3ve-网络虚假广告攻击事件分析

s小胖不吃饭 / 2018-12-02 08:21:00 / 浏览数 2514 技术文章 翻译文章 顶(0) 踩(0)

事件介绍

国际执法部门强烈抨击制造虚假广告的团队。

在10月22日（星期一）这一天，一项涉及全球执法机构的黑客行动将目标瞄准了被称为"3ve"的网络广告欺诈团体。在2018年11月27日，此事件中里8名被告的13项起诉书
在这八名被告中，有三名参与方被拘留并等待引渡。
多年来，广告欺诈活动一直困扰着互联网的广告生态系统。这些欺诈也使合法公司的收入逐渐减少。而在我们的分析中，这些广告欺诈的过程始终是相似的：尽管所有的诈
除了上述方法外，这里还存在另外一种广告欺骗策略——Stantinko。它监听了用户的点击次数，并将用户访问的页面重定向到具有欺诈信息的广告。在3ve的情况下，它并

上述的这些方案能够绕过现有欺诈防御措施的一个关键原因是其能确保伪造的请求来自大量拥有合法IP地址的用户。
3ve依靠至少两个不同的僵尸网络来访问这样一个地址：Boaxxe和Kovter。
自从ESET研究人员开始积极调查这两个僵尸网络以来，我们通过向执法部门提供技术数据来援助抗3ve的行动。当然，对于虚假网站的调查研究需要来自不同行业合作伙伴的

US-CERT发布了一个警告，交代了3ve的僵尸网络的攻击行为以及它如何与Boaxxe和Kovter僵尸网络进行交互。
除此之外，它还列出了一些预防措施，以避免受到这两个恶意软件的影响。如果用户部署ESET客户并且正在担心Windows系统可能会受到此威胁的危害，那么可以下载并使

在这篇文章中，我们将详细介绍我们如何获得中断操作所需的Boaxxe和Kovter基础架构技术相关的数据。

Boaxxe

我们已在2014年的两篇文章中发布了与此广告欺诈相关僵尸网络的详细分析。当时，Boaxxe（也称为Miuref）正在将用户流量重新路由到其控制的链接中来。
更具体地说，当受害者在搜索引擎中查找特定关键词时，它会将受害者的搜索结果点击链接重定向到它控制的网站而不是搜索引擎返回的网站。
这可以通过使用Firefox或Chrome浏览器扩展或在嵌入模式下使用Internet Explorer来实现。
但是，受Boaxxe攻击的系统能够代理流量，、使其看起来像是真正的链接。 3ve正在使用这种方式来实施它们的广告诈骗计划。

Boaxxe的代理功能非常简单：它从C■C服务器接收RC4加密的DNS或HTTP请求，之后解密并执行它，最后将结果发送回C■C服务器。
从3ve向受损Boaxxe系统发出的经典解密HTTP请求如下所示：

```
GET /banners/ajtg.js HTTP/1.1
Host: img.1rx.io
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36

Accept: */*
Referer: http://eatingwell.com/recipes/17986/side-dishes/

Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
```

受感染的系统将发出此请求，并有效地"访问"被托管广告页面，之后将响应发送回其C＆C服务器。 这就是3ve利用Boaxxe受损的系统来进行其广告欺诈的方式。
有趣的是，我们曾发现过类似的攻击请求，因为从2016年初开始，3ve就开始向Boaxxe中不安全的系统发送过类似的请求。那时，只有来自美国IP地址中的Boaxxe服务器被

