

# C&C控制服务的设计和侦测方法综述

phunter (/author/phunter) · 2015/11/06 9:40



(/author/phunter)  
phunter  
(/author/phunter)

这篇文章总结了一些我在安全工作里见到过的千奇百怪的C&C控制服务器的设计方法以及对应的侦测方法，在每个C&C控制服务先介绍黑帽部分即针对不同目的的C&C服务器设计方法，再介绍白帽部分即相关侦测办法，大家来感受一下西方的那一套。这里的白帽部分有一部分侦测方法需要一些数据和统计知识，我也顺便从原理上简单讨论了一下用数据进行安全分析的方法，从数学和数据原理上思考为什么这么做，可以当作数据科学在安全领域的一些例子学习一下。

## 0x00 什么是C&C服务器

C&C服务器（又称CNC服务器）也就是 Command & Control Server，一般是指指挥控制僵尸网络botnet的主控服务器，用来和僵尸网络的每个感染了恶意软件（malware）的宿主机进行通讯并指挥它们的攻击行为。每个malware的实例通过和它的C&C服务器通讯获得指令进行攻击活动，包括获取DDoS攻击开始的时间和目标，上传从宿主机偷窃到的信息，定时给感染机文件加密勒索等。

为什么malware需要主动和C&C服务通讯？因为多数情况下malware是通过钓鱼邮件啊等方法下载到感染宿主机，攻击者并不能主动得知malware被谁下载，也不能主动得知宿主机的状态（是否开机是否联网等），除非malware主动告诉他，所以malware都会内置一套寻找C&C主控服务器的方法以保持和C&C的联络和断线重连。C&C控制服务的攻防要点在于，攻击者能不能欺骗防御者成功隐藏C&C服务：如果防御者侦测到了隐藏的C&C服务，通过一些技术（封禁域名和IP等）或者非技术手段（汇报给安全应急中心等）切断malware和C&C之间的联系，就可以有效的摧毁botnet。

寻找到C&C之后malware和C&C之间的通讯方式并不是本文攻防重点，它可以是SSH文件传输也可以是简单的HTTP GET和POST，技巧性不是很大，不多的几个靠传输来隐藏的技巧比如用DNS隧道隐藏流量这类方法如果有需要以后再来一发详细阐述。

## 0x01 IP地址：难度低，易被抓

这是最常见的一类C&C服务器。攻击者在恶意软件的代码里硬编码写上C&C服务器的IP地址，然后在需要和C&C通讯的时候用HTTP拉取需要的攻击指令或者上传从宿主感染机上盗取的信息等等。

这并不是一个高级的办法，因为如果malware的二进制代码被获取，这种用IP的方法很容易被安全人员通过反向工程二进制代码或者检测蜜罐流量得到C&C服务器的地址，从而汇报给服务提供商封禁IP。所以这种方法并不能有效隐藏C&C服务，IP被抓了被反毒软件更新病毒库以后整个botnet就被摧毁了。现在国内的多数malware的主控服务器都是以这种拼运气不被抓的方式存在，他们靠的是malware数量多，今天抓一个当天就再出来三个，市场竞争很激烈。

国外用IP的C&C服务器一般是在Amazon AWS之类的云服务器上，通知了服务提供商很容易封禁IP。国内的云服务商态度暧昧，不过也算还行吧。有机智的国内malware作者在东南亚地区租用云服务IP，可以有效避开国内监管而且速度不错（我并不是教你这么做啊）。

安全人员也不要以为这个方法低级就以为能轻易有效防御，比如说如果感染机不能安装防毒软件或者根本你就不知道中毒了。最近的一个例子是最近比较火的植入路由器的Linux/Xor.DDOS，它的C&C控制就是在AWS上面的IP，造成的影响很大，因为多数人并不知道路由器会被大规模植入恶意软件，路由器本身也很少有防护，正好适合用IP做C&C，还省去了复杂的域名算法和DNS查询的代码保证了软件本身的轻量化。也由于路由本身常开的特性，路由木马也不用担心失去链接，一次C&C的通讯可以保持连接很久，降低了木马被发现的机会。技巧虽然不华丽，但是用的好还是威力强大。该木马的详细分析参见<http://blog.malwaremustdie.org/2015/09/mmd-0042-2015-polymorphic-in-elf.html> (<http://blog.malwaremustdie.org/2015/09/mmd-0042-2015-polymorphic-in-elf.html>)。

