Handling Less Than Zero Day Attack

A Case Study

InfoComm Security/QA
Computer Centre
ccecert@nus.edu.sg
https://security.nus.edu.sg/

NUS National University of Singapore

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

NUS National University of Singapore

Zero Day Exploit

- The vulnerability is known to public
- The patch is NOT yet available
- The exploit is released

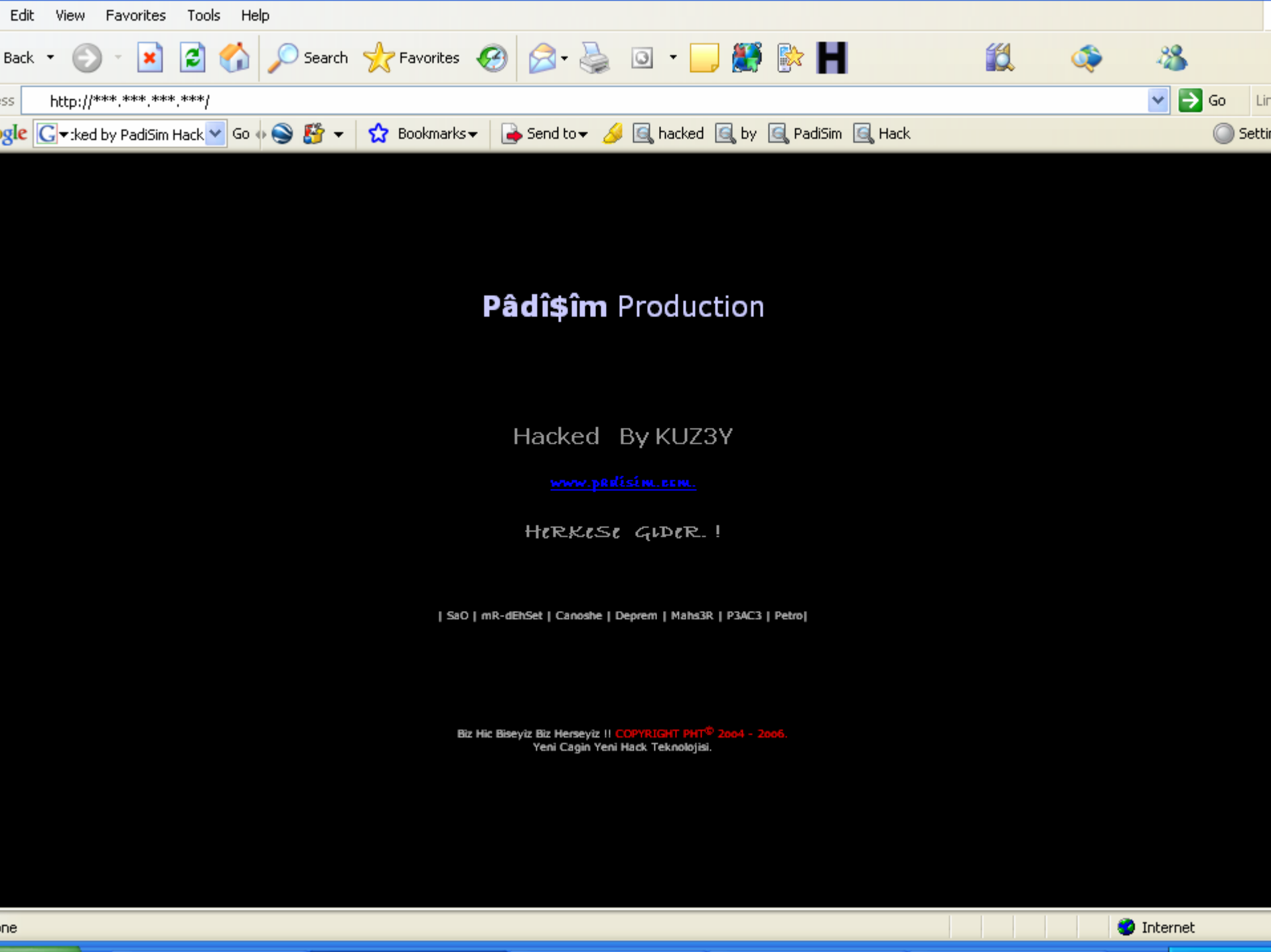
NUS National University of Singapore

Less Than Zero Day Exploit

- The vulnerability is NOT known to public
- The patch is NOT yet available
- The exploit is released

Agenda

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


Edit View Favorites Tools Help
Back Search Favorites
http://***.***.***.***/
Go
:ked by PadiSim Hack Go Bookmarks Send to hacked by PadiSim Hack
Pâdî$îm Production
Hacked By KUZ3Y
www.padisim.com.
HeRKeSe GiDeR. !
| SaO | mR-dEhSet | Canoshe | Deprem | Mahs3R | P3AC3 | Petro|
Biz Hic Biseyiz Biz Herseyiz || COPYRIGHT PHT© 2004 - 2006.
Yeni Cagin Yeni Hack Teknolojisi.
Internet

Agenda

Defacer: PadiSim Hack Team	**Domain: http://***.***.***.***	**IP address: ***.***.***.***
System: Win 2000	**Web server: IIS/5.0**	Attacker stats

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

Actions Taken

- Check out server logs

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

Actions Taken

- Check out uploaded files
- Find malicious uploaded files

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!

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,
****

Actions Taken

- Report to Cert CC

Actions Taken

- Back to our server:
  - ✓ Remove the forum application
  - ✓ Cleanup
  - ✓ Harden
  - ✓ Connect and back online

NUS National University of Singapore

Agenda

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

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

NUS National University of Singapore

Any questions?