Poison Ivy 2.3.0 Documentation

http://posionivy-rat.com

It is recommended that all users read through this document before using Poison Ivy.

Contents:

I. Description and features

Poison Ivy is an advanced remote administration tool for Windows (the client is reported to run on WINE or other emulators on various Linux/UNIX flavors), written in pure assembly (server), and Delphi (client).

The server contains no dependencies of any kind, and runs on 2000/XP/2003/Vista.

Since version 2.3.0, the server size is dependent on the settings, which means additional features (like key logger, etc.), will make the final server larger.
Even so, the maximum size of the server is around 7KiB, unpacked.

Being independent code, the server builder can produce PEs, or shellcode(in the form of arrays for C, Delphi, Python, or raw binary), depending on your needs.

The most important features are encrypted communications (256bit Camellia), compressed communications, full-featured file manager, registry manager, key logger, services manager, relay server, process manager, remote audio capture, screen capture, web cam capture, multiple simultaneous transfers, password manager, and the ability to share servers, based on privilege levels, and various other things that you will find useful.

Poison Ivy is also special compared to other similar tools, because the server doesn't need to be updated, even if new features are added.

Even though the server supports 3rd party plugins, it's important to know that all the features not listed in the “Plugins” section are self-contained in the server, and no additional files are used at any time.

The plugins (as well as the server and key logger file) are stored encrypted in ADS (Alternative Data Stream) on NTFS partitions (they are stored normally on FAT32).

Check the official website for screen shots.

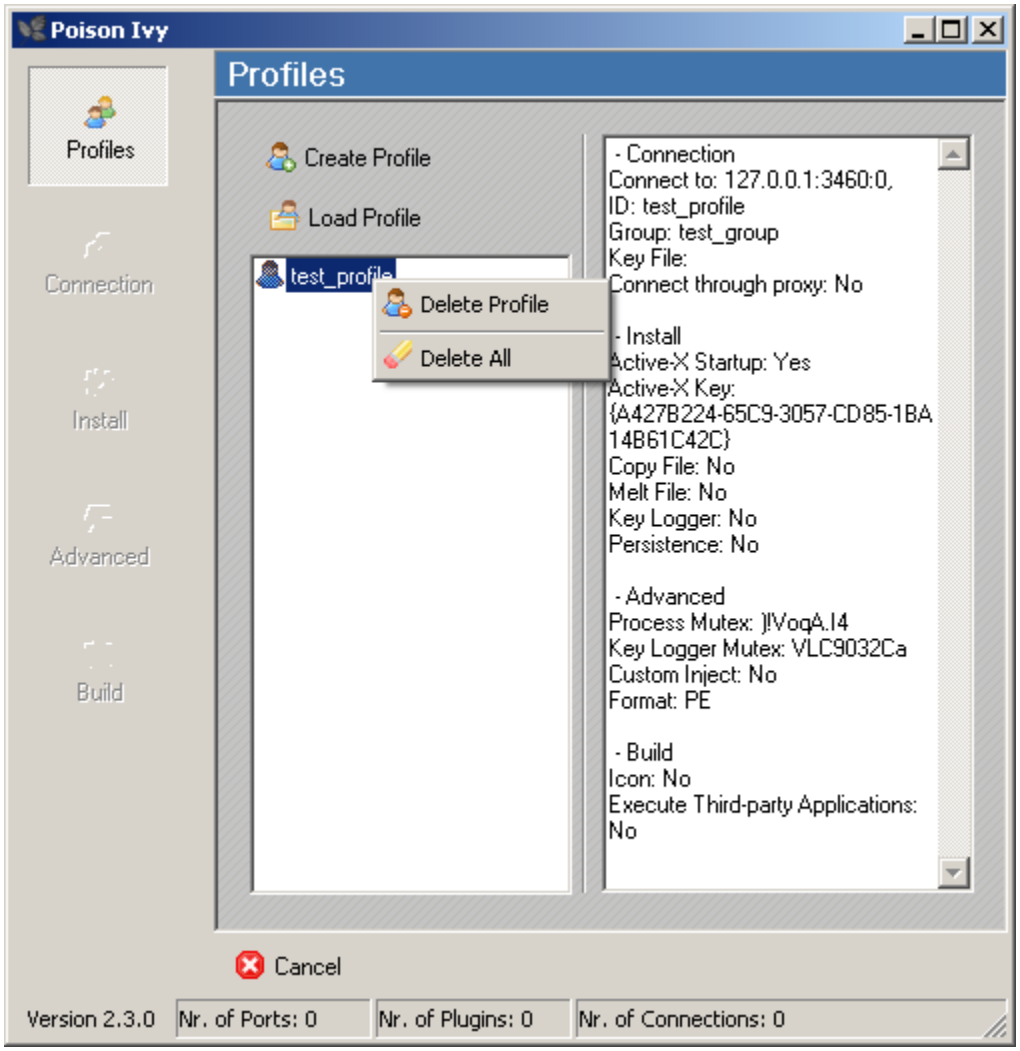
This document doesn't describe all the various features of the application, but tries to cover the basics.

