科来

第 07 章
如何找出伪造数据的内网主机

科来官微
CSNA 公众号
400-6869-069
www.colasoft.com.cn
support@colasoft.com.cn

内网的主机一旦被攻击控制，则可以伪造数据进行攻击，扰乱安全管理人员监控方向，如果只通过安全日志进行分析，很难定位到问题主机。

对于网页访问速度缓慢或断断续续无法访问的情况，我们一时无法确定是网络故障、网络性能还是网络安全问题，如果排查问题的方向出现偏差，往往耗时费力。网络分析技术帮助用户透过现象看到本质，达到事半功倍的效用。

7.1 问题描述

据用户反馈，网内访问互联网时打开页面速度非常缓慢，而且经常出现不能打开网页的情况。此现象已经持续一周时间，严重影响到公司业务进展。网络运维部门多方查找问题原因无果，于是邀请科来网络分析工程师帮助排查问题。

7.2 分析过程

7.2.1 问题现象分析

该用户网络出口带宽为20Mb，两台交换机下连30多个用户主机与服务器。在交换机 1 和交换机 2 分别配置镜像端口，部署科来网络分析系统，抓取上连接口的流量进行分析。

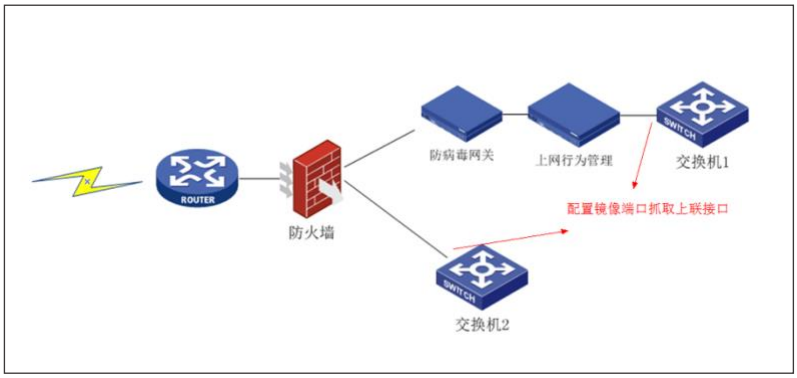

图 7-1

交换机 1：在交换机 1 抓取了二十分钟，并未发现异常情况与流量突发。

交换机 2：抓取短短十秒钟的数据包，就发现了网络中存在的问题，如下图所示。

统计项					当前值
⊞ 诊断统计					数量
⊟ 流量统计	字节数	数据包数	利用率	每秒位数	每秒包数
总流量	272.292 MB	500,928	100.000%	261.827 Mbps	57,420
广播流量	449 B	5	0.000%	368 bps	1
组播流量	0 B	0	0.000%	0 bps	0
平均包长					569.979 字节
⊟ 数据包大小分布	字节数	数据包数	利用率	每秒位数	每秒包数
<=64	970 B	16	0.001%	880 bps	2
65-127	236 B	3	0.000%	0 bps	0
128-255	247 B	1	0.000%	0 bps	0
256-511	651 B	2	0.000%	0 bps	0
512-1023	272.290 MB	500,906	100.000%	261.826 Mbps	57,418
1024-1517	0 B	0	0.000%	0 bps	0
>=1518	0 B	0	0.000%	0 bps	0
⊞ 地址统计					数量
⊞ 协议统计					数量
⊞ 数据流统计					数量
⊟ TCP统计					数量
TCP同步发送					500,916
TCP同步确认发送					0
TCP结束连接发送					0
TCP复位发送					0

图　7-2

不难看出，短短十秒钟的总流量达到了 272MB，基本全部是 512-1023 字节的数据包，并且 TCP 同步包达到了 50 余万个，没有收到任何的 TCP 同步确认包，存在明显的异常情况。

图　7-3

查看 TCP 会话，发现所有的 TCP 会话行为一致，全部是 X.X.81.2 向 X.X.227.102 的 80 端口发送 TCP 数据包。

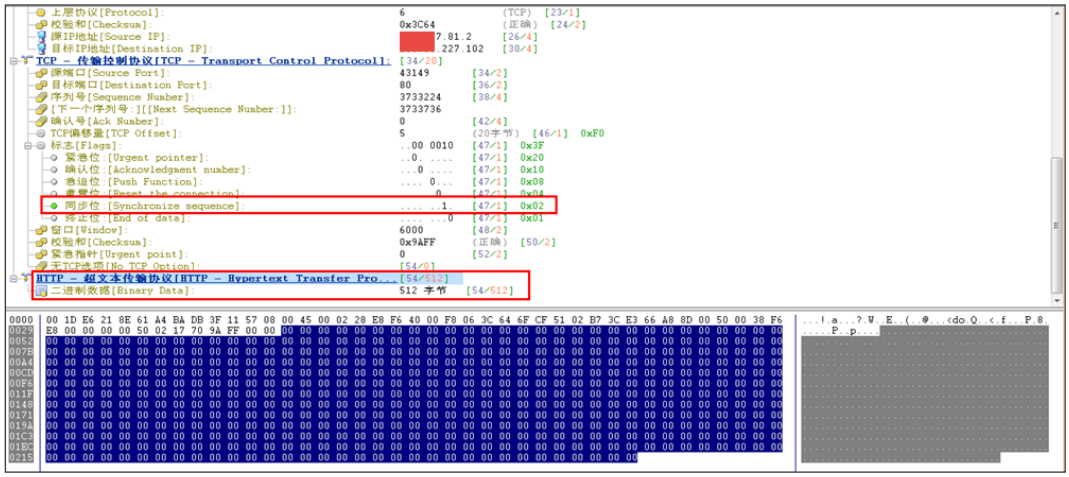

图　7-4

数据包的同步位（SYN）置 1，SYN 数据包是 TCP/IP 建立连接时使用的握手请求数据包，不应存在任何应用层数据。但是在上图中看到该数据包中还有 512 字节的 HTTP 数据，并且数据内容全部为 0，该数据包为明显的伪造数据包。

