Methbot 活动分析报告

2016 年 12 月 20 日

Methbot 活动分析报告

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	The Methbot Operation		
原文作者	White Ops	**原文发布日期**	2016 年 12 月 20 日
作者简介	White Ops 是广告欺诈防护的领导者，为广告业提供验证和优化解决方案。我们将数据科学和高级解决方案相结合，旨在检测和防止广告欺诈活动。 请参见文末的公司简介。		
原文发布单位	White Ops		
原文出处	http://go.whiteops.com/rs/179-SQE-823/images/WO_Methbot_Operation_WP.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

Methbot 活动分析报告

White Ops 揭露了迄今为止规模最大、利润最高的广告欺诈活动。

俄罗斯网络犯罪分子对美国媒体公司和广告主发动了广告欺诈活动，每天能够赚取数百万美元的广告费，这是目前发现的利润最高的僵尸机器行动。White Ops 发现黑客的代码中存在“meth”一词，因此将该活动命名为“Methbot”。该活动利用关键的互联网基础设施，伪造付费视频广告位，生成大量的欺诈性视频广告。

Methbot 活动使用大量的自动化网络浏览器，在伪造的网站上每天“观看”视频广告多达 3 亿次。黑客们注册了超过 6000 个域，每天能够赚取数百万美元的广告费。

本报告分析了 Methbot 活动的复杂性和快速演变，以及它对广告生态系统的供需造成的破坏。White Ops 只对它直接观察到的数据进行分析，可能不够全面，该活动造成的实际经济损失可能更大。

此时，Methbot 活动已经渗透广告生态系统的各个层面，关闭它的唯一方法是公布该活动的详细信息，帮助受影响的各方采取行动。为此，White Ops 发布了研究结果。

可下载的信息

- Methbot 活动的 IP 地址和 IP 代理，这是中断黑客获利的最快方法。
- 伪造的域列表和完整 URL 列表，能够显示该活动对广告业的影响程度。该活动对广告主造成了巨大的经济损失。

Methbot 活动概览

规模和估测的经济损失

- 黑客每天能够获利 300 万到 500 万美元。
- CPM 为 3.27 至 36.72 美元，平均值为 13.04 美元。（译者注：Cost Per Mille，每千人成本，是一种媒体或媒体排期表送达 1000 人或“家庭”的成本计算单位。这可用于计算任何媒体，任何人口统计群体及任何总成本。）
- 伪造的广告观看次数为每天 2 亿- 3 亿次。
- 伪造了 250267 个 URL。
- 注册了 6111 个域。
- 以高价值市场（包括 PMP[私有交易市场]）为目标。

基础设施

- 掌握了 571904 个 IP 地址，其中很多伪装为美国的互联网服务提供商（ISP）。
- 控制着 800-1200 台服务器，它们托管在美国和荷兰的多个数据中心。

规避检测的高级技术

- 模拟点击、鼠标移动和社交网络登录信息，使其看起来更真实。
- 操控与其 IP 地址相关的地理位置信息。
- 针对十多家广告技术公司的代码采取特殊对策。
- 完全自定义 http 库和支持 Flash 的浏览器引擎，所有这些都在 Node.js 环境下运行。

目录

简介

2015 年 9 月，White Ops 安全研究团队发现了一些类似僵尸机器活动的自动化网络流量，于是将其隔离并进行监控。当时，这些活动（称为 C3）很少，规模也不大；直到 2016 年 10 月，Methbot 活动迅速扩张。

Methbot 活动对广告生态系统的影响之大是前所未有的。黑客每天赚取高达 500 万美元的广告费，因此 Methbot 造成的经济损失远远超过了以前发现的僵尸网络。ZeroAccess 每天最多赚 90 万美元，Chameleon 僵尸网络每天最多赚 20 万美元，HummingBad 每天最多赚 1 万美元。

僵尸机器行动	类型	目标	估计每日损失
Methbot	僵尸机器农场	视频广告	300 万美元
ZeroAccess	恶意软件	广告欺诈和比特币挖掘	90 万美元
Chameleon	恶意软件	广告欺诈	20 万美元
Avalanche	恶意软件	身份窃取，访问控制	39139 美元
Ponmocup	恶意软件	盗窃	27778 美元
Metuji and Mariposa	恶意软件	身份窃取，访问控制	未知

