XFOCUS TEAM
from internet,for internet

# Active Defense System to Contain Internet Worm

Hui ZHENG
CERNET Computer Emergency Response Team
Zhenghui_at_ccert.edu.cn

X'CON 2004

# Contents

- Introduction
- Contain susceptible machines
- Contain infected machines
- Contain propagation path
- Architecture design and implementation
- Experiment with campus network

# Introduction

- Prevention phase
- Detection phase
- Containment phase
- Elimination phase
- Objects involved in worm defense process
- Related Work

# Objects involved in worm defense process

- infected machines，I(t)
- susceptible machines，S(t)
- worm spreading traffic，β
- a decrease in the number of any object will slow the speed of Internet worm propagation.

$$dI(t)/dt = bI(t)S(t)$$

# Contain susceptible machines

- Vaccination
- Definition of the vaccine of Internet worm
- Rules to choose an Internet worm vaccine
- Process of vaccination
  - Construct susceptible machines list
  - Take advantage of exploits
  - Embed vaccine
  - Execute vaccination

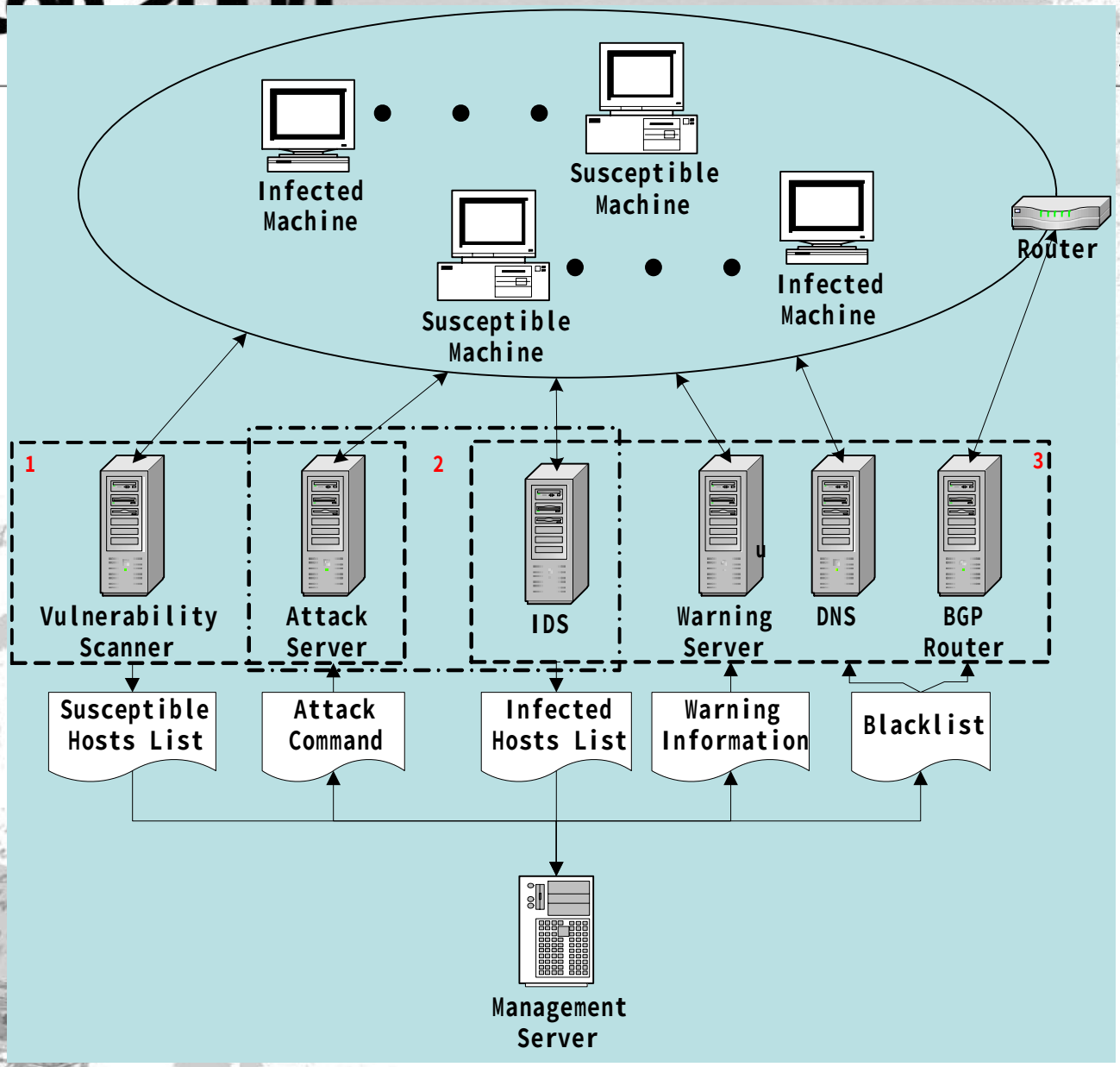
# Contain infected machines

- Forcing shutdown
- Through the vulnerability used by worm
- Through the vulnerability of worm
- Through the back door
- Common shutdown shellcode

# Contain infected machines traffic

- Bidirectional leading
- DNS hijacking for egress traffic
  - View configuration
  - Port forward
- Null Routing for ingress traffic
- Warning information to end users

