A strategy for Inexpensive Automated Containment of Infected or Vulnerable Systems

Steven Sim Kok Leong
Assistant Manager
Infocomm Security Group, NUSCERT
Computer Centre
National University of Singapore

steven@nus.edu.sg

NOTE: Updated slides available online at
https://selftest1.nus.edu.sg:9876/ppt/steven_sim_FIRST_2006.pdf

Agenda

- **NUS IT infrastructure**
- **The awakening**
- **A first step**
- **Exploring alternatives**
- **The evolution**
- **Track record**
- **What's next?**
- **Closing**

The NUS IT infrastructure

- **Not-for-profit**
- **Multi-gigabit, high speed network**
- **35,000 students and 6,000 staff**
- **30,000 concurrent online nodes**
- **Plug-and-play networks**
- **Wireless networks**
- **Heterogeneous and diverse IT**

The awakening

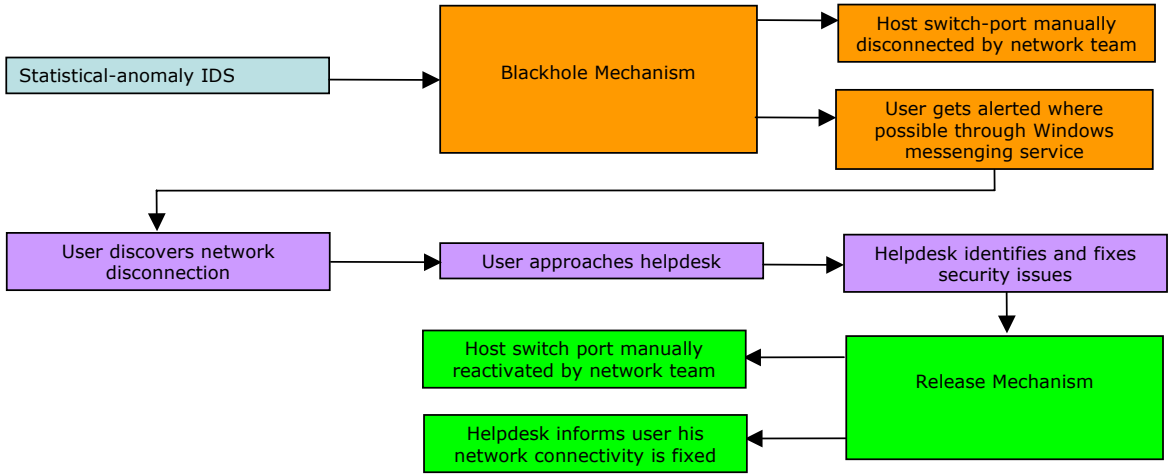
- **That blasted worm**
- **Expensive and labor-intensive containment**
- **Bottleneck in incident management**
- **Need to process re-engineer**
  - detection
  - containment
  - alert (response)
  - eradication (remediation)

A first step

- **Acceptable Use Policy**
  - Legal counsel
  - IT steering committee
  - Student union
- **Detection: Statistical-based anomaly IDS**
  - simple
  - low overheads
  - minimal false positives
- **Containment**
  - switch-port disconnection
- **Alert (Response)**
  - win-popup alerts
- **Eradication (Remediation)**
  - users not easily reached

The evolution

- **The process**



A first step

- **Limitations**
  - a DoS attack on innocent users
  - require OOB to alert users
  - difficulty with remediation
  - tendency for user to change ports
  - manual and fairly labor-intensive

Exploring alternatives

- **Commercial containment products**
  - route blackholing
  - admission control
- **Benefits**
  - robust
  - efficient