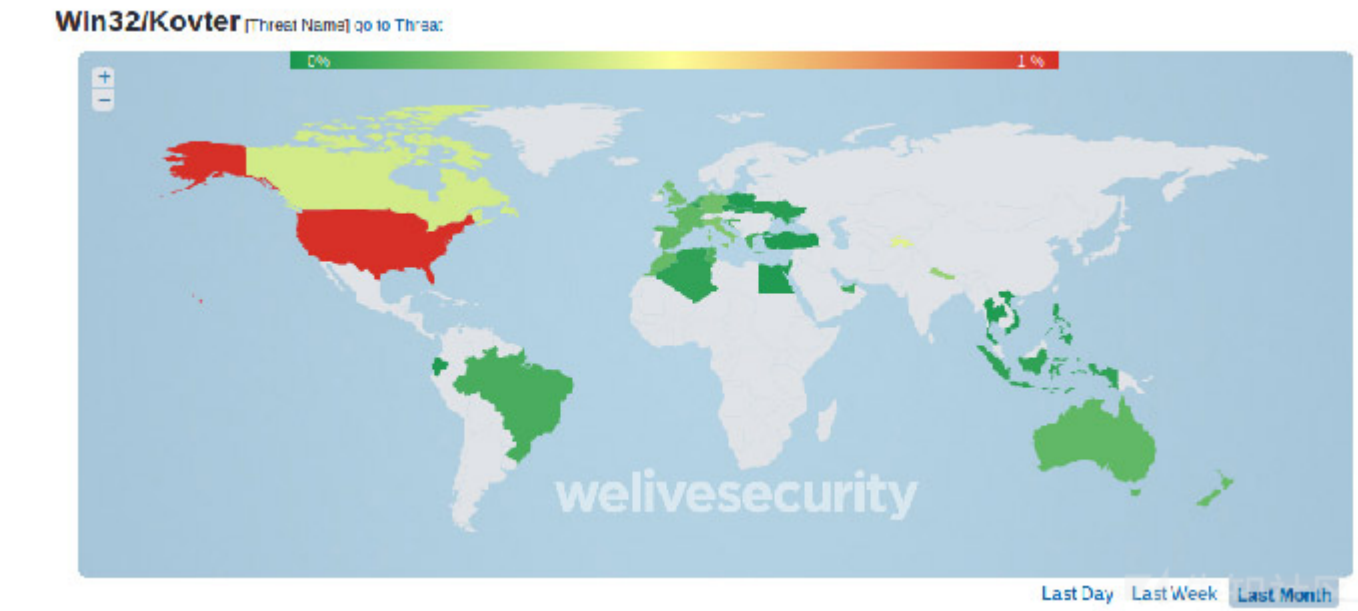
Kovter

ESET在2014年首次检测到当时是勒索软件的Kovter。
从那时起，Kovter系列的恶意软件就已经向广告诈骗的方向发展。并在这些年增加了一些功能更为强大的欺骗和隐身技术。
值得注意的是在欺骗方面，如果它检测到有网络监视器的存在，那Kovter就能够发送虚假流量。倘若Windows任务管理器已经启动，则终止其自己的衍生进程。
现在，通过将其加密的恶意有效负载存储在Windows注册表中，并使用所谓的"无文件"持久性的技术，此恶意软件的隐蔽性则更强了。
此外，它确保了系统仅在未被使用或者显示器断电的情况下执行广告诈骗的操作。它还能够在用户查看广告时屏蔽所有视觉效果或声音效果。这也使得攻击对于用户来说并不

3ve运营商利用Kovter僵尸网络的方式与Boaxxe不同。 受损的Kovter系统可以从其C＆C服务器接收任务，并使用隐藏的`Chrome Embedded Framework`浏览器直接执行该任务。
至今为止，我们已经通过僵尸网络跟踪器平台追踪Kovter两年之久。而该系统也使我们能够实时跟踪当下最活跃的僵尸网络。通过分析追踪平台的数据，我们可以发现：僵尸
其不同的配置文件情况; 下载其恶意软件更新; 查看网络收到的命令; 获取安装的恶意软件详情。
ESET平台的主要作用是维护用户的平台以达到最高的保护级别，并能够丰富ESET威胁情报源。但是，它也可以用于提供中断操作的技术数据，例如我们在2015年参加的`Dor / Gamarue`的技术数据情况。

如同Boaxxe一样，Kovter目前使用了多种不同的方式将恶意广告交付给毫无戒心的受害者，包括垃圾邮件，偷渡式下载和按次付费计划。
我们发现了一个有趣的现象，3ve在操作攻击的过程中使用Nemucod安装了这两个恶意软件。

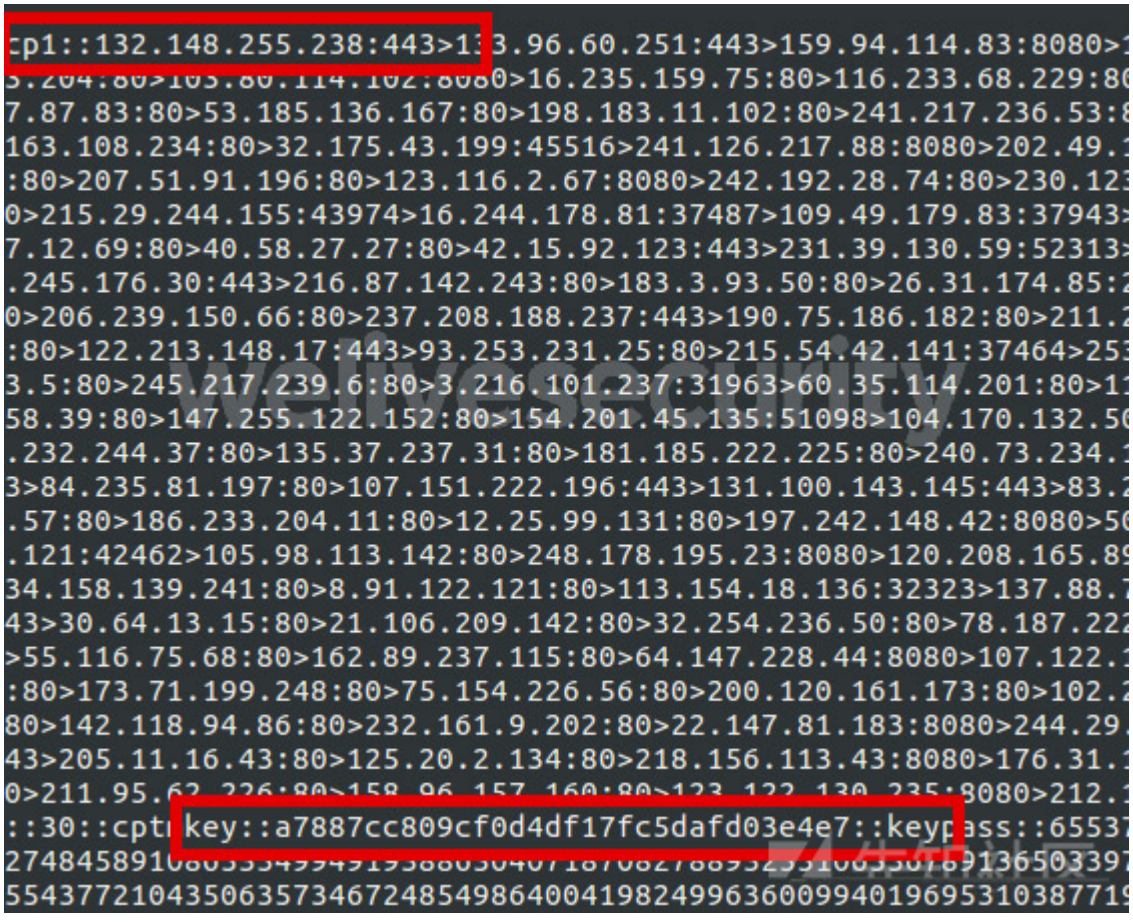
如前所述，通过我们的Boaxxe监控，我们看到的3ve操作的第一个步骤是位于美国的受损系统被用于代理广告的欺诈请求。
根据Kovter的测试，我们可以看到Kovter僵尸网络的目标主要针对北美。



