科来

第 02 章
如何分析网站遭受 DDoS 攻击的原因

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

网站出现不能正常访问的原因是多种多样的，问题可能发生在网站服务器端，也可能是互联网出口，或是受到网管限制等等。但种种原因中，网站遭受攻击从而导致无法正常访问的原因与预防手段是最为复杂和难以判定的。攻击者利用网站漏洞或特定攻击手法，往往隐蔽难以察觉，这就需要网站管理人员或安全分析人员针对特定事件进行分析，做到快速响应，定位根源与迅速恢复网站的正常访问。本案例详细分析了攻击者利用数据传输过程中 TCP 零窗口的特点，使得某网站遭受拒绝服务攻击的案例。

2.1 问题描述

某日上午，某部官网突然出现不能访问的情况，维护人员于 12 点 20 分左右重启应用，网站访问恢复正常，但在几分钟后又重复出现不能访问的情况。从流量上观察，并未发现流量异常突发的情况，具体问题需要进一步分析。事发期间的流量，如下图所示。

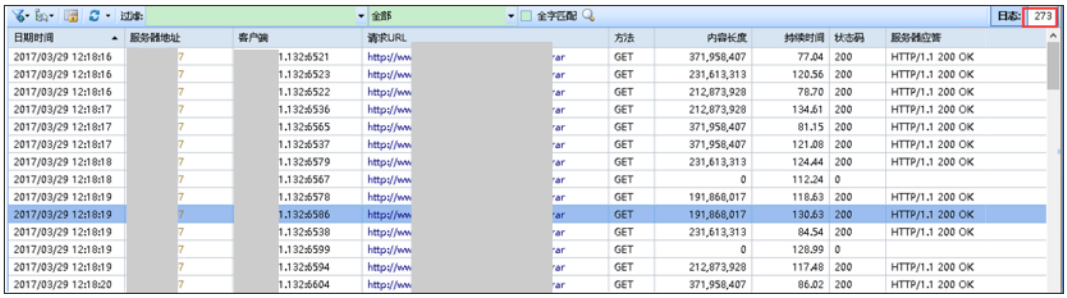
图 2-1

2.2 分析过程

2.2.1 对 12 点 20 分左右出现的异常现象进行分析

可疑互联网 IP X.X.1.132 在 2 分 30 秒左右内，请求下载了 13.rar、14.rar、15.rar 等文件共计 273 次，这些文件的大小均在 200MB 左右。从 12 点 18 分 16 秒第一次请求开始，到 12 点 19 分 35 秒服务器出现无响应的情况，再到 12 点

20 分 13 秒服务器出现 HTTP 502 报错，本次攻击只花费不到 2 分钟的时间就达到了拒绝服务的攻击效果。



日期时间	服务器地址	客户端	请求URL	方法	内容长度	持续时间	状态码	服务器应答
2017/03/29 12:18:16	7	1.132:6521	http://ww	GET	371,958,407	77.04	200	HTTP/1.1 200 OK
2017/03/29 12:18:16	7	1.132:6523	http://ww	GET	231,613,313	120.56	200	HTTP/1.1 200 OK
2017/03/29 12:18:16	7	1.132:6522	http://ww	GET	212,873,928	78.70	200	HTTP/1.1 200 OK
2017/03/29 12:18:17	7	1.132:6536	http://ww	GET	212,873,928	134.61	200	HTTP/1.1 200 OK
2017/03/29 12:18:17	7	1.132:6565	http://ww	GET	371,958,407	81.15	200	HTTP/1.1 200 OK
2017/03/29 12:18:17	7	1.132:6537	http://ww	GET	371,958,407	121.08	200	HTTP/1.1 200 OK
2017/03/29 12:18:18	7	1.132:6579	http://ww	GET	231,613,313	124.44	200	HTTP/1.1 200 OK
2017/03/29 12:18:18	7	1.132:6567	http://ww	GET	0	112.24	0	
2017/03/29 12:18:19	7	1.132:6578	http://ww	GET	191,868,017	118.63	200	HTTP/1.1 200 OK
2017/03/29 12:18:19	7	1.132:6586	http://ww	GET	191,868,017	130.63	200	HTTP/1.1 200 OK
2017/03/29 12:18:19	7	1.132:6538	http://ww	GET	231,613,313	84.54	200	HTTP/1.1 200 OK
2017/03/29 12:18:19	7	1.132:6599	http://ww	GET	0	128.99	0	
2017/03/29 12:18:19	7	1.132:6594	http://ww	GET	212,873,928	117.48	200	HTTP/1.1 200 OK
2017/03/29 12:18:20	7	1.132:6604	http://ww	GET	371,958,407	86.02	200	HTTP/1.1 200 OK