## 0x02 单一C&C域名：难度较低，易被抓

因为硬编码的IP容易通过在二进制码内的字符串批量regex扫描抓到，一个变通的办法就是申请一些域名，比如 `idontthinkyoucanreadthisdomain.biz` 代替IP本身，扫描二进制码就不会立刻找到IP字段。这是个很广泛使用的方法，通常C&C域名会名字很长，伪装成一些个人主页或者合法生意，甚至还有个假的首页。即使这么用心，这种方法还是治标不治本，侦测的方法也相对简单，原因是：

- 安全厂商比如Sophos等的资深安全人员经验丰富，他们会很快人工定位到恶意软件可能包含C&C域名的函数，并且通过监测蜜罐的DNS查询数据，很快定位到C&C域名。这些定位的域名会被上报给其他厂商比如运营商或者VirusTotal的黑名单。
- 新的C&C域名会在DNS数据的异常检测里面形成一些特定的模式，通过数据做威胁感知的厂商很容易侦测到这些新出现的奇怪域名，并且通过IP和其他网络特征判定这是可疑C&C域名。

所以常见的C&C域名都在和安全厂商的黑名单比速度，如果比安全研究员反向工程快，它就赢了，但是最近的格局是随着基于数据的威胁感知越来越普遍，这些C&C域名的生命周期越来越短，运气不好的通常活不过半个小时。攻击者也会设计更复杂的办法隐藏自己，因为注册域名需要一定费用，比如带隐私保护的 .com 域名需要好几十美元，寻找肉鸡植入木马也要费很大功夫，本来准备大干一场连攻半年结果半个小时就被封了得不偿失。

在这个速度的比赛里，一个低级但是省钱方便技巧就是用免费二级域名，比如3322家族啊vcp家族等不审查二级域名的免费二级域名提供商，最著名的例子就是 Win32/Nit0l 家族，搞的微软靠法院判来 3322.org 的所有权把他们整个端了（虽然后来域名控制权又被要回去了）。这个方法是国内malware作者最喜欢的一个方法，数据里常见一些汉语拼音类的C&C域名，比如 woshinidie.3322.org 等喜感又不忘占便宜的二级域名，可能因为在我国申请顶级域名麻烦还费钱容易暴露身份，不如闷声发大财。你看，这也不是我在教你这么做啊。

真正有意思的是技术是，比较高级的C&C域名都不止一个，通过一个叫做fast flux的办法隐藏自己。

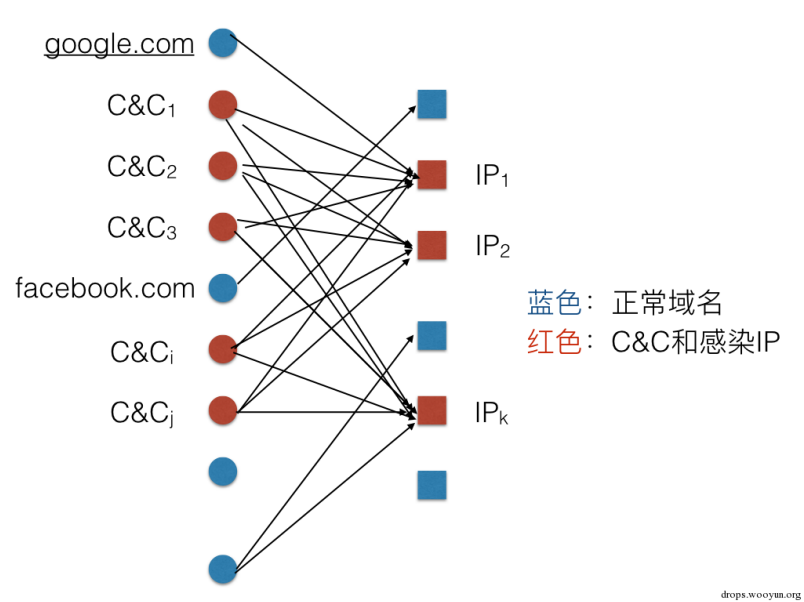
### 0x03 Fast flux, double flux and triple flux

