



X'CON 2003

智能分布式攻击与防御

作者: tone

日期: 2003-12

# 智能分布式攻击与防御

Tone

2003.12.23

Copyright © Tone 2003



X'CON 2003

# 主要内容

- 目前分布式攻击介绍

- ∅ 类型

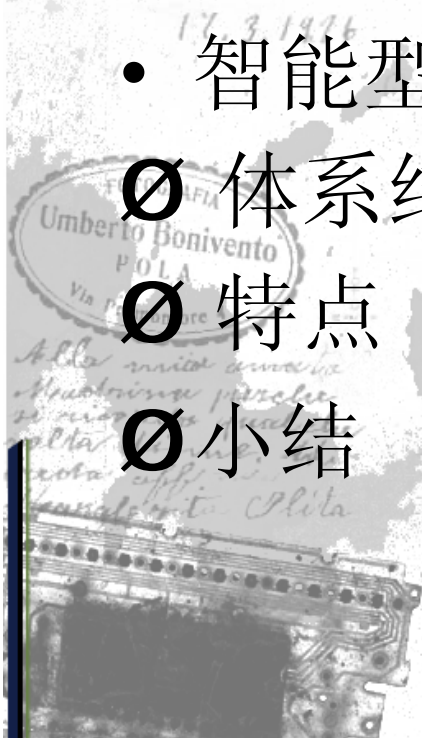
- ∅ 缺点

- 智能型分布式攻击

- ∅ 体系结构

- ∅ 特点

- ∅ 小结



POST CARD  
CANTON  
STUDIO FOTOGRAFICO  
DANTE MORONI  
Via S. ... N. 16  
TORINO



# 主要内容

- 智能型分布式防御

- Ø 体系结构

- Ø 异常行为判定

- Ø 特点

- Ø 实现关键



Atta mia amata  
Maurina perché  
si ricorda qualche  
volta di me. Ah  
nota aff.  
Umberto Plita

Mamma  
Contessa Plenta  
voglio abbracci.



# 目前分布式攻击类型

- 弱C/S模式型

客户端通过Ftp、Web、Mail等方式和控制端联系。

- 强C/S模式型

Tfn、Tfn2K、Trinoo。

# 目前分布式攻击类型

- 随机扩散型

SQL Slammer、冲击波病毒等

- 弱C/S模式型+随机扩散型

在具备弱C/S模型的基础上，自身具备传播机制，增加了一定程度的随机扩散的功能。

# 目前分布式攻击缺点

- 可控性差  
随机扩散型
- 传播机制单一  
被动传播、主动传播，传播条件受限
- 隐藏性差  
可使用第三方工具如Regmon、Filemon、Fport等发现并清除