图　2-2

查看 X.X.1.132 与网站的 TCP 会话，发现这些会话的持续时间都很长，因为发现攻击后，服务器在两分钟后进行了重启，所以看似持续时间只有 2 分多钟，但如果不重启会话会一直持续。

节点1 ->	端口1 ->	<- 节点2	<- 端口2	数据包	字节数	协议	持续时间	字节 ->	<- 字节	数据包 ->	<- 数据包	开始发包时间		最后发包时间
.1.132	6621	7	80	86	71.07 KB	HTTP	00:02:18.235049	2.24 KB	68.83 KB	27	59	2017	12:18:20	2017 2:20:39
.1.132	6655	7	80	90	75.35 KB	HTTP	00:02:16.490297	2.37 KB	72.98 KB	29	61	2017	12:18:21	2017 2:20:38
.1.132	6536	7	80	97	79.20 KB	HTTP	00:02:14.955237	2.68 KB	76.52 KB	34	63	2017	12:18:17	2017 2:20:32
.1.132	6686	7	80	75	70.96 KB	HTTP	00:02:14.687800	1.65 KB	69.31 KB	18	57	2017	12:18:23	2017 2:20:37
.1.132	6605	7	80	93	76.27 KB	HTTP	00:02:14.035326	2.56 KB	73.71 KB	32	61	2017	12:18:20	2017 2:20:34
.1.132	6586	7	80	94	81.69 KB	HTTP	00:02:10.976079	2.36 KB	79.33 KB	29	65	2017	12:18:19	2017 2:20:30
.1.132	6835	7	80	79	57.80 KB	HTTP	00:02:09.715288	2.34 KB	55.46 KB	29	50	2017	12:18:29	2017 2:20:39
.1.132	6599	7	80	98	80.51 KB	HTTP	00:02:09.037155	2.64 KB	77.86 KB	33	65	2017	12:18:19	2017 2:20:28
.1.132	6704	7	80	80	57.89 KB	HTTP	00:02:08.578058	2.49 KB	55.39 KB	31	49	2017	12:18:24	2017 2:20:32
.1.132	6729	7	80	92	76.08 KB	HTTP	00:02:08.282077	2.43 KB	73.65 KB	30	62	2017	12:18:25	2017 2:20:33
.1.132	6606	7	80	91	74.82 KB	HTTP	00:02:07.781597	2.51 KB	72.31 KB	31	60	2017	12:18:20	2017 2:20:27
.1.132	6734	7	80	83	62.22 KB	HTTP	00:02:07.707021	2.56 KB	59.67 KB	32	51	2017	12:18:25	2017 2:20:33
.1.132	6630	7	80	91	77.49 KB	HTTP	00:02:06.639576	2.38 KB	75.12 KB	29	62	2017	12:18:21	2017 2:20:27
.1.132	6728	7	80	75	54.89 KB	HTTP	00:02:06.263030	2.31 KB	52.59 KB	28	47	2017	12:18:25	2017 2:20:31
.1.132	6708	7	80	94	82.92 KB	HTTP	00:02:05.318624	2.24 KB	80.67 KB	27	67	2017	12:18:24	2017 2:20:29
.1.132	6579	7	80	93	78.97 KB	HTTP	00:02:04.483717	2.45 KB	76.52 KB	30	63	2017	12:18:18	2017 2:20:23
.1.132	6798	7	80	81	65.39 KB	HTTP	00:02:04.229118	2.31 KB	63.09 KB	28	53	2017	12:18:27	2017 2:20:31
.1.132	6629	7	80	87	74.55 KB	HTTP	00:02:04.207445	2.31 KB	72.24 KB	28	59	2017	12:18:21	2017 2:20:25
.1.132	6774	7	80	76	58.97 KB	HTTP	00:02:04.004491	2.17 KB	56.80 KB	26	50	2017	12:18:26	2017 2:20:30
.1.132	6659	7	80	79	63.32 KB	HTTP	00:02:03.197287	2.24 KB	61.07 KB	27	52	2017	12:18:22	2017 2:20:25
.1.132	6727	7	80	71	62.06 KB	HTTP	00:02:02.932278	1.85 KB	60.21 KB	21	50	2017	12:18:25	2017 2:20:28
.1.132	6762	7	80	90	74.59 KB	HTTP	00:02:01.538404	2.28 KB	72.31 KB	28	62	2017	12:18:26	2017 2:20:27
.1.132	6537	7	80	84	72.27 KB	HTTP	00:02:01.126495	2.16 KB	70.11 KB	26	58	2017	12:18:17	2017 2:20:18
.1.132	6693	7	80	76	62.98 KB	HTTP	00:02:00.632036	2.09 KB	60.89 KB	25	51	2017	12:18:23	2017 2:20:24

