Contents

• Botnets
• Mebroot
• Torpig via Mebroot
• Domain Flux
• Taking Control
• Analysis
• Threats
• Most Important Problem
• Human Behaviour
• Conclusion
Botnet

- Group of computers
- Affected by malwares
- Performs several tasks
  - Collecting private data
  - Attacks
    - DDoS
Mebroot

- Toolkit
- Affects MBR
  - At boot time
- From websites
- Explorer to Disk Driver
  - Access to the MBR
- Performs installing, upgrading malwares
  - C&C Server
Torpig via Mebroot

• Mebroot installs Torpig
• Injects to the system executables and DLLs
  o Especially services.exe
• Injects to the 29 popular programs
  o Browsers
  o Email Clients
  o IM Clients
  o etc
• Communication to the C&C
  o Simple XOR encryption
Domain Flux

• Changing C&C Server domain daily
• Avoiding blocking server address
• Changing IP address of domain
  o Registration fees
• Torpig's revenue
Taking Control

• Analyzing domain flux
• Registering proper domains
• Reverse engineering of C&C server messages
• For 10 days
• Big botnet size
  o Affected computers, active computers
  o Elimination
    ▪ Other researchers
    ▪ DHCP Changes
Analysis

• Data Transfer Type: HTTP Post
• Data Type
  o Mailbox, Email
  o Form data
  o HTTP, FTP, POP, SMTP accounts
  o Windows password
• Bot identification
  o By hard disk
  o Virtual Machine
• Versions: dxtrbc and gnh5
Threats

• Financial Data Stealing
  o Revenue
    ▪ $83K-$8.3M
• Proxies
  o Spacing
    ▪ Avoiding blacklists
• DoS
  o Bandwidth consuming
• Password
Most Important Problem

- Man-in-the-browser
  - Before SSL/TLS
- Password and Credit Card Information
  - Unencrypted
Human Behaviour

- Reusing passwords, Simple passwords
- Do not understand consequences of malwares
- Cannot contact easily with registrars, hosting companies, government,... etc
Conclusion

• Torpig has huge botnet
  o Collects data by man-in-the-browser
  o Spamming
  o Revenue
• Can update itself and avoid from blocks
  o Domain flux etc
• Uses human behaviors
  o Humans do not show same importance to computers like cars
• Organizations are not reachable
Thank you