SOCIAL ZOMBIES

YOUR FRIENDS WANT TO EAT YOUR BRAINS

STARRING...

TOM ESTON

KEVIN JOHNSON

SOCIAL NETWORKS

"THE NEW HOTNESS"

facebook®

225 MILLION USERS

myspace
.com

110 MILLION USERS

twitter

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!

SOCIAL NETWORK BOTS

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

KREIOS C2 DEMO

BROWSER BASED BOTS

BROWSERS AND FEATURES... OH MY!

- BROWSERS ARE GETTING MORE FEATURE-RCIH
  - 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

SOCNET 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" SOCNET 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?