.1 200 OK (application/octet-stream)

这是一个有趣的运行状况监控流，因为它是从攻击服务器向代理服务器发送的，代理服务器反过来将其定向至获得响应的攻击服务器。下面是返回的实际流量的示例。

```
GET /test.x.test HTTP/1.1
Host: eu.fabrikakids.com.br
Accept: */*

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 28 Mar 2016 22:35:01 GMT
Content-Type: application/octet-stream
Content-Length: 47
Connection: keep-alive
Last-Modified: Fri, 26 Jun 2015 00:53:10 GMT
ETag: "558ca276-2f"
Accept-Ranges: bytes

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

每次服务器都回复 47 个 x。此循环数据流担任运行状况监控功能，但是，我们并未发现通过其他服务器进行远程日志记录的任何证据。还有另一个奇怪的行为，有不同的 HTTP 版本被用于后端通信。发送给代理服务器的所有请求都使用 HTTP/1.1，这是网络流量的标准协议。但是，从代理服务器传送给攻击服务器的流量则使用 HTTP/1.0。下面是运行状况监控请求的一个示例。

144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
46.101.123.14	144.76.82.55	HTTP	212	GET /test.x.test HTTP/1.0
144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
46.101.123.14	144.76.82.55	HTTP	212	GET /test.x.test HTTP/1.0
144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
46.101.123.14	144.76.82.55	HTTP	212	GET /test.x.test HTTP/1.0
144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
46.101.123.14	144.76.82.55	HTTP	212	GET /test.x.test HTTP/1.0
144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
46.101.123.14	144.76.82.55	HTTP	212	GET /test.x.test HTTP/1.0
144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
46.101.123.14	144.76.82.55	HTTP	212	GET /test.x.test HTTP/1.0
144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1
46.101.123.14	144.76.82.55	HTTP	212	GET /test.x.test HTTP/1.0
144.76.82.55	46.101.123.14	HTTP	137	GET /test.x.test HTTP/1.1

攻击

我们分析的攻击数据证实，和大多数漏洞攻击包一样，Nuclear 大规模地利用 Adobe Flash 漏洞来入侵用户。一个有趣的遗漏是，在我们检查的所有流量中，我们却没有发现哪怕一个被利用的 Silverlight 漏洞。Angler 和 Rig 漏洞攻击包目前都普遍利用 Silverlight。但是，Flash 的漏洞却占全部漏洞的大约 80%，主要集中在几个 Flash 漏洞上。

在我们的研究过程中，我们从大约 45K 个 Flash 文件开始着手。但是，这些文件被大量使用，而我们发现这些文件在整整 24 个小时内仅使用了 96 个唯一哈希值。此外，每个哈希值仅处于活动状态 1 小时，然后就没看到重复使用。

就目前关注的负载而言，大多数都是勒索软件变体，还混杂了一些其他的威胁。这在很大程度上与当今的所有漏洞攻击包一致，因为勒索软件为这些非法活动提供了有效而直接的货币化。 最近，我们在 Talos 指出，Nuclear 已经开始投放 Tor，并利用它来匿名收集最终负载。 这可能标志着漏洞攻击包随着研究人员持续揭露它们的恶意负载而发生的另一个重大变化。

IOC

Nuclear 代理服务器清单

Nuclear 漏洞攻击服务器 - 144.76.82.55

Flash 哈希值

结论

漏洞攻击包一直很活跃，不断进化和侵害用户。Talos 致力于不仅通过开发内容阻止这些威胁，保护我们的用户，而且致力于揭露这些攻击包的运行，并且与运营商合作，将它们从威胁形势中彻底消除。我们一直坚信，研究人员和托管运营商之间的关系是取得成功的关键。这个例子很好地说明了乐于提供帮助的运营商对于揭露攻击者的活动有多大帮助，而这样做也有助于他们防止未来再受这种行为利用。

Aspis 项目就是专为这个目的而建立的。 Talos 欢迎愿意提供帮助的托管运营商随时与我们联系。不管您的环境目前是否有威胁，我们都始终期待与您建立这种合作。这样的行业合作对于有效阻止这类影响全球的威胁十分关键。

本研究揭示了漏洞攻击包趋于进行更具针对性的入侵行为的有趣变化。在研究人员不断研究美国/英国境内活跃的漏洞攻击包的同时，网络攻击者也在不断做出变化。如同我们会针对这些攻击包建立防护措施，他们也会不断改进自己的攻击包。像本文所讨论的 Nuclear 攻击者就将主要精力放在非英语国家，从而避免抢夺用户，并掩人耳目。显然，他们无法避开这些国家/地区的受害者，但是通过将主要精力放在非英语用户上，他们似乎更加难以捕捉。

只要攻击者还在使用这些攻击包来侵害用户，我们就会继续保持警惕，跟踪这些活动，保护我们的用户，并向全世界揭露这些活动。

覆盖范围

一旦我们发现这些域以及 Flash 文件被用于进行攻击活动，我们就立即通过思科的域信誉系统来进行屏蔽。

若要了解最新的规则信息，请咨询您的防御中心、FireSIGHT 管理中心或 Snort.org。

产品	保护
AMP	✔
CWS	✔
ESA	不适用
网络安全	✔
WSA	✔

高级恶意软件防护 (AMP) 非常适合于阻止执行这些威胁实施者使用的恶意软件。

CWS 或 WSA 网络扫描可阻止访问恶意网站，并检测这些攻击中使用的恶意软件。

IPS 和 NGFW 网络安全防护部门具有最新的签名，可检测威胁实施者进行的恶意网络活动。

发布者：Nick Biasini；发布时间：下午 12:04

标签：漏洞攻击包、Nuclear 漏洞攻击包、Talos、威胁研究、威胁聚焦