Satan is on my Friends List

Attacking Social Networks

Shawn Moyer
agura digital security
Blackhat {at} agurasec.com

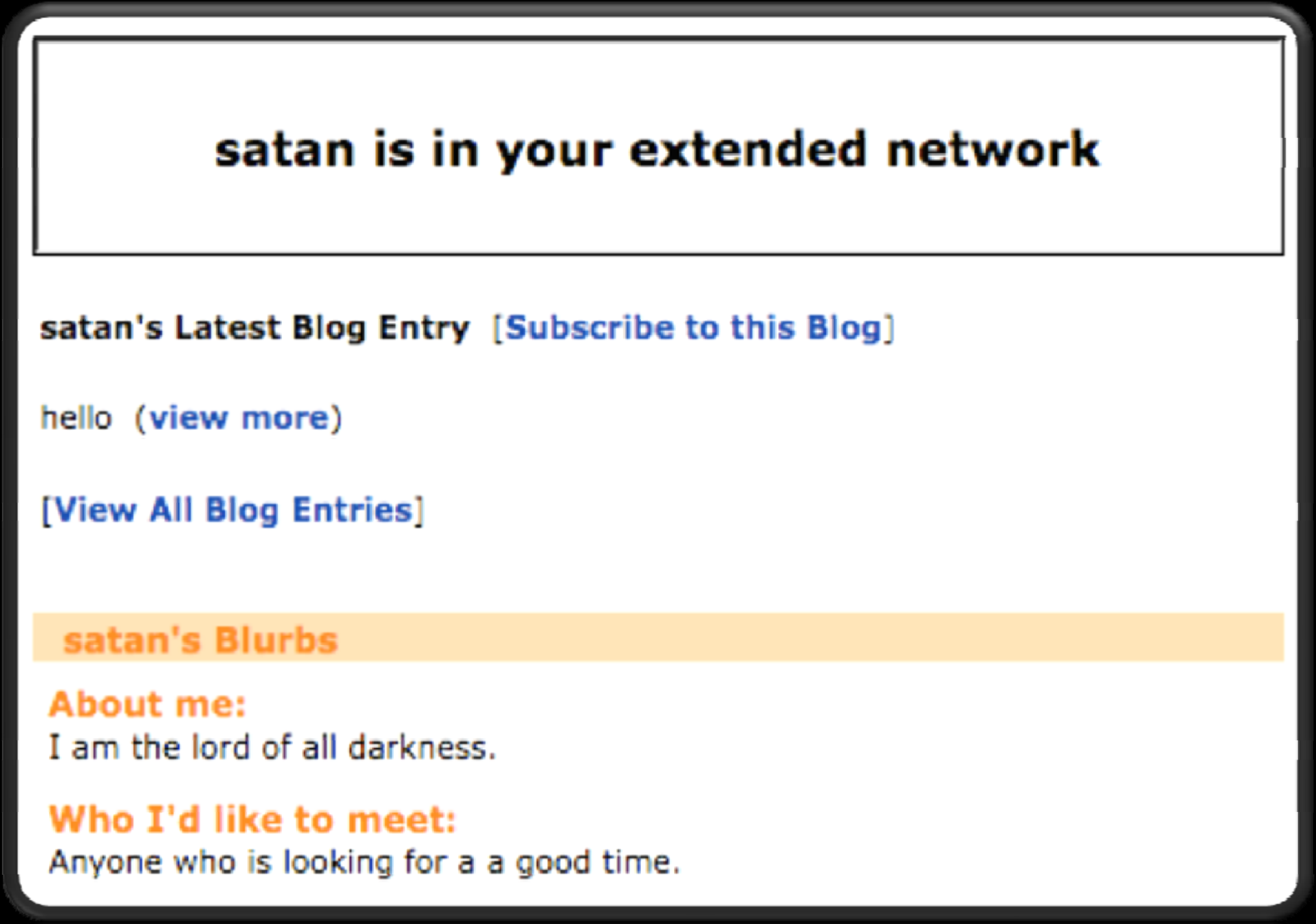
Nathan Hamiel
Idea Information Security
Nathan {at} neohaxor {dot} org

BlackHat

We're in your Extended Network!

- Nathan Hamiel
  - Senior Consultant at Idea InfoSec
  - Associate Professor at UAT
- Shawn Moyer
  - Too-frequent BH speaker
  - InfoSec Consultant @ AguraSec

And so is...



satan is in your extended network

satan's Latest Blog Entry [Subscribe to this Blog]

hello (view more)

[View All Blog Entries]

satan's Blurbs

About me:
I am the lord of all darkness.

Who I'd like to meet:
Anyone who is looking for a a good time.

