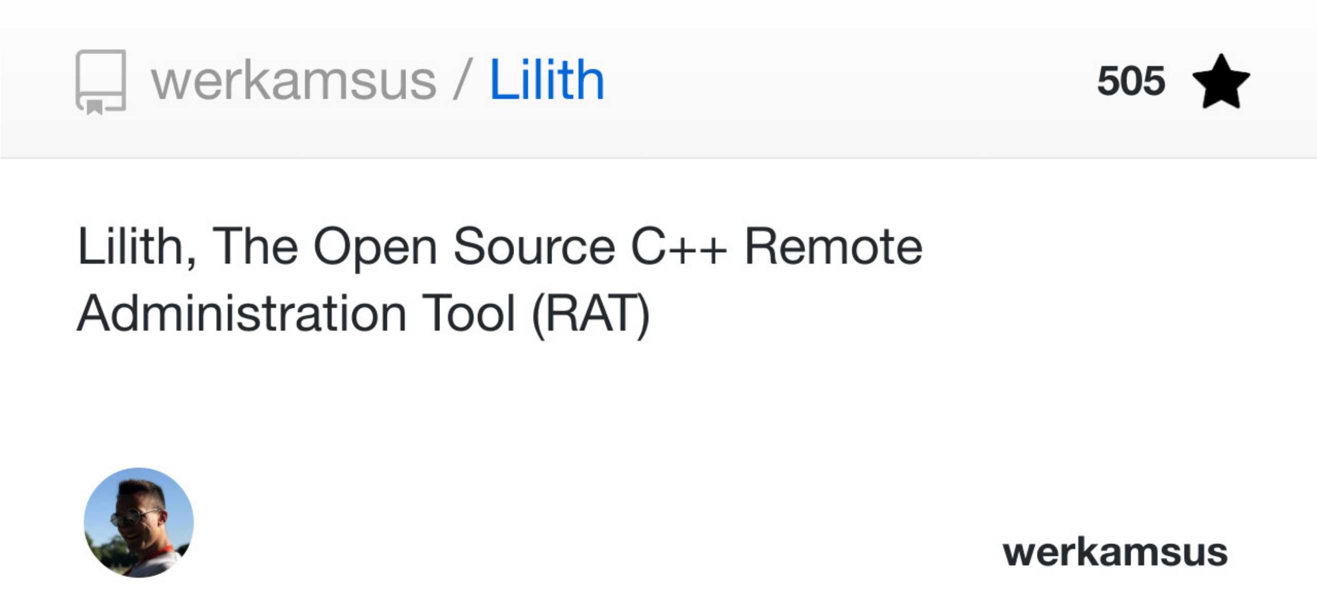
werkamsus/Lilith: Lilith, The Open Source C++ Remote Administration Tool (RAT)

github.com/werkamsus/Lilith

werkamsus



werkamsus / Lilith 505 ★

Lilith, The Open Source C++ Remote Administration Tool (RAT)

werkamsus

Lilith

build passing license MIT

Free & Native Open Source C++ Remote Administration Tool for Windows

Lilith is a console-based ultra light-weight RAT developed in C++. It features a straight-forward set of commands that allows for near complete control of a machine.

Disclaimer

The use of this software on any device that is not your own is highly discouraged. You need to obtain explicit permission from the owner if you intend to use Lilith in an alien environment, any illicit installation will likely be prosecuted by the jurisdiction the (ab)use occurs in.