为了规避检测，该黑客组织开发了一组专用于 Methbot 广告欺诈活动的基础设施。他们不采用传统的恶意软件僵尸网络结构（对现有的 IP 地址和相应的计算机进行攻击），而是开发了自己的浏览器，利用该浏览器在分布式网络中扩展活动。

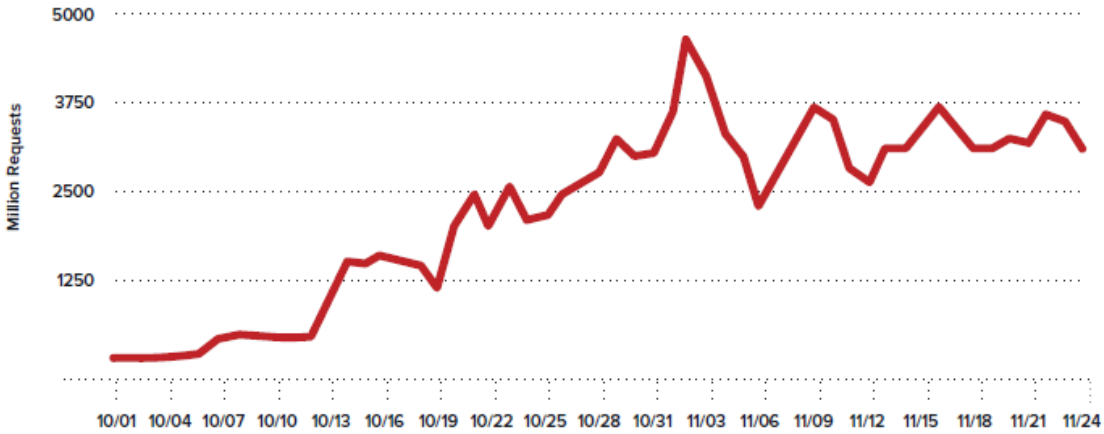
使用伪造的 IP 地址能够规避典型的数据中心检测方法。这是超越传统僵尸网络的一种创新，因此 Methbot 是一种新的僵尸机器欺诈类型。

发现和历史

2016 年 9 月，White Ops 发现一个小规模的僵尸机器活动（2015 年 9 月首次发现，当时称为 C3）出现了变化。White Ops 安全研究团队继续追踪 C3 的发展，一路见证它进化为所谓的“Methbot”活动。

2016 年 10 月 5 日，Methbot 开始大规模扩张，每天的广告收看次数多达 1.37 亿次。截至 10 月中旬，White Ops 媒体卫士防御服务（MediaGuard Prevention Service）每天能够检测到针对多个广告平台的 30 到 50 亿次出价请求。到 10 月底，Methbot 活动已经影响了 32 个客户。

在 10 月份的飙升之后，Methbot 继续生成大量的广告收看次数，同时每天调整其代码库，希望规避欺诈检测和厂商审查。



Methbot 广告收看次数（White Ops MediaGuard™）

广告生态系统（基础）

数字广告领域越来越依赖技术来处理广告和媒体计划，为促进广告主（需求方）和媒体（供应方）之间的交易而建立的技术平台已成为至关重要的组成部分。这创造了一个传统的市场，供需双方就在这个市场中做生意。

广告主

代理机构代表广告主规划广告并执行媒体规划，旨在精准地投放广告。这些规划可以通过需求方平台（DSP）来传递，该平台将广告交换和媒体联系起来，从而确定目标受众。通常，广告主会根据受众人口统计信息进行分层，或者在私有交易市场（PMP）中寻找广告资源，以完善媒体规划。

