Oh RATs!!

A look at Remote Access Trojans

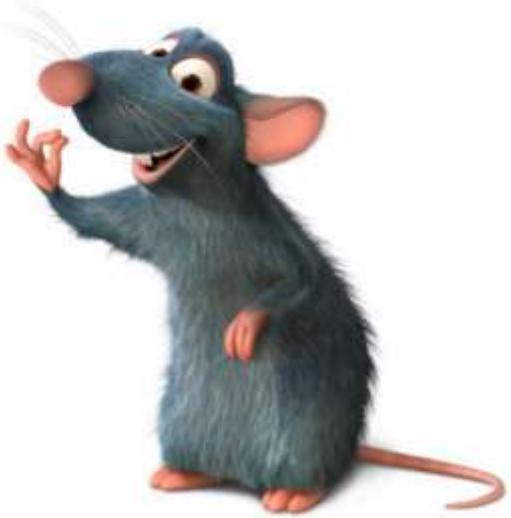
What about RATs?

No, we're not talking about the Animal.

We are talking about:

- Remote Access Trojans
- Remote Access Tools
- Remote Administration Tools
- Backdoors
- Trojan Horses

Commonly referred to as RATs



So what is a RAT?

Piece of software that allows a remote operator access to and/or control over a computer system as if physically present with the system.

https://en.wikipedia.org/wiki/Remote_administration_software

So these things are bad?

Nope

- Virtual Network Computing (VNC)
- PCAnywhere
- GoToMyPc
- Remote Desktop Connection
- Net Cat
- ETC …

So they are … good?

Nope

- NetBus
- Back Orifice
- Sub Seven
- Poison Ivy
- Dark Comet
- Meterpreter
- Net Cat
- ETC …

Okay, but what do they do?

Common Functionality:

- Screen/Camera capture
- File Management
- Command Prompt Access
- Power Control (Shutdown / Restart)
- Registry Editing / Querying
- And More …

How Do They Work?

Client / Server Architecture

VICTIM

- Malicious Application
- Server

Hacker

- Command & Control
- Client

NetBus “NetPrank”

- Keystroke logging
- Keystroke injection
- Screen captures
- Program launching
- File browsing
- Shutting down the system
- Opening / closing CD-tray
- Tunneling protocol

https://en.wikipedia.org/wiki/NetBus

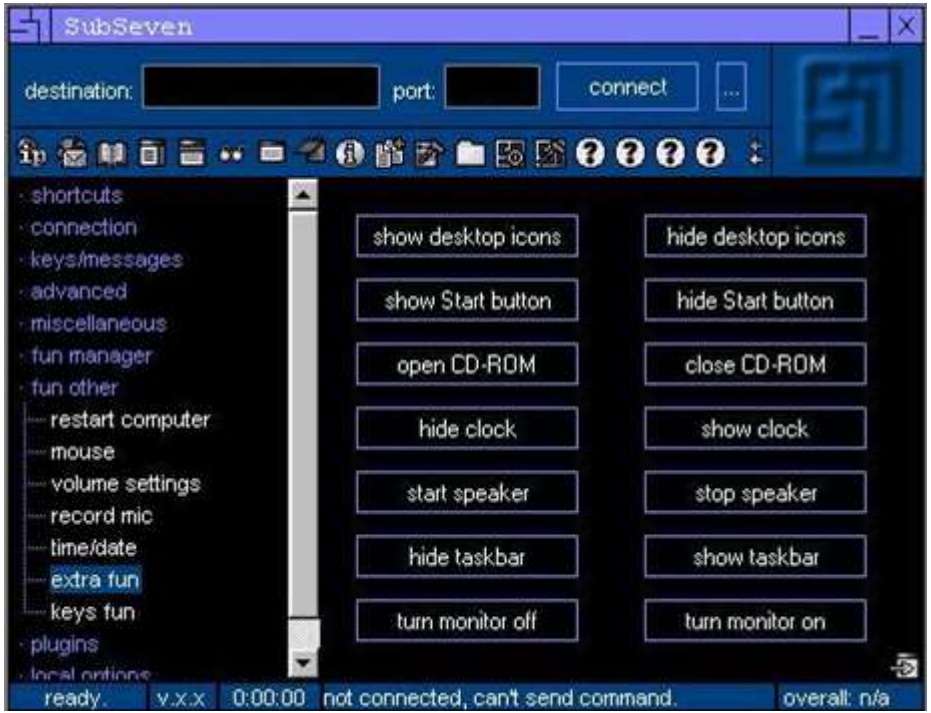
Back Orifice / BO2k

- GUI Client Interface
- Authored by Cult of the Dead Cow
- Debuted at DEFCON 6 and 7
- Plugin Architecture (BO2k)
  - Encrypted communication
  - File and Registry Control
  - Desktop viewing (Streaming Video)
  - Chat
  - Tunneling
  - Mouse and Keyboard Control / Logging
  - Hiding things from the system (based on FU Rootkit)

https://en.wikipedia.org/wiki/Back_Orifice
https://en.wikipedia.org/wiki/Back_Orifice_2000

Sub Seven (Sub7)

- GUI Client
- Recording
  - Audio
  - Screen
  - Webcam
- Cached / Recorded Passwords
- Take over ICQ account
- Pranks:
  - changing desktop colors
  - opening and closing the optical drive
  - swapping the mouse buttons
  - turning the monitor off/on
  - “text2speech” voice synthesizer
  - Matrix style chat “Hello Neo”



Dark Comet

- Spy Functions
  - Webcam Capture
  - Sound Capture
  - Remote Desktop
  - Keylogger
- Network Functions
  - Active Ports
  - Network Shares
  - Server Socks5
  - LAN Computers
  - Net Gateway
  - IP Scanner
  - Url Download
  - Browse Page
  - Redirect IP/Port
  - WiFi Access Points
- Computer Power
  - Poweroff
  - Shutdown
  - Restart
  - Logoff
- Server Actions
  - Lock Computer
  - Restart Server
  - Close Server
  - Uninstall Server
  - Upload and Execute
  - Remote Edit Service
- Update Server
  - From URL
  - From File

https://en.wikipedia.org/wiki/DarkComet

Dark Comet

- Fun Features
  - Fun Manager
  - Piano
  - Message Box
  - Microsoft Reader
  - Remote Chat

History

- Syria
- Target Gamers, Military and Governments
- Miss Teen America
- Je Suis Charlie

https://en.wikipedia.org/wiki/DarkComet

Poison Ivy

- Typical Windows RAT abilities
- Encrypted Communications
- Poison Ivy builder kit
  - Custom Password
  - Custom Port

History

- admin@338
- th3bug
- menuPass
- RSA / SecureID
- Nitro
- “strategic web compromise”

DEMO TIME

Thank You!

Any Questions?

Joshua Barone

joshua.barone@gmail.com

@tygarsai