Why should you care?

- 5 of the Alexa top 20 sites are SocNets

Why should you care?

- 5 of the Alexa top 20 sites are SocNets
- Hundreds of networks, millions of users*

Why should you care?

- 5 of the Alexa top 20 sites are SocNets
- Hundreds of networks, millions of users*

*And by "users", we mean "targets".

Why should you care?

- 5 of the Alexa top 20 sites are SocNets
- Hundreds of networks, millions of users*
- Rapid adoption as a business tool

*And by “users”, we mean “targets”.

Why should you care?

- 5 of the Alexa top 20 sites are SocNets
- Hundreds of networks, millions of users*
- Rapid adoption as a business tool
- Not just emo kids and camwhores anymore!

*And by “users”, we mean “targets”.

Samy is so… 2005.

- Not (just) about wormable XSS, etc

Samy is so… 2005.

- Not (just) about wormable XSS, etc
    - User-generated applications and content

Samy is so… 2005.

- Not (just) about wormable XSS, etc
  - User-generated applications and content
  - Complex and diverse attack surface

Samy is so… 2005.

- Not (just) about wormable XSS, etc
  - User-generated applications and content
  - Complex and diverse attack surface
  - Logic flaws and “innocuous” functions

Samy is so… 2005.

- Not (just) about wormable XSS, etc
  - User-generated applications and content
  - Complex and diverse attack surface
  - Logic flaws and “innocuous” functions
- Integration and shared exposure

Samy is so... 2005.

- Not (just) about wormable XSS, etc
  - User-generated applications and content
  - Complex and diverse attack surface
  - Logic flaws and “innocuous” functions
- Integration and shared exposure
  - OpenSocial and 3rd party development platforms

Samy is so… 2005.

- Not (just) about wormable XSS, etc
  - User-generated applications and content
  - Complex and diverse attack surface
  - Logic flaws and “innocuous” functions
- Integration and shared exposure
  - OpenSocial and 3rd party development platforms
  - Amalgamated XML-ified goop (REST/JSON/etc)

Samy is so… 2005.

- Not (just) about wormable XSS, etc
  - User-generated applications and content
  - Complex and diverse attack surface
  - Logic flaws and "innocuous" functions
- Integration and shared exposure
  - OpenSocial and 3rd party development platforms
  - Amalgamated XML-ified goop (REST/JSON/etc)
  - Convenient, well-documented APIs to craft attacks

Antisocial Networking

- Exploiting the web of trust

Antisocial Networking

- Exploiting the web of trust
  - Zero (or less) validation of identity, easy social proof

Antisocial Networking

- Exploiting the web of trust
  - Zero (or less) validation of identity, easy social proof
  - SocEng + client-side vuln mashups = FAIL

Antisocial Networking

- Exploiting the web of trust
  - Zero (or less) validation of identity, easy social proof
  - SocEng + client-side vuln mashups = FAIL
  - High hit rate and low line noise for directed attacks

Antisocial Networking

- Exploiting the web of trust
  - Zero (or less) validation of identity, easy social proof
  - SocEng + client-side vuln mashups = FAIL
  - High hit rate and low line noise for directed attacks
- “Your profile is incomplete!”

Antisocial Networking

- Exploiting the web of trust
  - Zero (or less) validation of identity, easy social proof
  - SocEng + client-side vuln mashups = FAIL
  - High hit rate and low line noise for directed attacks
- “Your profile is incomplete!”
  - Voluntary and indiscriminate info leakage

Antisocial Networking

- Exploiting the web of trust
  - Zero (or less) validation of identity, easy social proof
  - SocEng + client-side vuln mashups = FAIL
  - High hit rate and low line noise for directed attacks
- “Your profile is incomplete!”
  - Voluntary and indiscriminate info leakage
  - Data aggregation, inference and profiling

Antisocial Networking

- Exploiting the web of trust
  - Zero (or less) validation of identity, easy social proof
  - SocEng + client-side vuln mashups = FAIL
  - High hit rate and low line noise for directed attacks
- “Your profile is incomplete!”
  - Voluntary and indiscriminate info leakage
  - Data aggregation, inference and profiling
  - Cross-pollination of online personae

What we've been up to…

- Pro Bono security audits of major SocNets

What we've been up to…

- Pro Bono security audits of major SocNets
- Social experiments and misc tomfoolery

What we've been up to…

- Pro Bono security audits of major SocNets
- Social experiments and misc tomfoolery
- Finding new ways to get accounts deleted

What we've been up to…

- Pro Bono security audits of major SocNets
- Social experiments and misc tomfoolery
- Finding new ways to get accounts deleted
- Hastening the apocalypse (not really)