媒体

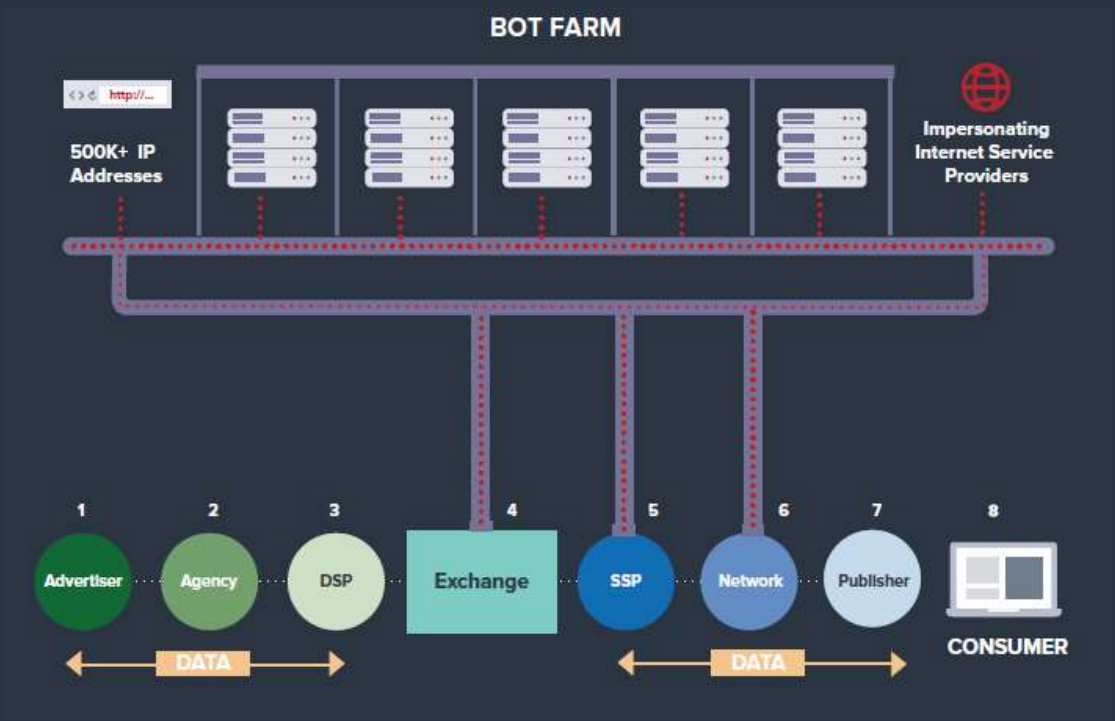
供应方平台（SSP）为媒体的广告投放进行全方位的分析和管理。通常，它会收集媒体和网络的广告资源，以便为 DSP 和其他出价者提供大量的受众。为了满足特定广告主的需求，SSP 和媒体可以打包优质的广告资源和受众群。当竞价完成后，系统会接受最高出价，加载并发送广告素材，以便消费者了解产品。

广告生态系统（基础）

Methbot 如何盈利

Methbot 如何渗透广告市场

人类受众和优质媒体资源的需求量很大，因此 Methbot 组织致力于生产这两种产品。他们造成大量受众“观看”其广告的假象，通过伪造域和广告来劫持知名媒体的品牌力量，骗取数百万美元的广告费。



MethBot 如何盈利：

- 模拟已建立的网站并伪造广告资源
- 运行自定义的桌面浏览器
- 模拟鼠标移动和社交网络登录

高级僵尸机器行为

模拟人类行为

广告主通常依赖于存储在用户机器上的 cookie 数据，根据人口统计信息、浏览历史、购买历史等数据，精准地投放广告。Methbot 组织利用这种方法，使用一个通用的开源库在伪造的网络会话中插入编造的 cookie 数据，让广告主认为这些信息是有价值的。通过这种方式，他们会显示较高的 CPM（每千人成本），欺骗广告主支付更多的广告费。

Methbot 组织还模拟真实的人类行为。他们伪造鼠标移动和点击，模拟用户观看广告的行为，使得这些行为看起来更加真实。此外，他们采用复杂的技术来提供更加令人信服的人类行为。Methbot 伪造社交网络登录信息，看起来就像是用户在收看广告时登录了。

