



务实、高效、可信的应急响应

东软 • 网络安全

曹斌

Neusoft东软



案例一：无间之道



事发

- 受攻击目标：某机关网站
 - 10月22日，机关领导在出差时上网发现自己的网站遭到入侵，主页被替换
- 10月23日下午响应开始，现场情况：
 - 网站服务器位于DMZ区，有东软NetEye防火墙保护
 - 服务器类型：Win2003 + IIS6 + ASP + Access
 - 位于DMZ区的东软NetEye IDS系统在攻击前一天被安全管理员配置成了不记录和分析TCP协议
 - 查看审计日志发现，12月13日上午，IDS服务器日志系统数据库被安全管理员重整
 - 防火墙没有配置针对Web服务器的应用层防护策略
 - 防火墙日志功能没有启用
 - 网络管理员于攻击发现当天使用同名覆盖恢复网站
 - 网站日志被删除



初步分析

○ 初步分析

- 通过分析网站源代码，初步判断攻击方式可能为SQL注入，攻击者利用论坛的配置缺陷，上载了asp木马程序，进而替换了页面
- 可疑对象：
 - 有内部作案的可能
 - 安全管理员：由于对IDS的异常配置，使安全管理员成为首要怀疑对象
 - 网络管理员：由于恢复网站的动作之前没有做任何保留现场的备份工作，也非常可疑
- 难点：没有任何可直接利用的取证机制



真相

- 通过恢复服务器上被删除的数据，取得了攻击者留下的入侵证据，证实了SQL注入的攻击方式，并取得了上载的ASP后门程序代码，再现入侵。
- 根据恢复出的日志数据，定位了攻击者的信息，为外部无关人员，基本解除了对内部人员的怀疑。




回味

- 入侵本可以避免
 - 动网论坛的代码没有分析其安全性，并进行配置上的修补；
 - 防火墙针的“防SQL注入”、“网站信息隐藏”等有效的网站保护措施没有被启用
- 定位本可以更快
 - IDS的审计功能被关闭了，否则即使入侵者扫除了痕迹也能够在IDS系统中留下完整的记录
 - 防火墙的日志功能没有启用
 - 恢复被攻击的网页前没有备份攻击现场



案例二：资源之战




某市级运营商的DDOS攻击

- 持续2个月的洪水攻击
- 1500多台Internet主机参与攻击，遍布互联网各处，部分在海外
- 运营商停止营运，公安部门介入，东软提供技术支持
- 通过在若干个地点的取证分析定位了策动攻击的15台主机
- 进一步分析确定攻击源头，找到发起攻击的现场，攻击发动者被拘捕，攻击停止



教训



大多数客户没有为安全事件做好准备

- 缺少对信息资产的全面了解
- 缺少必要的审计环节，使得发生的事情不容易追踪
- 网络安全防护设施不健全，有些时候需要临时部署防护设施
- 信息系统的日常安全性维护做得不够好



很多客户在事件处理中没有采取正确的措施

- 获取外部资源比较盲目，延误事件处理进程（案例：我们处理的一个案例，在我们到现场之前已有6家不同的公司到现场处理过）
- 现场保护不利，导致一些事件的处理时很难准确评估损失的范围，以及难以追踪攻击来源



很多客户没有在事件之后采取必要的措施

- 包括信息系统的整体加固、必要的安全设施的完善、安全管理体系的加强，以及与应急服务商的正式沟通渠道的建立。



应急处理的独特之处



应急处理的使命

- 在事件发生时阻止攻击
- 使被攻击的系统恢复到攻击前的状态
- 保留证据
- 分析攻击的机制，制定改进的策略，防止同样的攻击再次发生



应急处理面对的局面

- 每个安全事件都是独特的
 - 人的个性化导致攻击行为的个性化
 - 目标、角色、目的、手段、性格
- 为了停止攻击有时需要调动超过组织范围的资源



应急处理的策略

- 资源准备
 - 知识、技能
 - 关于自身系统方面的知识
 - 关于缺陷与攻击的知识
 - 掌握攻击者的技能
 - 现场分析的技能
 - 工具
 - 防御的工具
 - 分析的工具
 - 人员
 - 客户的决策人员、维护人员、应急处理人员
 - 来自外部的应急处理工程师
- 有效调度
 - 在事件发生的很短的时间内，如何有效的调动各种资源，有序的解决问题
 - 应急预案的制定和执行