The GUI is assumed to be self-explanatory, so users with a decent level of experience will have no problems discovering the features and using the application to its full potential.

On the other side, users which lack the very basic network skills (forwarding a port, knowing what a port is in the first place, knowing how a client - server application is supposed to work) or better off learning these things first before attempting to use Poison Ivy.

II. Building a Server

To build a new server, you need to start the application, and select “File” -> “New Server”.
You will see a screen similar to the following:



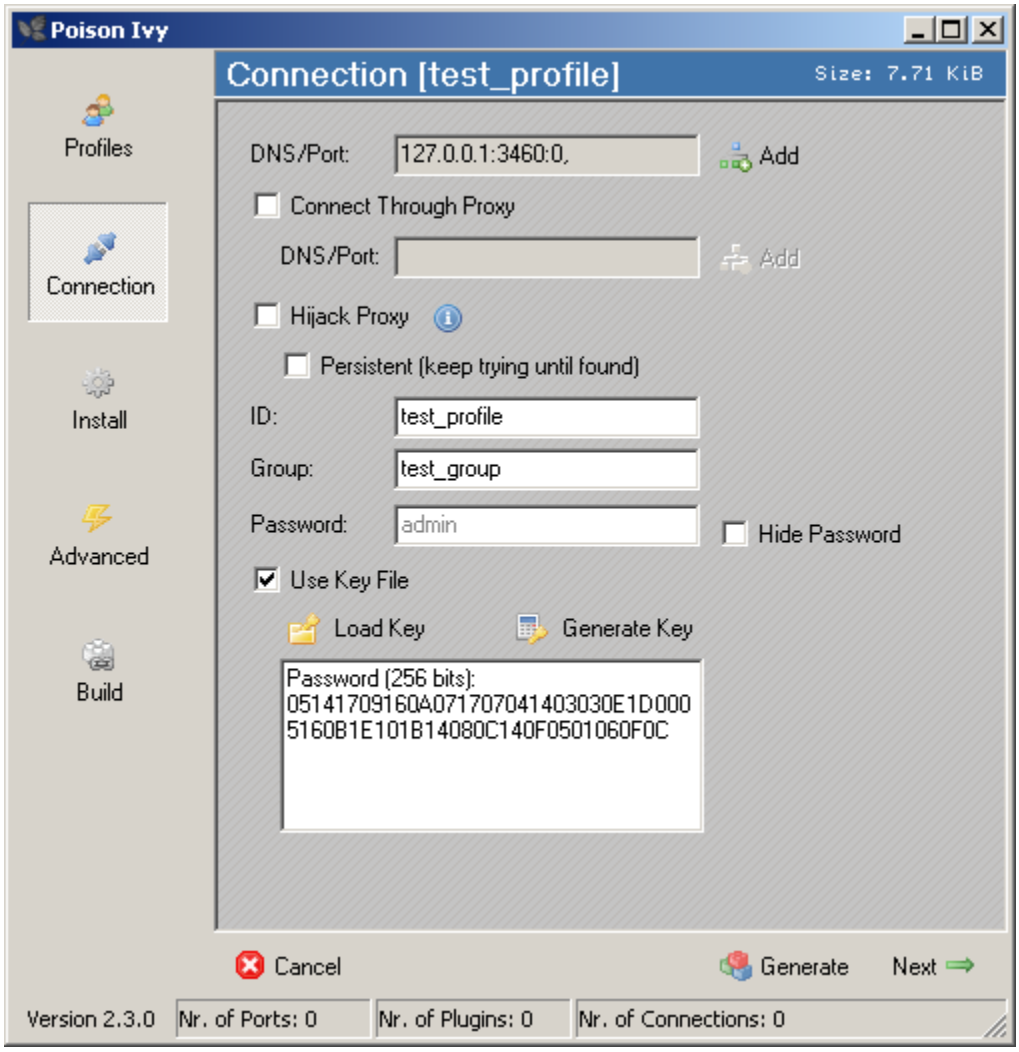
As you can see above, you can easily manage your profiles.

