科来

第 05 章
如何找出内网被控主机

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

内网哪些主机被控了，这是一个非常重要的问题。我们知道，入侵者对服务器的攻击几乎都是从扫描开始的。攻击者首先判断服务器是否存在，进而探测其开放的端口和存在的漏洞，然后根据扫描结果采取相应的攻击手段实施攻击。通常防火墙等安全设备，会拦截来自外部的扫描攻击，但是面对内部主机被控并对外扫描继而进行渗透攻击的情况，传统安全手段往往不能及时发现，也就起不到防护作用。

这时，如果拥有网络回溯分析技术的支持，通过对底层数据包的回溯分析，攻击的来龙去脉，便可一目了然。

5.1 问题描述

科来网络分析工程师就有很多这样的真实案例，在例行为某大型行业用户进行网络安全检查服务中，发现该用户的一台服务器（*.77）有大量扫描流量，疑似被感染病毒。该用户将科来网络回溯分析系统部署在内网的核心交换机上，对经过该核心交换机的流量，进行监控与回溯分析。科来网络分析工程师选择适当的时间窗口、特定的时间段之后进行透视分析，从而进一步判定该异常网络行为的性质，力求为用户提供可靠的安全保障措施。

5.2 分析过程

图 5-1

一般情况下，正常的内网 TCP 同步包与 TCP 同步确认包之间的比值应为 1:1，但当 TCP 同步包远大于同步确认包时，说明网络可能存在扫描行为。

通过视图可以看到在 13 点 32 分之前，*.77 通讯的 IP 地址只有 34 个，同步包与同步确认包数量很少，并且基本相等，因此不存在扫描行为。

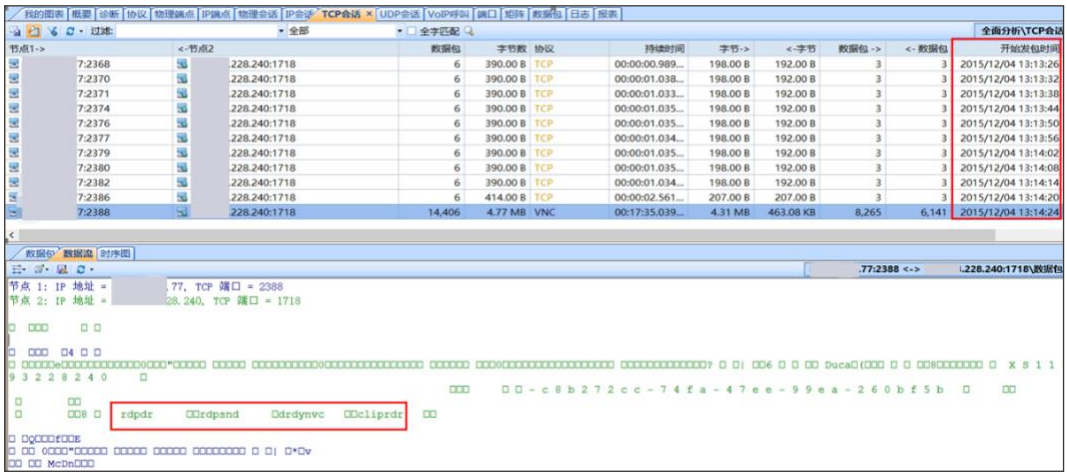

图　5-2

图　5-3

然而，*.77 每隔 6 秒主动发起一次对 X.X.228.240 的连接，直到 13 点 14 分 24 秒连接成功。从数据流的解码中我们可以看到 rdpdr，rdpsnd，drdynvc 和 cliprdr 等名字，而这些名字都是 FreeRDP 库的名字。FreeRDP 是一个免费开源实现的远程桌面协议（RDP）工具，用于从 Linux 下远程连接到 Windows 的远程桌面。