攻击者对付传统蜜罐和二进制分析的办法就是不要依靠单一C&C，取而代之的是快速转换的C&C域名列表(fast flux技术)：攻击者控制几个到几十个C&C域名，这些域名都指向同一个IP地址，域名对应IP的DNS record每几个小时或者几天换一次，然后把这些C&C域名分散的写到malware的代码里面。对于传统二进制分析来说，挂一漏万，如果不能把整个C&C域名列表里面的所有域名放到黑名单上，就不能有效的摧毁这个恶意软件。这就比赛攻击者的隐藏代码能力和防御者的反向工程以及蜜罐监测能力了。这种方法叫做Fast flux ([https://en.wikipedia.org/wiki/Fast\\_flux](https://en.wikipedia.org/wiki/Fast_flux))，专门设计用来对付安全人员的人工分析。

防御Fast flux的方法在流量数据里看相对容易，比如威胁感知系统只需要简单的把每个域名解析指向的IP的历史数据按照IP做一次 group by 就抓住了，利用数据并不难嘛。所以应运而生有更高级double flux和triple flux的办法。

如果攻击者比较有钱，租用了多个IP地址，那么他可以在轮换C&C域名的同时轮换IP地址，这样M个C&C域名和N个IP地址可以有  $M \times N$  种组合，如果设计的轮换时间稍微分散一些，会让蜜罐流量分析缺乏足够的数据支持。侦测double flux的办法需要一些简单的图知识（请系好安全带在家长陪同下观看）：

如果把每个域名和IP地址当做图的节点V，一个有效的 域名-IP 记录当做对应两个节点的边E，那么整个流量数据就可以表示为一个由 V\_域名 指向 V\_IP 的二分有向图 ([https://en.wikipedia.org/wiki/Bipartite\\_graph](https://en.wikipedia.org/wiki/Bipartite_graph))。Double flux的图就是这个巨大二分有向图里的互相为满射的完全二分图，换句话说就是，存在这样一个子图，当中每个 V\_域名 节点都指向同样一个集合的 V\_IP 节点，而每个 V\_IP 节点都被同一个集合的 V\_域名 节点指向。图示如下：



当然了，感染的IP可以访问别的域名，比如图中 google.com。在实际情况里，由于数据采集时间的限制，每个IP节点都要访问所有C&C域名这个条件可以放宽。

当攻击者得知安全人员居然可以用图论的方法干掉他们的double flux这么高级的设计方法之后，更疯狂的triple flux出现了：每个域名的记录里不仅可以添加A record也就是IP的指向，还可以选定不同的命名服务器Name server来解析这个域名，如果攻击者足够有钱（以及有时间精力），他可以控制K个name server定时或者不定时轮换，这样可以造成  $M \times N \times K$  种组合。

Triple flux方法看似机智，好像跑得比谁都快，其实在实现上聪明反被聪明误，漏洞就在name server的设置上：多数正常服务的name server都是专有服务，而多数C&C多架设在免费name server比如DNSpod的免费服务器上。如果攻击者能够控制自己的一系列name server专门作fast

flux，这些server并不是常见的name server。任何非常见的服务器域名都会在流量数据的异常检测里面被监测出来，上一节里面提到异常检测侦测C&C域名的方法对triple flux里面的name server也是可用的。你看，攻击者Naive了吧。

对于fast flux这一类特定flux类方法的监测还有另外一个基于数据和机器学习的方法：如果仔细思考一下fast flux，我们也会发现攻击者试图创造一个聪明的办法，但这种办法本身有一个致命缺陷，也就是追求fast，它的域名对IP的记录转换太快了，导致每个域名纪录的存活时间TTL被迫设计的很短，而绝大多数的正常服务并不会会有如此快速的域名对应IP的记录转换，大型网站的负载均衡和CDN服务的IP纪录转换和fast flux有截然不同的特征。这些特征可以很容易被机器学习算法利用判别fast flux的僵尸网络，相关研究可以参看比如

<https://www.syssec.rub.de/media/emma/veroeffentlichungen/2012/08/07/Fastflux-Malware08.pdf>

(<https://www.syssec.rub.de/media/emma/veroeffentlichungen/2012/08/07/Fastflux-Malware08.pdf>)等较早研究fast flux的论文。