操控地理位置数据库

程序化广告通常使用地理位置数据，以确保广告投放到所需的区域，这种广告的价格通常比较高。通过操控这些数据，使其看起来像是针对更多“高价”区域，这样能够提高广告费。

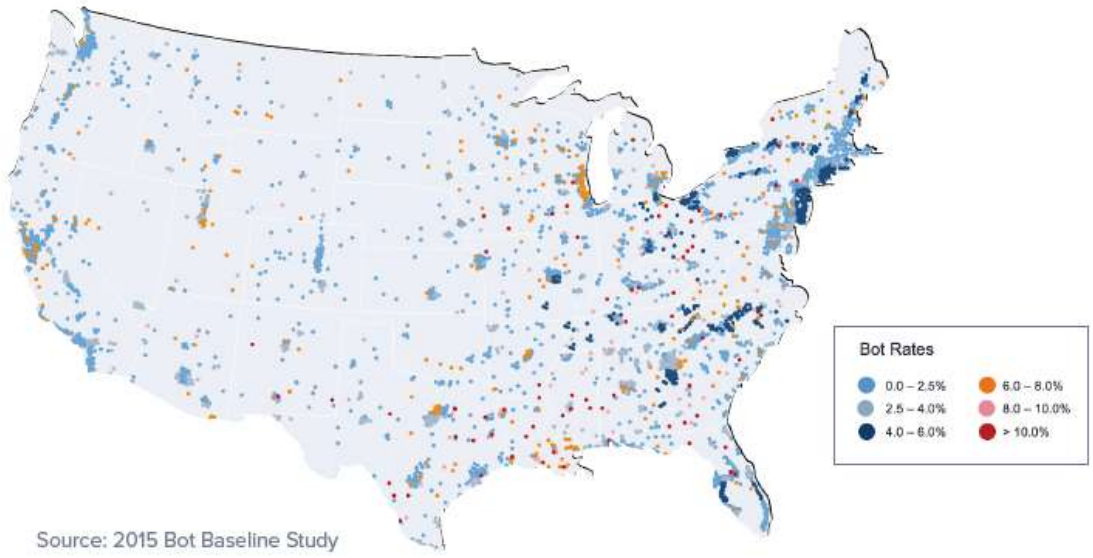
计数器检测行为

Methbot 使用几种技术来规避逻辑检测并欺骗验证，以确保伪造的广告能够带来收益。

一种新的僵尸机器活动

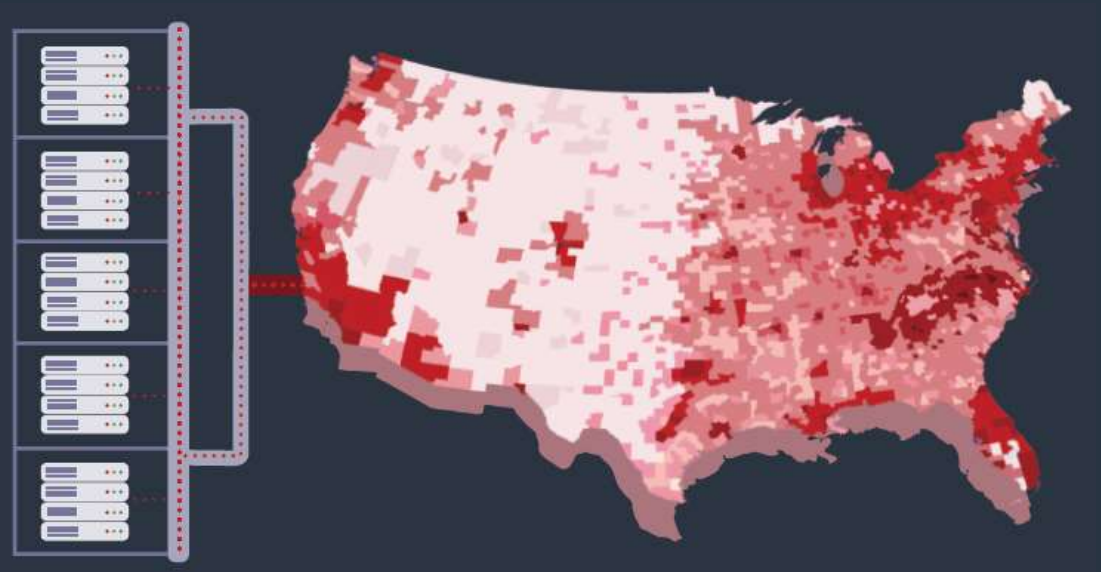
基于数据中心的广告欺诈活动通常很容易检测。传统上，大多数高级广告欺诈活动依赖于感染计算机的恶意软件（与人类用户位于相同的 IP 地址），这样一来，僵尸网络可以在后台运行伪造的浏览器会话并生成欺诈性广告活动。然而，这种方法需要不断地感染家庭计算机，有局限性，尤其是当现有的感染被反恶意软件厂商发现和清除之后。

了解这种情况后，Methbot 黑客们投入了大量时间和资源来开发和构建基础设施，希望消除这些限制，为他们提供无限制的规模。他们使用专用服务器来运行代理，以隐藏其活动的源头。他们使用伪造的文档，注册或租赁了 571904 个真实的 IP 地址，利用这些 IP 地址生成欺诈性广告，伪装为来自合法的互联网服务提供商，如 Verizon，Comcast，Spectrum 等。根据 IPv4 Market Group 公布的数据，仅这些 IP 地址的价值就超过了 400 万美元。