Youtube

Features

- Remote Command Execution via
  - CMD
  - Powershell
  - **Any** other console app
- Keylogger **(new)** [16.09.2017]
- Execute predefined Scripts **(new)** [16.09.2017]
- Extreme Modularity (see this)
- Broadcast Commands to all Clients **(new)** [15.09.2017]
- Multiple Connections
- Auto-Install
- Startup Persistence
- Self-Erases
- DNS Resolving
- Low Latency & Bandwith use
- Error-Handler with logs

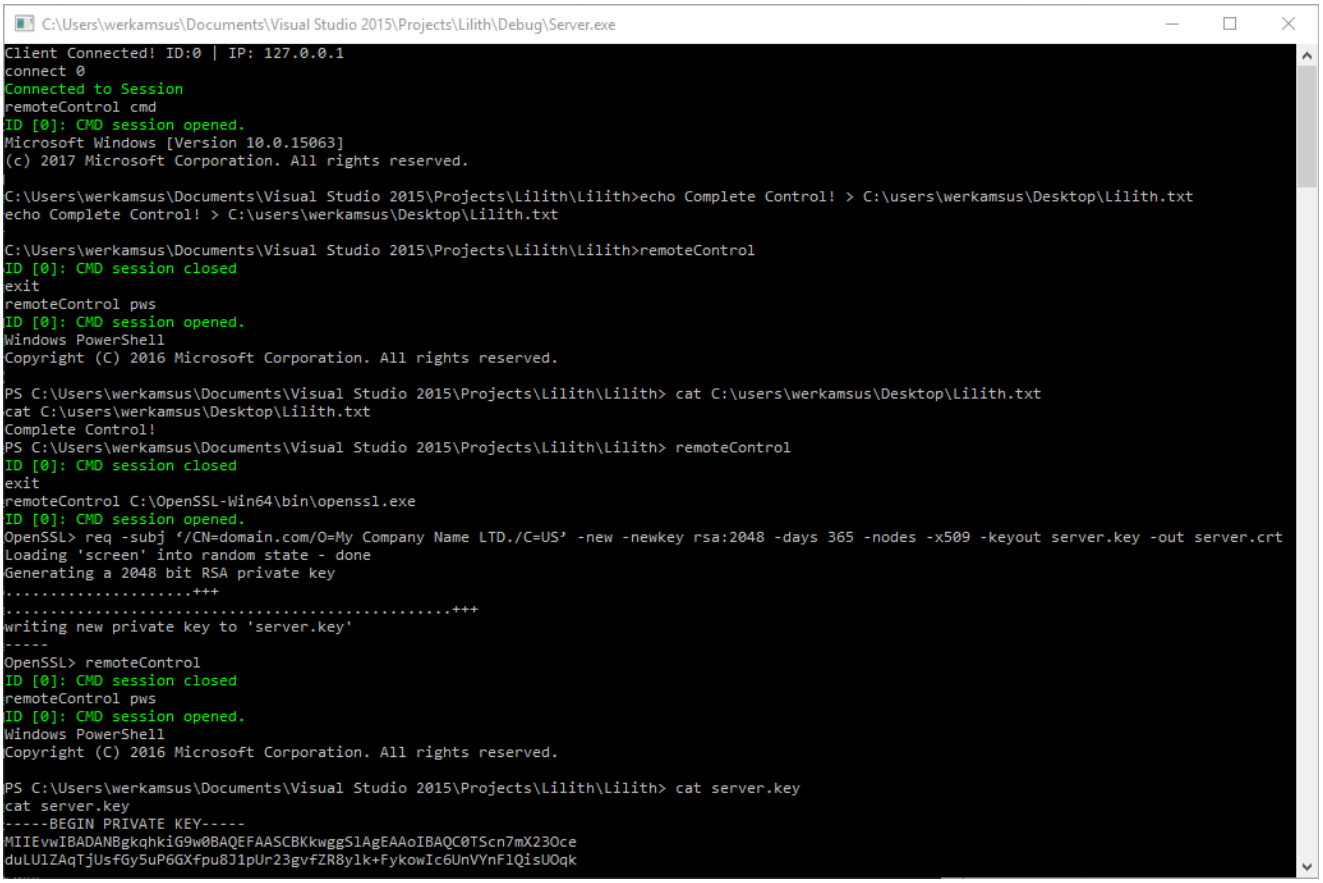
Modularity

The modularity and expandability of this RAT are what it's been built on. That's how it manages to stay very compact, light-weight and fast. You can download other utilities like password recovery or keylogging tools via Powershell scripts (link to some useful scripts will follow soon) and then execute them as if they were running on your own machine. Afterwards you're able to upload the results (also with a ps script) or evaluate them on the spot (via the `type` command) in cmd.

