科来

第 01 章

如何分析入侵门户网站的攻击行为

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

网站“被黑”是网络管理者在日常运维工作中极为头疼的问题，一方面黑客不断演进的手段使得攻击行为难以被感知，系统的高复杂度又让防范更加困难；另一方面，传统的应用及安防设备缺乏完整的通讯数据，这使得溯源工作难以开展。网站“被黑”事件，不仅影响了网站相关业务的正常运行，更严重影响了该网站所属单位的企事业形象。本案例将通过分析一起某门户网站“被黑”的真实案例，讲解如何准确定位攻击行为，并复盘整个攻击事件过程。

1.1 问题描述

某门户网站多次“被黑”，影响恶劣，已经引起相关领导的高度重视。由于运维管理人员不了解黑客的攻击手法，因此无法彻底避免这类安全事件发生，只能通过登录被黑服务器查找到被黑页面，并删除相关“黑链”信息等处理方式，这使得运维工作十分被动。

因此，该门户网站领导决定利用记录网络全流量的技术手段，经过多方比较，最终选择部署科来网络回溯分析系统（RAS）来收集全部网络流量，还原“事故现场”，从而彻底解决这一难题。当事件再一次发生之后，该网站运维人员第一时间联系了科来网络分析工程师，对本次安全事件进行针对性的分析工作。

1.2 分析过程

1.2.1 问题现象分析

首先，科来网络分析工程师和客户运维工程师合作，通过登录被黑服务器，删除相关“黑链”信息，及时恢复网站的正常访问，并确定“被黑”时间为 10 月 31 日 19 点 12 分（服务器时间），进而了解到相关“黑链”是由 172.X.X.2 为制作服务器并通过 FTP 上传至被黑服务器，详情如下图所示。

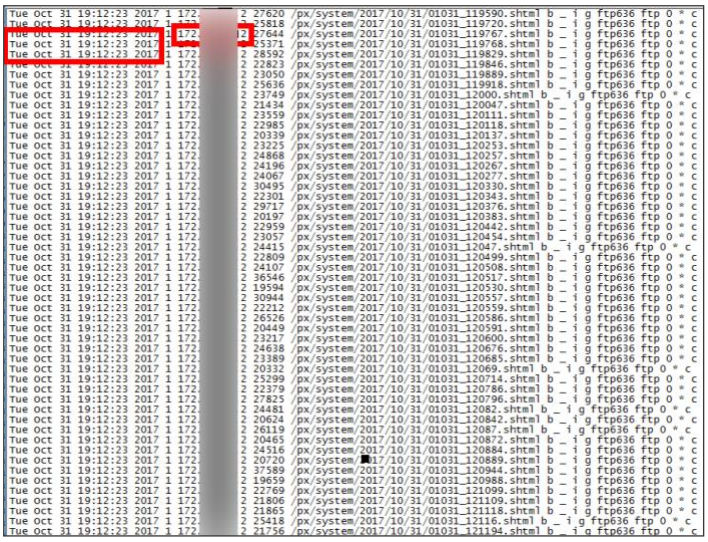

图　1-1

通过服务器相关日志提供的 IP 及时间信息，在科来网络回溯分析系统中找到该事件发生时段的流量，下载并回溯分析这段时间内的通讯数据，内容如下图所示。

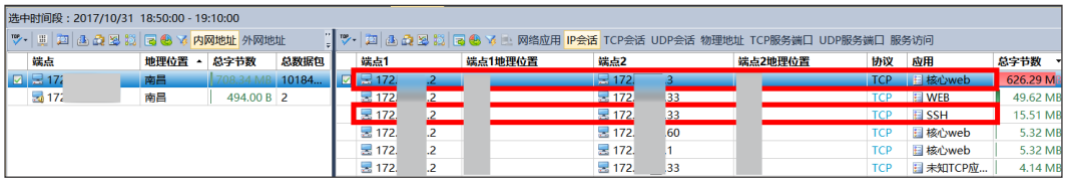

图　1-2

在事发时间段，存在两个可疑点：

1）制作服务器 172.X.X.2 与发布服务器 172.X.X.3 进行过数据通讯，且通信内容就是将“黑链”上传至发布服务器，内容如下图所示。

图　1-3

2）制作服务器172.X.X.2还与另外一台服务器172.X.X.33进行了数据通信，且使用的应用是 SSH。SSH 作为服务后台调试的软件，此时不恰当的出现而引起注意，如下图所示。

