Lessons from Malware

Radu State
Ph.D.

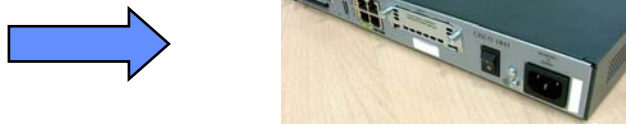
MADYNES

The MADYNES Research Team
LORIA – INRIA Lorraine
615, rue du Jardin Botanique
54602 Villers-lès-Nancy
France
Radu.State@loria.fr

Outline

- Major problems in network management
- What did we do wrong in network management ?
- Lessons from malware
  - Scalability
  - Security
  - Self organized middleware

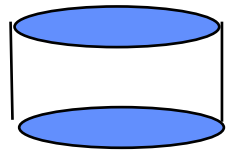
Netwok management at a glance



Manager connects to devices to perform operations

- **Standard management protocol**
- **Common information model (MIB) needed**

Managing more than just simple devices



Database services

Application services

Voice Services

Complex services need management for both software and network configuration

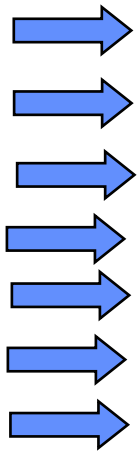
Management costs rank up to 90% of the total cost

Web server supporting business critical process services

Major challenges in network management

Residential with

- **service boxes @home**
- **VoIP devices (ATA devices, PBX)**
- **TV boxes (FreeBox, LiveBox, etc)**
- **OSGI boxes**

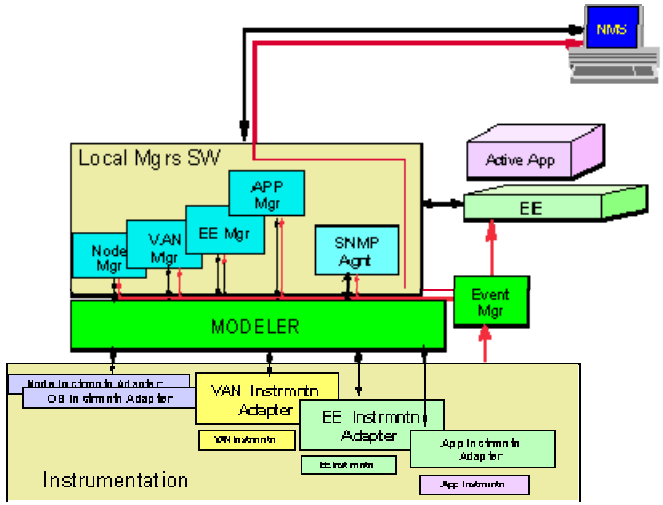


Today's questions :

Q) Can we manage millions of devices ?
A) Nope
Q) Is the management plane both secure and flexible ?
A) Nope
Q) Will we do it tomorrow ?
A) Maybe, but we have do it differently

Some great ideas in network management –flexibility

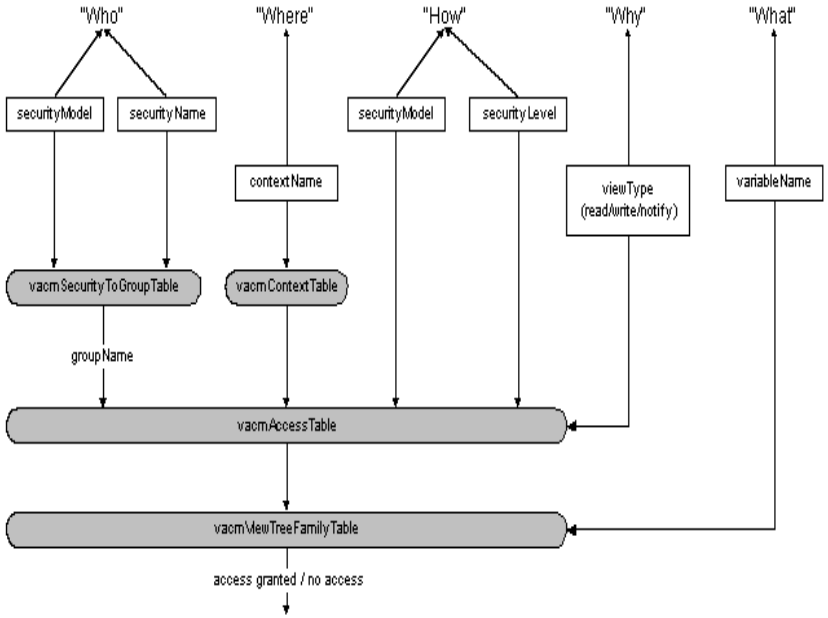
- Active Networking
  - Code is dynamically deployed over an network/service infrastructure
  - On the fly service creation and instantiation
  - Hundreds of research papers and special issues in journals
- We have never seen a real operational platform !



Source :
www.cs.columbia.edu/dcc/anm/anetmgmt.htm

Some great ideas in network management - security

- SNMP and security
  - SNMP v1 and v2 no security :
  - V3 has a very complex access control and very few use it
- CLI (CISCO)
  - multilevel access control
  - in practice we use only the most and the least privileged



Simple Network Management Protocol =Security is Not My Problem

Some great ideas in network management -middleware

- Middleware for network management
  - Self-managed middleware and all hot buzz words…
  - Component based middleware
  - Peer to Peer based network management
  - Autonomic management

- Very few notable real operational systems !!
  - JMX and a proprietary (and out of usage) Bull middleware are the only exceptions

CNN Friday, November 4, 2005. 6:26pm

Botmaster' arrested over computer spam network

US authorities have arrested a man for allegedly hijacking thousands of computers to launch spam attacks…..