趋势

- 互联网资源的无序利用正在转变为有组织的利用和有目的的攻击



感叹： 应急处理是艺术

决定应急处理成败的是： 应急资源的质量、
应急过程中相关人员的应变能力



东软如何做好应急响应工作

- 客户与应急处理小组的有效互动是解决问题的关键
- 研究、产品、服务三层技术团队，提供可随时调动的优质资源



攻防研究与应急处理中心

- 漏洞和攻击研究
- 及时向用户通告最新的安全威胁
- 由产品开发部门发布最新的产品升级，对新的攻击进行防御
- 帮助用户进行安全加固、应急预案、培训等工作
- 及时响应客户的应急事件，争取在尽可能短的时间内解决客户的安全问题
- 帮助客户进行事后的安全体系维护



提供有效防御的产品

- 东软NetEye IDS 与安全管理平台 — 提供全网的监控与审计
 - 入侵报警
 - 实时分析
 - 全方位的审计
 - 网络审计
 - 主机审计
 - 应用事件审计
 - 应用过程审计
- 东软NetEye防火墙“流过滤”平台 — 有效防御平台
 - 针对应用层攻击，提供丰富的应用层攻击防护策略
 - 快速扩充针对性防御部件



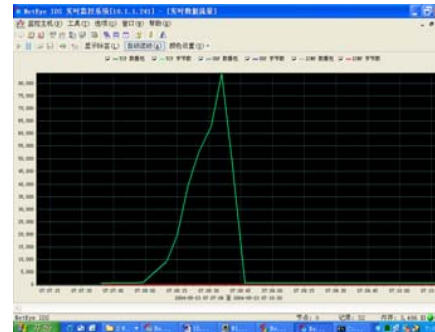
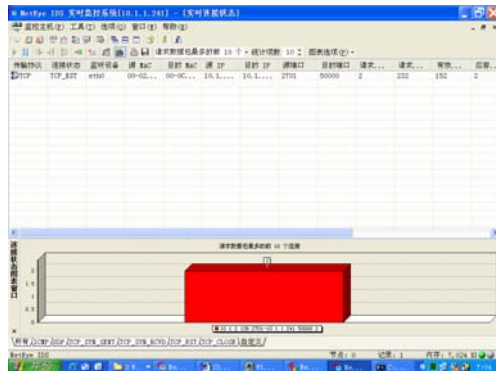
入侵检测与综合监控平台 — NetEye IDS

- 采用旁路侦听方式
- 提供实时流量分析和异常报警
- 对于入侵事件提供基于统计特征的报警机制（识别对骨干网有重大影响的大范围的攻击事件）
- 提供在海量目标中对少量重点目标的特别监控
- 对网络连接进行记录，为异常事件的分析提供审计的数据基础
- 报表工具


网络安全综合监控与审计平台

序	源 IP	传输协议	源 MAC	源 IP	源端口	目标 IP	目标端口	大小	时
1	10.1.1.80	TCP	00-0C-29-00-00-00	10.1.1.100	2002	10.1.1.100	2002	272	272
2	10.1.1.100	TCP	00-0C-29-00-00-00	10.1.1.100	2002	10.1.1.100	2002	272	272
3	10.1.1.100	TCP	00-0C-29-00-00-00	10.1.1.100	2002	10.1.1.100	2002	272	272
4	10.1.1.100	TCP	00-0C-29-00-00-00	10.1.1.100	2002	10.1.1.100	2002	272	272
5	10.1.1.100	TCP	00-0C-29-00-00-00	10.1.1.100	2002	10.1.1.100	2002	272	272