图　2-3

深入分析这些会话内容，可以看到从传输开始，客户端宣告的 TCP 窗口大小为 64860。

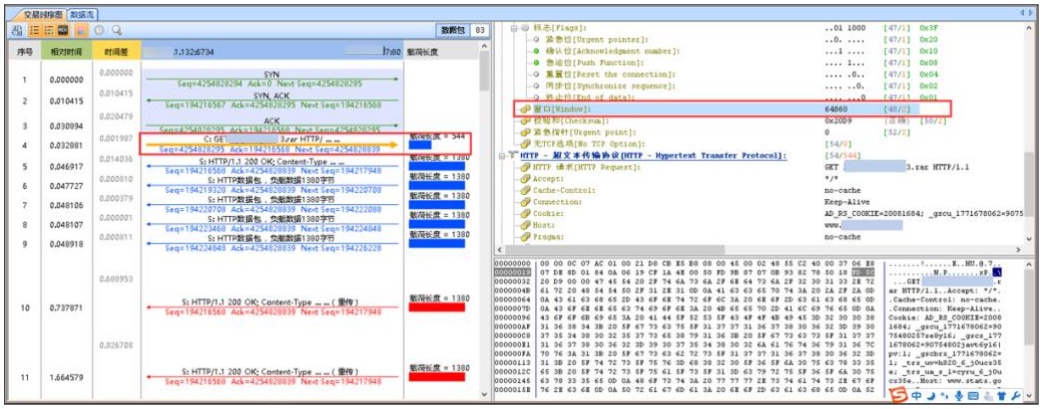


图　2-4

在客户端接收了一些数据后，在该会话的第 57 个包时，客户端宣告的 TCP 窗口大小减小到 17316。

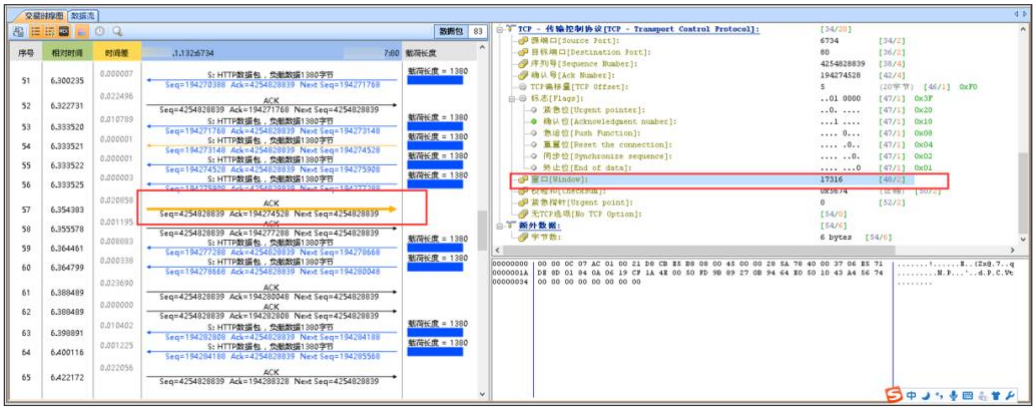


图　2-5

到此会话第 66 个包时，客户端宣告的 TCP 窗口为 756。

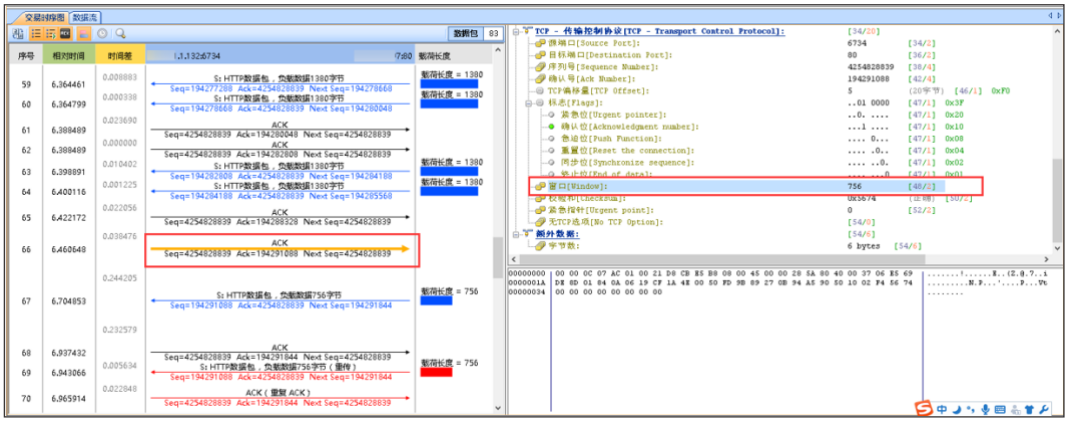


图　2-6

直到第 68 个包时，客户端宣告的 TCP 窗口变为 0，说明客户端已经不能再