# 智能型分布式攻击

Ø 体系结构

Ø 特点

Ø 小结

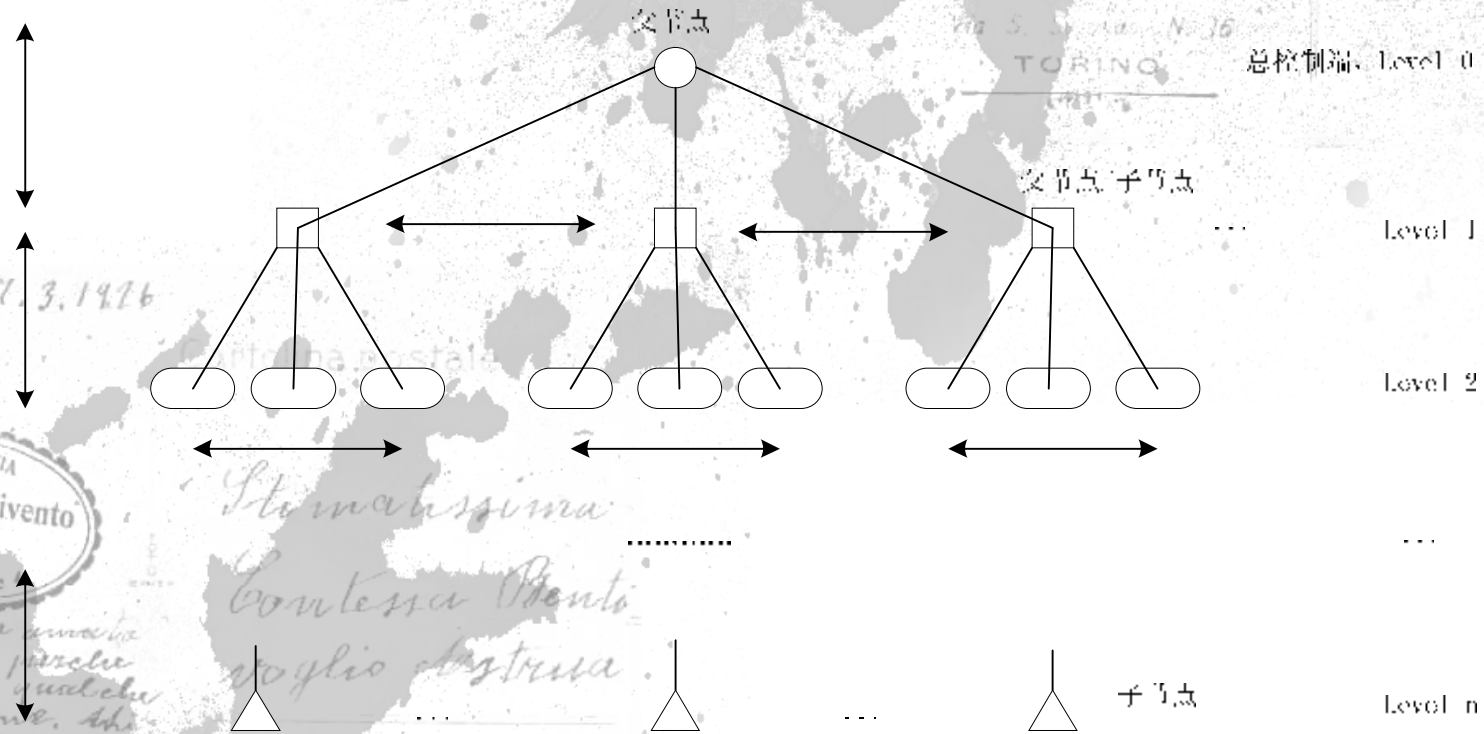


17.3.1976  
Cartolina postale  
Stimabilissima  
Contessa Otonio  
voglio abbracciarti.  
Alla mia amica  
Maurina perché  
si ricorda qualche  
volta di me. Ah  
nota affettuosi  
baciamenti. Plita





# 智能分布式攻击体系结构



注：双箭头线是指节点之间控制信息或数据的交互。

# 智能型分布式攻击特点

- 可控性强
- 隐蔽性强
- 可更新性
- 智能性
- 通信安全保密性



17.3.1976  
Alta di me. Ah  
nota aff. Piola



Contessa Obento  
voglio strizza.

POST CARD  
STUDIO FOTOGRAFICO  
DANTE MORONI  
Via S. ... N. 16  
TORINO

# 可控性

- 传播可控性

总控制端可以控制传播的范围、层次、传播目标等参数。

- 攻击可控性

可以控制攻击的开始时间、停止时间、攻击类型、攻击目标范围、攻击目标特征和攻击进行地层次等参数。

- 攻击效果可知性

客户端及时返回攻击效果至上层，并逐层传递。

# 隐蔽性

- Linux基于用户空间隐藏  
名字欺骗、文件替换

- Windows基于用户空间隐藏

- ∅ 改变文件属性，名字欺骗

相当一部分病毒，木马采用该手段，  
仍具备较大的迷惑性

- ∅ 基于用户空间的API Hook

# 基于用户空间的API Hook

- 文件隐藏  
替换Kernel32.dll中的CreateFileA/W、DeleteFileA/W、FindFirstFileA/W、FindNextFileA/W等函数。
- 注册表隐藏  
替换Advapi32.dll中的RegOpenKeyExA/W、RegEnumValueA/W、RegEnumKeyExA/W、RegQueryInfoKeyA/W等函数。
- 进程隐藏  
替换ntdll.dll中的ZwQuerySystemInformation函数。

