将病毒拒之门外

Cisco SIMS 解决方案成功识别和跟踪 SQL 服务器蠕虫病毒，将 Slammer 病毒拒之门外

“我总是让 Cisco SIMS Event Viewer 在我的 NOC 中随时保持运行，因此我能很容易地注意到我们正经历异常活动，这也就不奇怪了。我可以马上对 Slammer 病毒关闭端口。而这恰恰也是我希望 Cisco SIMS 能做到的。”

——Cellular South 公司
Charles Watson II

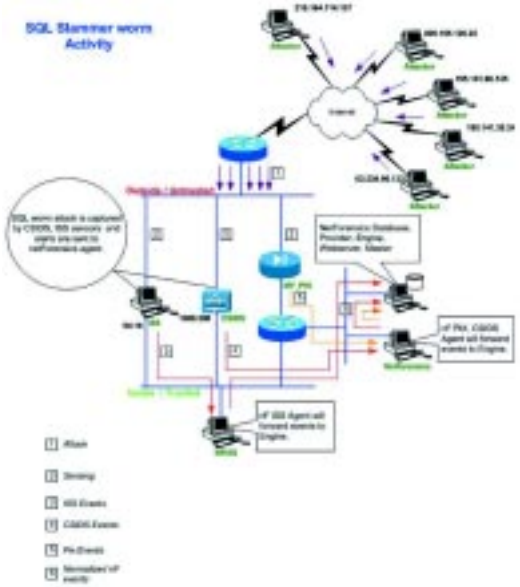
攻击

广泛感染的SQL服务器蠕虫病毒进一步强调了采纳 Cisco SIMS 安全信息管理(SIM)解决方案的必要性。这种恶意Slammer蠕虫病毒是一种驻留在内存中的蠕虫，它可通过UDP Port 1434 繁殖和传播，并可攻击SQL 服务器系统以及配备 Microsoft SQL Desktop Engine (MSDE) Version 2000 的系统中的漏洞。因为这种蠕虫是驻留在内存中的，所以就会非常快地发生缓冲区溢出，进而导致拒绝服务。

CISCO SIMS 解决方案

内部 Honeynet 研究小组对 Slammer 病毒进行了两天跟踪，并通过 SIM Real-Time Desktop

图 1



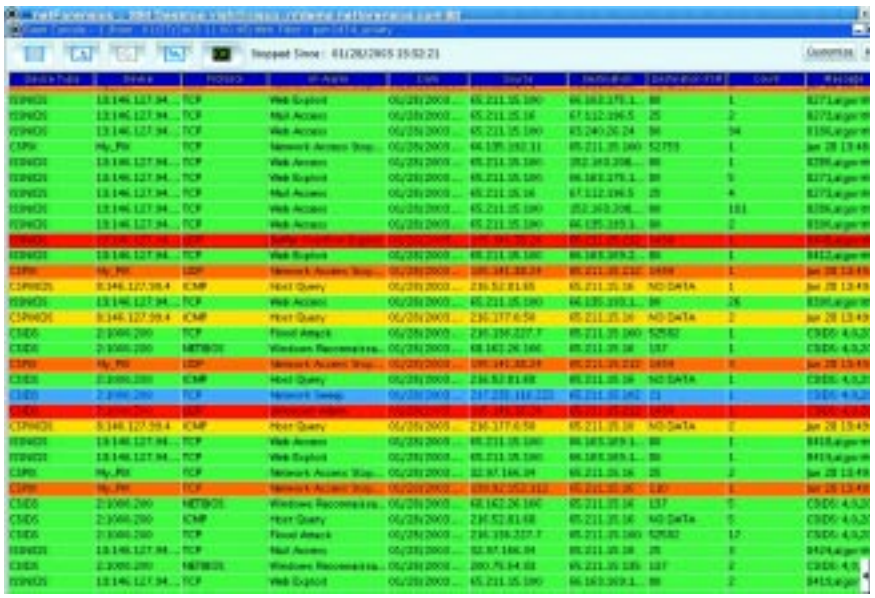
(实时桌面) 监控了该病毒的发展情况。图 1 简单描述了该病毒是如何企图攻击网络的。在 Cisco SIMS 控制台上(图 2)，来自 Cisco PIX、Cisco IDS 和 ISS 网络检测器等多种不同被监控设备的事件通知操作人员有异常活动正在发生。针对这种新的多层次攻击，Cisco SIMS 统计关联识别并捕捉了事件，并将这一 IDS 信息映射为“缓冲区溢出攻击”的高级威胁和所产生的防火墙响应“网络访问中断”。

在客户地点，也就是密西西比州杰克逊市的 Cellular South 公司，Cisco SIMS 系统对多设备事件进行了快速评估，从而使除网络主管人 Charles Watson以外的任何其他人都注意不到这一 Slammer 病毒。Charles 说：“我总是让 Cisco SIMS Event Viewer 在我的 NOC 中随时保持运行，因此我能很容易地注意到我们正经历异常活动，这也就不奇怪了。我可以马上对 Slammer 病毒关闭端口。而这恰恰也是我希望 Cisco SIMS 能做到的。”

CISCO SIMS™

安全信息管理的领导者

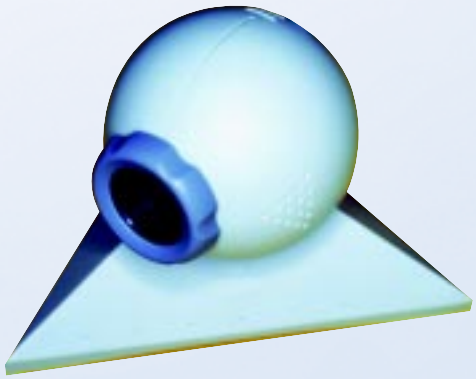
图 2



为了能快速而高效地对非标准数据进行捕捉和语法分析，Cisco SIMS结合采用了Java和XML来识别和分析这些数据以发现潜在的威胁和攻击次序。通过提供一种综合性关联方法，用户能同时采用统计输出和基于规则的输出来实时确定这些事件的性质。事件数据被呈现在多个视图和报告之中，系统还可实现全面而深入的分析和历史趋势观察功能。通过可扩展体系结构能捕捉到极大量的数据，还可毫无限制地实现数据管理的增长。

利用统计关联与基于规则的关联之间这一独特的组合，Cisco SIMS系统可进一步确保Slammer病毒永远死亡而不会给网络造成威胁。捕捉后，Cisco SIMS系统的规则创建功能现在就能持续监控相同的次序并可立刻表明在哪里有多少个事件正在发生。

作为具备互联网安全专业技术和知识的中心，CERT® 协调中心(CERT/CC)通过其网站：http://www.cert.org/advisories/CA-2003-04.html 提供了关于SQL服务器病毒的全部详细信息，包括关于其影响和补丁软件要求的详细情况。



思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19一21层
邮编：100738
电话：(8610)65267777
传真：(8610)85181881

上海
上海市淮海中路222号
力宝广场32一33层
邮编：200021
电话：(8621)33104777
传真：(8621)53966750

广州
广州市天河北路233号
中信广场43楼
邮编：510620
电话：(8620)87007000
传真：(8620)38770077

成都
成都市顺城大街308号
冠城广场23层
邮编：610017
电话：(8628)86758000
传真：(8628)86528999

如需了解思科公司的更多信息，请浏览http://www.cisco.com/cn

欢迎下载电子文档，http://www.cisco.com/cn/power/security/

2004年11月印刷