传统僵尸网络依赖于感染计算机的恶意软件

Methbot 僵尸机器农场



专用基础设施提供无限制的规模

- 800-1200 台 Methbot 服务器。
- 能够执行并行、可靠和冗余操作的分布式系统。
- 浏览器模拟，使伪造的域看起来更加真实。
- 模拟的浏览器对象包括屏幕信息、插件列表、内置函数和支持事件等。

经济损失

White Ops 咨询了一家程序化媒体情报公司 AD/FIN，以了解 Methbot URL 列表的成本。我们的联合分析表明，Methbot 的广告成本为 3.27 美元/CPM 到 36.72 美元/CPM，平均值是 13.04 美元/CPM。

Methbot 造成的经济影响继续震荡着广告业。White Ops 估计，自 2016 年 10 月初以来，Methbot 广告收看次数为每天 2 亿至 3 亿次。AD/FIN 的 CPM 数据显示，该组织每天能赚 300 万到 500 万美元。

Methbot 的利润计算

	低	最接近	高
每日广告观看次数	2 亿次	3 亿次	4 亿次
CPM（每千人成本）	13 美元	13 美元	13 美元
总数	260 万美元	390 万美元	520 万美元

White Ops 应客户和客户平台的要求继续监控和检测该活动。但是，鉴于该活动的规模和覆盖面很大，我们权限范围之外的其他公司也可能会受到影响。我们的目标是关闭 Methbot 活动，终止该组织的盈利能力。因此，我们发布了研究结果，希望能够帮助广告主、代理机构、平台和媒体掌握这些信息，阻止 Methbot 活动。

可下载的信息（地址 WWW.WHITEOPS.COM/METHBOT）

Methbot 组织的 IP 地址，帮助广告主、代理机构和技术提供商阻断这些地址，防止他们被欺骗。

伪造的域列表和完整 URL 列表，能够显示该活动对广告业的影响程度。该活动对广告主和媒体造成了巨大的经济损失。

呼吁透明度

当前的广告生态系统具有复杂性，互连性和匿名性，因此 Methbot 黑客能够利用整个市场。广告收看次数可能经过了多层处理。由于围墙花园、转售、竞争和人力资本的限制，在市场中追踪完整的路径是很困难的。

广告业可以通过调整供应和需求利益来防御这种威胁，保护整个生态系统。媒体和他们的广告客户之间的密切关系可以帮助规避这种模糊性并增加透明度，这将使得 Methbot 这样的高级活动更难利用该系统。广告欺诈活动是灵活的，通过转变、改变代码库，或者在被阻止时转向未受保护的目标，来适应环境。将人类最佳做法和防御技术相结合，增加广告市场的透明度，能够帮助该行业防御威胁并提高确定性。

White Ops 与可信赖问责组织（Trustworthy Accountability Group，TAG）业内反欺诈联盟合作，分享和传播必要的数据，以帮助终止 Methbot 活动。我们希望该报告的发布能够快速结束 Methbot 活动。

请联系我们：threatintel@whiteops.com。

技术分析

Methbot 技术分析

在下文中，我们将详细分析对广告生态系统造成巨大经济损失的 Methbot 工具、战术和程序（TTP）。

僵尸机器的特征

Methbot 使用定制的软件，专用 IP 地址空间和服务器基础设施。White Ops 检测技术能够使用名为“reflection”的 JavaScript 语言功能，广泛收集有关其内部工作的详细信息。僵尸机器运行于 Node.js 环境，并使用几个开源库来添加其他功能。它主要在大规模、多数据中心的分布式系统上运行，以执行并行、可靠和冗余操作。

僵尸机器使用的一些开源库和工具包括：

- tough-cookie，用于保留会话数据。
- cheerio，用于解析 HTML。
- JWPlayer，用于运行广告标签和请求视频广告。
- Node.JS

Methbot 可以模拟桌面浏览器的用户代理字符串，伪装为主要的桌面浏览器。White Ops 检测到的数量最多的浏览器标识是 Google Chrome，包括版本 53 和 54。Firefox 47，Internet Explorer 11，Safari 9.1 和 9.2 也常被模拟。Methbot 黑客还模拟操作系统，包括 Windows 10 和一些旧版本，以及 Mac OS X 的若干版本（从 10.6 到 10.12.1）。

