

How to build a C2 framework from scratch

Jakob Friedl

BSidesVienna0x7E9

> whoami

- **Jakob Friedl**
- Penetration Testing @ MM Group
- ~3 years in offensive security
 - Hacking Lab Enjoyer
 - Certification Enjoyer
 - Malware Development Enjoyer
- 6+ months, 200+ commits of “Conquest” C2 development



Chapter 1

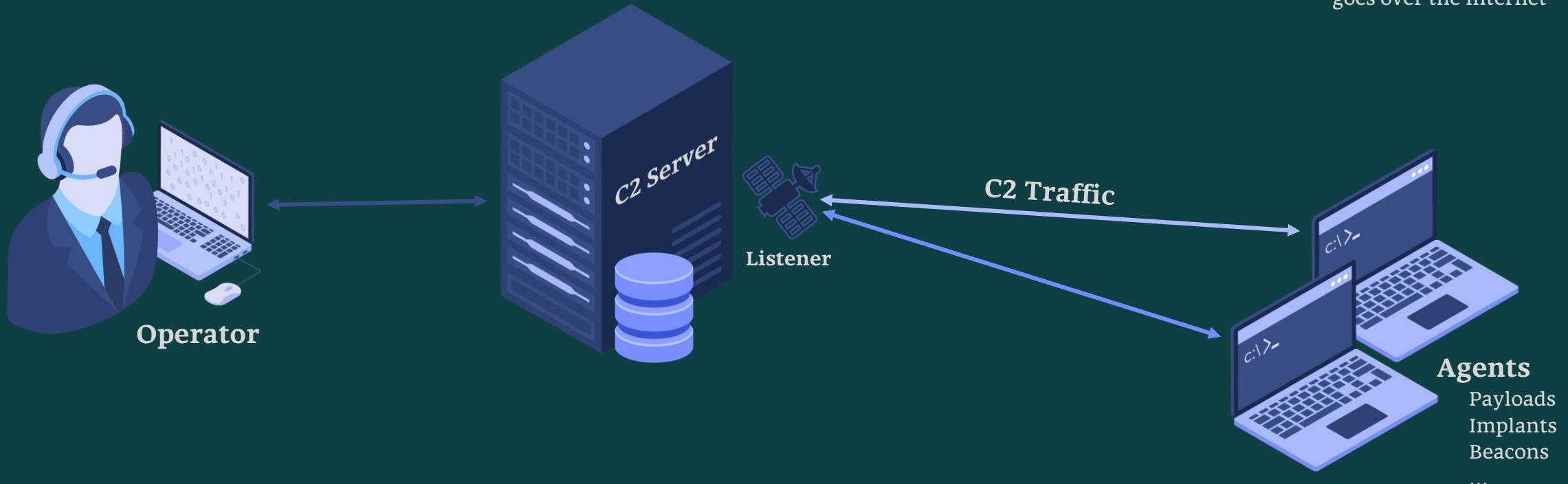
Command & Control 101



MITRE ATT&CK - TA0011

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network.

Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.



C2 Protocols:

HTTP(S)