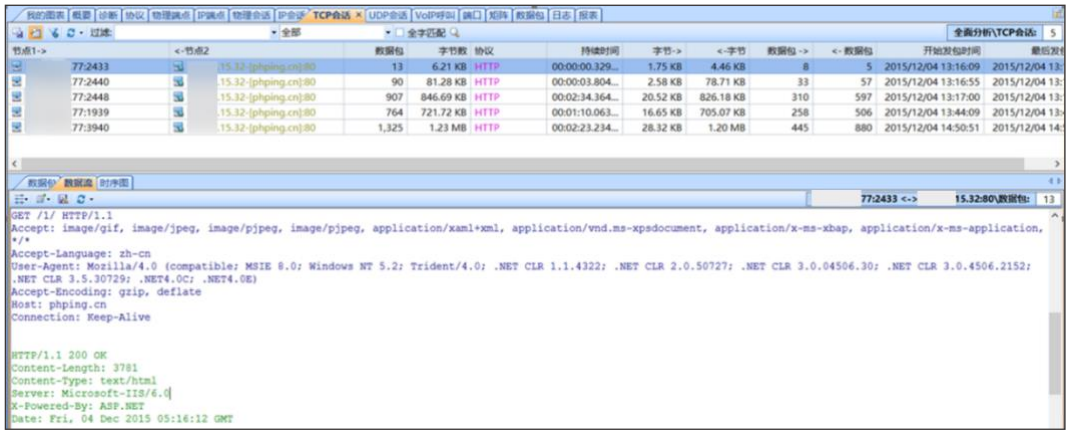

图　5-4

建立远程桌面后，13 点 16 分，*.77 开始访问 X.X.15.32，可以看到这个网站上有各种常用的黑客软件，如下图所示。

图　5-5

*.77 从这个服务器上下载了 DToolsSQL、ntscan、hsan、SSH 爆破等各种黑客软件，如下图所示。

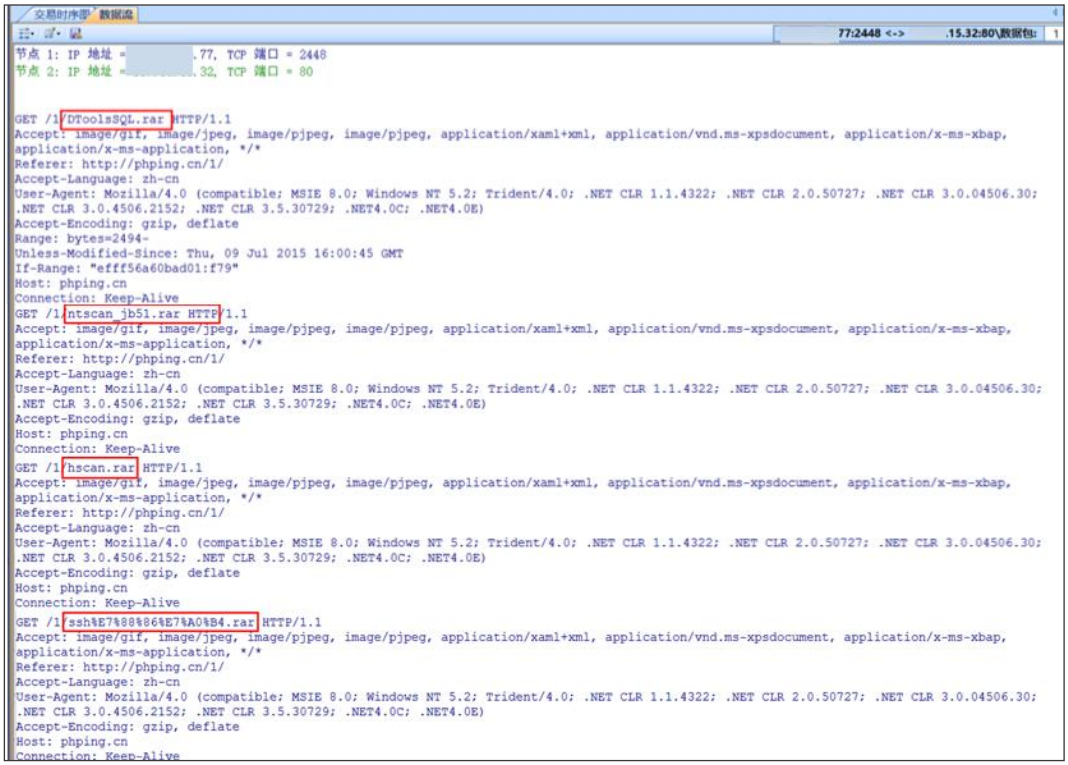

图　5-6

13 点 32 分到 13 点 36 分，IP 数猛增到 15000 以上，同步包也开始与同步确认包出现较大差值，如下图所示。

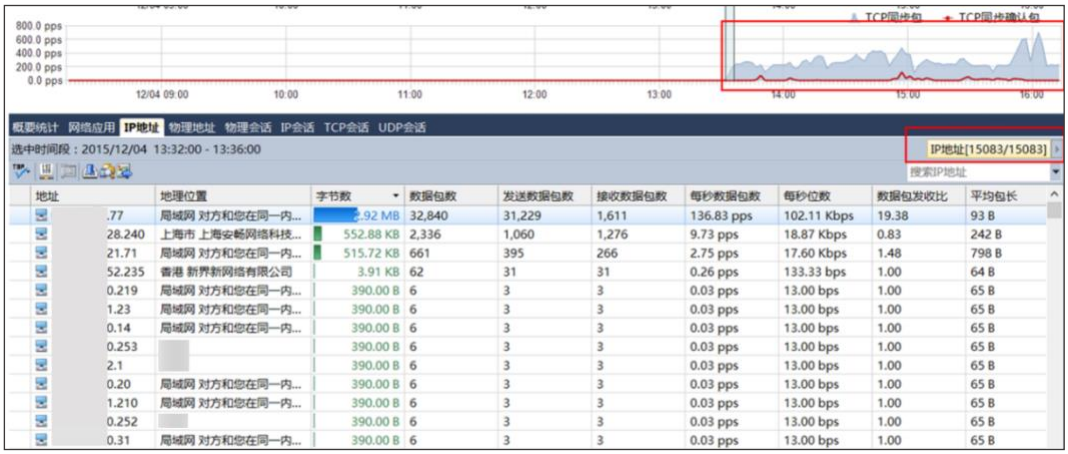

图　5-7

*.77 扫描内网地址，每个地址发 2 个 TCP 同步包，由于扫描的地址大多数不存在，因此不能得到回应，所以会造成上文提到的同步包与同步确认包出现较大差值，如下图所示。

