

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。



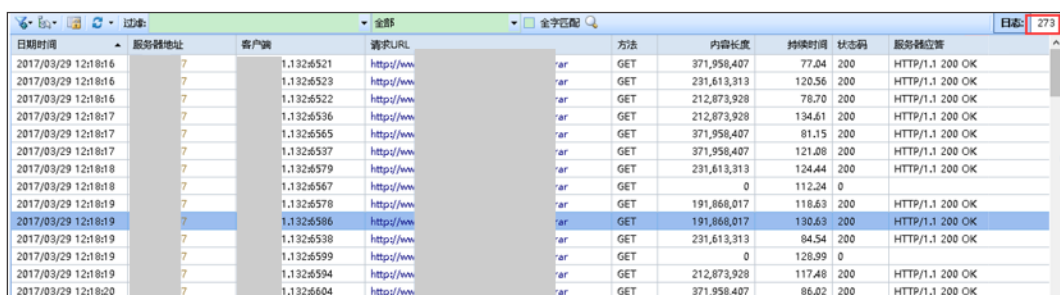
图 2-1

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	https://www...	GET	371,958,407	77.04	200	HTTP/1.1 200 OK
2017/03/29 12:18:16	7	1.132.6523	https://www...	GET	231,613,313	120.56	200	HTTP/1.1 200 OK
2017/03/29 12:18:16	7	1.132.6522	https://www...	GET	212,873,928	78.70	200	HTTP/1.1 200 OK
2017/03/29 12:18:17	7	1.132.6536	https://www...	GET	212,873,928	134.61	200	HTTP/1.1 200 OK
2017/03/29 12:18:17	7	1.132.6565	https://www...	GET	371,958,407	81.15	200	HTTP/1.1 200 OK
2017/03/29 12:18:17	7	1.132.6537	https://www...	GET	371,958,407	121.08	200	HTTP/1.1 200 OK
2017/03/29 12:18:18	7	1.132.6579	https://www...	GET	231,613,313	124.44	200	HTTP/1.1 200 OK
2017/03/29 12:18:18	7	1.132.6567	https://www...	GET	0	112.24	0	
2017/03/29 12:18:19	7	1.132.6578	https://www...	GET	191,868,017	118.63	200	HTTP/1.1 200 OK
2017/03/29 12:18:19	7	1.132.6586	https://www...	GET	191,868,017	130.63	200	HTTP/1.1 200 OK
2017/03/29 12:18:19	7	1.132.6538	https://www...	GET	231,613,313	84.54	200	HTTP/1.1 200 OK
2017/03/29 12:18:19	7	1.132.6599	https://www...	GET	0	128.99	0	
2017/03/29 12:18:19	7	1.132.6594	https://www...	GET	212,873,928	117.48	200	HTTP/1.1 200 OK
2017/03/29 12:18:20	7	1.132.6604	https://www...	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。

<div> <div> 概览 诊断 协议 IP地址 IP会话 TCP会话 UDP会话 VoIP呼叫 端口 矩阵 数据包 日志 </div> <div> 全部 全部匹配 </div> <div> 1.1.132:TCP:6835 441 </div> </div>														
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->	节点3->	端口3->	数据包->	开始发包时间	最后发包时间	
1.132	6621	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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	80	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。