## 0x04 使用随机DGA算法：难度较高，不易被抓

DGA域名生成算法 (Domain Generation Algorithm

([https://en.wikipedia.org/wiki/Domain\\_generation\\_algorithm](https://en.wikipedia.org/wiki/Domain_generation_algorithm)) 是现在高级C&C方法的主流，多见于国外各大活跃的恶意软件里，在VirusTotal里如果见到看似随机的C&C域名都算这一类。它的基本设计思想是，绝不把域名字符串放到malware代码里，而是写入一个确定随机算法计算出来按照一个约定的随机数种子计算出一系列候选域名。攻击者通过同样的算法和约定的种子算出来同样列表，并注册其中的一个到多个域名。这样malware并不需要在代码里写入任何字符串，而只是要卸乳这个约定就好。这个方法厉害在于，这个随机数种子的约定可以不通过通讯完成，比如当天的日期，比如当天twitter头条等。这种方法在密码学里称之为 puzzle challenge，也就是控制端和被控端约好一个数学题，有很多答案，控制端选一个，被控端都给算出来，总有一个答上了。

一个简单的例子（引用自wikipedia

([https://en.wikipedia.org/wiki/Domain\\_generation\\_algorithm](https://en.wikipedia.org/wiki/Domain_generation_algorithm)) 比如说这段代码可以用今天2015年11月3日当做种子生成 cqaqofiwtfrbjegt 这个随机字符串当做今天的备选C&C域名：

```
def generate_domain(year, month, day):
    """Generates a domain name for the given date."""
    domain = ""

    for i in range(16):
        year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFFF) << 11)
        month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFF)
        day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFFF) << 15)
        domain += chr(((year ^ month ^ day) % 25) + 97)

    return domain
```

DGA方法的代表做就是Conficker，它的分析论文可以在这里找

到：<http://www.honeynet.org/papers/conficker> (<http://www.honeynet.org/papers/conficker>) 它的基本思想是用每天的日期当做随机数种子生成几百到几千不等的伪随机字符串，然后在可选的域名后缀比如 .com .cn .ws 里面挑选后缀生成候选的C&C域名，攻击者用同样算法和种子得到同样的列表，然后选择一个注册作为有效的C&C。安全人员即使抓到了二进制代码，在汇编语言里面反向出来这个随机数生成算法也远比搜索字符串难的多，所以DGA是个有效防止人工破解的方法。最近几年使用DGA算法的恶意软件里，Conficker的方法是被研究人员反向工程成功，Zeus是因为源码泄漏，其他的解出来DGA算法的案例并不多。

如果一个DGA算法被破解，安全人员可以用sinkhole的办法抢在攻击者之前把可能的域名都抢注并指向一个无效的IP。这种方法虽然有安全公司在做，但费时费力，是个绝对雷锋的做法，因为注册域名要钱啊，每天备选的域名又很多，都给注册了很贵的。现在常见的Torpig之类的C&C域名被sinkhole。更便宜有效的另外一个方法就是和DNS厂商合作，比如Nominum的Vantio服务器上TheatAvert服务可以实时推送DGA名单并禁止这些域名解析，使用了ThreatAvert的服务商就不会解析这些C&C域名，从而阻断了恶意软件和C&C域名的通讯。

从数据分析上可以看到DGA的另一个致命缺点就在于生成了很多备选域名。攻击者为了更快速的发起攻击，比如攻击者的客户要求付钱之后半小时内发起DDoS攻击，那么C&C的查询频率至少是每半小时，这就导致botnet对于C&C的查询过于频繁。虽然DGA本身看起来像是隐藏在众多其他合法流量里，但是现在已经有很多针对DGA的各个特性算法研究，比如鄙人的用机器学习识别随机生成的C&C域名 (<http://drops.wooyun.org/tips/6220>)里面利用到了DGA的随机性等其它特性进行判别，安全研究人员可以用类似算法筛选疑似DGA然后根据频繁访问这些DGA域名的IP地址等其他特征通过图论或其他统计方法判别C&C服务和感染的IP等。

## 0x05 高级变形DGA：如果DGA看起来不随机

基于DGA侦测的多数办法利用DGA的随机性，所以现在高级的DGA一般都用字典组合，比如

ObamaPresident123.info 等等看起来远不如 cqaqofiwtfrbjegt.info 可疑，攻击者利用这种方法对付威胁感知和机器学习方法的侦测。最近的一个例子出现在Cisco的一篇blog