Exploring alternatives

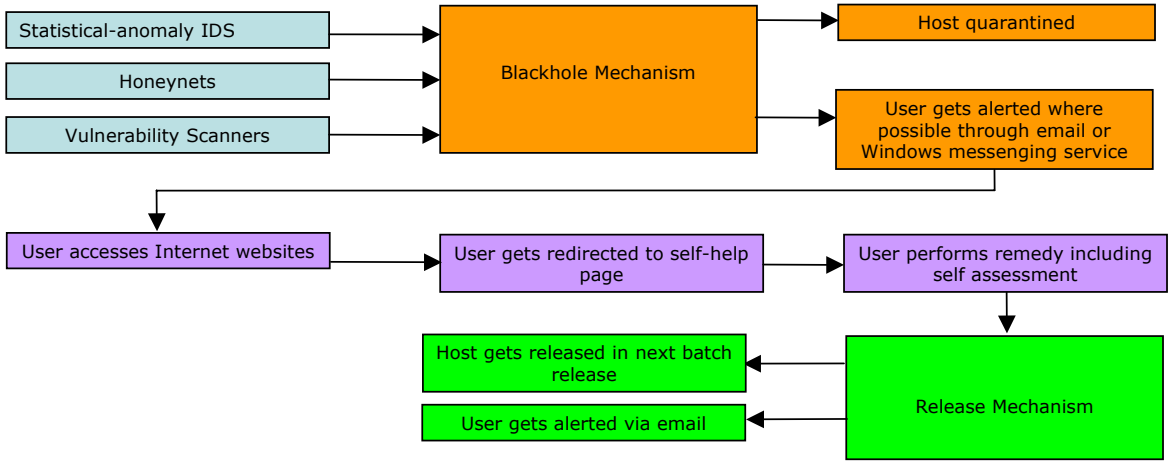
- **Limitations**
  - costly
    - **expensive ($$)**
    - **tremendous effort**
      - *overhaul of all unsupported switches*
    - **agent dependent**
  - integration with detection feeds not available
    - **lack of consideration for false negatives**
      - *in-house developed detection mechanisms*

The evolution

- **Detection**
  - statistical anomaly-based IDS
  - honeynets
  - vulnerability scanners
- **Containment**
  - DHCP blackholing
  - internal intruders quarantined
    - **botnet irc servers blocked**
- **Alert (Response)**
  - win-popup to infected machines
  - abuse contact of external origin auto-alerted
- **Eradication (Remediation)**
  - self-help

The evolution

- **The process**



Self -help

New Page 1 - SeaMonkey

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop file:///C:/Documents%20and%20Settings/AdminNUS/Desktop/FIRST/blackh Search Print

Home Bookmarks mozilla.org mozillaZine mozdev.org

What happened

If your internet access is normal, please ignore this page. If you find that **you are re-directed to this page whenever you launch Internet Explorer**, it means this computer's internet access has been restricted, as it is detected to be infected with virus.

What should you do

Step 1

Scan and clean all viruses from system.
If no viruses are detected on your system, it is likely that your PC is infected with a new unknown virus. **Please approach NUS IT Care for assistance.**

Step 2

- Change the local administrator password to non-guessable.
- Install or update Trendmicro Officescan. For staff, click here, then click Run. For students, click here, then click Run.
- Check and secure any open file shares.

Step 3:

[MUST DO] To re-activate, click here. Your system will be re-activated within two working hours.

Please ensure that all the above steps are followed. Failing to clean the virus properly will cause your computer be restricted again.

Should you encounter any problems, kindly contact Computer Centre NUS IT Care at ccehelp@nus.edu.sg or call 68742080 for assistance. Please take note of the error message and symptoms when problem is hit.

file:///C:/Documents and Settings/AdminNUS/Desktop/FIRST/blackhole_1/sos/chkpass.htm

- **Email on release**

[VULN-RPC] Your MAC address 00:02:b3:3b:b7:1f has been unblocked/released - Message (HTML)

Reply | Reply to All | Forward

File Edit View Insert Format Tools Actions Help

Follow up
This message was sent with High importance.

From: ccecert@nus.edu.sg
Sent: Thu 4/20/2006 12:04 PM
To:
Cc:
Subject: Your MAC address 00:02:b3: has been unblocked/released

Dear Sir/Madam,

The request generated on 20060420 at 1030 to unblock / release your MAC address 00:02:b3 :1f for network access has been successfully processed. **To reactivate your network connectivity, please reboot your PC.**

Thank you

Infocomm Security / QA
Computer Centre
National University of Singapore

Important: This email is confidential and may be privileged. If you are not the intended recipient, please delete it and notify us immediately; you should not copy or use it for any purpose, nor disclose its contents to any other person. Thank you.