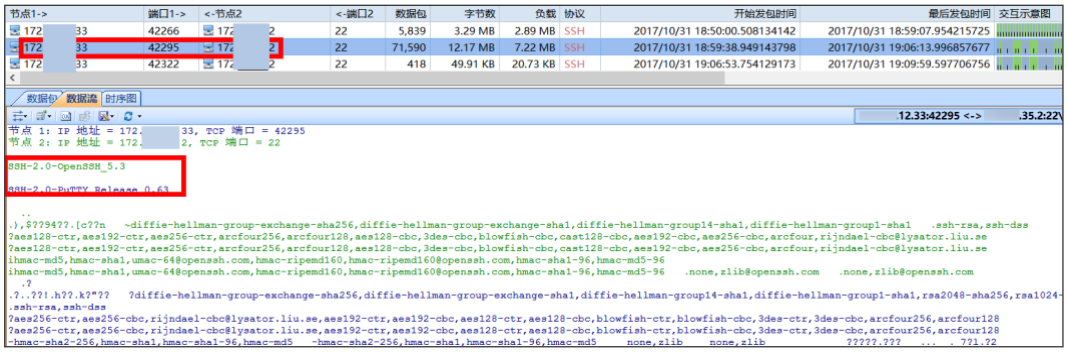

图　1-4

通过分析发现，172.X.X.33 向 172.X.X.2 发起了后台数据的调试访问，故 172.X.X.2 并非直接“真凶”，还需要对 172.X.X.33 的通讯数据进行进一步分析确认。

172.X.X.33 为该网站移动端发布系统的服务器，能够直接与外界的互联网 IP 进行通讯。通过科来设备进行数据回溯，梳理出事发时间段内该嫌疑主机与其他主机的通讯记录，如下图所示。

端点1	端点1地理位置	端点2	端点2地理位置	协议	应用	总字节数	每秒字节数	端点1发送字节数	端点2发送字节数	比特率
172.[redacted]2	南昌	172.[redacted]33	南昌	TCP	WEB	49.62 MB	42.34 KB...	759.23 KB	48.87 MB	346.84 Kbps
172.[redacted]33	南昌	111.[redacted].123	中国,湖北,武汉,,移动	TCP	WEB	47.81 MB	40.80 KB...	45.11 MB	2.70 MB	334.23 Kbps
183.[redacted].207	中国,四川,达州,,移动	172.[redacted]33	南昌	TCP	WEB	40.80 MB	34.82 KB...	2.52 MB	38.28 MB	285.22 Kbps
172.[redacted]33	南昌	42.4[redacted]204	中国,湖南,长沙,岳麓,联通	TCP	WEB	31.48 MB	26.86 KB...	30.29 MB	1.19 MB	220.04 Kbps
172.[redacted]33	南昌	117.[redacted].89	中国,江西,南昌,,电信	TCP	WEB	27.97 MB	23.87 KB...	26.47 MB	1.50 MB	195.52 Kbps
172.[redacted]33	南昌	42.4[redacted]238	中国,湖南,长沙,岳麓,联通	TCP	WEB	24.02 MB	20.49 KB...	22.75 MB	1.26 MB	167.88 Kbps
172.[redacted]33	南昌	117.[redacted].65	中国,江西,南昌,,电信	TCP	WEB	21.80 MB	18.60 KB...	20.74 MB	1.06 MB	152.40 Kbps
172.[redacted]2	南昌	172.[redacted]33	南昌	TCP	SSH	15.51 MB	13.23 KB...	13.53 MB	1.97 MB	108.40 Kbps
172.[redacted]33	南昌	117.[redacted].90	中国,江西,南昌,,电信	TCP	WEB	13.76 MB	11.74 KB...	13.04 MB	736.27 KB	96.18 Kbps
172.[redacted]33	南昌	112.[redacted].81	韩国	TCP	WEB	[redacted]	10.01 KB...	11.24 MB	503.57 KB	81.99 Kbps
172.[redacted]33	南昌	172.[redacted]1	南昌	TCP	Database	11.45 MB	9.77 KBps	4.09 MB	7.36 MB	80.05 Kbps
172.[redacted]33	南昌	113.[redacted].192	中国,广东,深圳,,电信	TCP	WEB	9.93 MB	8.47 KBps	9.21 MB	733.91 KB	69.40 Kbps
172.[redacted]33	南昌	116.[redacted].249	中国,湖北,武汉,,电信	TCP	WEB	8.78 MB	7.49 KBps	8.24 MB	555.17 KB	61.39 Kbps
172.[redacted]33	南昌	113.[redacted].193	中国,广东,深圳,,电信	TCP	WEB	8.06 MB	6.88 KBps	7.31 MB	771.09 KB	56.34 Kbps
172.[redacted]33	南昌	113.[redacted].138	中国,广东,深圳,,电信	TCP	WEB	6.90 MB	5.89 KBps	6.30 MB	618.07 KB	48.25 Kbps