Among the computers that Jeanson Ancheta, 20, is accused of infecting with malicious software are computers at the Weapons Division of the sensitive US Naval Air Warfare Centre in China Lake in California.

The US Attorney's office alleges that Ancheta, who lives in the Los Angeles, is a "botmaster" who controlled "botnets", which are armies of computers hooked up to the Internet.

Ancheta allegedly wrote and spread a malicious code, which caused the computers to become part of the bot network without the knowledge or consent of their owners.

Ancheta allegedly advertised the sale of his botnets for spam purposes - thereby illegally profiting from his crime - or for launching denial-of-service attacks.

After receiving payment from customers, Ancheta would allegedly give customers control of enough botnets to accomplish their specified task, along with an instruction manual.

He is also accused of allowing advertising software to be downloaded onto the infected computers that were part of his botnet armies.

In all, he allegedly made about $US60,000 ($A81,000) in advertising affiliate proceeds by causing the installation of adware on about 400,000 computers.

If convicted of all the charges in the indictment, Ancheta faces up to 50 years in prison.

Food for thought

1. **Can we manage 400 000 devices with one manager ?**
   NO
2. **Can we allow flexible third party partial control (customer network management) over a network infrastructure ?**
   NO

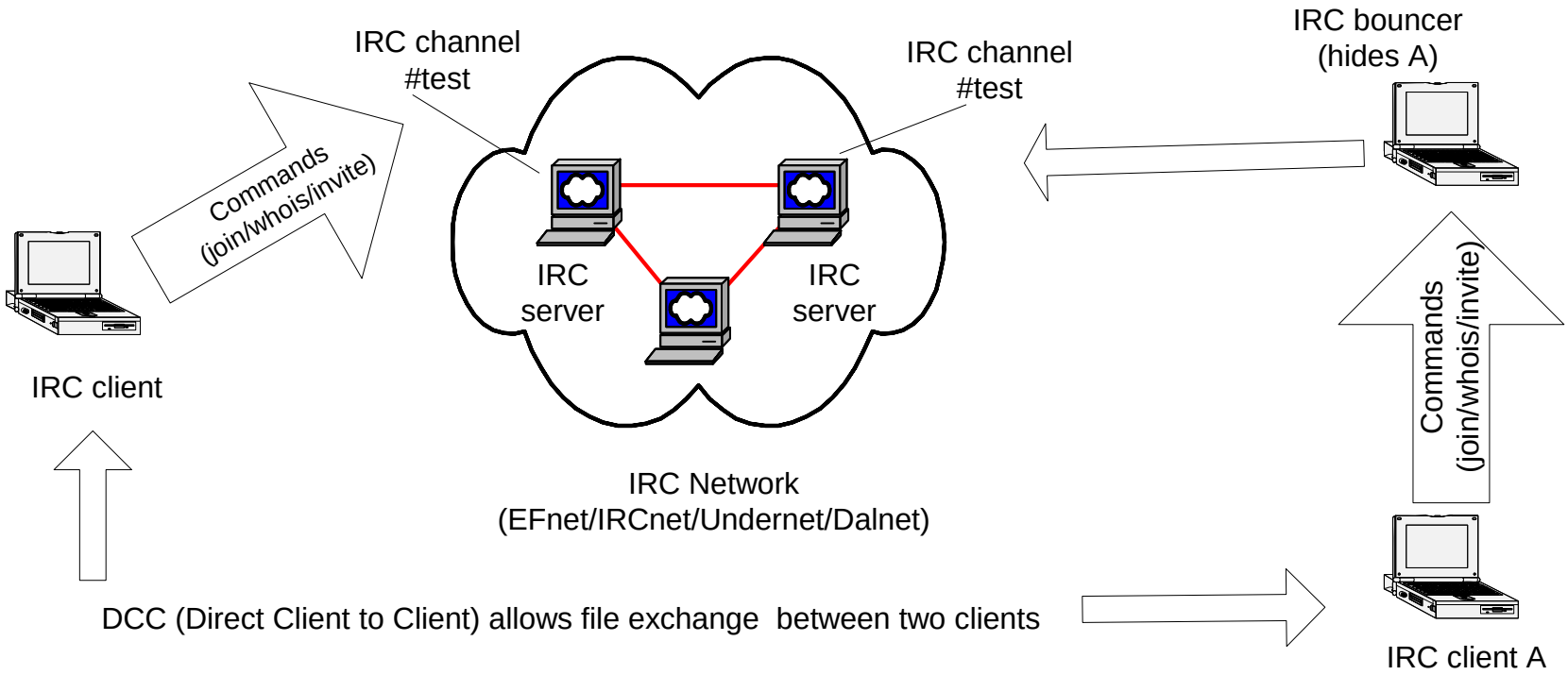
3. **Can we make more money (50000 Euros) with Network Management ?**
   YES !