除了浏览器模拟，Methbot 还使用各种方法来规避反欺诈技术，嵌入适当的上下文响应，以进一步造成人类用户使用浏览器的错觉。

分布式硬件

Methbot 节点是位于美国德克萨斯州（达拉斯）和荷兰阿姆斯特丹的数据中心的物理服务器。每台服务器都运行 Methbot 浏览器组件的多个实例和一个代理。截至 2016 年 12 月，我们估计 Methbot 组织拥有 800 到 1200 台服务器。

代理网络

与大多数广告欺诈活动不同，Methbot 通过运行于其服务器的代理获取多种 IP 地址。通常，由于 IP 元数据提供者能够识别与数据中心有关的流量，广告业能够识别属于数据中心的 IP 地址并将其列入黑名单，因此这种单源方法并不太有效。

Methbot 黑客直接控制大量连续的 IP 地址，并伪造注册信息，使其看起来像是属于美国的互联网服务提供商（ISP），如 Comcast，Cox，AT&T，Verizon，Centurylink 等，这样就能够避免这个问题了。通过一些早期的记录，我们发现黑客完全编造实体，如“HomeChicago Int”,或使用类似于知名公司的名称,如“AmOL wireless Net”和“Verison Home Provider LTD”。根据发现的流量，我们确定 Methbot 组织控制着 571904 个 IPv4 地址。这是什么概念呢，Facebook 也不过拥有这个数字的一半而已。

关键行为

知名网站上的视频广告的价格会比较高。Methbot 伪造知名媒体的 URL 地址，利用他们的品牌能力，诱骗广告主支付广告费用，手段如下：

1. **伪造页面：**Methbot 从知名媒体列表中选择域或 URL，并伪造页面。该页面只包含支持广告所需的内容，不会与媒体的服务器联系。

2. **提供广告资源：**Methbot 使用行业标准 VAST 协议，使用 Methbot 的标识符之一从网络请求视频广告，以便提高其可信度。（译者注：Video Ad Serving Template 是互联网广告署 IAB 制定的视频广告开放协议，视频播放器直接请求某个 VAST 内容的 URL，读取 VAST 中相关的素材及监测代码即可获取广告素材内容并播放广告。大部分视频媒体同自己广告投放系统对接均采用该协议。请参见 https://zhuanlan.zhihu.com/p/22832134。）

3. **伪造观看和点击次数：**视频广告通过代理加载并在模拟浏览器中“播放”。任何指定的反欺诈和可见度验证码也会被加载，并反馈伪造的信号，使活动看起来是合法的。

截至目前，我们发现 Methbot 共生成了 6111 域和 250267 个 URL。

URL 示例

- http://ibtimes.co.uk/video
- http://vogue.com/video
- http://economist.com/video
- http://espn.com/video
- http://www.cbssports.com/CBS_Air_Force_Falcons_Fall_Gear
- http://fortune.com/2016/09/28/department-stores-closings/
- http://foxnews.com/video

规避反欺诈服务的对策

Methbot 使用几种技术来规避反欺诈和可见度检测公司的审核。

欺诈检测公司通常测量浏览器环境并查找数据中的异常情况。例如，用户代理字符串可能显示 Firefox 浏览器，但是浏览器的行为可能与此不一致。通过伪造浏览器行为，Methbot 希望让欺诈检测公司认为他们的流量是合法的，从而继续欺诈活动并赚钱。

Methbot 使用几种技术来规避可见度检测和欺诈检测公司的审核。模拟的浏览器对象包括屏幕信息、插件列表、内置函数和支持事件等。

```
function Screen(browser) {
    var oss = browser.os[0];
    this.availWidth = browser.screenW;
    this.availHeight = browser.screenH - ((oss==='W')? 40: 27);
    this.width = browser.screenW;
    this.height = browser.screenH;
    this.colorDepth = 24;
    this.pixelDepth = 24;
    this.availLeft = 0;
    this.availTop = (oss==='W')? 0: 23;
    this.orientation = {angle:0, type:"landscape-primary"}
}
```