因为数据包被伪造成互联网地址，所以会通过互联网出口向外发送。由于本网络互联网出口为 20Mbps，而伪造数据包却达到了 261Mbps，明显超过了最大处理能力，此时内网主机在访问互联网时就会出现连接十分缓慢，甚至不能访问互联网的情况。

7.2.2　问题定位

查看 MAC 地址我们得知发送大量数据包的 MAC 地址为 x:x:x:3F:11:57，如下图所示。

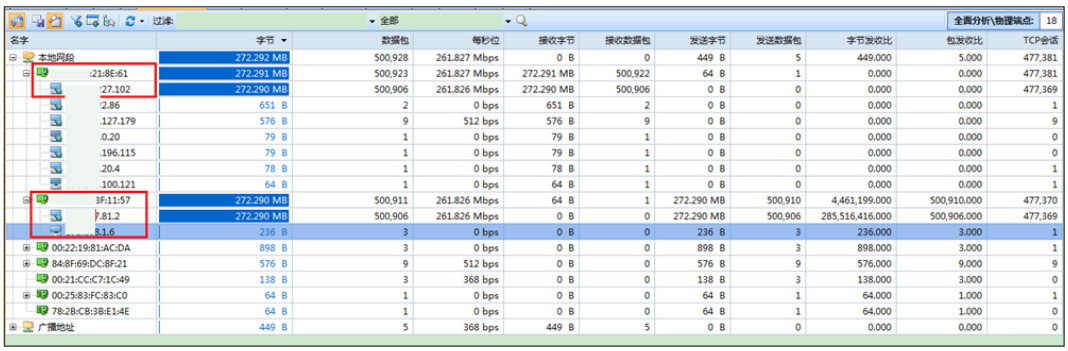

图　7-5

掌握了发起攻击的 MAC 地址后，通过查看交换机 MAC 地址表，可以找到相应端口，如下图所示。

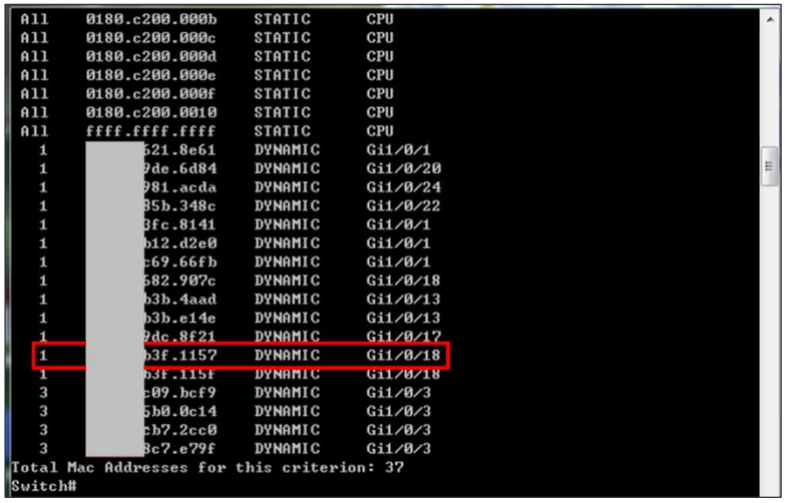

图　7-6

该 MAC 地址对应的交换机 2 端口为 G1/0/18 口，通过断掉该接口的方式来排查，断掉该端口后网络恢复正常，能够正常流畅的浏览网页。

7.3　分析结论

科来网络分析工程师排查发现交换机 2 的 G1/0/18 接口发送大量互联网地址伪造数据包，其通过大量发送此类数据包堵塞网络的互联网出口，达到攻击的作用。而 G1/0/18 接口为邮件网关连接端口，建议用户联系邮件网关设备厂商，对设备进行问题排查。

7.4 价值

通过本案例，可以了解到网络分析技术不仅能快速发现网络中的异常流量，还能透析异常流量，找到产生问题的根源，从而快速、准确的进行故障定位，减小异常数据对网络的危害。管理者需要通过对数据包的分析，获得真实的数据。

科来 MAC 地址扫描器

科来 Ping 工具

科来数据包播放器

科来数据包生成器

科来介绍

科来成立于 2003 年，是专注于网络流量分析技术研究与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络安全分析及网络智能运维等关键领域。科来连续入围 GartnerNPMD 魔力象限，并荣获“远见者”称号，是唯一入选“远见者”象限的中国企业。科来产品还曾被美国权威评测机构 PC Magazine 评选为《全球最佳科技产品》。

科来专业的技术服务在用户的业务保障上起到关键作用，已经成为对网络时效性高要求的企业的最佳选择，得到了社会各界的广泛认可。同时，科来创办的《CSNA 网络分析认证培训》是我国广具影响力的网络分析认证体系，为国家培养了大量的网络分析技术高级人才。

由于科来公司在网络安全领域的技术优势，受邀为青岛“上合峰会”、多届“两会”、“十九大”、杭州“G20 峰会”、“九三”阅兵、“世界田径锦标赛”、多届“数博会”等重大国家级活动做网络安保工作，做出突出贡献。

- 100 余家世界 500 强企业选择科来
- 为全球 10000 余家商业客户提供网络分析解决方案
- 全球 90 余万用户正在使用科来的产品
- 科来的技术服务于世界 110 个国家和地区