Handling Less Than Zero Day Attack
A Case Study

InfoComm Security/QA
Computer Centre
ccecer@nus.edu.sg
https://security.nus.edu.sg/
Handling Less Than Zero Day Attack

Agenda

• What is Less Than Zero Day Attack
• Threat - A Case Study
• What We Can Do About It
• Q & A
What is Less Than Zero Day Attack

Zero Day

- Software, videos, music, or information unlawfully released or obtained on the day of public release.
What is Less Than Zero Day Attack

Zero Day Exploit

- The vulnerability is known to public
- The patch is NOT yet available
- The exploit is released
What is Less Than Zero Day Attack

Less Than Zero Day Exploit

• The vulnerability is **NOT** known to public
• The patch is **NOT** yet available
• The exploit is released
Handling Less Than Zero Day Attack

Agenda

• What is Less Than Zero Day Attack
• Threat - A Case Study
• What We Can Do About It
• Q & A
Pâdîşîm Production

Hacked By KUZ3Y

www.padisim.com

Herkese Gider !

| SaO | mR-dEhSet | Canoshe | Deprem | MahaS3R | P3AC3 | Petro |

Yeni Çağın Yeni Hack Teknolojisi.
Threat – A Case Study

Agenda

<table>
<thead>
<tr>
<th>Defacer: PadiSim Hack Team</th>
<th>Domain: http://<em><strong>.</strong></em>.<em><strong>.</strong></em></th>
<th>IP address: <em><strong>.</strong></em>.<em><strong>.</strong></em></th>
</tr>
</thead>
<tbody>
<tr>
<td>System: Win 2000</td>
<td>Web server: IIS/5.0</td>
<td>Attacker stats</td>
</tr>
</tbody>
</table>
Threat – A Case Study

Actions Taken

• Inform the administrator
• Disconnects the server
• Investigate
Actions Taken

- Clean result from previous scan
- Open the server to scanner
- Scan again
- Clean result again
Actsions Taken

• Check out server logs

```plaintext
yyyy-mm-dd hh:mm:ss ***.***.***.*** - ***.***.***.***.*** GET 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
http://***.***.***.***/conference/forum/admin/***/***/*upload.asp
```
Threat – A Case Study

Actions Taken

• Check out uploaded files
• Find malicious uploaded files
Threat – A Case Study

Actions Taken

- Web site powered by database
- Database can be updated by Internet Guest Account
- Run malicious file and deface the website
- Boom!
Actions Taken

• Download and install the forum application

• Try out
  http://127.0.0.1/forum/admin/***/***/upload.asp

• Boom!
Threat – A Case Study

Actions Taken

• Less than zero day attack!
• Report to vendor

Huijan,

I understand what you are saying now. ****************************
******************************************************************************
**********.

Thank you so much for pointing out the security issue with the upload.asp page. We will work to fix it ASAP!

Regards,

**********

4/24/2007
Threat – A Case Study

Actions Taken

• Report to Cert CC
Threat – A Case Study

Actions Taken

• Back to our server:
  ✓ Remove the forum application
  ✓ Cleanup
  ✓ Harden
  ✓ Connect and back online
Handling Less Than Zero Day Attack

Agenda

• What is Less Than Zero Day Attack
• Threat - A Case Study
• What We Can Do About It
• Q & A
What We Can Do About It

Mitigation Measures

- Patch management not enough
- Harden the server
  - Remove unnecessary service
  - Remove unnecessary component in application
  - Audit the application
Mitigation Measures

• Monitor and alert
Any questions?