# 隐蔽性

- Linux基于内核空间的隐藏  
LKM；注意自身的隐藏；避免输出符号
- Windows基于内核空间的隐藏  
ntrootkit，修改服务描述表  
进一步研究
- 内核空间隐藏和用户空间隐藏相结合

# 可更新性

- 主动更新

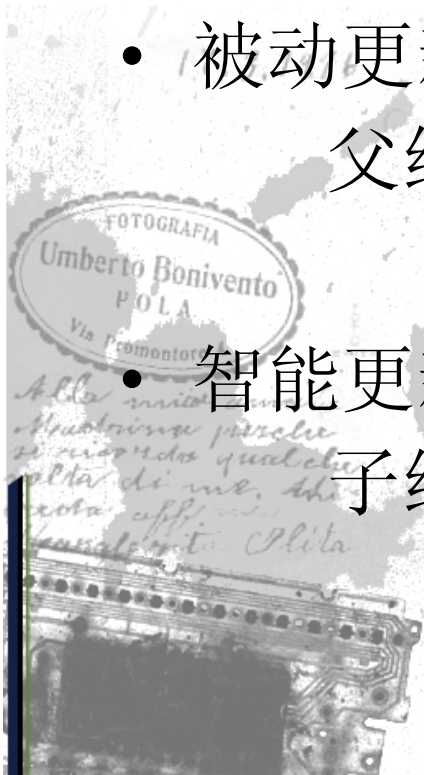
子结点发送更新请求至父结点或者同层结点

- 被动更新

父结点强制更新子结点，并依次向下更新

- 智能更新

子结点通过自学习进行更新



# 智能性

- 传播智能性

根据不同的传播环境选择不同的传播方式

- 攻击智能性

同层结点或子父结点互相协调，生成最佳攻击方式

- 未来移动设备智能性

手机、PDA、3G、家电、汽车等终端



# 智能型分布式攻击特点

- 通信安全保密性

通信过程安全、保密；具有较好的隐蔽性，可采用数字水印的思想

- 小结

- 过程

理想结果：可智能完成一体化的攻击



# 智能型分布式防御

- Ø 体系结构
- Ø 异常行为判定
- Ø 特点
- Ø 实现关键

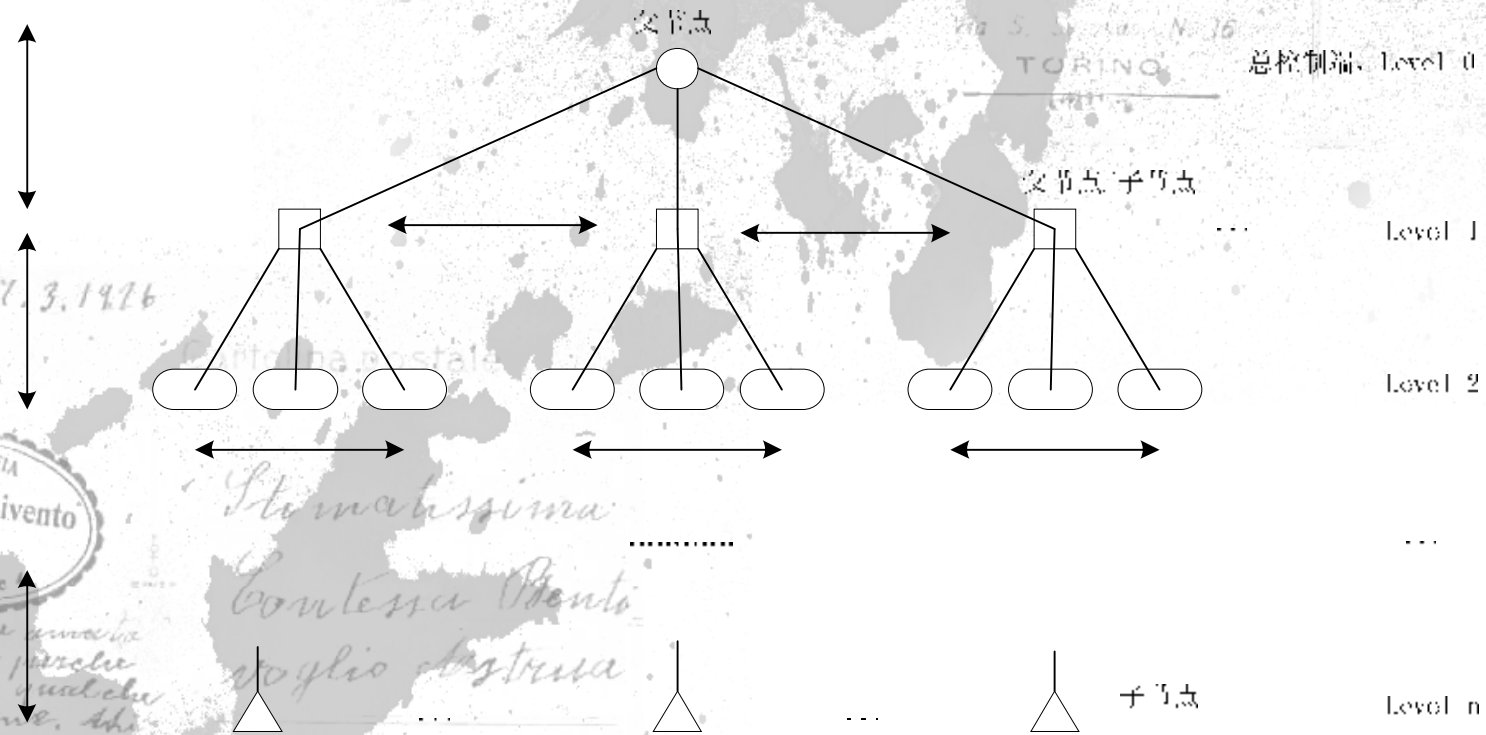
17.3.1976  
Cartolina postale  
Umberto Bonivento  
PIOLA  
Via Piemontese 4

Alle mie amiche  
Maurina perché  
si ricorda qualche  
volta di me. Ah  
nota affettuosa  
Margherita Piola

Maurina  
Contessa Orenti  
voglio abbracciarti.



# 智能型分布式防御体系结构



注：双箭头线是指节点之间控制信息或数据的交互。

# 异常行为判定

- 异常网络行为判定  