First, you will want to create a new profile, by pressing “Create Profile”, and selecting a name.

You will notice that until you create your profile, you need to go through each section (on the right, the others being disabled). After you have created the profile, you are able to edit anything is whatever section.

This behavior is intentional, to prevent skipping a section by mistake.

Next, in the “Connection” section, you should see the something like this:



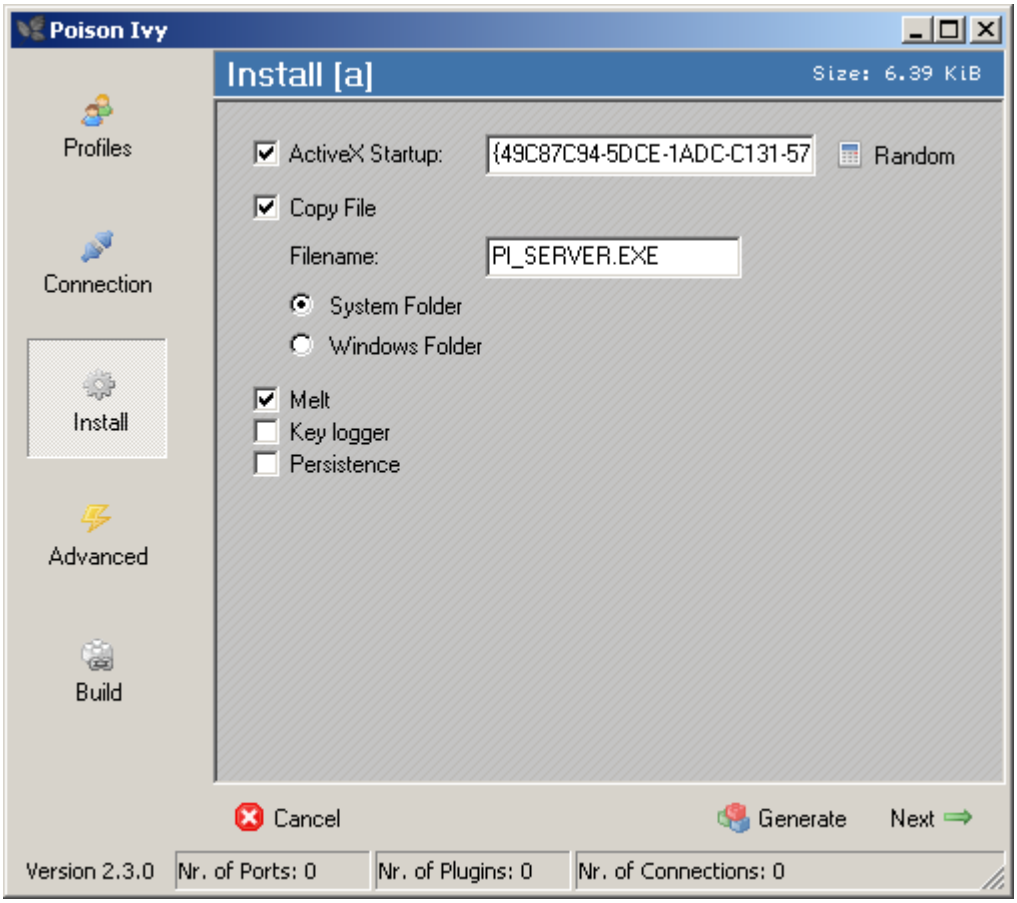
Since PI is a “reverse connection” administration tool, you need to specify at least one valid DNS/IP and a Port combination where the server will find a listening client.
You do this with the “Add” button.