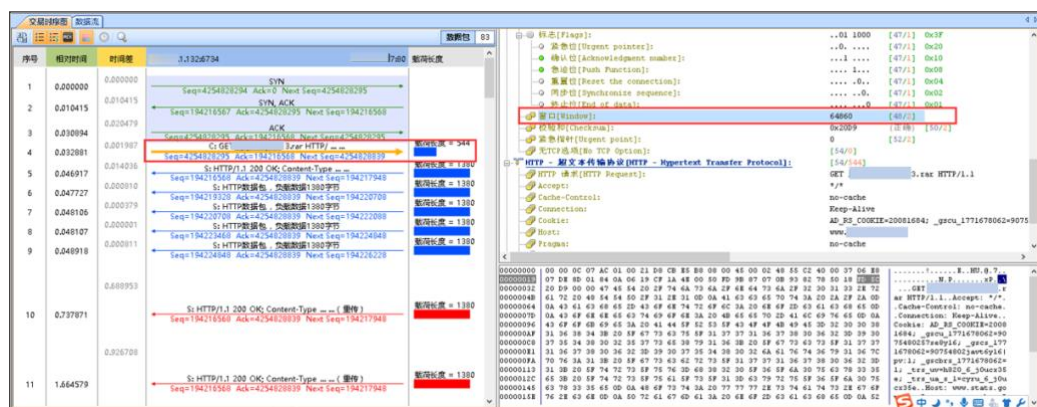


图 2-4

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。

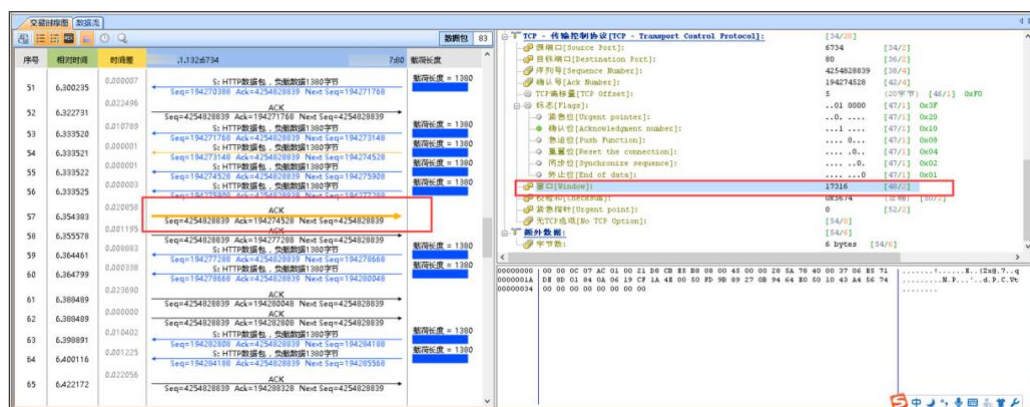


图 2-5

到此会话第 66 个包时，客户端宣告的 TCP 窗口为 756。

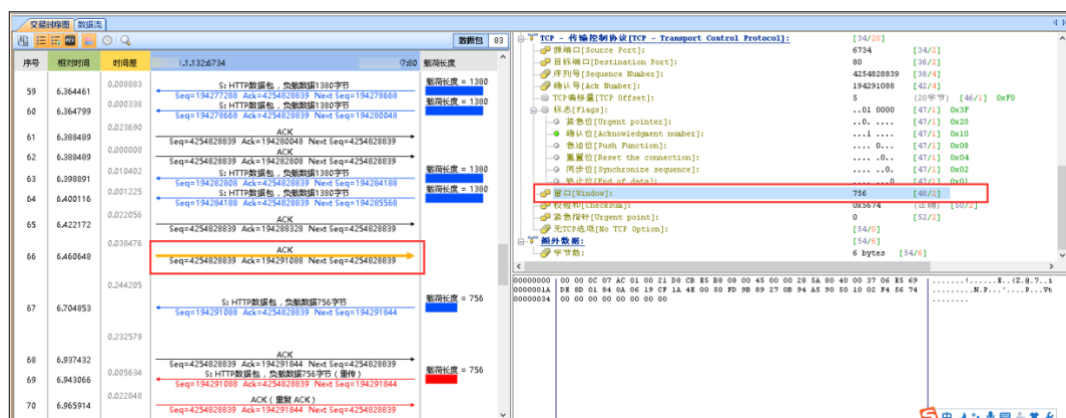


图 2-6

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。

