科来

第 06 章

如何发现被植入后门的内网主机

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

6.1 问题描述

科来网络分析工程师在对某政府单位的网络进行测试时，通过科来网络全流量安全分析系统（TSA）对前几天的网络流量进行全流量回溯分析，凭借 TSA 强大的安全告警功能，发现了内网主机被植入后门程序，并在内网进行扩散的行为。

6.2 分析过程

经过前几天的数据收集及分析，TSA 产生大量的告警信息。分析发现多条告警信息与 IP X.X.56.120 有关，需要对其进行挖掘与深度分析。

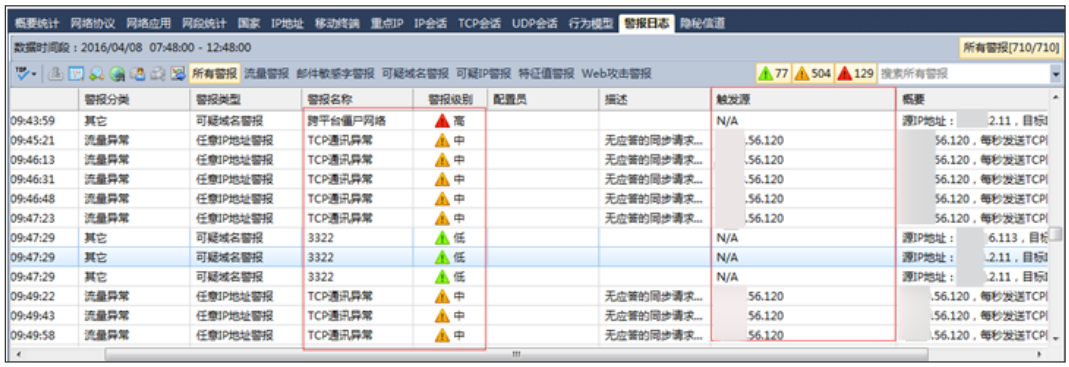

图 6-1

对可疑 IP X.X.56.120 进行多天的流量回溯分析，都存在异常的流量突发，突发流量以 CIFS 协议（文件共享）居多，下图为 4 月 7 日突发流量。

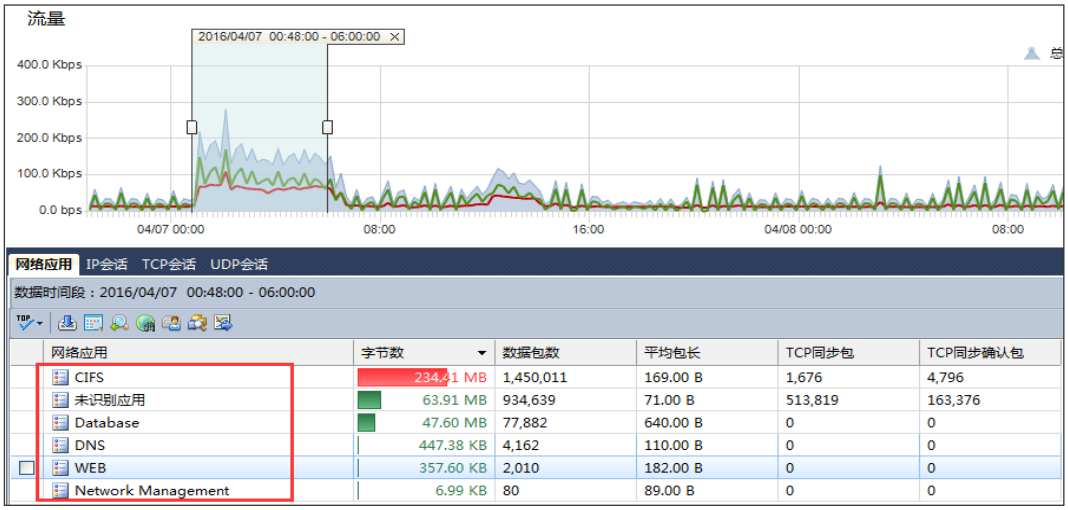

图 6-2

下图为 4 月 8 日突发流量。

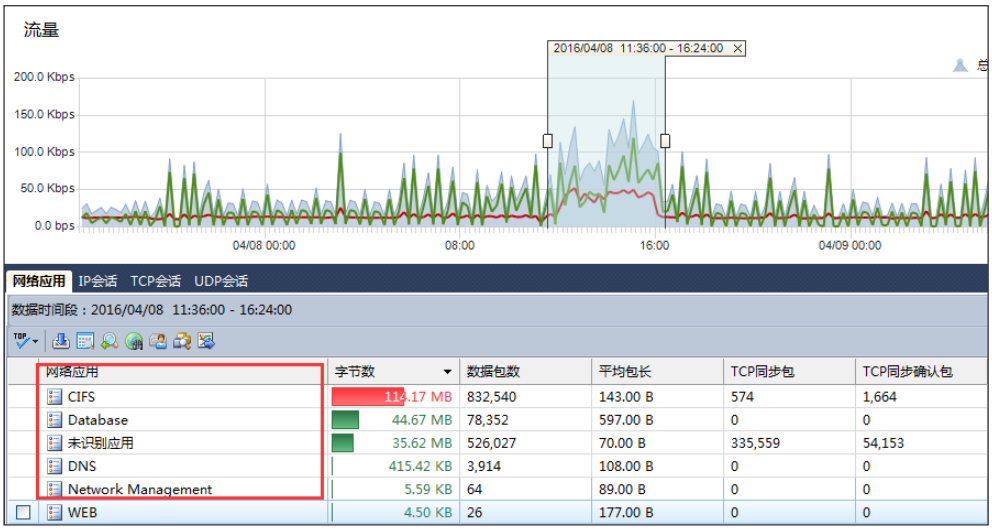

图 6-3

下图为 4 月 9 日突发流量：

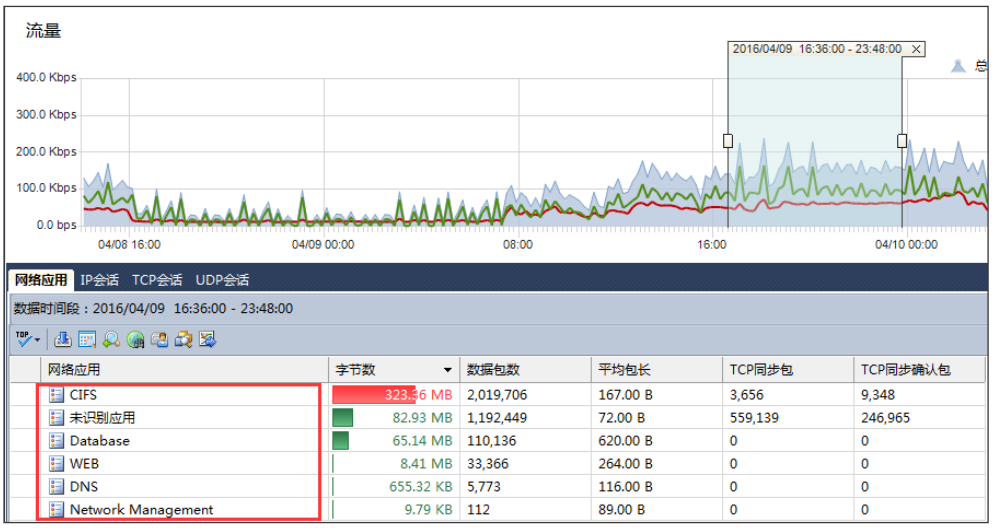

图　6-4

深度挖掘数据包，精细分析可疑 IP X.X.56.120 与内网主机的可疑行为：