Generally it is a good idea to “Test Connection” after you have set everything up (for this to work, a client must be listening, with the correct password/port, and the DNS/IP must be valid and must point to the client).

The password can be a user-defined string, or you can use a random-generated key file (recommended).
The key file will be saved in the “Profiles” directory, and will be named <profilename>.pik.
In either cases, losing your password/key file will make you unable to connect to the specified server.

Starting with v2.3.0, a server can be assigned to a group, for easier management.

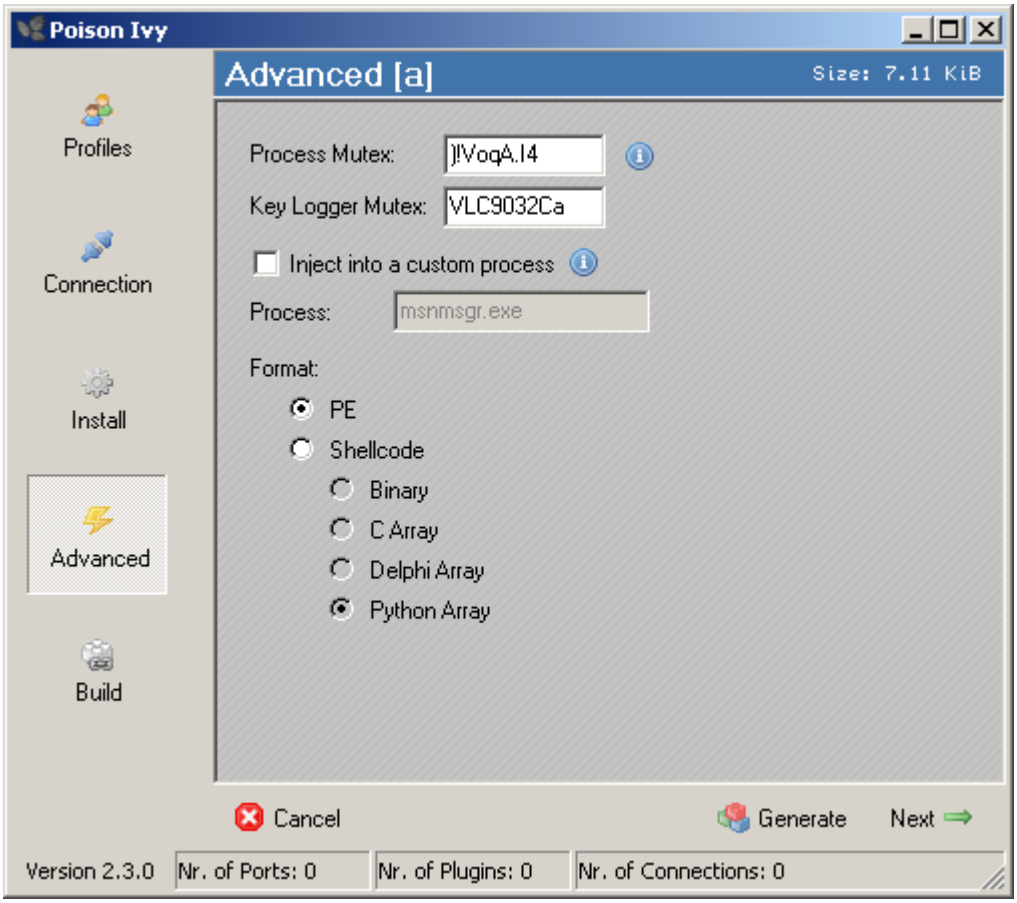
Press “Next ->” at the bottom to get to the “Install” section.



The “Persistence” option, worth an explanation here, will monitor the default browser process (or another process if specified in “Advanced” section), and restart it if it gets closed, as well as monitoring registry startup entries for deletion.

It will also keep the server file locked (to prevent deletion), since the server is actually running inside other processes.

The “Advanced” section:



If you don't know what these options mean, it's best to leave them as they are.

Regarding the shellcode, it ends with 'ret', which means it doesn't ExitProcess.

Finally, in the “Build” section, you get to choose and icon (this will obviously increase server size) if you like, and optionally execute another application, possibly to pack the server.

If you chose and icon, and want to revert to the 'no-icon' state, right click on the icon box.