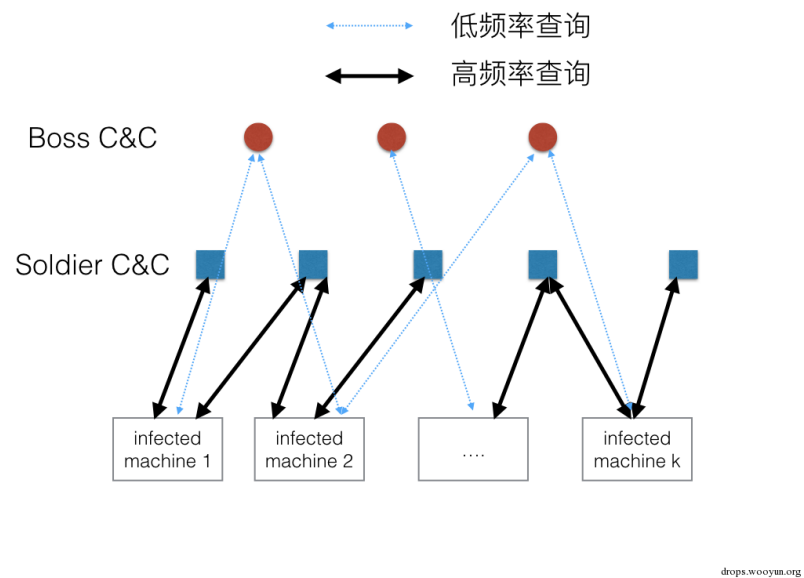
(<http://blogs.cisco.com/security/talos/detecting-dga>)里面提到的DGA就是一个很小的硬编码在代码里字典文件，通过单词的组合生成C&C域名。这些字典组合的DGA看起来并不随机，多数论文和blog里针对随机DGA机器学习的办法就不管用了。

对于这种DGA暂时并没有成熟有效的侦测方法，因为字典是未知的，可以是英语词汇，可以是人名，可以是任何语言里的单词。常用的方法还是基于随机DGA里面用过的 n-gram 方法，比如用已知的DGA的 n-gram 分布判断未知DGA，同时结合其它的特征比如解析的IP等等，或者利用DGA频繁查询的特性用 n-gram 特征作聚类。相关论文可以自行使用“Algorithmically Generated Domains”等关键词搜索。

## 0x06 多层混合C&C，跟着我左手右手一个慢动作：难度最高，不易被抓

在DGA部分提到了，DGA的致命缺点在于被动查询，如果想要快速启动攻击就必须让malware频繁查询C&C，导致C&C查询数据上异常于正常的查询流量。多层混合C&C可以有效避免这个问题，是个丢卒保帅的战术。这种方法在亚洲区的malware里面见到过很少几次。

比如攻击者设计一个两层的C&C网络，Boss级的C&C使用主域名列表比如 .com 域名，Soldier杂兵级C&C用免费二级域名列表比如 woshinidaye.3322.org，malware每天查询一次Boss级C&C拉取当天杂兵C&C域名列表，然后以一分钟一次的频率查询杂兵C&C域名，接受攻击指令，示意图如下：



侦测和封禁这类高级混合C&C难点在于：

- 在数据里，Boss级的C&C出现几率很低，可以不定期也可以一周一次，如果用一些早就注册过的域名或者通过黑进他人服务器利用无辜域名，Boss级的C&C很容易逃过异常检测。
- 数据里可以检测到的是频繁查询的低级的杂兵C&C域名。如果把这些域名封禁，malware在下一轮更新杂兵C&C列表后会使得这种封禁方法无效。杂兵域名就是主动跑上来送死的，反正二级域名不要钱。
- 更高级的做法是，如果Boss级的C&C列表里的域名用完了，它可以通过这个两层网络实时推送新的Boss级C&C列表。你看人家都不需要DGA这么麻烦。

侦测和防御方法需要一些数据和图论的知识，具体参考侦测double flux的模型，同样是两层网络，不同点在于两层节点都是域名节点，留作课后作业，这里就不赘述了。针对实现上另一个特征是，杂兵域名主要目的是来送死，他们的价格往往不高，比如免费二级域名或者免费的ccTLD或者gTLD后缀，利用这个特征可以把第二层网络的尺度缩小，从而在图数据库的计算速度上有不小的提升。