嗅探对端主机操作系统版本

下图中，可疑 IP 通过 Netbios 收集对端主机的操作系统版本信息。

图　6-5

探测共享 IPC$、ADMIN$

下方两图中，可疑 IP 主动探测大量地址的 IPC$、ADMIN$。攻击者常会通过这些默认共享，发起一些如账户暴力破解等攻击行为，可能存在安全问题。

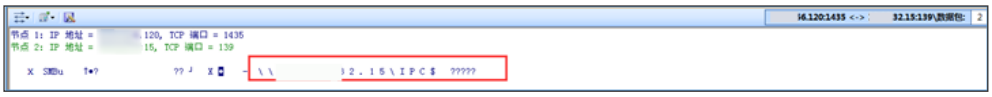

图　6-6

图　6-7

外联服务器 mail.vspcord.com

服务器一般是主动响应客户端的连接请求。但下图数据显示，可疑内网服务

器主动外联境外 IP（葡萄牙），属于高危行为，需要密切关注的。

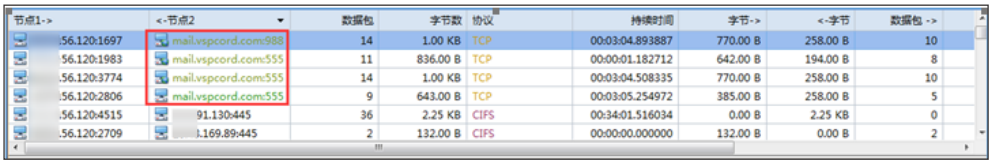

图　6-8

释放程序 eraseme_xxxx.exe 程序

下图数据显示，可疑 IP X.X.56.120 随后主动向被攻击主机释放 PE 程序 eraseme_XXXX.exe，通过多次抓包发现 XXXX 为随机数值。

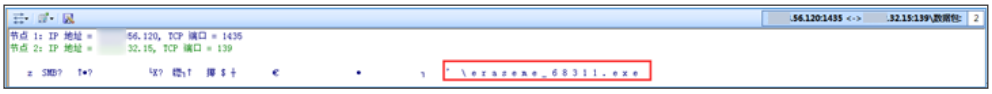

图　6-9

6.3　分析结论

由于数据包中发现了 PE 实体程序 eraseme_xxxx.exe，结合搜集的资料，确定主机 X.X.56.120 被植入 eraseme 后门程序，并试图向内网其他主机进行扩散。下面列出的该后门程序一些关键特征，也与实际数据包展示的行为一致。

