Sign in

This repository has been archived by the owner on Oct 21, 2024. It is now read-only.

kavika13 / **RemCom** Public archive

🔔 Notifications   🔱 Fork **94**   ☆ Star **336**

⟨⟩ Code   ⊙ Issues **28**   ⊰↰ Pull requests **2**   ▷ Actions   ▦ Projects   📖 Wiki   ⊘ Security   ⁓ Insigh

⎇ master ⌄   ⁑   🏷

Go to file   ⟨⟩ Code ⌄

🕘

📁 ProcComs		
📁 RemComSvc		
📁 bin		
📄 .gitignore		
📄 ProcFunctions.cpp		
📄 ProcFunctions.h		
📄 README.md		
📄 RemCom.cpp		
📄 RemCom.dsp		
📄 RemCom.dsw		
📄 RemCom.h		
📄 RemCom.rc		
📄 RemCom.vcxproj		
📄 Remote Command Ex...		

About

Remote Command Executor: A OSS replacement for PsExec and RunAs - or Telnet without having to install a server. Take your pick :)

🔗 talhatariq.wordpress.com/2006/...

📖 Readme

╴╱╲╴ Activity

☆ **336** stars

◉ **30** watching

⑂ **94** forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

● C++ 95.9%   ● C 4.1%

📄 clean.cmd

📄 resource.h

📖 **README**

#RemCom

This is a fork of the RemCom project, since that project seems dead, and there are patches to be made.

For the most "official" documentation of this branch, see the wiki. The rest of this description is a placeholder for now.

Changes since fork:

From their site:

RemCom - The open source psexec

Terminal Services are expensive in terms of bandwidth, Utilities like GotoMyPC and remote control programs like PC Anywhere let you execute programs on remote systems, but they take time to set up and require that you install client software on the remote systems that you wish to access and are extremely costly when it comes to running just some administrative commands over a group of systems.

What is RemCom : RemCom is a small (10KB upx packed) remoteshell / telnet replacement that lets you execute processes on remote windows systems, copy files on remote systems, process there output and stream it back. It allows execution of remote shell commands directly with full interactive console without having to install any client software. On local machines it is also able to impersonate so can be used as a silent replacement for Runas command.

Platform and Language : RemCom is written in C++ and works on NT 4.0, Win2K, Windows XP and Server 2003 including x64 versions of Windows.

Project Insipiration : Mark Russinovich [sysinternals] Psexec.

Backgound: I started this this project to make my own RAT [Remote Administration Tool]. Before this for numerous tasks i used the sysinternals pstools, but my ability to use / extend it was always limited by its liscensing and usage terms. That is why started of writing my own version of something similar to psexec and RemCom was the result.

Some Features :

- RemCom is open source :) ([source available here](#)).
- You can run as many remote commands on the machine as you want
- You can execute internal commands (net, netsh, ipconfig) directly : RemCom \foo-bar-system net start snmp
- You can start a light "telnet" connection with a remote machine without any telnet server : RemCom.exe \foo-bar-system cmd
- You can also copy any file on the remote machine and receive its output.
- RemCom creates a small (< 1 KB) service on the remote machine (which it extracts it from itself at runtime).
- All communication is done via named pipes & RPC .
- The application removes its traces of the connection and the service on successful disconnect (neat huh?). RemCom is also used in OCS Inventory NG. See [this post](#).

Future Roadmap :

- A Pretty UserInterface.
- Multi Consoles in a single session.
- A builtin option for fetching files.

Any comments, bugs, wishlists: email to: talha [dot] tariq [at] gmail [dot] com

Source & Download : The most recent version of RemCom is available here