« HP OpenView Compliance Manager will be available this September. HP said price has not been finalized, but will tentatively start at $250,000.
HP OpenView SOA Manager costs$10,000 per agent, $22,000 per broker, with the services platform starting at $25,000 »
source: Hewlett-Packard beefs up OpenView portfolio
By Colleen Frye, News Writer
06 Jun 2005 | SearchWebServices.com

What should we learn from Malware ?

- Flexible Middleware
- Advanced and secured updates
- Deployment speed
- Ubiquitous System management with rootkits and flexible comand support
- Code quality – sometimes even open source

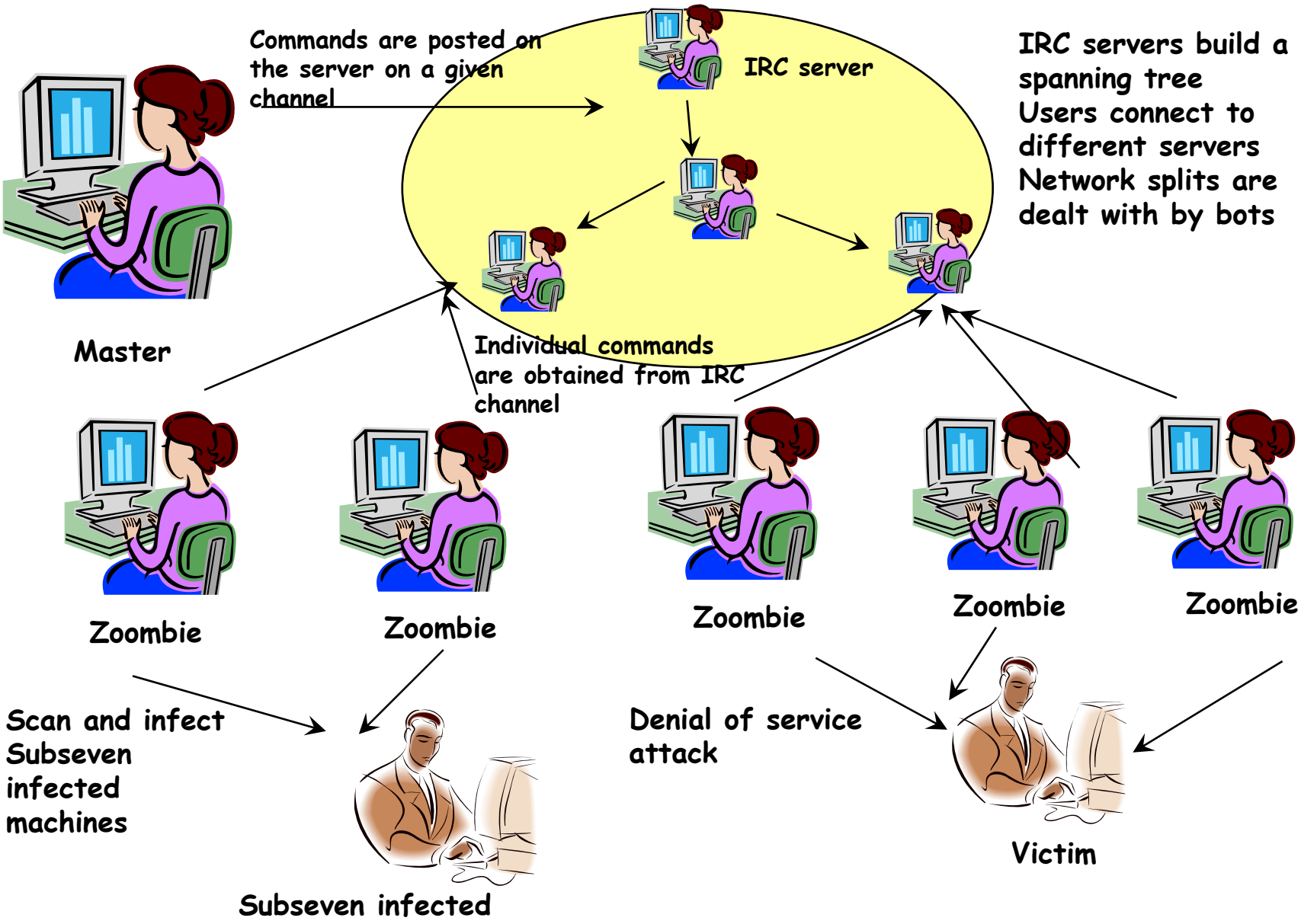
IRC communication



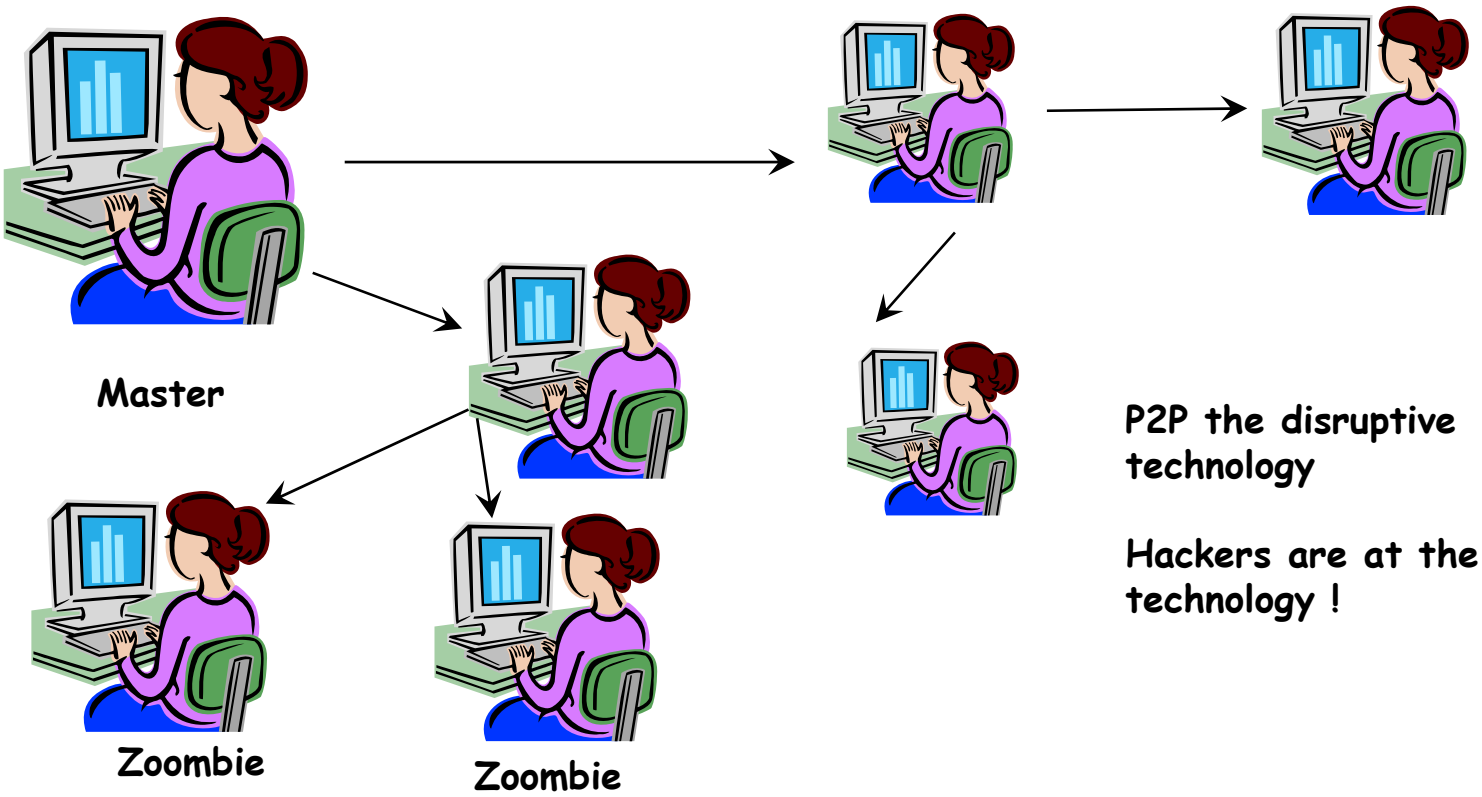
Reliable Chat Network

- Channels regroup similar multiple clients interested in the same topic/communication
- Each channel is available on all servers
- High Fault-tolerant : deals with network partition/crashes
- IRC bouncer (proxy) assures privacy and maintenance of open channels
- Scripted/compiled automatic commands (Bots)

Worms signalling on IRC W32/Tendoolf



P2P the new communication paradigm: Linux/Slapper

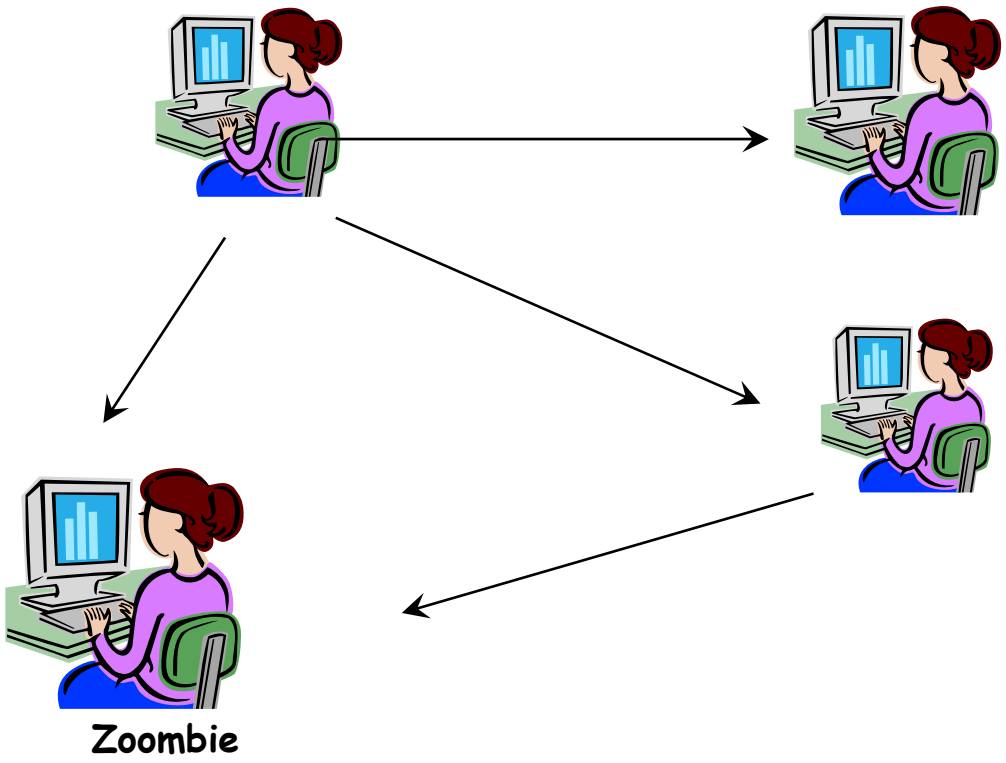


P2P the disruptive technology

Hackers are at the edge of technology !