The evolution

- **Email alert to external abuse**

[Network Abuse] Intrusion attempts from 192.83.166.250 targeting 137.132.X.X. - Message (Plain Text)

Reply | Reply to All | Forward

File Edit View Insert Format Tools Actions Help

From: ccecert@nus.edu.sg
Sent: Sun 4/9/2006 1:15 PM
To: abuse@moe.edu.tw
Cc:
Subject: [Network Abuse] Intrusion attempts from 192.83. targeting 137.132.X.X.

Dear abuse contact for 192.83. , abuse@moe.edu.tw

The system 192.83.166.250 belongs to your domain and is sending illegitimate/malicious traffic to our network 137.132.X.X within the last hour on 2006-04-09. Herewith is an extract of the log (all timings in GMT+8):

```
12:26:30.815338 IP 192.83.      .2300 > 137.132.X.X.1433: S 4278417421:4278417421(0) win 16384 <mss 1380,nop,nop,sackOK>
12:26:30.818324 IP 192.83.      .2301 > 137.132.X.X.1433: S 3913146089:3913146089(0) win 16384 <mss 1380,nop,nop,sackOK>
12:26:30.823322 IP 192.83.      .2306 > 137.132.X.X.1433: S 1481635737:1481635737(0) win 16384 <mss 1380,nop,nop,sackOK>
12:26:33.832281 IP 192.83.      .2300 > 137.132.X.X.1433: S 4278417421:4278417421(0) win 16384 <mss 1380,nop,nop,sackOK>
12:26:33.833277 IP 192.83.      .2306 > 137.132.X.X.1433: S 1481635737:1481635737(0) win 16384 <mss 1380,nop,nop,sackOK>
12:26:33.835641 IP 192.83.      .2301 > 137.132.X.X.1433: S 3913146089:3913146089(0) win 16384 <mss 1380,nop,nop,sackOK>
```

Kindly investigate and stop the intrusions. Thank you.