屏幕构建

```
function __MethSetSetters() {
    Object.defineProperties(this, {
        prompt: {
            get: function() {
                var f = function() {}
                f.toString = function(){
                    return "function prompt() { [native code] }"
                }
                f.toString.toString = function(){
                    return "function toString() { [native code] }"
                }
                return f
            },
            enumerable: true
        },
        onrejectionhandled: {
            value: null,
            writable: true,
            enumerable: true
        },
```

Methbot 在上下文中定义属性 ,以模拟浏览器的 “窗口” 和 “文档” 对象。

```
onload: {
    get: function() {
        return null
    },
    set: function(func) {
        this.addEventListener('load', func);
    }
},
```

允许第三方 JavaScript 注册到上下文事件中的代码。

```
var event = win.document.createEvent('UIEvents');
event.initEvent('beforeunload', false, true);
win.dispatchEvent(event);

event = win.document.createEvent('UIEvents');
event.initEvent('unload', false, false);
win.dispatchEvent(event);
```

人工创建和分派事件。

动态代码修复

当模拟太过麻烦时，Methbot 就会动态修改第三方脚本以返回“已知正常”值，避免需要实现复杂的 API（应用程序编程接口）。该技术针对各种欺诈检测措施，多个厂商的可见度代码，以及各种社交网络的登录状态功能。

```
var text = resp.body.toString();
if (text.indexOf('{}.toString.apply(') !== -1) {
    //function(){}.toString.apply(
    text = text.split('function() {}.toString.apply(').join('window.__MethFakedFuncToString(');
    text = text.split('function(){}.toString.apply(').join('window.__MethFakedFuncToString(');
    text = text.split('Function.prototype.toString.call(').join('window.__MethFakedFuncToString(');
    text = text.split('{}.toString.apply(').join('window.__MethFakedToString(');
    //text = text.spli
    text = text.split(
    //text = text.spli
    text = text.split(
    //setTimeout(function(){self.__fire()}, 150);
}
```

通过修复代码来击败功能分析代码

White Ops 安全研究团队发现了分析代码（Methbot 开发人员解析了最广泛采用的欺诈检测厂商的逻辑）的痕迹。显然，他们花了一些时间逆向工程这些功能，在合法浏览器中手动运行测试代码，以了解其输出值，然后利用该逻辑模拟这些值。

可见度伪造

可见度是一种技术测量手段，用于验证数字广告是否在屏幕上显示，并且通常用作广告客户支付广告费用的指标。除了专门设计代码来对抗特定厂商的可见度测量手段，Methbot 组织还伪造行业标准。特别是，VPAID 事件。（译者注：Video Player-Ad Interface Definition，视频播放器广告接口定义，因其区别 VAST 能够实现更加丰富与互动的流媒体视频体验，于是在中国市场俗称互动贴片。简单讲就是视频广告通过 VPAID 获取了一些视频媒体播放器的控制权，可以完成很多 VAST 模式下无法完成的互动和监测的功能。但由于媒体丧失了一定控制权，视频媒体目前政策上大都不是十分的支持。请参见 https://zhuanlan.zhihu.com/p/22832134。）

例如，根据接收的事件，对以下功能进行模拟：

```
if (typ in this.__MethVastTrackings) {
    var tts = this.__MethVastTrackings[typ];
    for (var i = 0, l = tts.length; i < l; i++) {
        this.__get(tts[i], function(){}, 'image/webp,*/*;q=0.8');
    }
}
```

接收到第一个事件时调用 VAST 追踪 URL。

```
if (typ === 'complete' || typ === 'error' || typ === 'Mtimeout')
    return this.__MethFlashKill(typ);
```

在接收到事件时销毁 flash 对象。

```
if (typ === 'impression' && rand < 0.01)
    return this.__MethFlashKill('rand imp');
if (typ === 'start' && rand < 0.01)
    return this.__MethFlashKill('rand start');
if (typ === 'firstQuartile' && rand < 0.01)
    return this.__MethFlashKill('rand first');
```

在不同的点随机中断回放，以模拟人类行为。

```
if (typ === 'firstQuartile' && rand < 0.017)
    this.__MethFlashClick();
```

最后，以随机生成的方式模拟点击，使其看起来更真实。

```
if (this.document.querySelectorAll("a").length === 0){
    var im = this.document.querySelectorAll("input[type=image]")[0];
    if (im !== undefined) {
        var browser = this.__MethBrowser;
        return setTimeout(function() {
            browser.humanEvents();
            browser.humanEvents();
            im.click(undefined, parseInt(10+Math.random()*490),
                    parseInt(50+Math.random()*440));
        }, 1000*(2 + 10 * Math.random()))
    }
}
```