DNS

SMB

literally anything else that goes over the Internet

Agents

Payloads

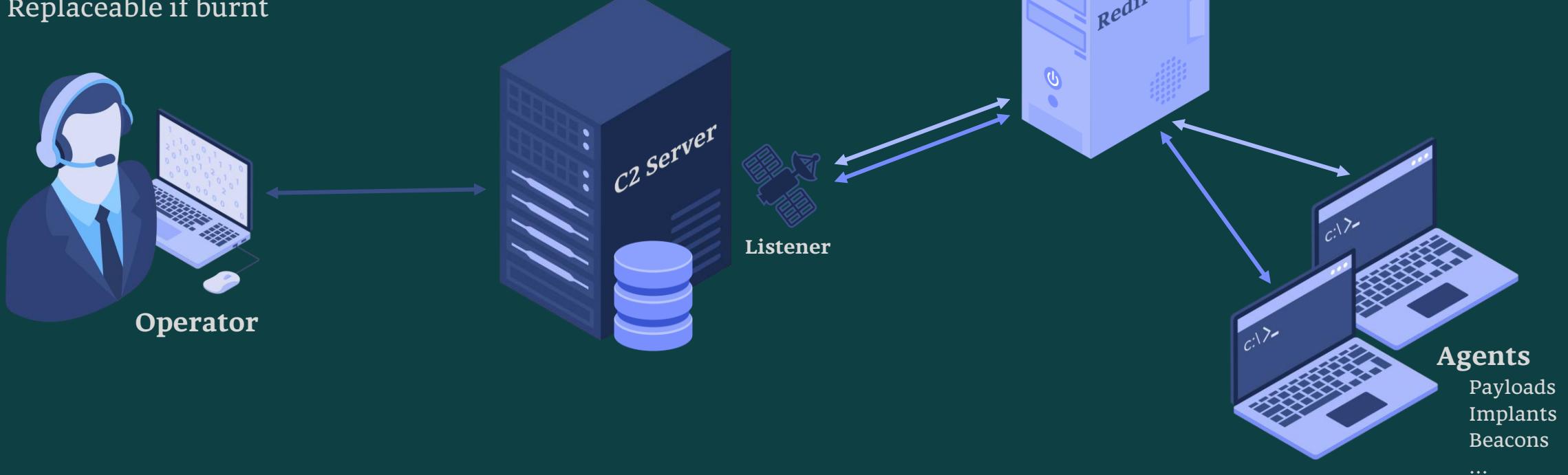
Implants

Beacons

...

C2 Redirectors

- First point of contact for agents
- Forward C2 traffic
- Hide and protect the C2 server
- Replaceable if burnt



C2 Protocols:

HTTP(S)

DNS

SMB

literally anything else that goes over the Internet

Agents

Payloads

Implants

Beacons

...

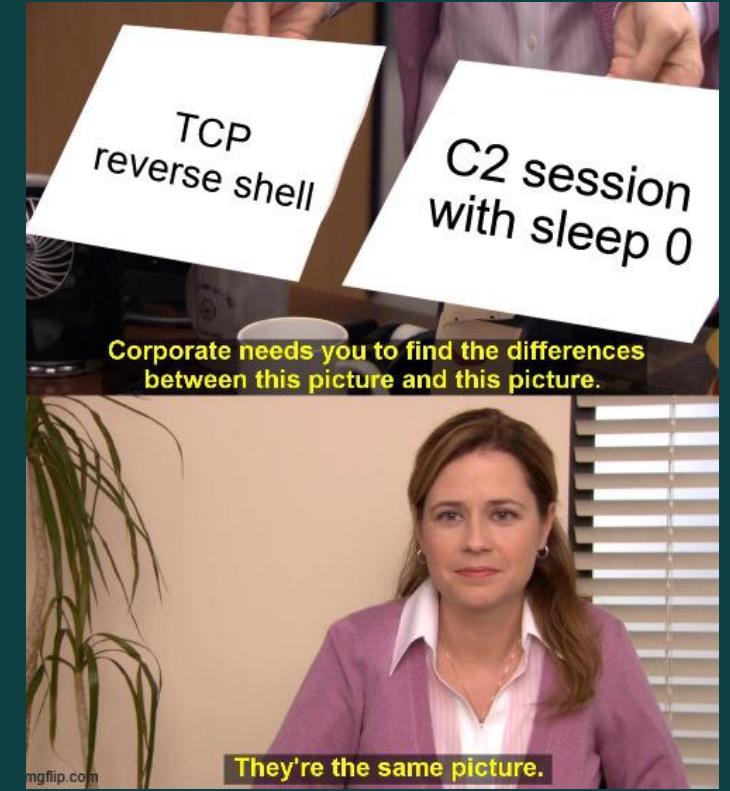
Why C2?

Task queueing

Persistence

Post-exploitation

Multiple sessions & users



C2 Frameworks

More at:
<https://howto.thec2matrix.com/>



Chapter 1.5

Nim 101

Why Nim?

- Enjoyable development experience
- Static type system
- Low-level performance
- Cross-compilation
- Easy access to Windows API using *winim* library



SuedBeyg • 5y ago • Edited 5y ago

Intended selling points of Nim: Statically-typed, native binaries, minimalist syntax, extensive metaprogramming

Actual selling point of Nim: H A C K I N G

(coincidentally, the first useful program I wrote in Nim was a password-brute-forcing script for my cybersec course).

Θ Up 11 Down Reply Award Share ...

A screenshot of a Reddit post by user SuedBeyg. The post discusses the intended and actual selling points of the Nim programming language. The intended selling points include static typing, native binaries, minimalist syntax, and extensive metaprogramming. The actual selling point, however, is hacking, specifically mentioning a password-brute-forcing script written for a cybersecurity course.

Why Nim?