图　1-5

如上图所示，除了正常来自国内互联网的访问 IP，还隐藏着一个来自韩国的 IP 地址 112.X.X.81。网站作为某省的著名门户网站，其主要的访问源都在国内，通常情况下不会有来自境外的访问，故此韩国 IP 有重大嫌疑。

对此，我们将 172.X.X.33 与 112.X.X.81 的通讯流量进行单独的回溯分析，其流量趋势，如下图所示。

图　1-6

通过上图可直观的看到，172.X.X.33 与 112.X.X.81 在 17 点 20 分至 19 点 30 分都存在持续性的流量通讯行为，通过进一步数据挖掘，可以看到 172.X.X.33 在 17 点 20 分对 112.X.X.81 首先发起了主动外联，并与境外主机建立了心跳检测的链接，如下图所示。

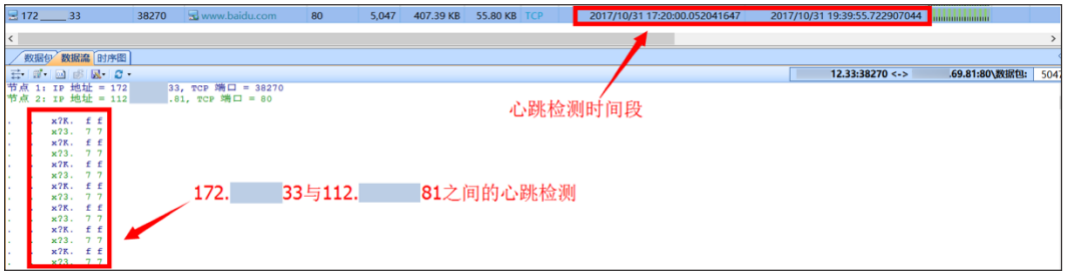

图 1-7

由于传统的安全防护设备只对由外至内的通讯流量进行安全监测，而本次连接是由内网 IP 主动发起，故成功避开了防火墙等安全设备的检测。由此可见，172.X.X.33 这台服务器早已被黑客渗透，并被写入了恶意程序。

