

Hax by Jaku

by Jaku & Alk

WTF is Hax by Jaku?

- Awesome
- Funny
- Informative
- w00t tastic
- Free
- Pyramid Scheme

Hair today, gone
tomorrow.

What does hair have to do with
a hack??

Everything.



Before and After



Before

Hax by Jaku



After

Hax by Jaku

So this is Hax by Jaku?

- ⦿ No
- ⦿ Not really
- ⦿ Nope
- ⦿ Maybe
- ⦿ Do you want it to be?
- ⦿ What if it was?

Real Hax by Jaku!

What really is Hax by Jaku?

- Informative
- Cool
- Fun
- Free
- w00table
- Pyramid Scheme

Hax by Jaku

How many times can I say
that without you hating me?



AimJect

- Aimject facilitates man-in-the-middle attacks against AOL Instant Messenger's OSCAR protocol
- sign-on/off detection
- message interception/decoding
- message injection into arbitrary conversations
- cloning of font styles/screenname formatting to avoid detection
- selective muting of conversation participants
- integrated ARP/DNS spoofing

Aimject

Local ID	Remote ID	Chat Log
binaryjonomobile	binaryjono	(Oct 1 21:26:49) binaryjonomobile : hey hows it going?
keysursoze	smarterchild	(Oct 1 21:27:00) fuchungdow : pretty good, yourself?
	moviefone	(Oct 1 21:27:52) MUTED binaryjonomobile : great! i just finished my exam and did really well!
	shoppingbuddy	(Oct 1 21:28:10) INJECT binaryjonomobile : terrible, i definitely flunked my exam...
	fuchungdow	(Oct 1 21:28:40) MUTED fuchungdow : aww, that sucks, better luck next time
		(Oct 1 21:29:34) binaryjonomobile : what are up to tonight?
		(Oct 1 21:29:53) MUTED fuchungdow : not much, just lazing around
		(Oct 1 21:30:00) INJECT fuchungdow : HUGE PARTY AT MY HOUSE!!!
		(Oct 1 21:30:40) MUTED binaryjonomobile : ill see you there!
		(Oct 1 21:30:52) binaryjonomobile : adios!
		(Oct 1 21:30:54) fuchungdow : tyl

Add
Delete

Mute To

Mute From

Statistic	Value	Direction
Initial Conn	192.168.0.10:57485	<input type="radio"/> binaryjonomobile -> fuchungdow
BOS Conn	192.168.0.10:57997	<input checked="" type="radio"/> fuchungdow -> binaryjonomobile
Conv Count	5	
Msg Recv Count	27	
Msg Sent Count	16	
Last Recv Msg	Sun Oct 1 21:30:54 2006	
Last Sent Msg	Sun Oct 1 21:30:54 2006	
Sequence In	13204	
Sequence Out	89	

Inject
 Quit

Who can use AimJect?

- What you need for AimJect to work
- Linux, BSD, Mac OS X, and Win32 (2000/XP)
- libdnet >= 1.10
libpcap >= 0.8.3
gtk+-2.0 >= 2.6
glib-2.0 >= 2.6
libglade-2.0 >= 2.5.1
- <http://jon.oberheide.org/projects/aimject/>

Real world uses



SPYING

(Ruining lifes one IM at a time)*

(Not that thats what we used it for)**

(Can you read this?)***

(09 F9 11 02 9D 74 E3 5B D8 41 56 C5 63 56 88 C0)

Real Uses

General Uses	Professional Uses
Eavesdrop	Monitor co-workers\family
Impersonate people	Test security of AIM
Mess with friends	Make presentations about it
SPYING	

Where we did it at?

- Colleges
- Libraries
- Coffee Shops
- Fast food restaurants
- Hotels
- Open APs
- Work
- Home

What we did

- Tested the various wireless networks in the Chicago area

What we found

- Places with free wifi
- Personal Information
- Funny stories
- Dumb stories
- That Joey likes Krystal but Krystal likes John and Sara

Ways to stay secure

- Use Adium on the Mac
- Use GAIM with encryption on Windows/Linux
- Keep static ARP tables
- Keep firewalls up
- #1 one way to stay secure
- USE GTALK

Why we did it

- To show that AIM really doesn't encrypt everything (sorry fox)
- Why not?
- For fun
- ???
- Profit

Credits

- Created by: Jon Oberheidee
- Found at: <http://jon.oberheide.org/projects/aimject/>

- Presentation by:
- Jaku & Alk3