Infocomm Security Group
Computer Centre
National University of Singapore

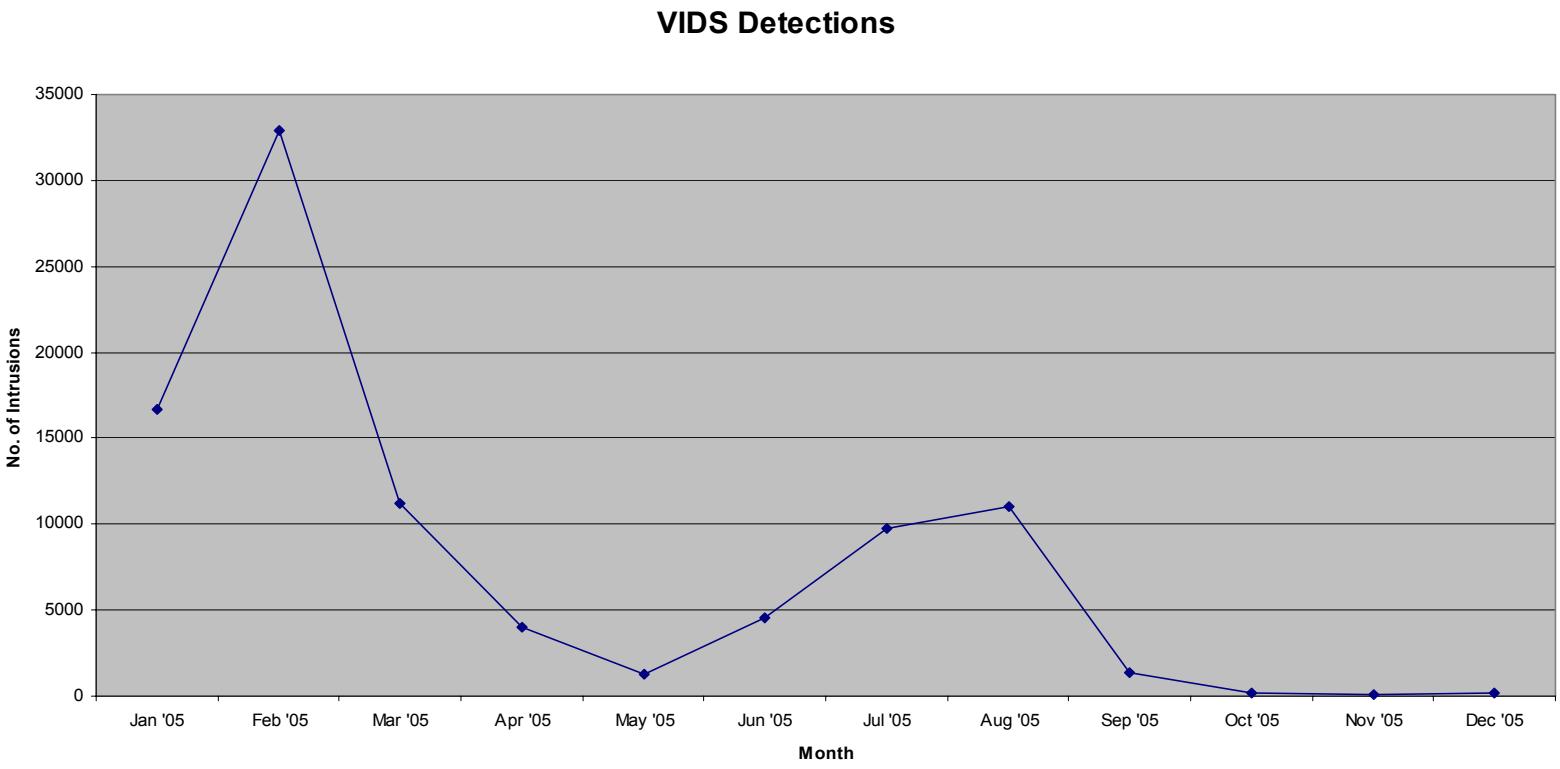
The evolution

- **Beneficial features**
  - cost and effort
    - **cost of implementation**
    - **ease of implementation**
  - user management
    - **managing user expectations**
    - **empowering users**
  - minimal false negatives
    - **efficacy of current antivirus detection pattern can be determined**
    - **new antivirus-undetected malicious trojans, backdoors and worms can be discovered**