在连接建立以后，112.X.X.81 开始对 172.X.X.33 进行远程操作，详情如下图所示。

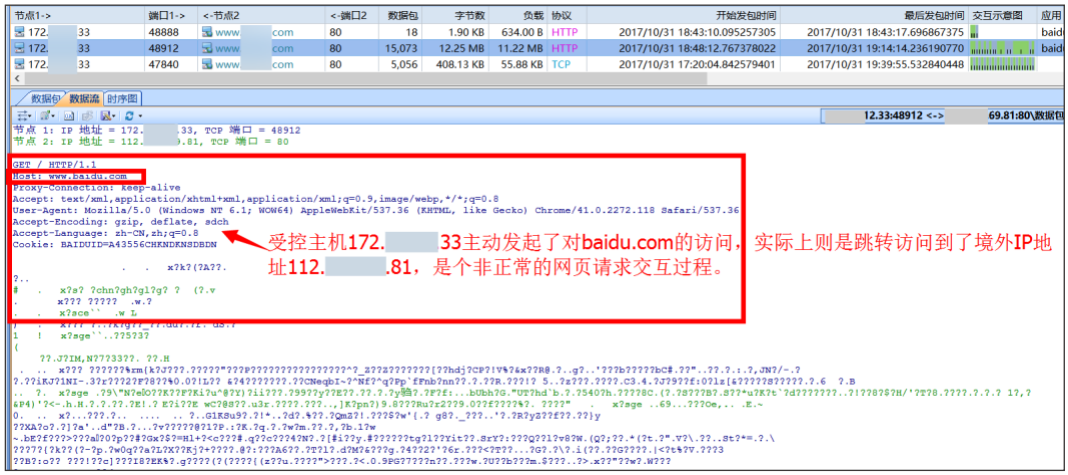

图 1-8

受控主机 172.X.X.33 主动发起一个对 www.baidu.com 的访问请求，而实际地址却指向了境外 IP 地址 112.X.X.81，由此可知，这是一个伪装的网页访问交互过程。本次会话持续时间段为 18 点 48 分 12 秒至 19 点 14 分 14 秒，表明黑客通过对受控主机 172.X.X.33 进行了长达 26 分钟的实际操控。

1.2.2 事件复盘

复盘整个事件需要我们将观察点返回至 172.X.X.33、制作服务器 172.X.X.2 及发布服务器 172.X.X.3 上，还原整个“犯罪过程”：

1）经过黑客与受控主机 172.X.X.33 的相关准备工作后，出于隐匿行踪的考虑，172.X.X.33 首先与制作服务器 172.X.X.2 建立联系，并在 18 点 59 分 38 秒成功登录 172.X.X.2 的调试后台，并将其作为攻击跳板。

图　1-9

2）然后 172.X.X.2 在 18 点 50 分 24 秒对 172.X.X.33 进行反向访问，将黑客事先上传至 172.X.X.33 服务器的压缩文件 jxpx10_31.rar 进行下载，并解压得到 01031_100111.shtml 文件。

图　1-10

3）最后，再由“跳板”172.X.X.2 将恶意文件上传至发布服务器 172.X.X.3。经过发布服务器后台查询，01031_100111.shtml 文件正是被上传至发布服务器的“黑链”文件。

图　1-11

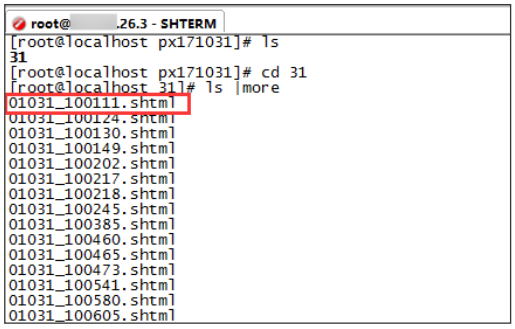

图　1-12

1.3　分析结论

首先攻击者在该网移动端发布系统 172.X.X.33 上写入恶意程序，并通过其建立与网站的连接。通过该系统制作服务器 172.X.X.2 下载要发布的“黑链”，并上传给发布服务器 172.X.X.3，最终实现了恶意链接的发布。由此可见，整个攻击过程隐蔽性高且经过长期策划，攻击者利用该网战作为门户网站的流量优势，发布恶意“黑链”谋求暴利，极大的损伤了该网站的声誉。

1.4　价值

网络全流量回溯分析，实现长期网络实时数据的完整保存，可以在发现问题时提供一定时间范围（根据采用设备的存储容量而定）内的回溯分析，为迅速定位问题发生原因提供了全面的分析依据，同时为网络安全事件发生后的数据取证提供了强有力的数据支撑。

另外，我们说网络全流量分析是应对安全问题行之有效的手段，因为再高级的攻击都会留下网络痕迹。通过对这些蛛丝马迹的跟踪分析，可以感知并发现未知威胁，复盘攻击手法，从而采取应对措施，及时止损。

科来网络流量分析解决方案

科来业务性能解决方案

- 科来业务性能管理系统(UPM)
- 科来网络回溯分析系统(RAS)
- 科来网络分析系统(CSNAS)

科来网络安全分析解决方案

- 科来大数据安全态势感知平台(BAP)
- 科来网络全流量安全分析系统(TSA)
- 科来APT攻击检测系统(APT)

CSNA 网络分析认证培训

课程介绍

培训报名

科来网络流量分析技术资料

网络攻击与防范图谱

科来网络通讯协议图

科来网络故障诊断图

CSNA 网络分析经典实战案例

数据包样本

网络分析过滤器

术语表

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