

# 恶意代码来源定位

Hui ZHENG

Network Research Center, Tsinghua Univ.  
CERNET Computer Emergency Response Team  
zhenghui@ccert.edu.cn

# 实例

## ■ 红色代码

- 据美国国会超党派调查机构审计局(GAO, General Accounting Office)称, 电脑病毒“代号红色”(Code Red)可能诞生于中国南部广东省一所大学。据估计, 该病毒上个月所耗费的扫毒费用可能高达24亿美元。
- 佛山大学否认是“红色代码”的源头,  
<http://www.zaobao.com/special/newspapers/2001/09/dayoo010901.html>
- “红色代号”病毒编写者来自广东佛山大学?  
<http://duba.dta.net.cn/c/2001/0806/3027.htm>

## ■ 震荡波

- 德国, 18岁少年

# 网络相关信息分析

- 作者自述
- 发现（上报）时间、发现（上报）区域
- 研究人员分析

# 文件自含信息分析

- 恶意代码样本反向工程

# 传播链反溯

- 中断补偿
- 多路追溯

# 目标选择流程分析

- 其他版本300线程； 中文版本 600线程；
- 日文版本无操作，其他版本下载补丁；

# 代码比对技术

- 行为比对
- 结构相似度比对

# 地理信息辅助系统

# 时间分析法

- 对比被感染主机上病毒文件创建时间，较早者接近攻击源；

# 空间分析法

- 多点检测
- 单点检测

# 攻击目标锁定

# Mytob

- <http://www.ando.net.cn/andocd/ando-chengdu/news/2005.11.07.htm>
- 2005年八月底在摩洛哥和土耳其拘捕了两个年轻人

# SASSER蠕虫（震荡波）

- Sven Jaschan，德国人，18岁
- 2004年5月7日抓住
- Netsky同一作者

# AgoBot

- Agobot was written by Ago alias Wonk, a young German man who was arrested in May 2004 for computer crime.

# 黑客贴图分析

- 操作系统类别、版本
- 控制软件类别、版本（中文？）
- 系统时间（黑客活动时间）
- 控制的规模
- 客户端昵称特征（命名规则，随机）
- 客户端加入的频度
- 管理员名称、聊天室名称的关联度

# References

- [http://www.icst.pku.edu.cn/honeynetweb/honeynetcn/KnowYourEnemy/Know%20your%20Enemy%20Tracking%20Botnets\\_EC.htm](http://www.icst.pku.edu.cn/honeynetweb/honeynetcn/KnowYourEnemy/Know%20your%20Enemy%20Tracking%20Botnets_EC.htm)