SOCIAL ZOMBIES

YOUR FRIENDS WANT TO EAT YOUR BRAINS
STARRING...
TOM ESTON
SOCIAL NETWORKS

"THE NEW HOTNESS"
225 MILLION USERS
110 MILLION USERS
Grew 752% in 2008!
8 MILLION VISITORS IN MARCH 2009
“Social networks & blogs are now the 4th most popular online activity, ahead of personal email.”

-Nielsen Online Report, March 2009
HOW DO SOCNETS MAKE $$$?
IT'S IN YOUR PROFILE!

- MORE INFORMATION YOU SHARE...MORE $ IT’S WORTH!
- TARGETED ADVERTISING
- SELL YOUR DEMOGRAPHIC INFO
- SKETCHY PRIVACY/TOS POLICIES....
IN SOCIAL NETWORKS WE TRUST...
TRUST IS EVERYTHING!

• IT'S HOW SOCIAL NETWORKS WORK
• MORE TRUST, THE BETTER FOR THE SOCNET!
• ATTACKERS LOVE TRUST RELATIONSHIPS!
FAKE PROFILES
IT'S BUILT TO EXPLOIT TRUST

• Who is the person behind the account?
• Bots are everywhere
• Accounts are easy to create
• Socnet user verification = fail
• Connections based on other "friends"
PRIVACY CONCERNS
25 RANDOM THINGS ABOUT YOU...

• I'M YOUR FRIEND, I WANT TO KNOW MORE ABOUT YOU!

• INNOCENT?

• THESE ARE PASSWORD RESET QUESTIONS PEOPLE!!
CORPORATE ESPIONAGE?

- Very effective in a penetration test
- Socnet information = gold
- Information leakage on a mass scale!
DEFAULT PRIVACY SETTINGS

• WIDE OPEN FOR A REASON!
• FACEBOOK HAS VERY GOOD CONTROLS...BUT...
• DO YOU KNOW WHERE THEY ARE?
• DO YOUR FRIENDS/FAMILY?
• DO THEY CARE?
SECURITY CONCERNS

- Socnets are #1 Target for Malware
- Spam
- Disinformation
- XSS, CSRF and More!
TWITTER CLICKJACKING & XSS
RETURN OF KOOBFACE

• RECYCLED EXPLOITS
• EXPLOITS TRUST
• STILL EFFECTIVE!
DELIVERY VIA SOCNET API

- TWITTER BOTS (NOTABOT, REALBOY)
- AUTOMATED TOOLS AND SCRIPTS...
AUTOMATED TOOLS
PAY SERVICES
SOCIAL NETWORK BOTNETS?
FACEBOT POC

- MALICIOUS FACEBOOK APPLICATION (LOOKS NORMAL)
- TURNS YOUR PC INTO A BOT USED FOR DDOS!
INTRODUCING...
KREIOS C2
BROWSER BASED BOTS
BROWSERS AND FEATURES... OH MY!

• BROWSERS ARE GETTING MORE FEATURE-RICH
  • READ THAT AS MORE VULNERABLE!
• FORGET EXPLOITING VULNS
• ABUSE THE FEATURES WE ARE PROVIDED
BROWSER ZOMBIES

- JavaScript used to hook the browser
- Other technologies will work
- Many frameworks available
  - BeEF
  - BrowserRider
  - Anehta
SOCKET DELIVERY

- Embedded applications can insert JavaScript
- Multiple options
  - Hook scripts are pushed
  - Users are redirected to hook sites
- Why would we allow this!?!?
OH YEAH MAFIA WARS
SERVER SIDE INFORMATION COLLECTION
Information is Power

- Information gets us access
- Social networks are littered with info
- By how do we connect it together
THIRD PARTY APPS TO
THE RESCUE

- THIRD PARTY APPS HAVE ACCESS TO EVERYTHING
- PERMISSIONS ARE OPEN BY DEFAULT
- ONCE A USER SAYS ACCEPT
API's FTW

- MySpace and Facebook both provide access to an API
- These APIs provide the access we want
- Allows connecting different users
- Based on friends, groups, jobs or interests
SOCIAL BUTTERFLY

• SOCIAL BUTTERFLY IS A THIRD PARTY APPLICATION
• RUNS ON ATTACKER CONTROLLED SERVERS
• COLLECTS THE DATA FROM APPLICATION USERS
• CROSSES THE LINE BETWEEN DIFFERENT SITES
• FINE LINE BEFORE VIOLATING TOS!
SOCIAL BUTTERFLY DEMO
PREVENTION

• USER EDUCATION
• END "OPT-IN" SOCGNET DEVELOPER MODELS
• CONTROL API USAGE
• BETTER ACCOUNT VERIFICATION
• SPAM THROTTLING
CONCLUSIONS
MORE INFORMATION

• FACEBOOK PRIVACY & SECURITY GUIDE
  SPYLOGIC.NET

• KREIOS C2
  WWW.DIGININJA.ORG

• NEW WEBSITE DEDICATED TO SOCIAL MEDIA SECURITY (ANNOUNCED AT DEFCON)
QUESTIONS FOR THE ZOMBIES?