序	源 IP	传输协议	源 MAC	源 IP	源端口	目标 IP	目标端口	大小	时
1	10.1.1.113	TCP	00-0C-29-00-00-00	10.1.1.113	2002	10.1.1.113	2002	272	272
2	10.1.1.113	TCP	00-0C-29-00-00-00	10.1.1.113	2002	10.1.1.113	2002	272	272
3	10.1.1.113	TCP	00-0C-29-00-00-00	10.1.1.113	2002	10.1.1.113	2002	272	272
4	10.1.1.113	TCP	00-0C-29-00-00-00	10.1.1.113	2002	10.1.1.113	2002	272	272
5	10.1.1.113	TCP	00-0C-29-00-00-00	10.1.1.113	2002	10.1.1.113	2002	272	272



序	源 IP	传输协议	源 MAC	源 IP	源端口	目标 IP	目标端口	大小	时
1	10.1.1.100	TCP	00-0C-29-00-00-00	10.1.1.100	50000	10.1.1.100	2720	1024	1024
2	10.1.1.100	TCP	00-0C-29-00-00-00	10.1.1.100	50000	10.1.1.100	2720	1024	1024
3	10.1.1.100	TCP	00-0C-29-00-00-00	10.1.1.100	50000	10.1.1.100	2720	1024	1024
4	10.1.1.100	TCP	00-0C-29-00-00-00	10.1.1.100	50000	10.1.1.100	2720	1024	1024
5	10.1.1.100	TCP	00-0C-29-00-00-00	10.1.1.100	50000	10.1.1.100	2720	1024	1024



针对关键基础设施的应用级防火墙— NetEye Firewall

- 流过滤平台提供应用级保护基础
- 应用级保护插件，提供针对特定服务、特定攻击的保护
 - 使运营商在遇到针对服务协议的攻击时，不需要关闭服务端口，有效防御攻击
 - 提供对蠕虫、SQL注入等应用层攻击手段的防护



NetEye 防火墙的硬件革命

- 告别“工控机+软件”的方式
- 自主设计专用硬件系统
- 采用以网络处理器(NP)为核心的硬件架构
- 专用的嵌入式实时操作系统
- 从主板到上层软件全部自主知识产权
- 更高的性能、更好的可靠性



安全服务体系

- 位于北京的客户服务中心提供专业的网络安全服务
 - 客户信息资产调查和风险分析
 - 客户信息系统加固（包括必要的安全设施建设）
 - 网络安全体系规划和设计
 - 网络安全系统的实施和维护
 - 客户应急处理预案的制定
 - 客户关键人员培训



东软的应急事件处理联合体系

- 联合体系是客户与东软共同构成的处理安全危机事件的运作体系
 - 客户信息系统的评估与加固
 - 制定应急处理预案
 - 培训相关人员
 - 东软NCSIRT小组定期提供安全威胁预警
 - NCSIRT呼叫中心提供电话支持
 - NCSIRT现场救援小组



培训客户

- 培训可以提高电信运营商规划安全、维护系统、处理事件的能力
- 培训可以提高电信运营商对服务和产品供应商的鉴别能力

- 以CIW为基础的网络安全课程
- 以实际动手进行攻防演练的高级安全工程师课程



构建有效防御体系的几个建议

- 努力提高电信运营商自身的安全能力
 - 整体的安全规划（组织、策略、流程）
 - 基本的安全技能
 - 事件协同处理能力
- 选择更新及时的安全防御和检测部件
- 必须具备较强的审计能力
 - 主动安全审计
 - 事后审计
- 寻找可靠的外援力量



客户应该为安全事件的发生做好准备

- 发生网络安全事件，是迟早的问题
- 一切网络安全的投资的效果都在事件发生的那一刻表现出来



谢谢！

<http://neteye.neusoft.com>