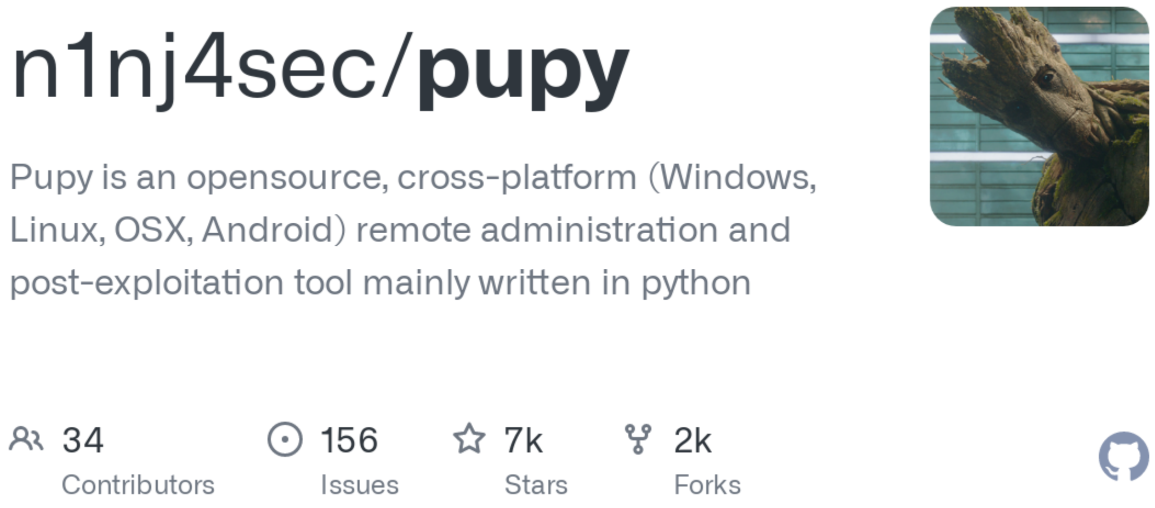
Pupy

github.com/n1nj4sec/pupy

n1nj4sec



n1nj4sec/**pupy**

Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python

34 Contributors

156 Issues

7k Stars

2k Forks

build passing

Installation

Installation instructions are on the wiki, in addition to all other documentation. For maximum compatibility, it is recommended to use Docker Compose.

Refer to the wiki

Description

Pupy is a cross-platform, multi function RAT and post-exploitation tool mainly written in python. It features an all-in-memory execution guideline and leaves a very low footprint. Pupy can communicate using multiple transports, migrate into processes using reflective injection, and load remote python code, python packages and python C-extensions from memory.

Features

- Windows payload can load the entire Python interpreter from memory using a reflective DLL.

  Pupy does not touch the disk.
- Can be packed into a single .py file and run without any dependencies other than the python standard library on all OSes.

  PyCrypto gets replaced by pure Python AES & RSA implementations when unavailable.
- Reflectively migrate into other processes.
- Remotely import pure python packages (.py, .pyc) and compiled python C extensions (.pyd, .so) from memory.

  Imported python modules do not touch the disk.
- Easily extensible, modules are simple to write and are sorted by os and category.
- Modules can directly access python objects on the remote client using rpyc.
- Access remote objects interactively from the pupy shell and get auto-completion of remote attributes.
- Communication transports are modular and stackable. Exfiltrate data using HTTP over HTTP over AES over XOR, or any combination of the available transports.
- Communicate using obfsproxy pluggable transports.
- Execute noninteractive commands on multiple hosts at once.
- Commands and scripts running on remote hosts are interruptible.
- Auto-completion for commands and arguments.
- Custom config can be defined: command aliases, modules. automatically run at connection, etc.
- Open interactive python shells with auto-completion on the all-in-memory remote python interpreter.
- Interactive shells (cmd.exe, /bin/bash, etc) can be opened remotely.

  Remote shells on Unix & Windows clients have a real tty with all keyboard signals working just like an SSH shell.
- Execute PE executable remotely and from memory.
- Generate payloads in various formats:

Format	Architecture	Short Name
Android Package	x86 & ARMv7	apk
Linux Binary	x86	lin_x86
Linux Binary	x64	lin_x64
Linux Shared Object	x86	so_x86
Linux Shared Object	x64	so_x64
Windows PE Executable	x86	exe_x86
Windows PE Executable	x64	exe_x64
Windows DLL	x86	dll_x86
Windows DLL	x64	dll_x64
Python Script	x86 & x64	py
PyInstaller	x86 & x64	pyinst
Python Oneliner	x86 & x64	py_oneliner
Powershell	x86 & x64	ps1
Powershell Oneliner	x86 & x64	ps1_oneliner
Ducky Script	N/A	rubber_ducky

- Deploy in memory from a single command line using python or powershell one-liners.
- Embed "scriptlets" in generated payloads to perform some tasks "offline" without needing network connectivity (ex: start keylogger, add persistence, execute custom python script, check_vm, etc.)
- Multiple Target Platforms:

Platform	Support Status
Windows XP	Supported
Windows 7	Supported
Windows 8	Supported
Windows 10	Supported
Linux	Supported

Platform	Support Status
Mac OSX	Limited Support
Android	Limited Support

Documentation

All documentation can be found on the wiki.

Refer to the wiki

FAQ

> Does the server work on windows?

Pupy has not been tested on Windows. Theoretically, it should work on any platform that supports Docker and Docker Compose. However, you will need to adapt the Docker Compose installation instructions for the Windows platform.

> I can't install Pupy. The installation fails.

1. Please refer to the wiki. It is possible that your answer is there.
2. Search the Github issues and see if your issue was already solved.
3. If you issue was not solved, open a new issue following the issue guidelines.

If you do not follow these steps, you issue will be closed.

> Android and/or Mac OSX payloads and modules don't work.

Pupy has *limited* support for Android and OSX. These platforms may not be well maintained and may break intermittently. Some modules (i.e. keylogger) may be missing for these platforms.

Development

If some of you want to participate to pupy development, don't hesitate! All help is greatly appreciated and all pull requests will be reviewed.

Also there is small note about development. Please run flake8 before doing any commits. File with config is here.

Contact

Platform	Contact Info
Email	contact@n1nj4.eu
Twitter	https://twitter.com/n1nj4sec

This project is a personal development, please respect its philosophy and don't use it for evil purposes!

Special thanks

Special thanks to all contributors that help improve pupy and make it a better tool! :)