Malware Design

Decent Malware Makers

Darcy Meyer
Muzammil Hussain
Mella Liang

Implant

The **implant** retrieves commands from the C2 server, carries out those commands, and sends back command results, such as details about the victim computer and looted user information.

Communication Channel / P2P

Some implants communicate directly to the C2 using HTTP. Other implants communicate with the C2 by sending messages to their “parent” implant which then forwards the message on to the C2, and forwards back the reply.

Cryptography

1) Strings in the code are manually encrypted and replaced in the code. When a module runs, the strings that it uses will be decrypted using the cryptography module code.

2) Each implant has the public key of the server. To establish a session, an implant generates a key, encrypts it with the public key of the server, and sends the result to the server.

Situational Awareness

The situational awareness module has a function to get basic information about the computer on which it is running, specifically: the current user, the environment variables, and all information from the `systeminfo` command.

Execution

The execution module allows the operator to execute programs by sending the program name and its arguments. It is also able to run commands in powershell.

File I/O

The file I/O module reads file content when given a file path. It also downloads a file to the victim computer via url when given the url and a file path to download to.

Persistence

For the implant to persist on the computer, its executable file is written to disk and added to the run registry keys.

Looting

The looting module loots the default user’s login information and cookies from the files stored by Google Chrome.

Defense Evasion

When the implant executable is first executed, it will sleep for a random amount of time. Then it will make a few checks.

1) It’s running on a computer without a C:\malware\ch0nky.txt file present.
2) It’s running in a virtual machine.
3) It’s running with a debugger.

If any of those checks are true, the implant will pretend to be a faulty binary by dereferencing a null pointer, which will cause an exception to be thrown and exit the binary.

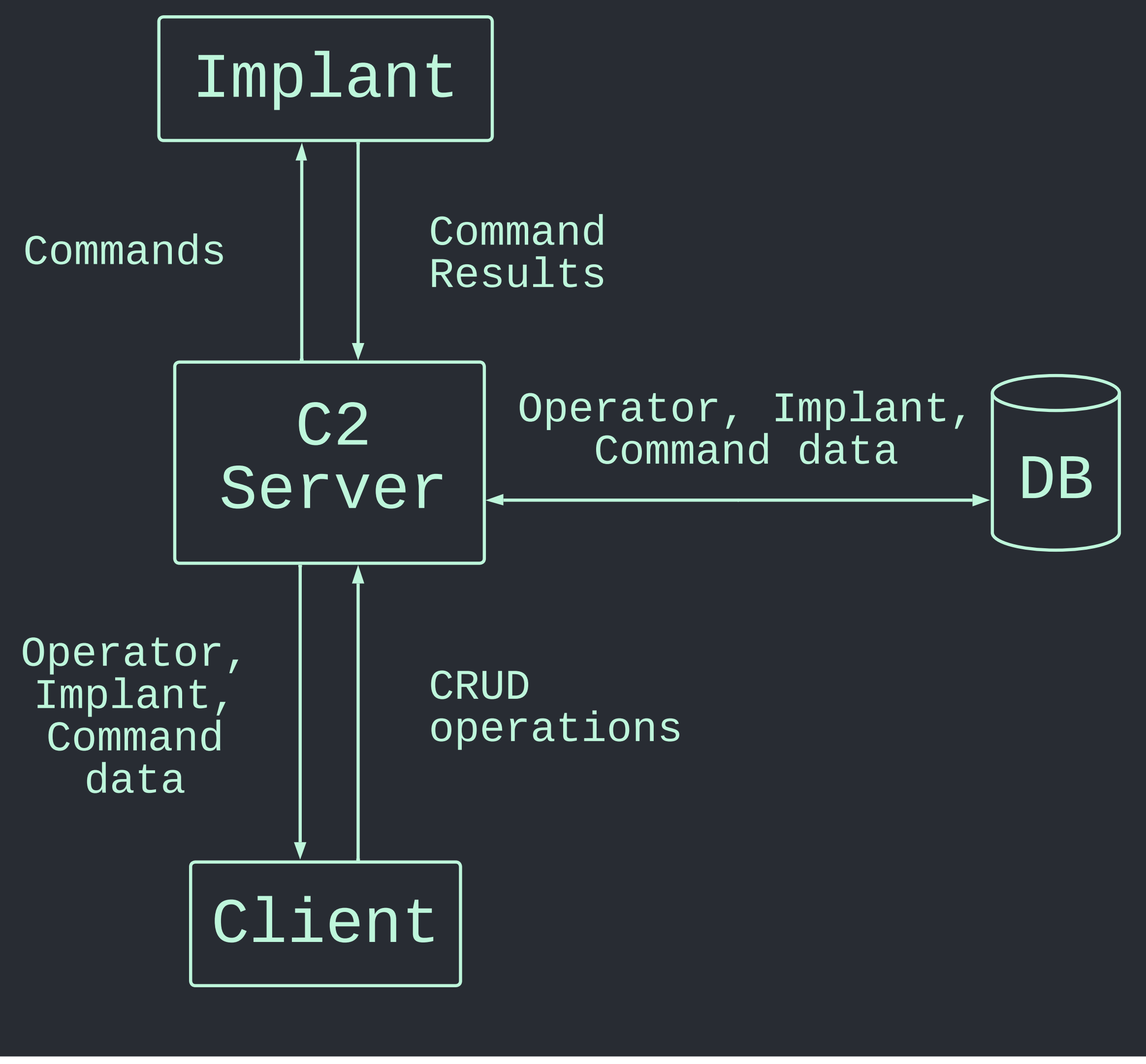
C2 & Client

C2

The C2 server is the middleman between the client and the implant and also the backend to the client. It has a database containing data of operators, implants, and commands; it manages the CRUD operations on those data for the client.

Client

The client is the UI for the server. In the client, an operator could view the list of operators and implants. They could choose an implant, view details on it, send commands, and view the statuses/results of commands.



Implant
Commands
Command Results
C2 Server
Operator, Implant, Command data
DB
Operator, Implant, Command data
CRUD operations
Client