接收任何数据。随后服务器将需要继续传输的数据放在发送缓存中，等待客户端窗口恢复正常后再继续发送。

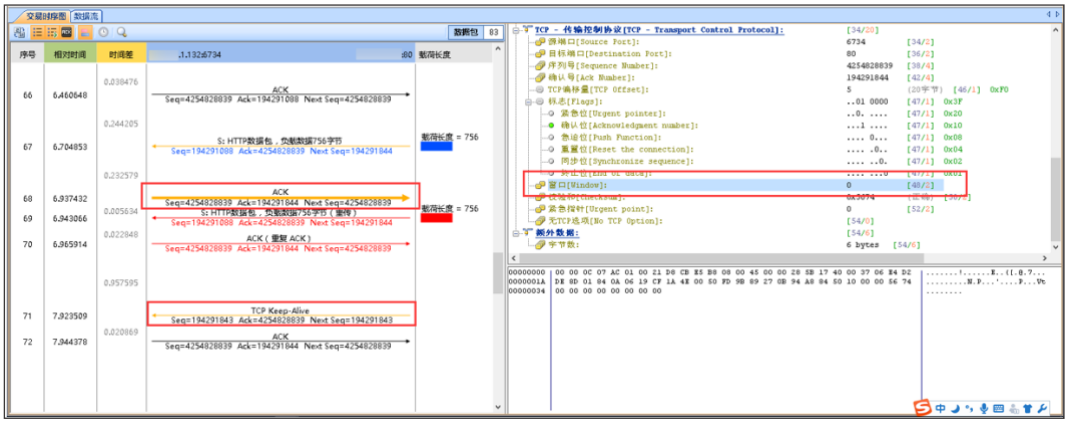


图　2-7

网站服务器不断的发送 ACK 数据包去进行 TCP 窗口探测，每次探测时间为双倍的探测计时器时间，但每次探测的结果均为客户端 TCP 窗口为 0，如下图所示。

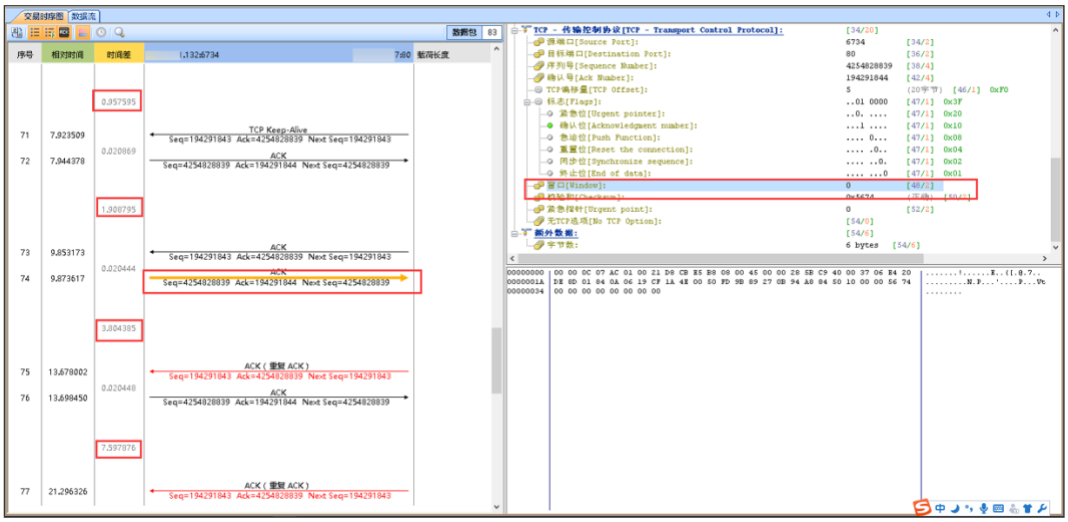


图　2-8

2.2.2　对 14 点 30 分左右出现的异常现象进行分析

该部网站在 14 点 30 分又受到来自 X.X.23.250 发起的攻击，攻击方式与 12 点 20 分发生的攻击行为一致，最后看到探测器时间一直保持在 120 秒探测一次，