- Enjoyable development
- Static type system
- Low-level performance
- Cross-compilation
- Easy access to VCS

11.8k results (2 s)

Sort by: Most stars

nim-lang/Nim

Nim is a statically typed compiled systems programming language. It combines successful concepts from mature languages like Python, Ada and C/C++.

language nim compiler metaprogramming efficient

Nim · 17.5k · Updated 2 hours ago

zedeus/mitter

Alternative Twitter front-end

privacy twitter nim self-hosted x

Nim · 11.8k · Updated on 12 Oct

WyattBlue/auto-editor

Auto-Editor: Efficient media analysis and rendering

audio video nim audio-editing video-processing

Nim · 3.7k · Updated 8 days ago

byt3b3d3r/OffensiveNim

My experiments in weaponizing Nim (<https://nim-lang.org/>)

Nim · 3k · Updated on 13 May 2024

oakes/vim_cubed

Vim rendered on a cube for no reason

Nim · 2.7k · Updated on 15 Apr 2022

chvanocten/maldev-for-dummies

A workshop about Malware Development

hacktoberfest

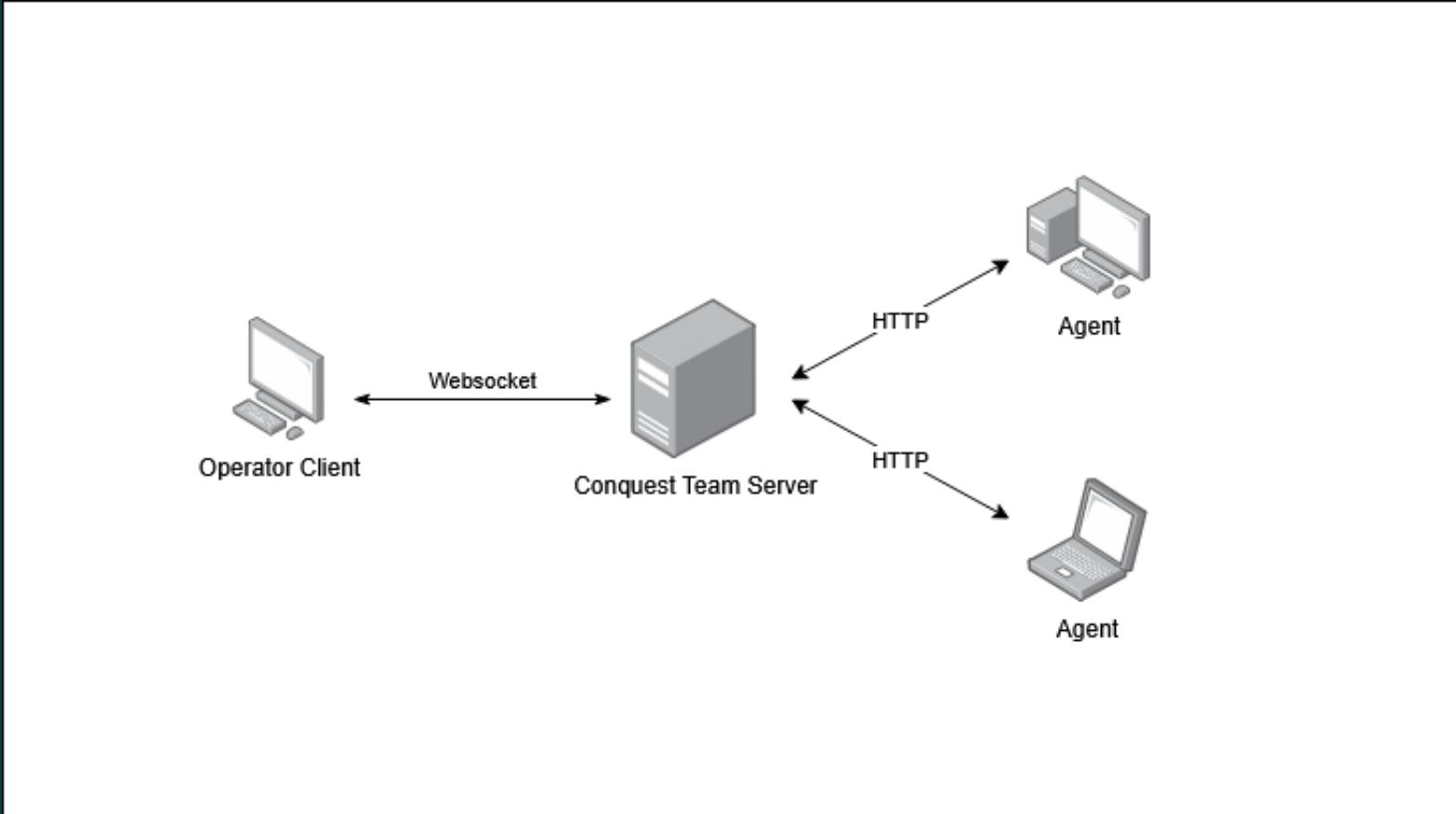
Nim · 1.7k · Updated on 2 Jun 2023



Chapter 2

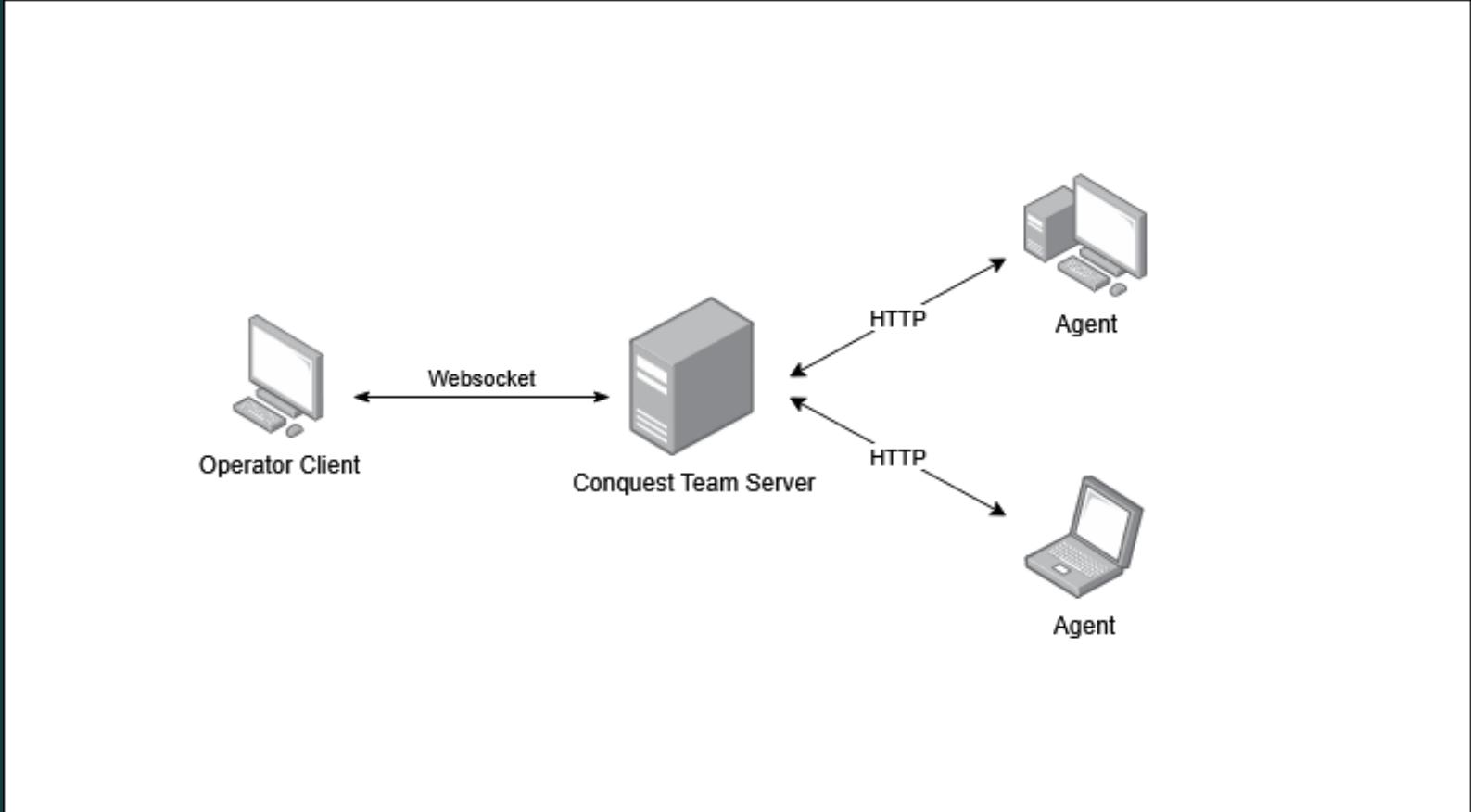