# Architecture design and ntation



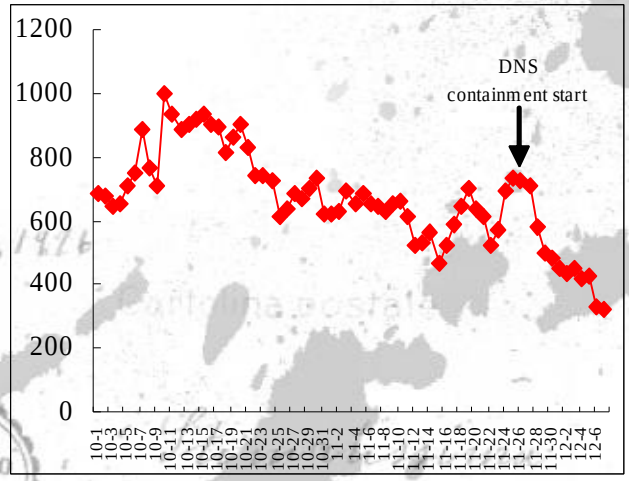
# Architecture design and implementation

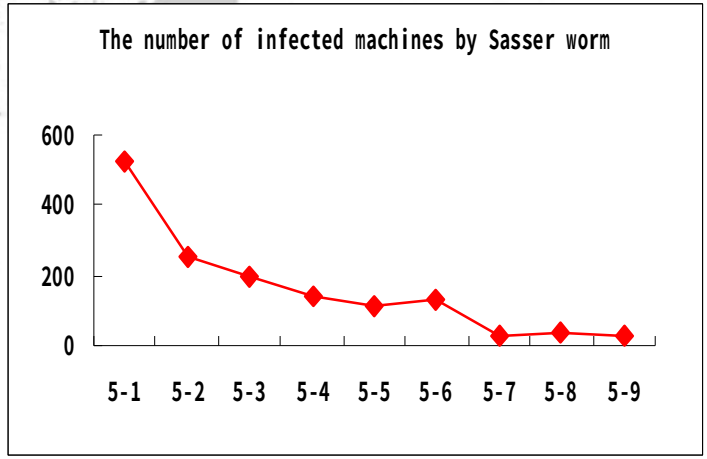
- Susceptible machine automated containment system
  - Components: vulnerabilities scanner and attack server;
  - Process
- Infected machine automated containment system
  - Components: IDS, scanner and attack server
  - Process
- Infected machines traffic automated containment system
  - Components: IDS, DNS, BGP router and warning server;
  - Process
- Systems integration
  - management server;

# Experiment with campus network of Tsinghua University

- Campus network
- Effect of partial automated containment system
  - Nachi worm
  - Sasser worm

# Figures of cases




# Discussion

- from the point of view of technologies and few legitimate problems are concerned;
- false positive of anti-virus software;
- forcing susceptible machines to be shut down;
- not protect the machines directly selected with IP address;
- defense system can be extended to contain varieties mobile malicious codes even spam mails.

# Appendix.

- I. Vaccine and shellcode for Nachi worm:
- II. Common shutdown shellcode

# References


- Eugene H. Spafford. The Internet Worm: Crisis and aftermath. CACM, June 1989, vol 32, number 6.
- Steve White, Open Problems in Computer Virus Research. Presented at Virus Bulletin Conference, Munich, Germany, October 1998. http://www.research.ibm.com/antivirus/SciPapers/White/Problems/Problems.html
- David Moore, Colleen Shannon, Geoffrey Voelker and Stefan Savage, Internet Quarantine: Requirements for Containing Self-Propagating Code. Proceedings of the 2003 IEEE Infocom Conference, San Francisco, CA, April 2003.
- Zesheng Chen, Lixin Gao, Kevin Kwiat. Modeling the Spread of Active Worms. IEEE INFOCOM, 2003.
- J. Wu, S. Vangala, L. Gao, and K. Kwiat. An Effective Architecture and Algorithm for Detecting Worms with Various Scan Techniques. Network and Distributed System Security Symposium 2004.
- Cliff Changchun Zou, Weibo Gong, Don Towsley. Worm propagation modeling and analysis under dynamic quarantine defense. ACM CCS Workshop on Rapid Malcode (WORM'03), Oct. 27, Washington DC, USA, 2003.
- Hui Zheng. Internet worm research. Ph.D. Dissertation, Nankai University at Tianjin City, China, 2003 (in Chinese). http://worm.ccert.edu.cn/doc/InternetWormResearch.pdf
- Nachi worm writer. Explanations on Nachi worm programming (in Chinese). https://www.xfocus.net/bbs/index.php?act=SE&f=1&t=26924&p=87845
- Rolf Rolles. Recode from disassembly of the Win32 DCOM worm. http://archives.neohapsis.com/archives/vuln-dev/2003-q3/att-0086/RPC_DCOM_recode_and_analysis.TXT
- Microsoft. Microsoft security bulletin MS03-026, Buffer overrun in RPC interface could allow code execution. http://www.microsoft.com/technet/security/bulletin/MS03-026.asp
- flashsky. Analysis of LSD RPC buffer overflow (in Chinese). http://bbs.nsfocus.net/index.php?act=ST&f=3&t=147160&page=all#entry188617
- mandragore. Sasser Worm ftpd Remote Buffer Overflow Exploit. http://www.k-otik.com/exploits/05102004.sasserftpd.c.php
- Austin Kasarda. The Lion Worm: King of the Jungle? http://www.giac.org/practical/gsec/Austin_Kasarda_GSEC.pdf