而会话的时间达到了十几分钟甚至更长。

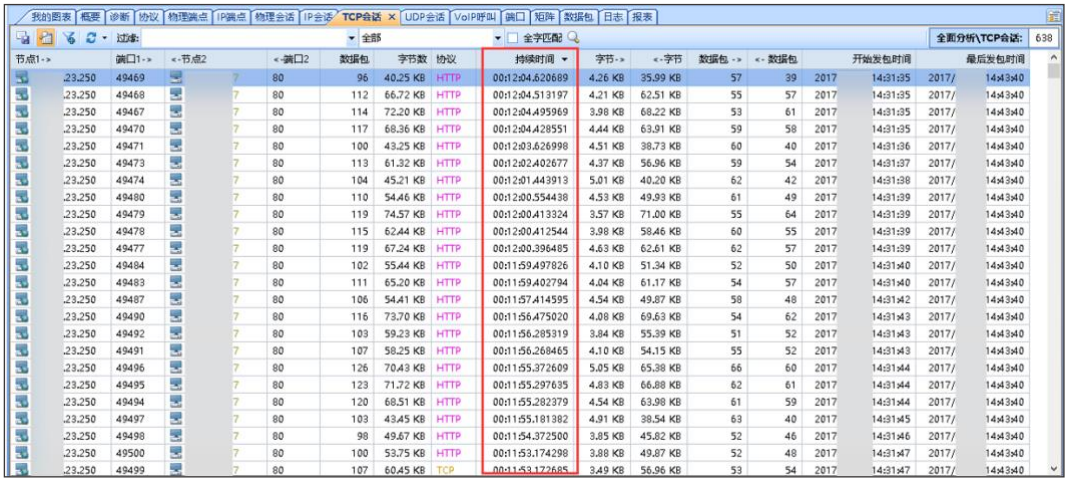


图　2-9

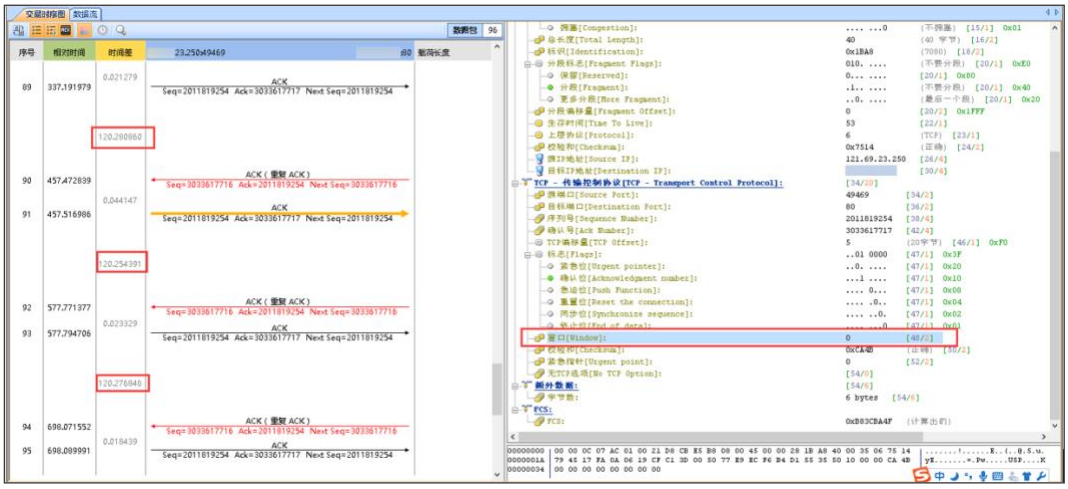


图　2-10

2.3　分析结论及建议

攻击者利用官方网站现有的大文件，向服务器发送下载请求，但在传输过程中利用 TCP 零窗口的特点，只接收少量文件后便不再继续接受文件，从而导致大文件一直积压在服务器的发送缓存中，造成服务性能消耗，进而造成官网不能访问的现象。

处置建议：

在负载均衡设备上设置 TCP 零窗口超时时间；

将大文件单独放在另外一台服务器中，将官网链接指向到此文件服务器。

2.4 价值

网站正常运行涉及的元素十分繁杂，当遭受黑客的攻击后，维护人员往往很难做到快速响应，使网站恢复正常访问，更难以确定对方是利用的何种手段或漏洞发起的攻击。在本案例中我们通过网络流量分析技术，实现了对网络攻击的可视化，精准监控网络数据流向，进而第一时间将攻击行为梳理出来，大幅缩短了解决问题的时间。

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