Presenter

» Jeff Yestrumskas
  » Sr. Manager, InfoSec @ SaaS org.
  » Personal DEFCON attendee:presenter ratio = 10:1
Presenter

Matt Flick

- Principal, FYRM Associates
- Information Assurance Consulting
- Beer connoisseur

fyrmassociates.com
Agenda

» What is XAB?
» XAB History
» What’s New?
» Nitty Gritty
» XAB Process Flow
» Live Demo
» Wrap-up

fyrmassociates.com
What is XAB?

- Anonymous browsing tunneled over XSS
- Victim/Participant transfers data
XAB History

» Idea
» Introduced @ Black Hat DC 2009
  » Working Demo
» Released PoC

fyrmassociates.com
What’s New?

Solution to the HTTP referrer problem

Improved content handling

...
Nitty Gritty

Three components

- XABAttacker (core of it all)
- HTTPProxab (everyday HTTP proxy with XAB mods)
- CDProxy (it’s seedy alright)
XAB Process Flow

---

fyrmassociates.com
Live Demo

Host OS
- Web browser
- Victim Client
- Web browser
- Attacker Client

Virtual Machine
- Website vulnerable to HTML injection attack
- Website with content desired by attacker

Firewall
- www.vulnsite.xab
- www.target.xab

Attacker controlled webserver
- www.attacker.xab

Free cgi hosting server
- www.freehost.xab

fyrmassociates.com
Wrap-up

» That was fast!

» Further reading...

» Download XAB @ www.fyrmassociates.com