## 0x07 利用Twitter Reddit等论坛：难度低，被抓看运气

前面提到的办法多是攻击者自己架设服务器，如果攻击者的C&C域名被发现封禁了，这个botnet就被摧毁了。机智的攻击者就想到了通过论坛发帖的办法，比如在Twitter发一条在特定冷门话题下的包含C&C指令的tweet或者reddit上面找个十分冷门的subreddit发个包含控制指令的贴，这样即使被运营商或者安全研究小组发现了，人家总不能把推特和reddit封了吧（我说的是美国政府没有这个权利）。去年被抓住的名为 Mac.BackDoor.iWorm (<http://vms.drweb.com/virus/?i=4161206>)的恶意软件就是利用reddit做C&C控制服务器，具体细节请参考<http://news.drweb.com/show/?i=5976&lng=en&c=1> (<http://news.drweb.com/show/?i=5976&lng=en&c=1>) 也有把C&C信息隐藏在一篇看起来很正常的文章里面防止被发现，比如MIT的这个把加密消息隐藏在一篇论文里的有趣的demo

https://pdos.csail.mit.edu/archive/scigen/scipher.html  
(https://pdos.csail.mit.edu/archive/scigen/scipher.html) 不过在实际工作里暂时还没有看到这么高科技的C&C做法（你看我也不是教你这么做啊）。

这种方法不适合国内的大环境，因为国外论坛发帖是不举报不删帖很容易闷声发大财，但是水能载舟，亦可赛艇，国内由于发帖的身份控制严格，如果用这个方法很可能被眼尖的版主发现汇报给警察叔叔。而且新浪微博发C&C控制微博也不现实，微博为了防爬虫要强制登陆而且微博那个API的麻烦程度你也是知道的。所以这个方法只是拓展视野，顺便写个段子。

这里必须要插入一个段子了。一个真实的故事就是，我们抓到了一个做DDoS攻击的botnet，我们的模型告诉我这些攻击流量和 twitter.com 的访问流量有强相关，经过细致研究发现，这个bot可能用twitter的关键词当随机数种子生成攻击DGA域名。但奇怪的是，同一个bot感染的IP列表里面，中国区IP的随机数种子似乎有初始化的问题，每次的种子都是一样的。我们机智的抓住了这一点，把中国区当做对比组反向出了DGA算法：因为一个特殊的原因中国区感染IP不能访问twitter，如果认为中国区的DGA种子总是空字符串，我们对比中国区的DGA和其他地区的DGA差不多可以猜出来它的DGA的方法，从而反向工程出来它们的DGA算法。这里需要感谢一下国家。

## 0x08 一些其它的高级技术

限于篇幅限制有一些现阶段不太常用的C&C技术在这里仅仅简单描述一下，有兴趣的观众朋友们可以自行搜索。

- 利用P2P网络的C&C。如果一个僵尸网络里面所有的感染IP互相成为对方的C&C控制服务器，看起来很难摧毁所有的C&C。侦测重点在这个网络初始化的时候，就好比其它的BT下载必须从一个种子或者磁力链开始，当感染IP访问初始化C&C的时候，它还是需要上面说到的C&C方法，只是频率很低。
- IRC通讯.这是一个传统历史悠久的C&C控制方法。因为现在日常生活里IRC已经被一些即时信息服务比如微信等等取代，很少有普通群众会用到IRC，年轻的安全人员可能会忽视IRC这个老办法。办法虽老，但是用处广泛，好比T-800机器人，"Old, but not obsolete."
- 你知道还可以手动C&C么？我就见过在乡镇政府内网留了Windows Server 2003后门手工进去挨个启动的，毫无PS痕迹，嗯。

## 0x09 结语


说了这么多，主要目的是想介绍一下国际先进的恶意软件C&C设计和侦测经验，我们国内的malware不能总纠结于易语言啊VC6.0啊之类的我国特色，也需要向国际靠拢。同样的，我国的安全研究人员也需要国际先进经验，走在攻击者前面。C&C的设计和防御一直都是猫鼠游戏，不定期会出现一些大家都没想到的很机智的办法。在侦测C&C服务的过程里，数据科学和机器学习是很重要的工具，C&C的侦测现在越来越多的用到数据方法，在文中大家也看到了，攻击者已经设计出来一些对抗数据分析和机器学习的更高级C&C设计方法，足可以看出数据科学在安全领域的重要作用，连攻击者都体会到了。很多C&C服务看似随机，分布也广泛，但是在统计分析上会显示出一些特定规律从而让安全人员发现。没有人可以骗的过统计规律，不是吗？

☆收藏      分享

EGF6


写下你的评论...

