Owning the koobface botnet
intro

• web 2.0 botnet
• spreads through social networks
  – facebook
  – myspace
  – twitter, etc.
You must see this video now! :)  
http://dejaramarcos.com/554/

Amazing Video

Source: dejaramarcos.com

October 13 at 3:30am
EkmKaynakoglu: ANATÜRK: You must see this video now! :) http://dejaramarcos.com/554/

Amazing Video
Source: dejaramarcos.com

Jhkb My Home Film ;) http://lnk.ms/135tn 22 seconds ago
Mood: good 😊

view more | comment | message

view my updates | view all
Amazing Video
Source: dejaramarcos.com

I love this video! :) http://i-dare-you.co.za/639/

© 2009 Twitter / About Us / Contact / Blog / Status / Goodies / API / Business / Help / Jobs / Terms / Privacy
Video posted by * Tiger *

Video Responses: 10  Text Comments: 70

- habachi (4 hours ago)
  Funniest thing EVER!!

- cmwd1199 (6 hours ago)
  Woohoo! Love this vid!!! Congrats on the front page!!! :-)

- snrinket (7 hours ago)
Welcome to Video

Welcome to Facebook Video. Upload videos and share them with your friends.

Share your personal videos. Upload and tag videos of you and your friends on Facebook. Upload a new video.

Record and send video messages. Use your webcam to record yourself in a video message. Record a video message.

Publish videos from your mobile. Send mobile videos via email or MMS to your personal upload address.

Flash Player upgrade required
You must download and install the latest version of the Adobe Flash Player to view this content.

Download Flash

Latest Videos

Hong Kong
by Bruno Carlet
View Bruno's Videos (1)

None of your friends are tagged... yet.

Upload a video of a friend

View All Latest Videos...
koobface loader

- Social network (Facebook, Myspace, Twitter, etc.) spreader
- Personal information and credentials stealer
- Google accounts creator
- Facebook auto-registration module
- Search hijacker
- Fake AV module
- Web server component
web server component

• makes every koobface zombie a web server
  – serves the fake YouTube/Facebook pages
  – serves the koobface loader
1. User visits social network, clicks on a koobface-spammed URL.

2. User visits the koobface-spammed URL, which is actually a compromised site.

3. User redirected to a koobface zombie.

4. The web server component serves "setup.exe" – the koobface loader.
what about it?

• installed on all koobface zombies as a system service (*webserver service*)

• adds exemption in Windows Firewall for TCP port 80 (HTTP)

• reachable from the Internet
which means...

• further exposes koobface zombies to attacks from the Internet

• exposes the koobface botnet itself to attacks from the internet
what kind of attack?

- security holes in the web server component
  - buffer overflow
  - auto-update
buffer overflow

```assembly
lea  eax, [ebp+NumberOfBytesWritten]
push eax
lea  eax, [ebp+var_78]
push eax
lea  eax, [ebp+Src]
push offset aSS_0 ; "%s%s"
push eax ; Src
call ds:scanf
add esp, 10h
cmp  eax, 2
jnz  loc_402286
```
very long string in HTTP request
control of eip
auto-update

• can be used to remotely update the koobface web server binary

• triggered by the following web request

how it auto-updates

- when triggered
  - download the new web server binary
  - drop and execute a batch file
    - stop the webserver service
    - replace the existing web server binary
    - restart the webserver service
exploiting auto-update

• koobface blindly downloads “updated” binaries

• trigger auto-update to download arbitrary binaries

• new binary should cooperate nicely with the NT Service Controller
where are the targets?
revisiting the infection chain

1. User visits social network, clicks on a koobface-spammed URL

2. User visits the koobface-spammed URL, which is actually a compromised site.

3. User redirected to a koobface zombie

4. The web server component serves "setup.exe" – the koobface loader
koobface sites

```javascript
// KROTEG
var bwhyx5 = [
  ['facebook.com', 'fb2'],
  ['tagged.com', 'tg'],
  ['friendster.com', 'fr'],
  ['myspace.com', 'ms'],
  ['msplinks.com', 'ms'],
  ['lnk.ms', 'ms'],
  ['myyearbook.com', 'yb'],
  ['fubar.com', 'fu'],
  ['twitter.com', 'tw'],
  ['hi5.com', 'hi5'],
  ['bebo.com', 'be']
];

var eldcwonhkptgru0 = [
  '76.78.' + '140.72',
  '88.' + '168.167.135',
  '76.113.' + '.49.61',
  '74.79.' + '128.243',
  '70' + '.142.15.164',
  '67.' + '182.76.118',
  '99.20.' + '.116.16',
  '6' + '5.60.143.12',
  '24.' + '125.193.28',
  '83.' + '49.211.4',
  '208.35' + '.24.20',
  '75.81.' + '189.14',
  '66.30.' + '178.159',
  '7' + '0.119.15.248'
];
```
koobface zombies

• create simple scripts to harvest all of the IP addresses

• 79,000+ zombies
zombie distribution
checklist

✓ web server vulnerabilities
✓ exploits
✓ list of targets

☐ take over?
questions?