P2P overlay network and communication protocol
An infected node, will obtain the IP address of it's infector as well as other IP addresses for other infected node
When new IP address information is obtained, a random subset of peers is selected to which this information is broadcasted

Linux/Slapper –message processing



Each message has an ID

Each node keeps track of last 128 generated IDs and 128 received IDs.

Each sent message is associated with

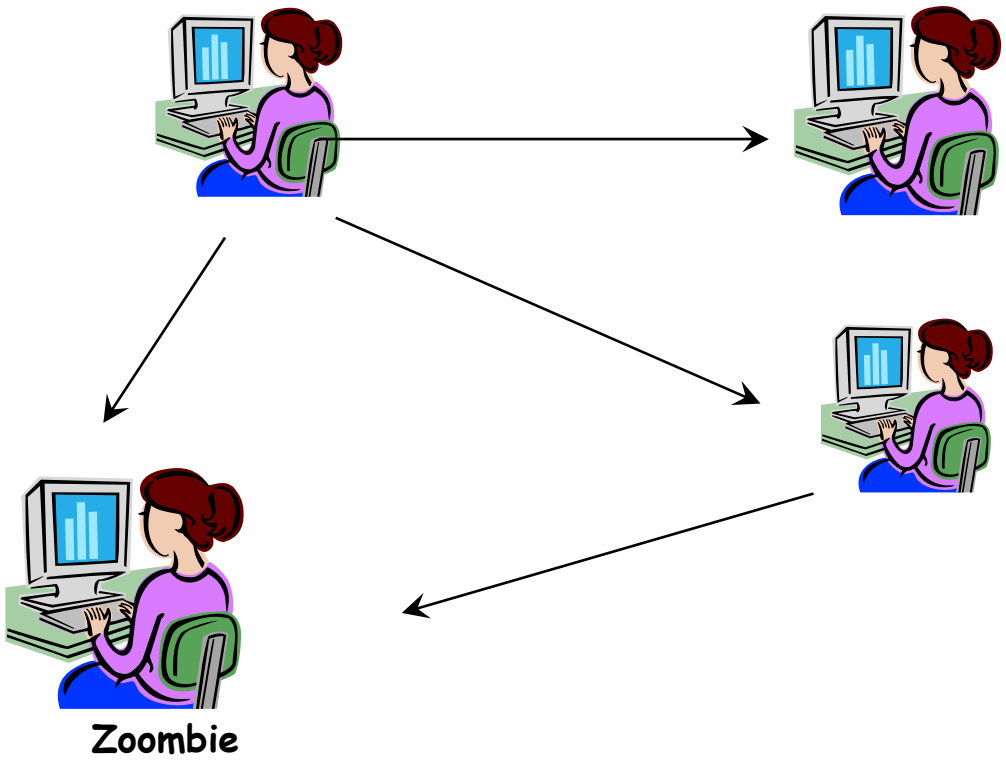
1) Time of emission
2) Destination IP's (up to 20)
3) Number of nodes to send to
4) Destination ports
5) TTL

Messages are sent to randomly generated infected nodes or to a specific node IP

A message is routed by a node only if ID is different from the stored ID's

A message will not be retransmitted if acknowledgment is received or a timeout is expired