Designing a C2 Framework

Architecture

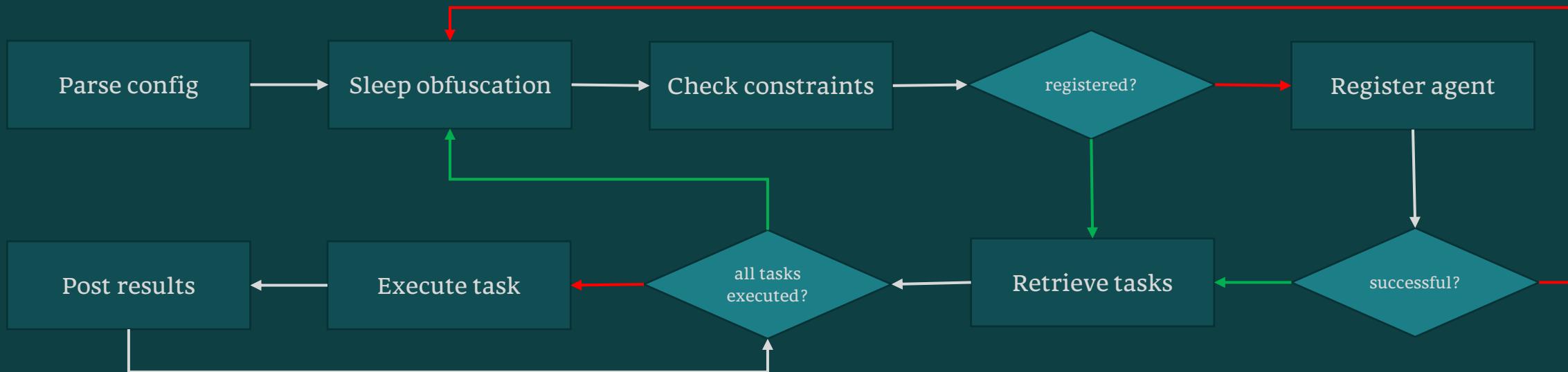


Architecture

- Client tells Server what to do
 - Start Listener
 - Stop Listener
 - Add new task to queue
 - ...
- Server tells Client to update UI
 - New Agent connected
 - Task output received
 - ...
- Agents use HTTP endpoints to GET tasks and POST results

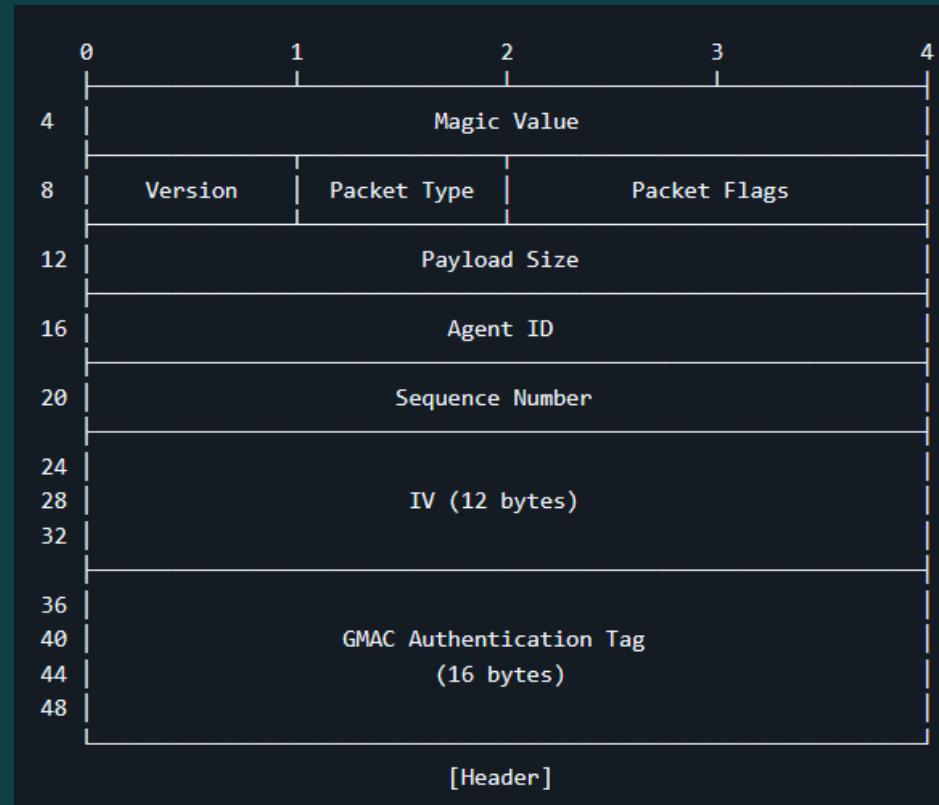


Agent Routine



C2 Communication

- 4 packet types
 - Registration 📝
 - Heartbeat 💬
 - Task 📦
 - Result 🎊
- 48-byte header for packet & agent identification