数据包特征值匹配和攻击模式匹配结合
- 异常主机行为判定  
挖掘主机特征，正常行为模式  
特征匹配和异常主机行为匹配相协调
- 异常“网络+主机”行为判定  
提高准确度

# 智能型分布式防御特点

- 尽量在底层解决问题

无法处理时，逐级上传至父节点进行处理；处理完毕后子节点更新处理方式并反馈处理结果

- 可控性

父节点可指定子节点的处理方式及添加、删除等

# 智能型分布式防御特点

- 智能性
  - ∅ 能够学习本机正常行为，自动进行正常行为建模。
  - ∅ 对异常的行为具有学习记忆功能。
  - ∅ 可根据父节点反馈的信息智能更新异常行为判定模式。
  - ∅ 针对攻击的协同防御。

- 可更新性

同智能型分布式攻击

# 实现关键

- 高效可靠的检测算法
- ∅ 计算机免疫技术
- ∅ 神经网络技术
- ∅ 遗传算法
- ∅ 综合应用数据挖掘、模型推理、关联技术、人工智能等技术
- 可移动代理技术
- 各节点智能迁移



STUDIO FOTOGRAFICO  
DANTE MORONI  
Via S. ... N. 16  
TORINO

POST CARD



Thanks !

POST CARD

DATE

Cartolina postale



STUDIO FOTOGRAFICO  
DANTE MORONI  
Via S. Spirito, N. 36  
TORINO

17.3.1926

Cartolina postale



Stimabatissima  
Contessa Oberto  
voglio abbracciarti

Alle mie amiche  
Maurina e Paola  
se ricordo qualche  
volta di me. Ah  
non affrettarsi  
lasciatevi Plita



X'CON 2003