Linux/Slapper –Routing and synchronisation

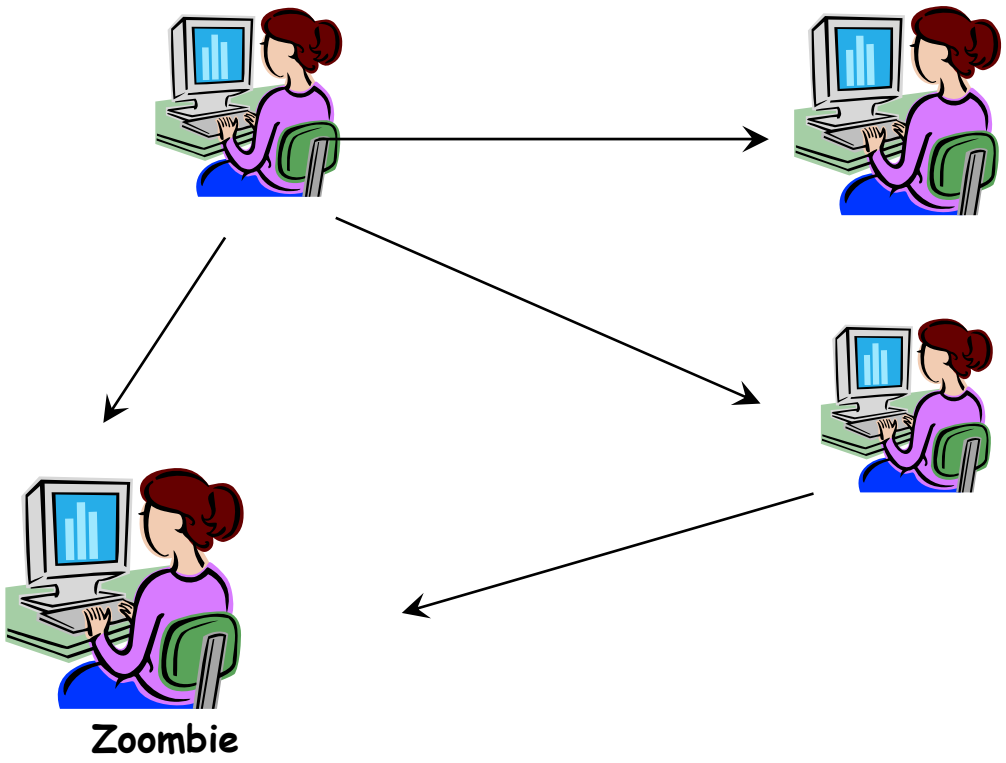


Replies can be send to the source IP address if message request was not routed

Via a return path, if message was routed: each node maintains a return path routing table

Worm network keeps track of infected machines. Every 10 minutes a global synchronization is perfomed.

Linux/Slapper –initialization



Each new infected node receives a list of already infected IP addresses

A new infected node will join the P2P network

If joining is not possible, a new P2P nework will be spawned

A message can be sent
- directly to a node by using the node's IP address
- routed over the P2P network, where IP address is encapsulated in a route command.

Anonymity is achieved by probabilisitic routing

·Broadcasts are also possible : a received message is sent to 2 nodes selected at rnadom

Secure software upgrades (W95/Hybris)

Attacker

Attacker
1 private key to sign
1 public key distributed in the worm body
1 symmetric key computed from the worm body

New modules are sent to the server
Module is encrypted with a secret key
Update is signed with a private key (RSA)

News server
Hosts mailing lists
Worm modules are posted as messages

Downloads new modules

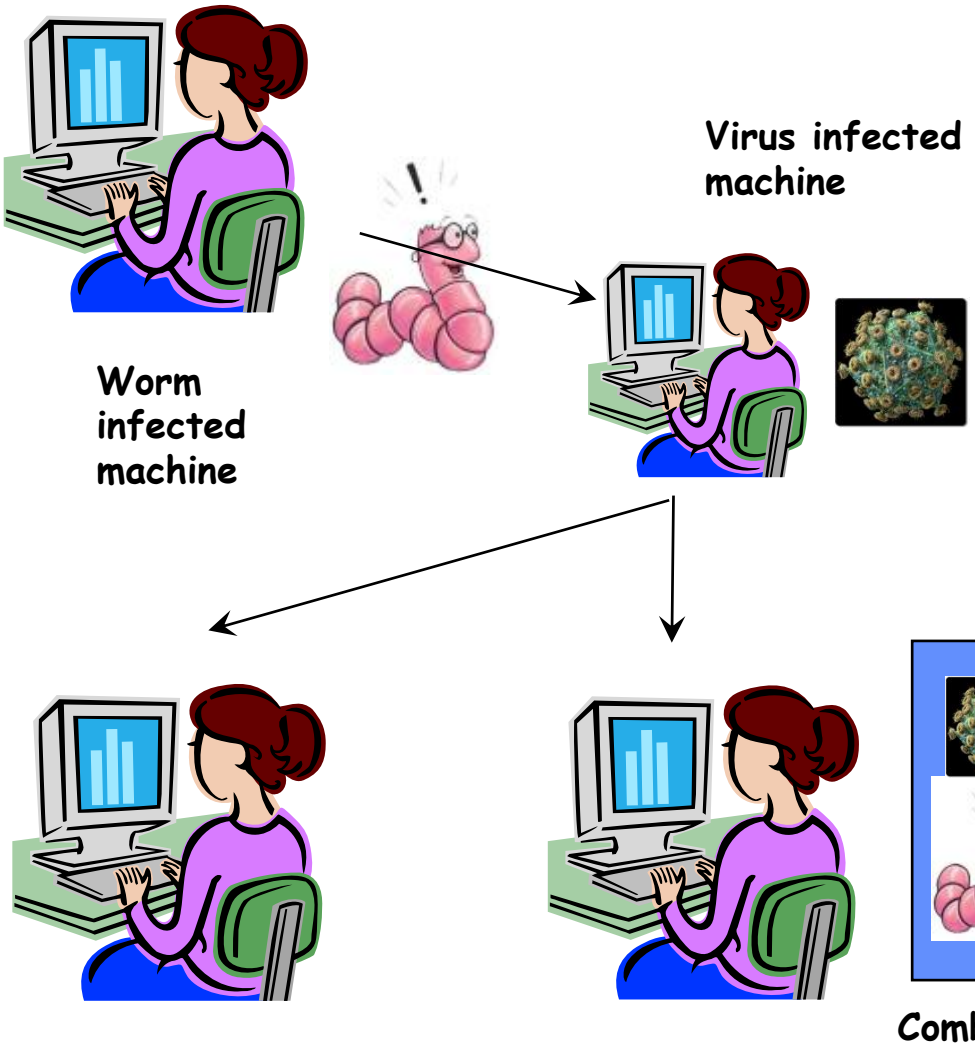
Muliple infection modules

Infected machine
Signature is checked wih public key
Contents is decrypted with secret key

Interesting facts
World wide contribution (France, Spain,Russia)
Public domain crypto (XTEA succesor of TEA/ cracked XBOX)

Modules examples (32)
- PE infection module
- Subseven infector
- Additional crypto modules
- Antivirus site blocker
- Antivirus attacker
- WORD infector

Mutant worms – Artificial Life at work



Worm+Virus = Mutant WORM/Virus

Precondition: Worm uses Virus infected files

Real world:

Worm: W32/Cholera
Virus: W32/CTX

Author: GriYo….