Commands

Command	Syntax	Comment
connect	`connect <clientID>` (`connect 0`)	Connects to a Client
exitSession	`exitSession`	Exits current session
switchSession	`switchSession <clientID>` (`switchSession 2`)	Switches to another Client
broadcast	`broadcast`	Broadcasts your commands to all clients
keydump	`keydump`	Dumps Keylog File
script	`script <scriptname> <scriptparameter>` (`script keydump keylog.txt`)	Executes a predefined Script

Command	Syntax	Comment
listClients	`listClients`	Displays the number of clients connected
remoteControl	`remoteControl <C:\program.exe>` OR `remoteControl cmd`	More Info
remoteControl	`remoteControl`	Exits remoteControl if already in remoteControl
restart	`restart`	Restarts the Client
kill	`kill`	Quits the Client


C:\Users\werkamsus\Documents\Visual Studio 2015\Projects\Lilith\Debug\Server.exe

```
Client Connected! ID:0 | IP: 127.0.0.1
connect 0
Connected to Session
remoteControl cmd
ID [0]: CMD session opened.
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\werkamsus\Documents\Visual Studio 2015\Projects\Lilith\Lilith>echo Complete Control! > C:\users\werkamsus\Desktop\Lilith.txt
echo Complete Control! > C:\users\werkamsus\Desktop\Lilith.txt

C:\Users\werkamsus\Documents\Visual Studio 2015\Projects\Lilith\Lilith>remoteControl
ID [0]: CMD session closed
exit
remoteControl pws
ID [0]: CMD session opened.
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\werkamsus\Documents\Visual Studio 2015\Projects\Lilith\Lilith> cat C:\users\werkamsus\Desktop\Lilith.txt
cat C:\users\werkamsus\Desktop\Lilith.txt
Complete Control!
PS C:\Users\werkamsus\Documents\Visual Studio 2015\Projects\Lilith\Lilith> remoteControl
ID [0]: CMD session closed
exit
remoteControl C:\OpenSSL-Win64\bin\openssl.exe
ID [0]: CMD session opened.
OpenSSL> req -subj ‘/CN=domain.com/O=My Company Name LTD./C=US’ -new -newkey rsa:2048 -days 365 -nodes -x509 -keyout server.key -out server.crt
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....................+++
..................................................+++
writing new private key to 'server.key'
-----
OpenSSL> remoteControl
ID [0]: CMD session closed
remoteControl pws
ID [0]: CMD session opened.
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\werkamsus\Documents\Visual Studio 2015\Projects\Lilith\Lilith> cat server.key
cat server.key
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQC0TScn7mX23Oce
duLU1ZAqTjUsfGy5uP6GXfpu8J1pUr23gvfZR8ylk+FykowIc6UnVYnFlQisUOqk
```

General Description

At the core of this RAT lies it's unique ability to remotely execute commands via CMD, Powershell and almost all console-based applications. It has the capabilities to automatically install on startup and clean up behind itself. It also features an error-handler that logs any issues. As of now, it is not 100% stable. Under 'normal' conditions it runs smoothly and without any disturbances, but severe irregularities in input (i.e. messing around with it *a lot*) may cause crashes. This will be resolved in the near future.

Requirements

- None!
- Supported Operating Systems (32/64-bit)
    - Windows XP SP3
    - Windows Server 2003
    - Windows Vista
    - Windows Server 2008
    - Windows 7
    - Windows Server 2012
    - Windows 8/8.1
    - Windows 10

To-Do

More Info on Commands

remoteControl

Shortcuts are: `cmd` , `pws` , `pws32` which stand for Command Prompt, Powershell and Powershell 32-Bit respectively. You can use these instead of a full path to the executable. Example: `remoteControl pws` will remote-control `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe` .