发表



**Her0in** 2015-11-08 01:27:04  
@EtherDream 思路是好的，而且目前也有类似的木马诞生了，只是实现起来还是很麻烦的，要做很多编码的工作，DGA技术目前还是很成熟的。

回复



**EtherDream** 2015-11-07 22:57:38  
不能编辑回复。。。说点正经的。----- 以前想到一种方法，用搜索引擎做入口。比如11月10日，搜索 'XXX11月10日去哪玩' 之类的，看似平常但又特殊的查询。搜索结果不要求在首位，但能在前几页里找到，通过特殊的暗号能够识别出来。可能是篇博客，或者贴吧的帖子。然后把C&C服务器地址隐写在内容里，就很隐蔽了。就算博客或帖子被删，从新开一篇新的，主动扔给搜索引擎，很快就会被收录。



 回复



**EtherDream** 2015-11-07 11:12:29

水能载舟，亦可赛艇。。。。。

 回复



**cool\_fire** 2015-11-06 21:05:28

写的非常好，分析过程中若遇到与文中相似的情景会体会的更深！

 回复



**BeenQuiver** 2015-11-06 17:43:13

僵尸网络的研究在国内并不风靡啊

 回复



**Demon** 2015-11-06 15:58:14

请收下我的膝盖

 回复



**RPC\_宫城俊** 2015-11-06 15:08:12

漂亮！

 回复



**vvun91e0n** 2015-11-06 14:10:45

楼主好文 期待新作

 回复



**caomaocao** 2015-11-06 13:52:29

果然0x08在我天朝没啥威胁。

 回复



**Insight-labs** 2015-11-06 13:38:59

居然用写论文的方法膜，真是一颗赛艇。我以前设想过一种P2P的botnet，使用DHT或者KAD，完全没有C2，控制端作为bot加入到网络里，指令用bot的公钥和时间戳一起加密，然后用控制端私钥签名。DHT和KAD的初始化完全不用域名，在bot里写入一个IP段，比如Azure，AWS，阿里云的某区的IP段，比如某/20 ip段,不大不小。控制者在这个ip段随便开台机器，开个web server，在80端口把其他node的信息加密就行了，bot初始化的时候扫描这个ip段，读取80端口点信息，如果能成功解密就可以获取其他节点的信息了，完全不需要域名。至于take down方法，我相信ip资源这么宝贵，不能全部黑洞了吧.....

 回复



**Woodisgood!** 2015-11-06 13:37:06

又学到新知识了，好开心。

 回复



**phunter** 2015-11-06 13:24:23

感谢各位赞赏，里面有一些小的例子和链接错误，等我收集总结一下单独贴个勘误，也请大家积极指出和讨论相关内容啊。其实写这篇的意思是想鼓励安全人员多接触数据，用数据搞安全是个广阔天地，我们不去占领，黑产就去了，他们都已经开始设计对抗机器学习的C&C了，我们更要加紧啊。

 回复



**杯中取月** 2015-11-06 12:40:46

mk

 回复



**火丁笔记** 2015-11-06 12:18:00

本想吃饭前看一遍，结果没理解透彻，饭后接着看。

 回复



**winsyk** 2015-11-06 11:32:25

厉害，科普很到位！

👤 回复



楚安 2015-11-06 11:20:49

这边综述写得很好，推荐一下，二部图抓FastFlux那部分跟我们的做法很相似呀，哈哈。

👤 回复



6666 2015-11-06 10:21:43

看得过瘾

👤 回复



小荷才露尖尖角 2015-11-06 10:02:24

牛，大开脑洞

👤 回复



珈蓝夜宇 2015-11-06 10:00:10

你们在渗透别人的网络，雪花在渗透你们的衣襟

👤 回复

感谢知乎授权页面模版