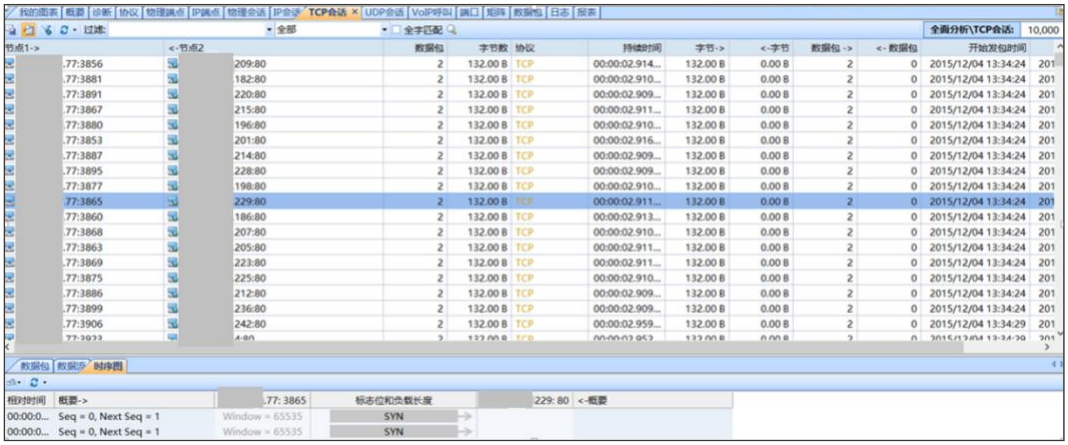

图　5-8

当扫描到存在的 IP 地址时，如下图（以*.71 为例）：三次握手建立成功后，*.77 会直接发 RST 包断开连接，继续扫描后面的 IP 地址，但*.71 应对方式会被记录下来并用于后续攻击，如下图所示。