Kovter C■C服务器进行分层工作。 首先，Kovter bot将检索存储在其资源部分中的静态配置。 配置文件使用以下格式加密存储：

<16 bytes reversed RC4 key><base64-encoded, encrypted data><16 bytes of padding>

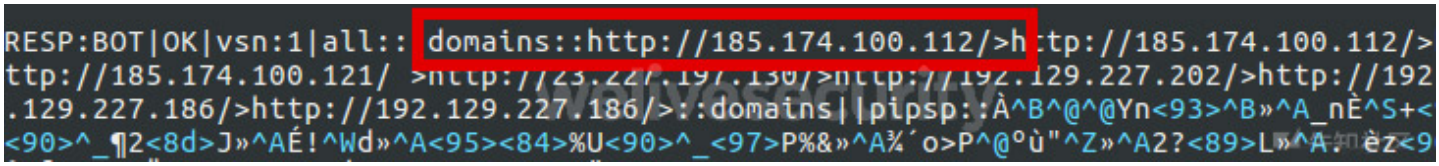
此配置文件包含一级C＆C服务器列表以及网络通信所需的RC4密钥。



为了检索二级C■C服务器，自动部署程序使用以下格式向第一级C■C服务器发送HTTP POST请求：

RESP:BOT|c:IPS|vsn:1|<random hex string>

十六进制字符串由随机十六进制字符[0-9a-f]组成，并且其长度在32到128个字符之间。 POST请求使用随机RC4密钥加密。
而此随机密钥被附加到数据包，并使用静态配置文件中的RC4密钥对整个消息进行加密。
生成的通信通过原始套接字直接发送到第一级C＆C服务器。之后第二级C＆C服务器进行相应。这些过程负责将广告欺诈任务移交给自动化代码程序。



通过我们的Kovter跟踪，我们能够识别出几个一级和二级C＆C服务器。 这些数据已传递给执法部门并用以帮助进行中断操作。

```
1st skimmer: bootstrap-js[.]com
2nd skimmer: g-statistic[.]com
1st skimmer's exfil domain: bootstrap-js[.]com
2nd skimmer's exfil domain: onlineclouds[.]cloud
```

令人感到有趣的是，自中断操作以来我们已经看到当前第一级C＆C服务器的行为发生了变化。
他们目前将消息返回到传统的“localhost”IP地址（即127.0.0.1）作为他们的第二级C＆C服务器。
当然，我们无法知道这种变化背后的原因，但他们这样做很可能是为了暂停他们的僵尸网络，同时分析自己被打击的原因。

最终评论

广告诈骗僵尸网络已存在很长时间，并在此阶段花费了大量资金用于向全球的广告商家推广自己的诈骗网站。

通过打击其运营面，我们能够对其诈骗事件进行反击。除此之外，此方法也对破坏3ve运行规模以及维持互联网生态系统的完整性至关重要。ESET很自豪能够尽可能地发挥作

如果你认为自己感染了Boaxxe或Kovter病毒，我们将为您提供免费工具。ESET Online Scanner可检测并删除恶意软件，包括数千种Boaxxe和Kovter模块。

有关3ve广告欺诈机制的更多详细信息可以通过在此处阅读有关此操作的Google和White Ops白皮书进行获取。

■■■■■■■https://www.welivesecurity.com/2018/11/27/3ve-online-ad-fraud-disrupted/

上一篇：[译]如何在任意进程中修改内存保护属性 下一篇：Vulnhub Raven:2
1. 0 条回复
   - 动动手指，沙发就是你的了！