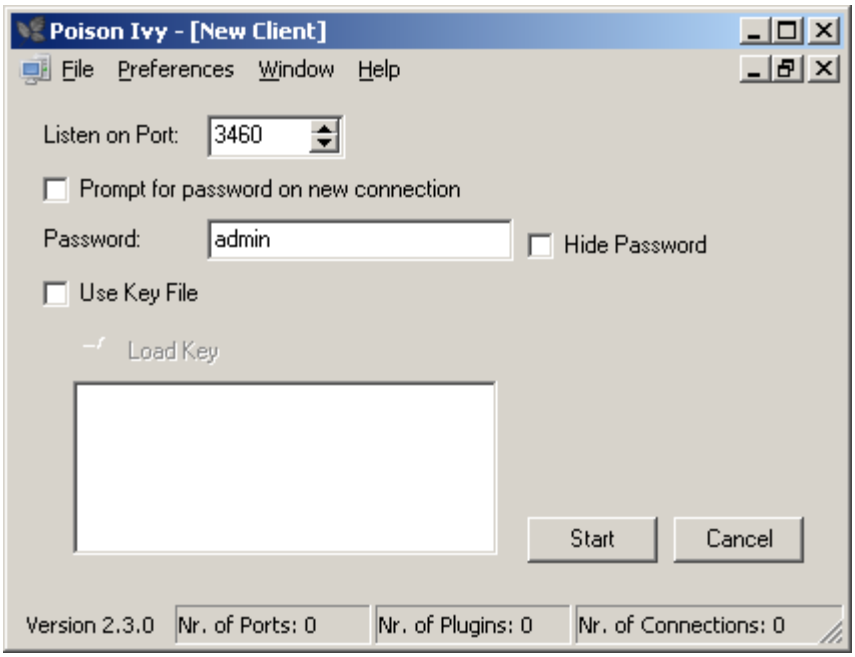
The last step is to hit “Build” and save your server to the desired location.

The profile is automatically saved.

III. Accepting Connections

In order to accept connections, you must set up your network, i.e. forward a port if you need to, punch a hole in your firewall, make sure your software firewall allows the Poison Ivy client to listen, etc.
These preparations are beyond the scope of this document.

Start the client, and go to the “File” -> “New Client” menu:



Enter the port/password/key file you used when building the server, and press “Start”.
You can have multiple clients listening on different ports, with different passwords, etc.

You are now ready to accept connections, which will appear in the list that will pop up.

To use a server, double click on its connection.
Right clicking on a connection reveals various options.

IV. General usage and information

You will notice that the GUI is pretty much self-explanatory, and most of the buttons/etc that do not have a text description have a tool tip.
The general rule of thumb is that right-clicking shows the options.

If a connection appears in the list with red, it means that the server is outdated.
To take advantage of the new features, and update the server, simply restart it (right click and select “Restart”).

To display current transfers, there's a button at the top (with a corresponding tooltip) of the window, when using a server.
When the transfer view is shown, you will be able to pause/cancel transfers.

Authentication is based on challenge-response, so it's invulnerable to replay attacks (every time the challenge is a different random chuck of data).

The server has a (reasonably high) connection limit, which is intended to prevent misuse of the application (botnets, etc.)

Be advised that modifying the server in any way might render it unusable.
The author does not offer support of any kind if you played with the server.

V. Plugin System

On the server side, plugins are stored encrypted in the ADS (on NTFS).

Old plugin versions on the server side are updated automatically if the client has a newer version.

To load a plugin, goto “File” -> “Manage Plugins” menu.
Click the “Load” button, and select the file ending in “C”, like mypluginC.dll. The “C” at the end means that the specified dll is for the client.
In order to load a plugin, the corresponding server dll must be present in the same folder.

There should be a plugin SKD in the PI package, along with an example plugin, with source.
Consult both of them when writing plugins.

VI. FAQ

Q: I can't extract the archive contents, or i can't execute the client.
A: You probably have an anti virus application running. Disable it and try again.

Q: The remote server is working fine, until it suddenly disappears, and i can't connect anymore.
A: The other user might be running an anti virus application, which picks up the server and deletes it.