当执行并未中断时，如果在上下文中创建了链接图片（VAST 随播广告就是这样），就会模拟人类行为并点击这些图片。

模拟人类输入

我们发现，Methbot 组织多次调用一个名为 humanEvents 的函数，这都是通过一个随机定时器触发的。

```
return setTimeout(function() {
    browser.humanEvents();
    browser.humanEvents();
    im.click(undefined, parseInt(10+Math.random()*490),
             parseInt(50+Math.random()*440));
```

点击模拟，欺骗寻找输入事件的点击验证逻辑。

```
var event = doc.createEvent("HTMLEvents");
event.initEvent("load", false, false);
next.dispatchEvent(event);
browser.humanEvents();
win.__MethScripts = win.__MethTempScripts.concat(win.__MethScripts);
win.__MethTempScripts = [];
win.__MethNextScript();
```

在 DOM(文档对象模型)初始化之后，创建和分派 onload 事件。

White Ops 安全研究团队发现的代码显示，Methbot 能够模拟社交网络登录，用于增加其可信度。

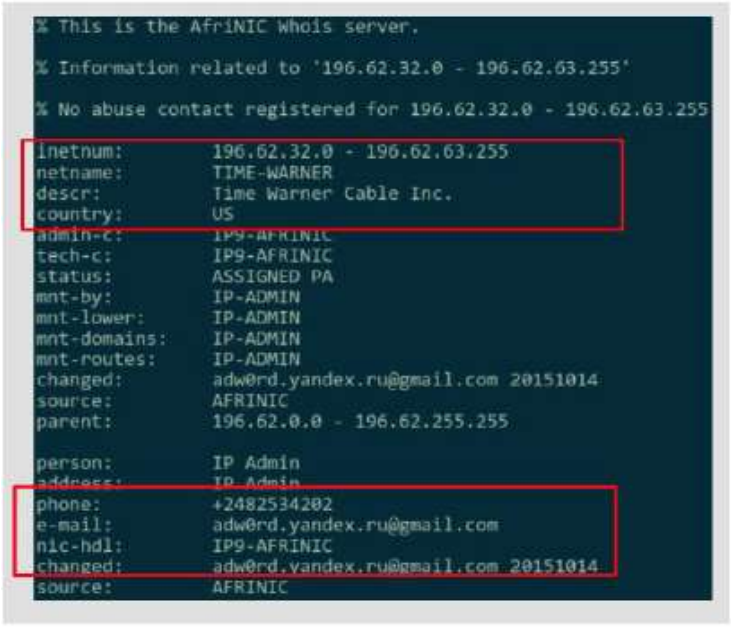
伪造 IP 注册信息

虽然我们常见到被恶意软件感染的计算机构成僵尸网络，这样能够实现 IP 多样性。但是，这是我们第一次发现数据中心模拟家庭互联网连接。Methbot 活动不需要持续感染家庭计算机，不受这一问题的限制，因此其规模是无限的。

Methbot 使用的代理允许其流量来自 571904 个 IP 地址中的任何一个。它伪造这些 IP 地址的注册信息，使它们看起来像是属于美国的互联网服务提供商（包括 Comcast，Cox，AT&T，Verizon，Centurylink 等），从而规避典型的数据中心检测。除了真实的公司，该组织还编造实体名称，如“HomeChicago Int”，“AmOL wireless Net”和“Verison Home Provider LTD”。

除了简单地规避黑名单，Methbot 组织还利用这种伪造诱骗广告主支付广告费。

举例来说：



- 伪造时代华纳有线公司等的 IP 地址。
- 注册国家是美国。
- 可疑的联系人电子邮件地址。
- 塞舌尔电话号码。

关于 White Ops

White Ops 是广告欺诈防护的领导者，为广告业提供验证和优化解决方案。我们将数据科学和高级解决方案相结合，旨在检测和防止广告欺诈活动。我们的使命是通过人类验证技术阻止广告欺诈活动的传播。我们与业界团队合作，致力于阻止广告业的恶意活动，并提高整个行业的透明度。White Ops 总部位于纽约市，卫星节点遍布世界各国。

欲了解更多信息，请访问 www.whiteops.com。

Methbot 活动分析报告

请联系我们：threatintel@whiteops.com。