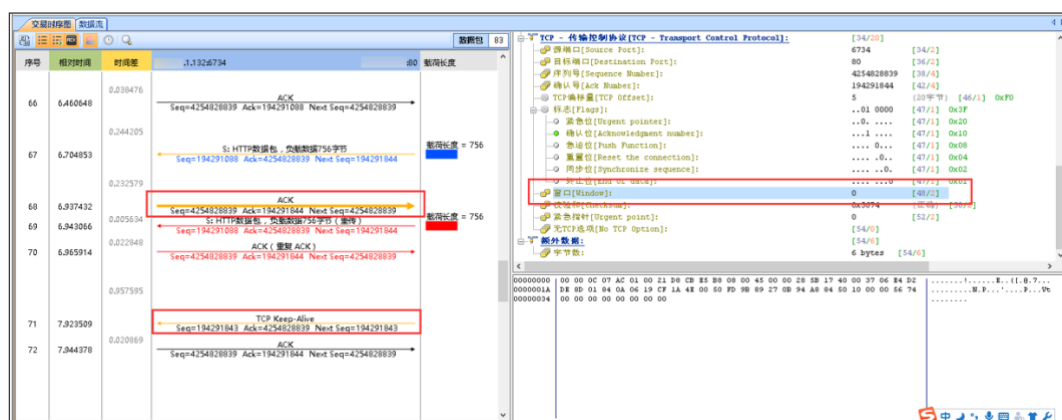


图 2-7

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。

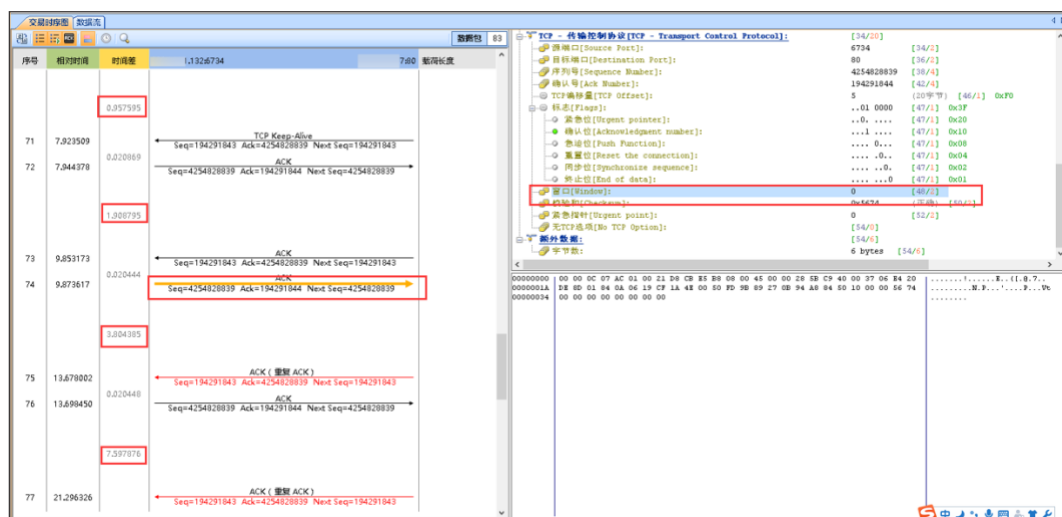


图 2-8

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。

我的图表

概要

诊断

协议

物理端口

IP端口

物理会话

IP会话

TCP会话

UDP会话

VoIP呼入

端口

矩阵

数据包

日志

报表

过录:

全部

全字匹配

全部分析/TCP会话: 638

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
23.250	49469	7	80	96	40.25 KB	HTTP	0001204.620689	4.26 KB	35.99 KB	57	39	2017	14:31:35	2017/14:31:40
23.250	49468	7	80	112	66.72 KB	HTTP	0001204.513197	4.21 KB	62.51 KB	55	57	2017	14:31:35	2017/14:31:40
23.250	49467	7	80	114	72.20 KB	HTTP	0001204.495969	3.98 KB	68.22 KB	53	61	2017	14:31:35	2017/14:31:40
23.250	49470	7	80	117	68.36 KB	HTTP	0001204.428551	4.44 KB	63.91 KB	59	58	2017	14:31:35	2017/14:31:40
23.250	49471	7	80	100	43.25 KB	HTTP	0001203.626998	4.51 KB	38.73 KB	60	40	2017	14:31:36	2017/14:31:40
23.250	49473	7	80	113	61.32 KB	HTTP	0001202.402677	4.37 KB	56.96 KB	59	54	2017	14:31:37	2017/14:31:40
23.250	49474	7	80	104	45.21 KB	HTTP	0001201.443913	5.01 KB	40.20 KB	62	42	2017	14:31:38	2017/14:31:40
23.250	49480	7	80	110	54.46 KB	HTTP	0001200.554438	4.53 KB	49.93 KB	61	49	2017	14:31:39	2017/14:31:40
23.250	49479	7	80	119	74.57 KB	HTTP	0001200.413324	3.57 KB	71.00 KB	55	64	2017	14:31:39	2017/14:31:40
23.250	49478	7	80	115	62.44 KB	HTTP	0001200.412544	3.98 KB	58.46 KB	60	55	2017	14:31:39	2017/14:31:40
23.250	49477	7	80	119	67.24 KB	HTTP	0001200.396485	4.63 KB	62.61 KB	62	57	2017	14:31:39	2017/14:31:40
23.250	49484	7	80	102	55.44 KB	HTTP	0001159.497826	4.10 KB	51.34 KB	52	50	2017	14:31:40	2017/14:31:40
23.250	49483	7	80	111	65.20 KB	HTTP	0001159.402794	4.04 KB	61.17 KB	54	57	2017	14:31:40	2017/14:31:40
23.250	49487	7	80	106	54.41 KB	HTTP	0001157.414595	4.54 KB	49.87 KB	58	48	2017	14:31:42	2017/14:31:40
23.250	49490	7	80	116	73.70 KB	HTTP	0001156.475020	4.08 KB	69.63 KB	54	62	2017	14:31:43	2017/14:31:40
23.250	49492	7	80	103	59.23 KB	HTTP	0001156.285319	3.84 KB	55.39 KB	51	52	2017	14:31:43	2017/14:31:40
23.250	49491	7	80	107	58.25 KB	HTTP	0001156.268465	4.10 KB	54.15 KB	55	52	2017	14:31:43	2017/14:31:40
23.250	49496	7	80	126	70.43 KB	HTTP	0001155.372609	5.05 KB	65.38 KB	66	60	2017	14:31:44	2017/14:31:40
23.250	49495	7	80	123	71.72 KB	HTTP	0001155.297635	4.83 KB	66.88 KB	62	61	2017	14:31:44	2017/14:31:40
23.250	49494	7	80	120	60.51 KB	HTTP	0001155.282379	4.54 KB	63.98 KB	61	59	2017	14:31:44	2017/14:31:40
23.250	49497	7	80	103	43.45 KB	HTTP	0001155.181982	4.91 KB	38.54 KB	63	40	2017	14:31:45	2017/14:31:40
23.250	49498	7	80	98	49.67 KB	HTTP	0001154.372500	3.85 KB	45.82 KB	52	46	2017	14:31:46	2017/14:31:40
23.250	49500	7	80	100	53.75 KB	HTTP	0001153.174298	3.88 KB	49.87 KB	52	48	2017	14:31:47	2017/14:31:40
23.250	49499	7	80	107	60.45 KB	TCP	0001153.122685	3.49 KB	56.96 KB	53	54	2017	14:31:47	2017/14:31:40

图 2-9

序号	相对时间	时间差	数据包
89	337.191979	0.021279	ACK (Seq=2011819254 Ack=3033617717 Next Seq=2011819254)
90	457.472839	0.044147	ACK (Seq=2011819254 Ack=3033617717 Next Seq=2011819254)
91	457.516986	0.0254301	ACK (Seq=2011819254 Ack=3033617717 Next Seq=2011819254)
92	577.771977	0.023329	ACK (Seq=2011819254 Ack=3033617717 Next Seq=2011819254)
93	577.794706	0.018439	ACK (Seq=2011819254 Ack=3033617717 Next Seq=2011819254)
94	698.071552	0.018439	ACK (Seq=2011819254 Ack=3033617717 Next Seq=2011819254)
95	698.089991	0.018439	ACK (Seq=2011819254 Ack=3033617717 Next Seq=2011819254)

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