Dynamic reconfiguration :The Antiworm

Worm infected machine

Anti Worm infected machine

Real world:

Worm: CodeREd
Antiworm: CodeGreen
Antiworm removes worm and patches machine.

Ethical worm ? The author of CodeGreen went to jail

Real world:

Worm: Sasser
Antiworms: Gaobot.AJS and Dabber

Sasser has a buffer overflow vulnerability in a crude ftp server. Dabber exploits this vulnerability and kills Sasser.

Gaobot.AJS competes with Sasser for the same (LSASS vulnerability). Gaobot modifies Sasser such that Gaobot code is uploaded on new infected machine

Flexible Middleware (Happy 99 worm)

Mary sends an email to Bob

Infected Machine

Worm intercepts the message and adds itself as attached file

Worm is installed on Bob's machine
WSOCK32.DLL is patched and new implementations are added for the « « connect » and « send » API

Bob receives email and executes attached file

Victim Machine

Use already existing backdoors

Machine infected by BWORM

Machine with Back Orifice
Listens on UDP port 31337

BO_PING (port 31337)

BO_PING reply

BO_HTTP_ENABLE

Back Orifice opens HTTP on port 12345

Worm uploades itself
Encoded « borm.exe »

Worm requests the execution of borm.exe
Back Orifice command BO_PROCESS_SPAWN

Worm takes over the machine

Chatting can be dangerous

Machine with MSN
Or connected on the
IRC

Machine infected by W32/Choke
Sends itself attached as a game

BO_PING (port 31337)

Worm is sent to MSN client

IRC server

User is asked to accept download
Many IRC clients accept automatic
download
Especially those using FSERVE

Flexible middleware (W32/TariPox)

Worm listens on port 25

Every message is added with a little worm ☺

Outgoing Email before infection

After Infection

B is Default SMTP server
(for outgoing mail)

1) Worm modifies the SYSTEM32\DRIVERS\ETC\HOSTS file and SMTP server address is remapped to localhost
2) Every outgoing email is infected and next relayed to the legitimate SMTP server

Bring your own SMTP agent (Klez, Mydoom, Sobig, Nimda)

Alice is infected

Bob will be infected…

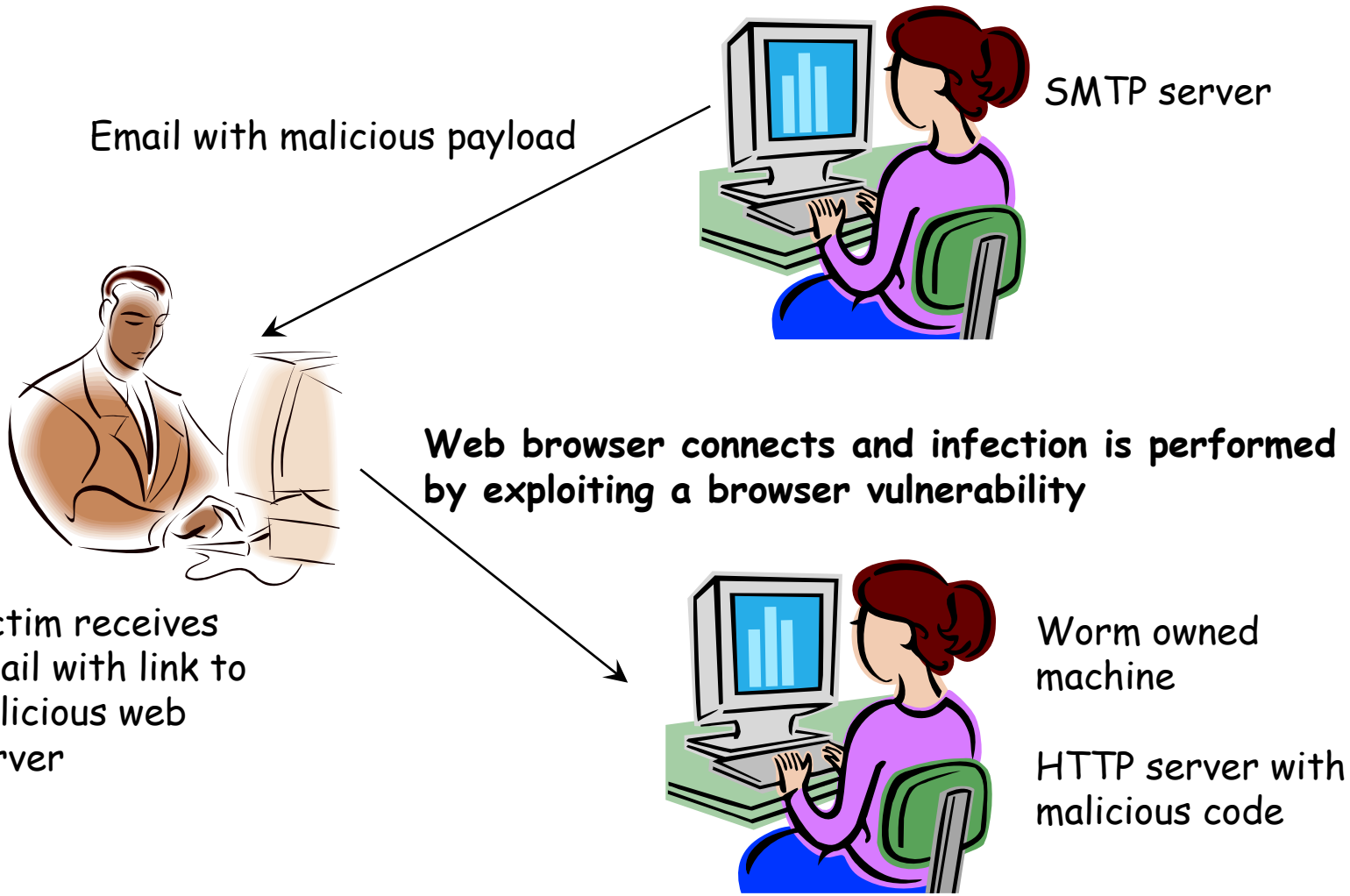
Love letter from Alice
Signed : the worm