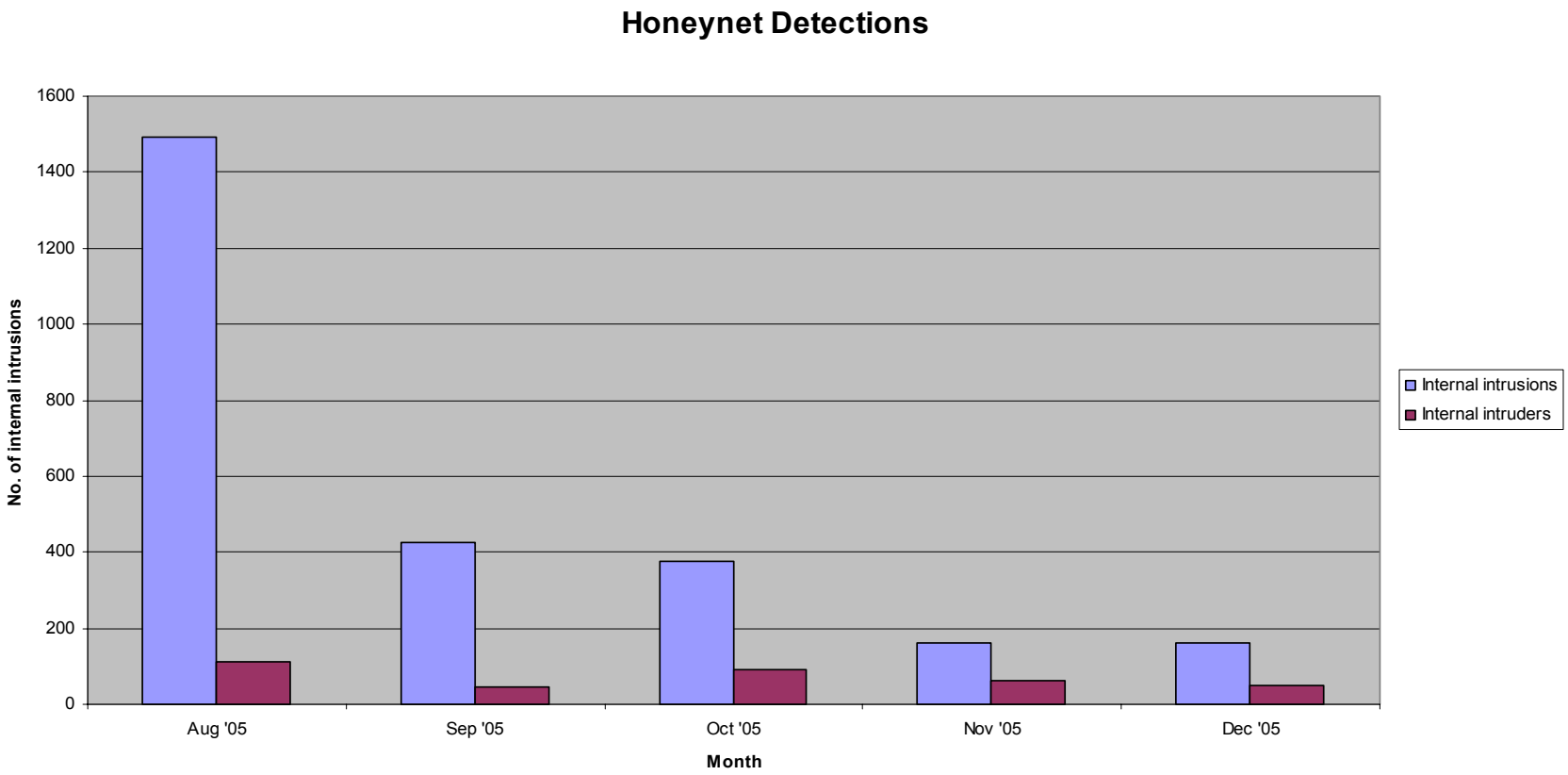
The evolution

- **Limitations**
  - does not handle non-DHCP based hosts
    - **rely on switch-port disconnection**
  - longer time window of infection/vulnerability
    - **need to be improved upon**
  - loopholes to circumvent DHCP blackhole and remediation steps
    - **mitigated through monitoring of re-infections**
  - self-help is Windows specific
    - **eradication for other OS infections handled onsite.**