Q: The client seems to be connecting somewhere. What's going on?
A: By default, the client connects to the poison ivy website and retrieves the latest version number, which is compared to the version you have. If you run an older version, you are notified. This can be turned off in “Preferences”.

Q: When retrieving the key log file, parsing/displaying it takes a very long time.
A: For very long key log files (also depends on your CPU), you might want to disable 'Key log colors' in the 'Settings' tab.

Q: Sometimes it takes very long for a server to connect, even if the other computer is online.
A: This is because the interval at which the server tries to establish connection with the client is dynamic, and you probably started the client just before the longest interval. Be patient.

Q: I modified the client file (in any way), and it will no longer run.
A: As stated above, do not modify the client application in any way. Re-download it.

Q: Can i pack/crypt the server?
A: On your own responsibility.

Q: I packed/encrypted/scrambled the server and it doesn't seem to work.
A: Some packers trash the server. It's not a bug in Poison Ivy.

Q: I found a bug. What do i do?
A: If you're sure it's a bug, and not something else, post an exact description and steps to reproduce it, on the board.

Q: What is this “Camellia encryption”?
A: Camellia is a block cipher, and it was chosen because it is free and unpatented, and offers a very high degree of security. You will find the official document describing it at the Poison Ivy website.

VII. Undetected Versions

You can buy an undetected, unique version of Poison Ivy.

Doing so shows your support to the project, which is provided for free, and helps pay for the hosting/etc expenses,

If you do, you are entitled to another version, should your initial one get detected by anti virus software.

You don't have to worry about future versions either; as said above, servers need to be updated very rarely (in case of major protocol changed), because of the special way Poison Ivy works.
If it's the case, you will receive a new version.

For prices and other details, contact the author.

VIII. Credits and Contact Information

Poison Ivy is written by shapeless.

Beta Testers: Crazy Boris, eNerGie, e-e, giuliano, Heike, hnZ^, Lord, p0ke, redlime, SpyDir.

Thanks also go to: ksv, Andvare, Aphex, Billy Belceb, Caecigenus, Erwan, Gary Darby, Geiger Tamas, Joachim Bauch, Laszlo Toth, Mark James (famfamfam.com), Markus Stephany, Mike Lischke, p0ke, Salvatore Meschini, Th3ChaS3r, TM.

A big thank you goes out to all users who have contributed with ideas to make Poison Ivy even better.

IX. Changelog

v2.3.0

[+] - Feature added
[-] - Feature removed
[*] - Bug fixed on existing feature

[+] New user interface.
    -> Listen on multiple ports.
    -> Save and Load build settings in form of Profiles.
    -> Execute third party applications after build.
    -> Configure the Connection list's columns.
    -> Place connections in groups.
[+] Key File for password.
[+] Connection log.
[+] Highlight File Types in File Manager and File Search.
[+] Route connections through HTTP proxies (possible to mix HTTP and Socks4 proxies).
[+] Proxy Hijack; route through Internet Explorers HTTP or Socks4 proxy settings.
[+] Server file and ALL the files (keylog file and plugins) it drops to disk get stored into the Install Folder's ADS.
[+] Show/unload modules in Process Manager.
[+] Shellcode server. Generate a shellcode of the server in form of: binary, C Array, Python Array and Delphi Array.
[+]Plugin support.
    -> Plugins will be stored in the install folder's ADS (if NTFS).
    -> Optional to store it remotely.
    -> The remote dll (server side) will be loaded in memory and is encrypted on disk.
    -> The remote dll will be automatically updated if a newer version is available locally.
[+] Execute files with parameter.
[+] Notes.
[-] Packet Analyzer has been removed.
[*] ID and Group names are now 255 chars long when building.
[*] Fixed an Uninstall bug on limited accounts when autostart is being used.
[*] When a server disconnects, the client waits for all threads to clean up before removing the connection.
[*] Fixed a bug when downloading drives using Download Folder.
[*] "Test Connection" now runs in an own thread and you can cancel it by pressing OK or Cancel.
[*] "Test Connection" now also tests if the password is correct (not with Proxy DNS).
[*] Fixed a startup bug that occurred when explorer.exe was restarted.
[*] An "Access violation" bug has been fixed in the data transfer.
[*] Auto save in Audio Capture now appends the "Received time" to the file name.
[*] Folders that begin with "." are now visible in file manager.