DNS requests for MX entries

I've got a big list of email addresses,
I want to send myself to Bob : bob@loria.fr
Problem: where is Bob's email server ?

DNS server for the loria.fr domain

Multiplatform support (W32/Beagle, W32/Aplore)



Key idea: even message scanning by antivirus software on the server will not detect it

Deployment speed : Slammer and Code Red

Source: The Spread of the Sapphire/Slammer Worm

http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

Doom day: 05:30 UTC on Saturday, January 25, 2003.

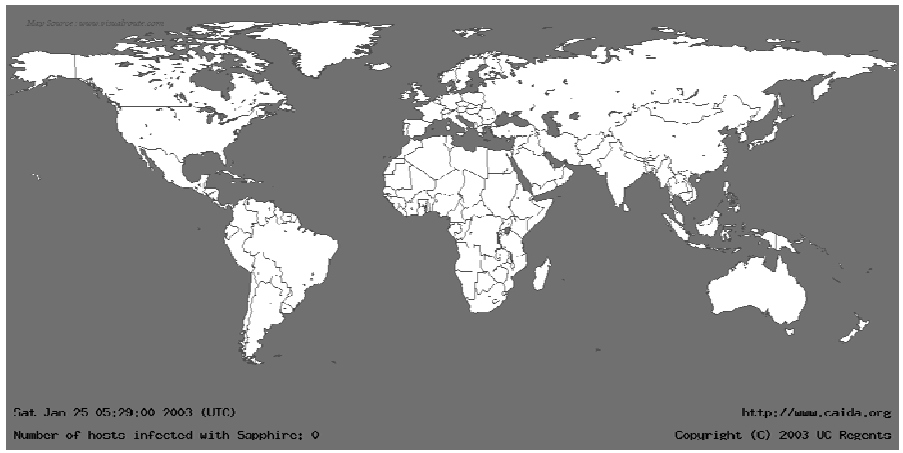
Infected population doubles every 9 seconds

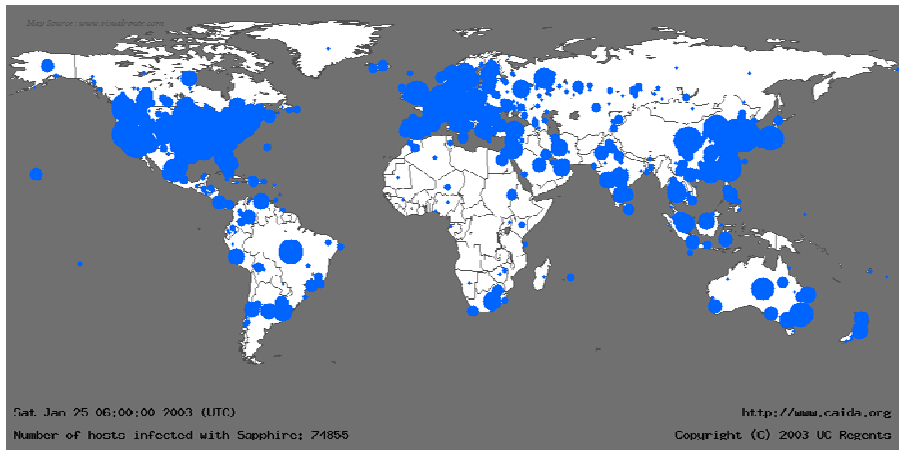
55 million scans/second after 3 minutes

Most (90%) vulnerable machines were infected after 10 minutes

More than 75000 infected machines

Code Red (July 19, 2001) infected 359000 hosts





Conclusions

- Many lessons can be learnt from malware
  - Scalability
  - Rapid deployment
  - Security
  - Flexible Configuration support (rootkits/bots)
- Blackhats are sometimes more advanced than academic research
- Current work on making a better management plane with these concepts