科来

第 15 章
如何分析邮件系统遭受的攻击行为

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

邮件系统是信息化使用频率最高的业务系统之一，大量的信息是通过邮件进行沟通和共享的，由于这些信息都非常有价值，所以也成为被攻击的主要目标。

15.1 环境描述

客户为某大型保险公司，邮件系统是该单位使用最为频繁的系统之一。该单位邮件系统分为两种：Web 登录方式和使用标准的 SMTP、POP3 协议收发方式。科来网络回溯分析系统部署在数据中心的核心交换机上，通过 SPAN 将 DMZ 区的所有服务器流量引入回溯系统进行采集和分析。

15.2 针对暴力破解邮件系统分析

在 9 月 20 日，针对该用户的流量数据进行网络分析时，发现其分公司的一些 IP 在针对邮件服务器进行暴力破解攻击。我们选择 2 天的时间窗口，然后选择其中 9 月 19 日上午的数据进行分析。点击“发 tcp 同步包”选项进行排名，我们发现 IP X.X.200.66 的流量只有 9.35MB，但“tcp 发送同步包”却排名第三位，达到了 20592 个。这种 TCP 会话很多，流量又特别小的 IP 比较异常。我们选择下载分析该 IP 数据包，进行深入分析。

下载该 IP 的通信数据后，我们发现该 IP 在 9 月 19 日上午对邮件服务器发起超过 2 万次 TCP 请求，而且密集时候每秒能发送 100 多个 TCP 同步包，如下图所示。

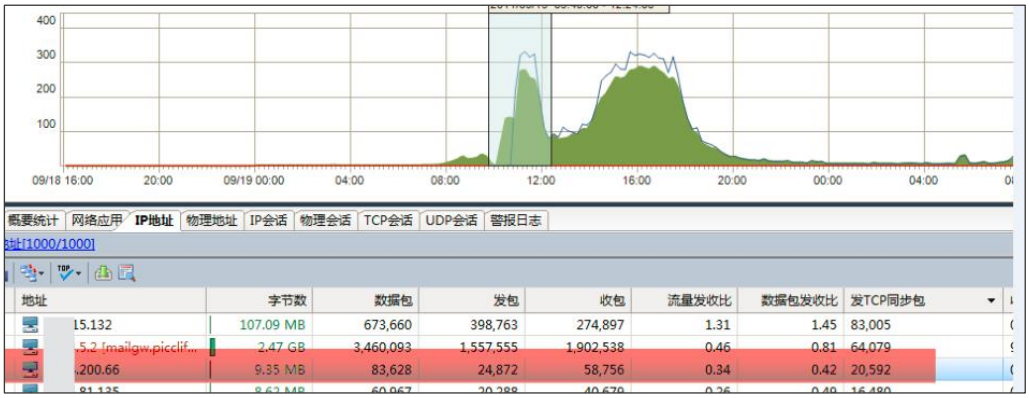

图　15-1

在下图中，我们可以看到 IPX.X.200.66，在很短时间内向邮件服务器 X.X.4.3 做了多次重复的会话。从行为上来看，X.X.200.66 在向邮件服务器进行请求，但又始终不发送三次握手中最后的 ACK 数据包。这样导致它与服务器的 TCP 会话始终无法建立，而且服务器为了等待 X.X.200.66 回送 ACK，会消耗一定的系统资源。这样高频率、不正常的请求访问，就造成了对 mail 服务器的攻击。