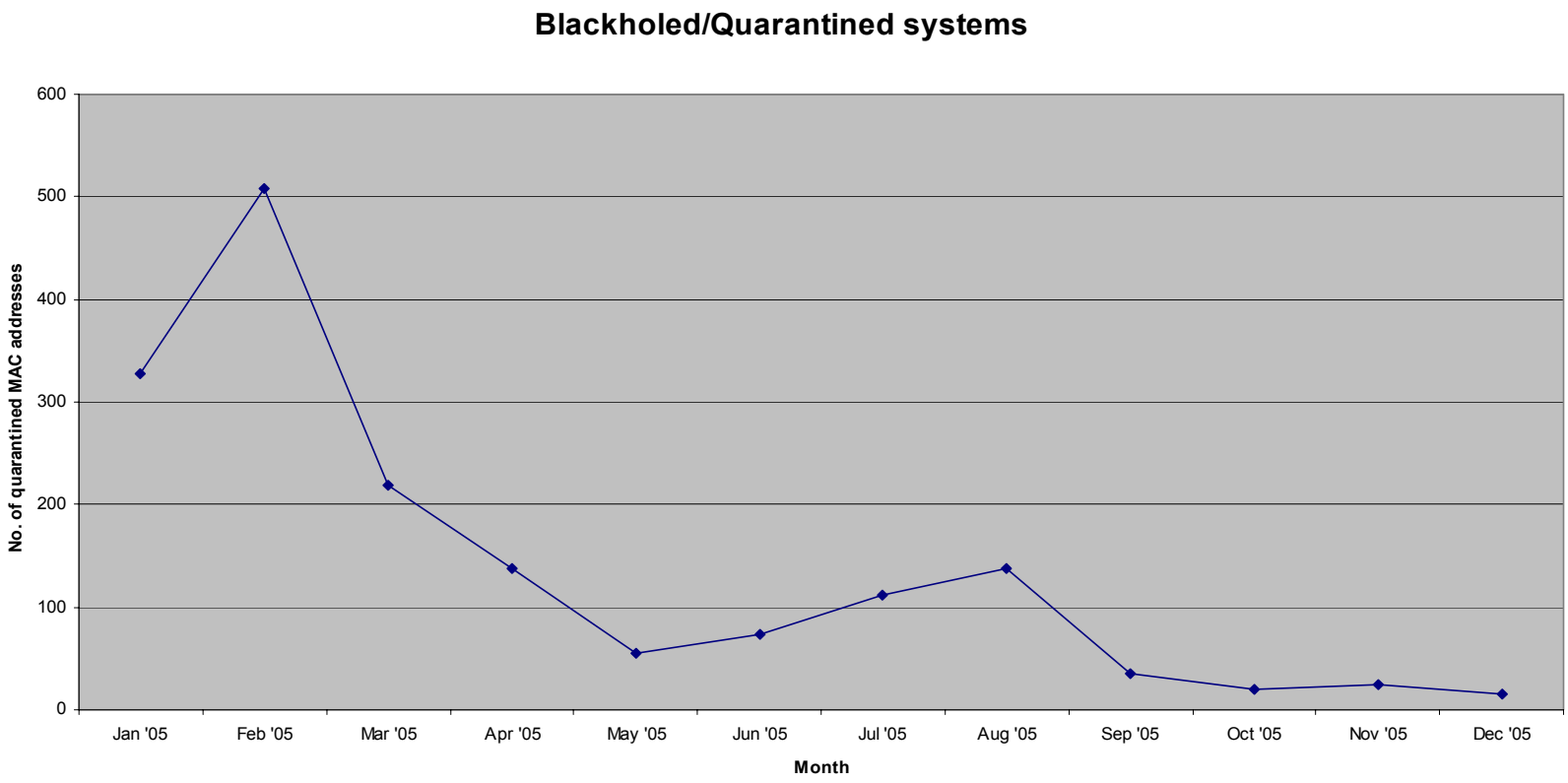
Track record



Track record



Track record



Track record

- **Some signatures created that is based on discovered binaries in containment**
  - TSPY_AGENT.AX
  - TSPY_AGENT.AK
  - TROJ_DROPPER.GG
  - TROJ_SMALL.AHE
  - TROJ_AGENT.XT
  - TROJ_AGENT.XU
  - TROJ_AGENT.XV
  - WORM_RBOT.BWC
  - WORM_RBOT.BZC
  - HKTL_PROCKILL.I
  - BKDR_NORUNORG.A
  - BKDR_SERVU.AS
  - BKDR_SERVU.AZ
  - BKDR_HACDEF.AQ
  - BKDR_SHELL.B
  - WORM_NETSKY.DAM
  - WORM_SOBER.DAM
  - WORM_MYTOB.DAM
  - WORM_LOVGATE.DAM
  - WORM_MYDOOM.DAM

What's next?

- **Enhance containment for non-DHCP based systems**

  – new server allowed on network after risk accessed and managed (this includes administrative, network and host vulnerability assessments)

  – existing server switch-port disconnected from network should any periodic network vulnerability assessment fail

Acknowledgements

The development of the automated incident containment strategy would not be possible without the support and assistance from the following people:

- Ms Yong Fong Lian (IT Security Manager)

- Dr Ma Huijuan (IT Security Engineer)

- Mr Gong Wei (IT Network Engineer)

Closing

Containment strategy

- **Inexpensive**
- **Simple**
- **Easy to develop**
- **Easy to implement**
- **Easy to maintain**
- **Effective**

NUS National University of Singapore

"The virus may be spreading despite the control measures already taken. Far more human and animal exposure to the virus will occur if strict containment does not isolate all known and unknown locations where the bird flu virus is currently present."

Dr Juan Lubroth