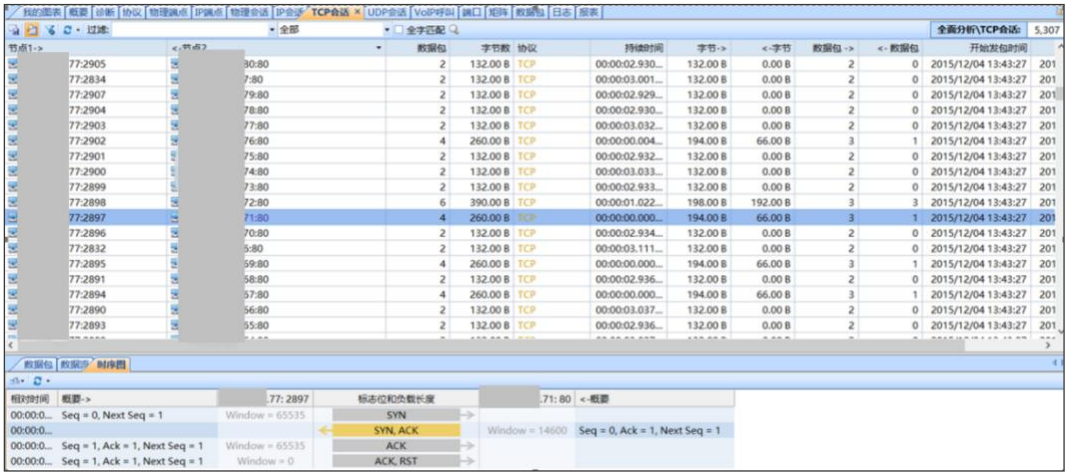

图　5-9

接着*.77 开始扫描*.71 的一些常用端口，确定*.71 开了哪些端口可以用于进行后续攻击，下图中看到只有 80 端口的会话有 7 个数据包，说明有过回包。

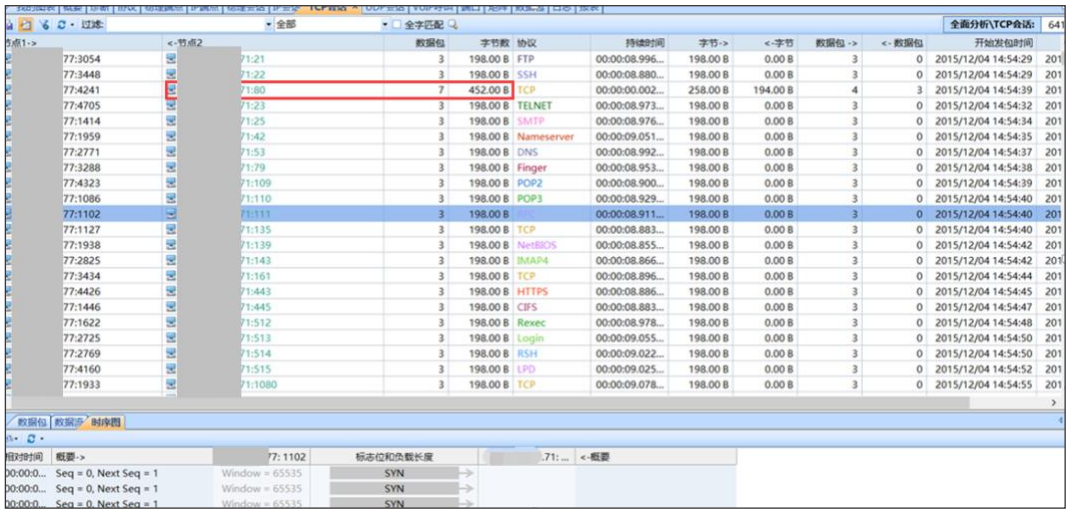

图　5-10

端口扫描结束，*.77 会对*.71 打开的端口进行漏洞测试，尝试找到漏洞进行入侵。

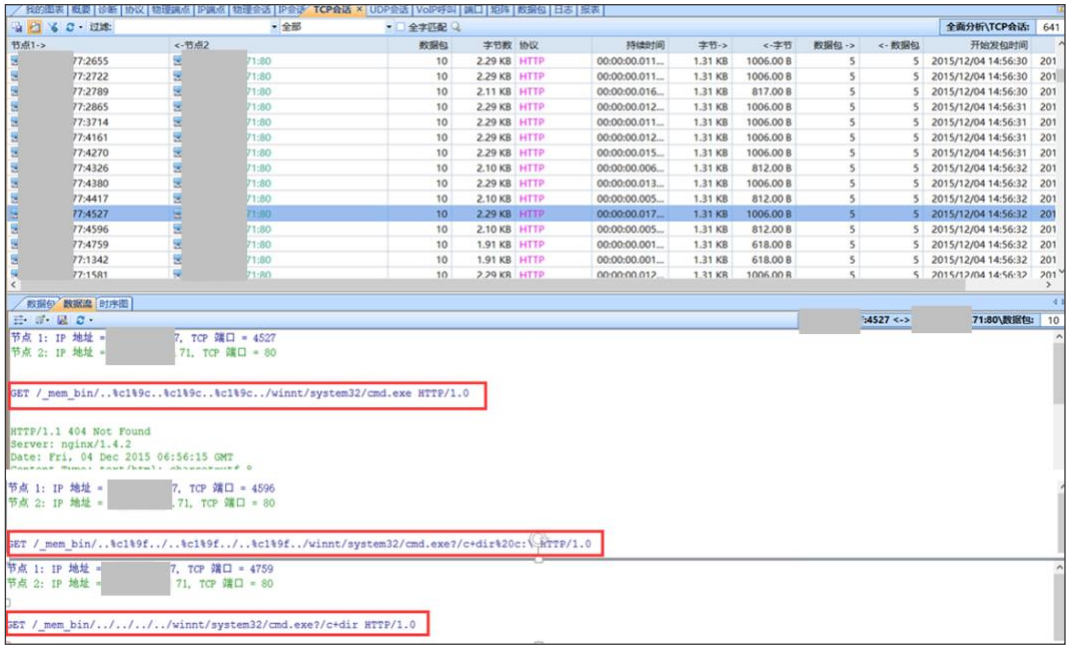

图　5-11

5.3　分析结论及建议

通过上述透视分析，可以确定*.77 已经被黑客控制，并且黑客正在以此为跳板尝试向内部入侵。建议该用户的网络安全管理人员，即刻禁止*.77 访问上文中提到的外网 IP 及端口（X.X.228.240 TCP 1718，X.X.15.32 等），并对*.77 进行处

理。

5.4 价值

通过本案例我们可以看到，利用网络回溯分析技术，通过对特定流量的简单分析，便可定位到被控的问题主机，判断出该异常行为是否为恶性网络安全事件，并通过追踪溯源，成功阻止入侵者的进一步计划，避免内网的主机信息泄漏，同时成为黑客的攻击武器。

科来网络流量分析产品下载(免费版)

科来网络分析系统

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