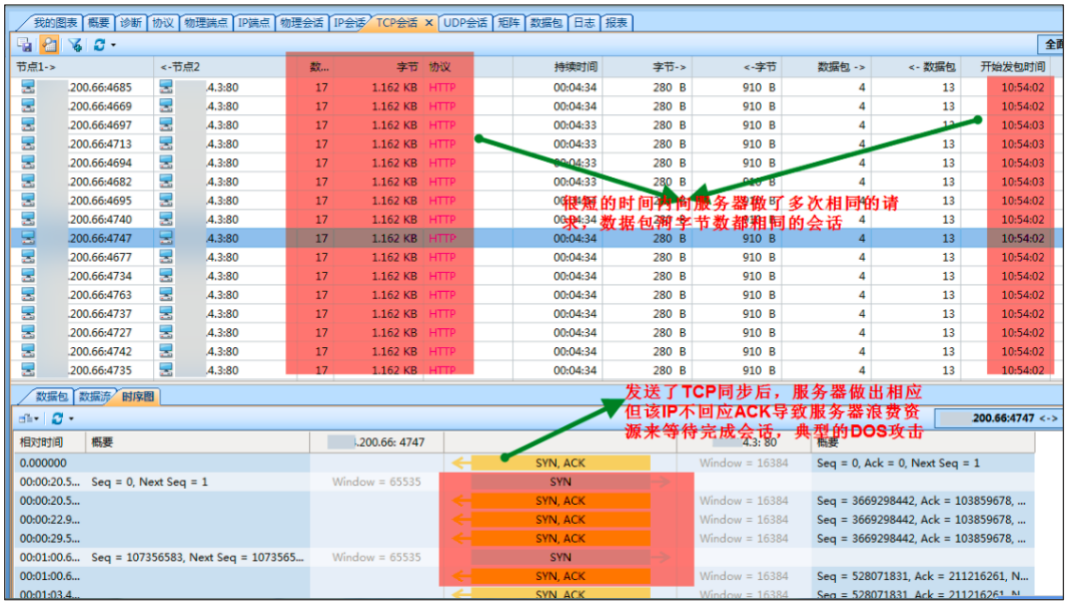

图　15-2

而 X.X.200.66 在与服务器建立的成功的会话中，是有较大异常情况。通过“HTTP 日志”分析我们可以看到以下不正常现象，如下图所示。

图　15-3

我们看到，X.X.200.66 每次访问的 URL 是一模一样的，而且出现每秒钟多达 10 次以上的访问。从该频率看，不是人为访问，应该是病毒程序自动访问导致。分析这个 URL 发现，打开后是邮件服务器的 Web 登录界面。因此，我们可以判断这种行为应该是在进行密码尝试。

本次分析同时发现，服务器段的 IP X.X.5.2 也在向邮件服务器进行密码尝试行为，如下面两幅图所示。

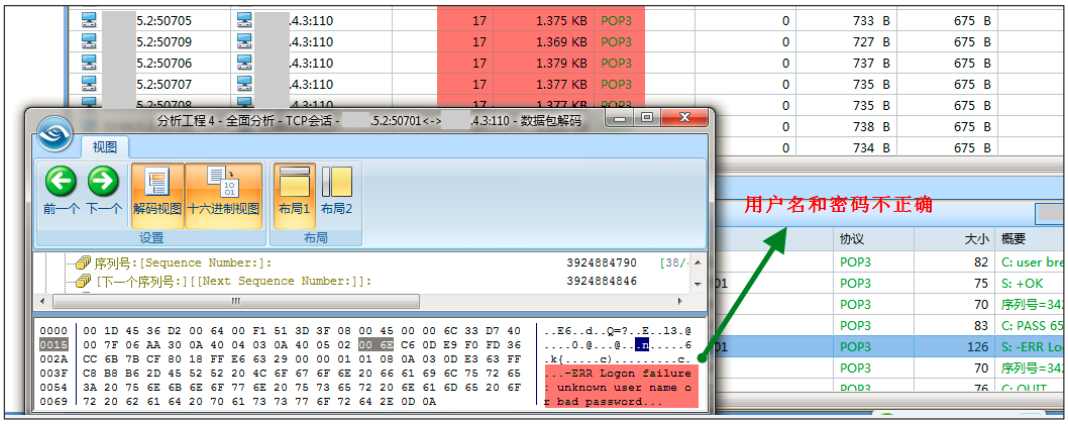

图　15-4

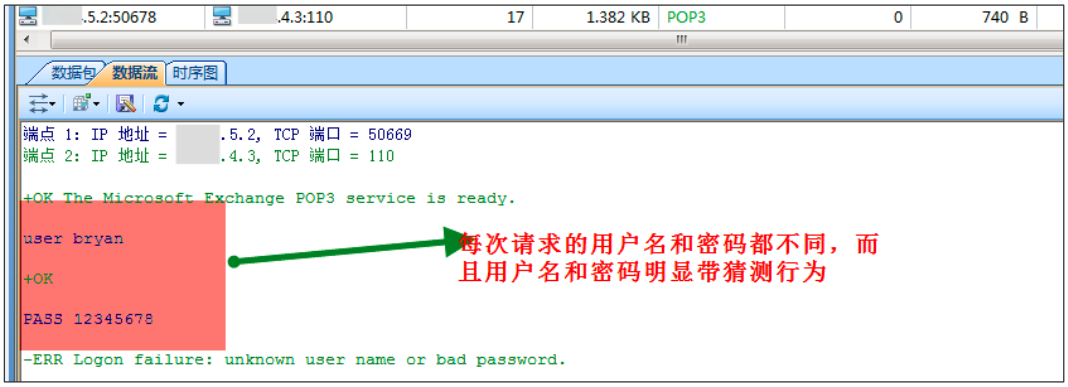

图　15-5

通过以上针对邮件服务器数据的分析，我们发现网络中存在很多针对邮件服务器的不正常会话，这些会话对邮件服务器形成了攻击。攻击以和用户名密码的猜测较多，属于渗透攻击。

这些攻击猜测行为，一旦被取得真实的用户名和密码后，就能够对邮件服务器做数据偷窃，那么每封邮件的信息将会没有秘密可言。如果黑客通过攻击得到了邮件服务器的用户名和密码，就可以潜伏到网络中侦听他想要的信息，造成信息窃密事件的发生，对公司业务造成损失。

