登录

【应急响应】定位内网中毒主机IP经历小记

zzzhhh / 2017-06-19 04:02:07 / 浏览数 3493 安全技术 技术讨论 顶(0) 踩(0)

---

一、事件起因

客户向公司反映使用IDS设备捕获到木马上线域名需要处理，虽然是逆向岗但还是有预感未来应急响应的工作只会越来越多。所以作为新人的我选择了跟带头BOSS去现场学

二、前置知识

1）动态域名解析
用户每一次上网时运营商都会随机分配一个IP地址。安装在用户主机里的动态域名软件会把这个IP地址发送到动态域名解析服务器。Internet上的主机要访问这个域名时动态
这就叫动态域名解析。

2）木马类型
木马控制就是开启一个端口，双方主机建立网络连接成功后，传送控制命令实现控制受害者主机的目的。其中有两个概念：正向连接和反向连接。

正向连接：恶意程序在受害者的主机上监听个端口，而攻击者通过这个端口去连接受害者的主机。这要求受害者IP不变的情况下，才能够连接。

反向连接：在攻击者主机上监听个端口，然后由受害者主机来访问攻击者主机。就算受害者主机的IP怎么改变，也可以达到控制的目的。

3） 木马上线连接方式
当前木马为了增加隐蔽性和反追踪能力，上线方式会采用第三方域名进行通信。
被控制端首先访问动态域名，动态域名中指向控制端的真实IP。使被受害主机与攻击者主机连接，再由控制端发送控制命令。
常见上线方式：HTTP、FTP、DNS、第三方网站（Qzone、csdn等）、IP
上线的流程是被控端访问动态域名获取控制端主机真实IP，建立连接后控制端可向被控端发送控制命令。（被控端指的是受害者的主机，控制端指的是攻击者主机）

图1 木马上线简图

三、处理过程
经过与客户单位负责人沟通中得知这几个月IDS断断续续的时间里捕获到f33**88.3322.org这个域名,而这个域名被IDS设备报为木马动态域名。
但由于受攻击单位的主机是统一配置DNS服务器（10.0.0.13）进行解析上网的，所以IDS抓到的发包主机IP其实是DNS服务器的IP（10.0.0.13）。
期间因为攻击者的木马动态域名一直没有解析过，所以IDS无法查出到底是哪台主机中了木马。

图2 木马动态域名无法解析

客户单位负责人希望我们能够定位到内网中毒的主机IP，还有对木马的行为做分析，确定业务受影响的情况。
经过交流后我们决定采用两种方式对中毒主机的IP进行定位。
1.导出IDS设备的回显日志，定位中毒主机位置
2.在单位中的DNS服务器抓取数据包

2.1 导出IDS设备的回显日志，定位中毒主机位置

因为中毒主机向外发送数据一定会经过DNS服务器，流程如下：

```
■■■■■■■■■■ ---> DNS■■■  ---> ■■■■■■■■
■■■■■■■■■■ <--- DNS■■■  <--- ■■■■■■■■
```

这里遇到的麻烦就是IDS设备捕获的数据包日志过大时查询功能很慢，由于f33**88.3322.org这个域名一直没有解析成功，通过IDS设备只能根据回显数据包才可以查询到通
所以我们借助了ThreatBook、VirusTotal这两个网站。首先查询ThreatBook上关于这个域名的网络。

图3 ThreatBook 查询动态域名

然后查询这两条HASH值对应的网络活动，查看是否有其他的上线域名。

图4 ThreatBook 网络活动

取出【b35878a825daceeb2de5602fb6268da80c32a908ec646bcf035b0bce792b7747】
、【4dc695732112e2552f6bc67a38aefa406ac7201de6994a48f134c96301dbf8ef】这两条hash值在virustotal.com这个网站上查询得到另外一个通讯的域名。【ilo.br

图5 ilo.br*nz.pl

这一次的难点在于
ilo.br*nz.pl这个域名的确是与内网主机成功进行过通讯，可是在取样后进行分析时却发现取出来的病毒跟我们预计的行为不符合，说明我们误打误撞又发现了新的病毒。

于是我们就又回到f33**88.3322.org这个域名无法被正常解析的问题上。

通过思考然后我们又决定借助内网的上网行为管理、流量控制、IPS等设备进行捕获。增加一条TCP访问策略监控访问f33**88.3322.org这个域名任意端口的内网主机IP。而

最后通过在出口DNS服务器上增加解析策略，将f3322**.3322.org木马动态域名解析到我们公司官网的IP，解决了这个上网行为管理设备增加策略的问题。在后续的分析中

2.2 在单位中的DNS服务器抓取数据包

考虑过可以使用Wireshark、TCPdump这两类抓包工具在DNS服务器上进行数据包的捕获，但是全单位的上网访问都是通过这台DNS服务器的情况下。抓包数据有可能很成

四、个人总结

重心点：在这次的事件中感受到应急响应中，很多情况都是WEB方面的日志查询。但对于内网中了木马病毒，我们需要做的工作会始终重点围绕着定位、取样、分析。

全局观：而应急响应工作也非常需要建立全局观。了解网络拓扑并结合业务，知道出了问题的主机中存在什么应用。这个应用涉及多少台主机，采用何种方式进行管理（域控

影响度：判断业务受损状态，检查应用是否存在安全隐患,网络区域内的主机是否被横向入侵或是被种植了远程控制。网络影响程度。



上一篇：强制通过VPN上网,VPN断线就断网 下一篇：Django两则CVE-2017-...

1. 1 条回复


hades 2017-06-19 05:30:36

辛苦了

0 回复Ta

---