特征点 1：与 C&C 服务器 mail.vspcord.com:555 端口建立 TCP 连接，连接成功后发送机器相关信息，等待接收命令，根据指令发送相关信息。

特征点 2：查找内网所有开放 139、445 端口的主机。并对这些主机进行 IPC$ 暴力破解，破解程序将其复制到远程主机上，重命名为 Eraseme_%d%d%d%d%d.exe（%d 为 1-9 的随机数）。

符合点 1：TSA 捕获中招主机与 C&C 服务器 mail.vspcord.com 通讯行为。

符合点 2：TSA 捕获的端口 139 流量中存访问主机的系统默认共享 IPS$的流量。

符合点 3：TSA 发现的 eraseme.exe 程序的命名方式也报告描述一致。

6.4 价值

主机被攻击后再被植入后门，用户是很难察觉到的。仅仅依靠防火墙、入侵检测系统，无法发现这些行为，只有采用全流量的回溯分析手段，才能发现这些隐蔽行为。

本案例中描述的攻击行为发生在内网，由于传统的安全设备（firewall、IPS）的部署区域和静态检测技术的限制，导致其无法发现此类后门攻击行为。TSA 以全流量分析为核心，结合灵活的告警机制，可以实时监测后门类攻击，有效识别后门攻击过程中的流量特征，为用户提供应对该类攻击行为的有效检测和分析手段，弥补了现有安全体系的短板。

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