建议加强邮件服务器的防护，并对攻击者强制杀毒。同时，在防火墙上做一些 TCP 会话的强制会话时间限制。例如：在防火墙上做策略，使邮件每次 TCP 会话空闲时间不超过 2 秒，如果 2 秒得不到 ACK 回应则重置会话。

15.3 针对邮件蠕虫攻击分析

通过以上分析，我们发现网络中的邮件服务器的状况不太安全。那么，是否还存在其他问题呢？

由于邮件服务器的数据量很大，每天有超过 10GB 的流量，因此我们决定使用采样分析的方法，对邮件服务器进行数据采样分析。我们选择上午 9-10 点之间数据（该单位 9 点上班，邮件系统比较繁忙）。然后，选择网络应用中的 SMTP 进行挖掘分析。在查看会话时，我们发现 IP10.82.184.35 的会话数很多，在近 1 小时内该 IP 的 SMTP 会话到达几百个。明显的异常现象。于是，我们选择将该 IP 一上午的数据包，全部下载分析。

科来网络分析工程师打开“TCP 会话”，看到最多的是 X.X.184.35 和邮件服务器 X.X.4.3 之间的 13 个数据包的会话。

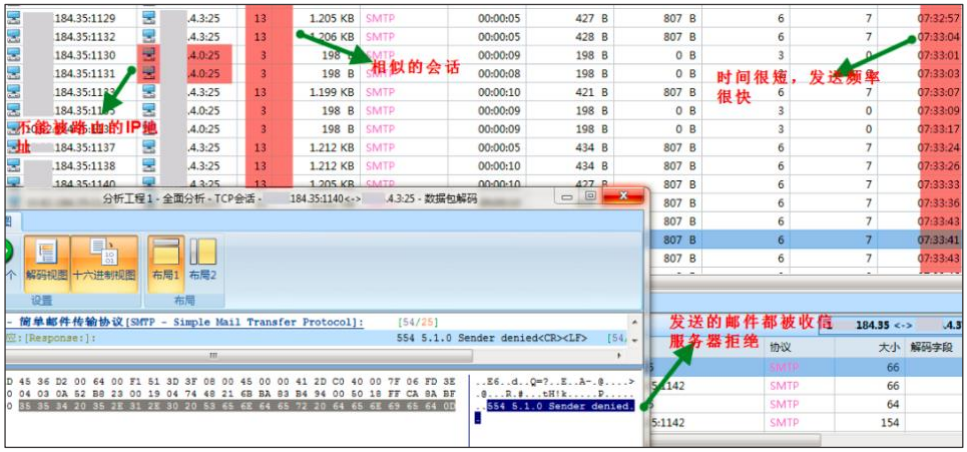

图 15-6

该 IP 还向 X.X.4.0 发起请求，但接收方 IP 并不存在，所以只有三次 SYN 包，没有任何回应。X.X.184.35 在 1 分钟内，就能发送近 10 封内容相似的邮件，而且这种邮件收信者多是比较大的门户网站，如下图所示。

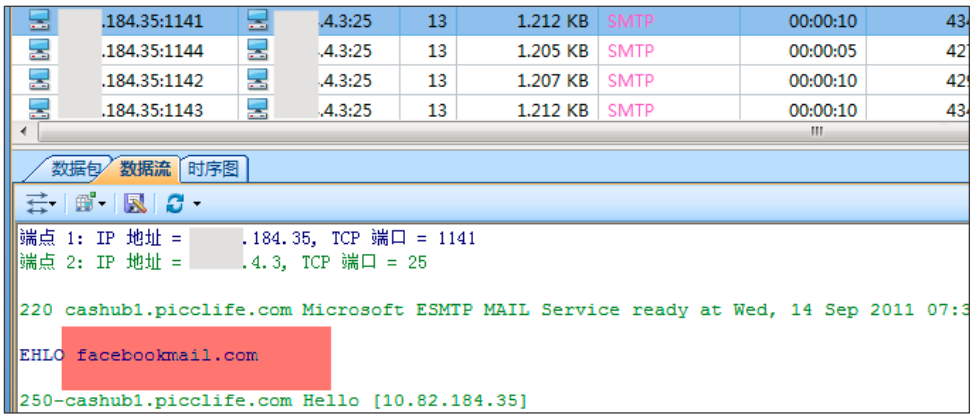

图　15-7

统计发现，该主机在一上午时间内发送了超过 2000 封类似的邮件。而这么高频率的发送显然不是人工所为。产生这种现象的原因应该是该主机中了僵尸程序，然后僵尸程序自动向其他网站发送大量的垃圾邮件所致。建议对该主机进行杀毒后再接入网络。

15.4　价值

邮件系统，是企业单位经常遭受攻击的网络应用，如本文中针对邮件系统的攻击。面对此类攻击事件，科来网络回溯分析系统可对网络通讯流量进行实时记录及保存，通过网络流量分析技术实现对关键业务系统中行为异常的秒级发现，精准定位异常原因，提高邮件系统安全保障能力。

- 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