Protecting C2 Traffic

- C2 traffic contains highly-sensitive data
 - System information
 - Command output
 - Files
 - Credential material
- Packet Encryption 
 - AES256-GCM

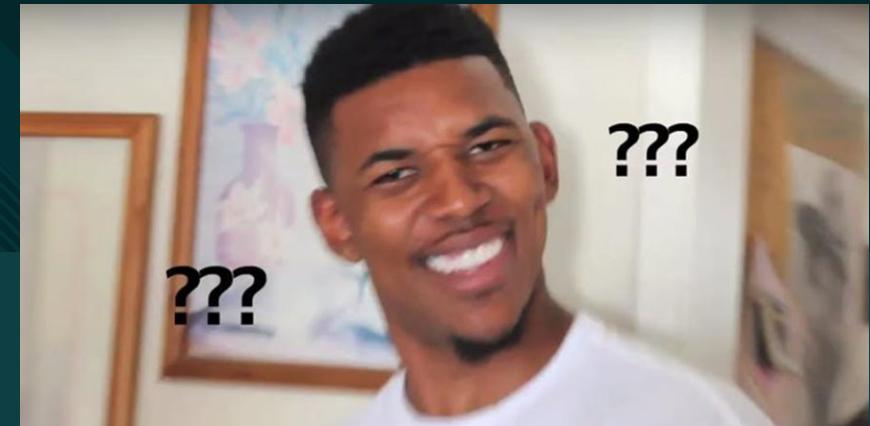


Key Exchange

- ECDH based on X25519
- Encryption key is derived from the shared secret

$$\text{derive}(\text{Server}_{\text{private}} + \text{Agent}_{\text{public}}) = \text{derive}(\text{Server}_{\text{public}} + \text{Agent}_{\text{private}})$$

- Agent is generated with server's public key embedded
- Registration packet contains agent's public key
- Client uses Websocket events to initiate key exchange



Chapter 3

Agent Activities

Activity 1: Sleeping



Sleep Obfuscation

```
monarch.x64.exe (7148) (0x7ff704090000 - 0x7ff704199000)

00000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....  
00000010 b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....  
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000030 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 .....  
00000040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 .....!L.!Th  
00000050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno  
00000060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS  
00000070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 mode....$.....  
00000080 50 45 00 00 64 86 0b 00 f9 ca 0d 69 00 00 00 00 PE..d.....i.....  
00000090 00 00 00 00 f0 00 2e 02 0b 02 02 29 00 18 0c 00 .....).  
000000a0 00 fc 0f 00 00 20 00 00 10 14 00 00 00 10 00 00 .....  
000000b0 00 00 09 04 f7 7f 00 00 00 10 00 00 00 02 00 00 .....  
000000c0 04 00 00 00 00 00 05 00 02 00 00 00 00 00 00 00 .....  
000000d0 00 90 10 00 00 04 00 00 6a f6 10 00 03 00 60 01 .....j.....`.  
000000e0 00 00 20 00 00 00 00 10 00 00 00 00 00 00 00 00 .....  
000000f0 00 00 10 00 00 00 00 10 00 00 00 00 00 00 00 00 .....  
00000100 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 .....  
00000110 00 30 10 00 68 0a 00 00 00 60 10 00 28 02 00 00 .0..h....^...(.  
00000120 00 d0 0e 00 bc 94 00 00 00 00 00 00 00 00 00 00 00 .....  
00000130 00 70 10 00 c4 12 00 00 00 00 00 00 00 00 00 00 .p.....  
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000150 00 a9 0e 00 28 00 00 00 00 00 00 00 00 00 00 00 .....(.....  
00000160 00 00 00 00 00 00 00 b0 32 10 00 70 02 00 00 .....2..p..  
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000180 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 .....text...  
00000190 78 16 0c 00 00 10 00 00 00 18 0c 00 00 04 00 00 x.....  
000001a0 00 00 00 00 00 00 00 00 00 60 00 00 60 00 00 00 .....`.  
000001b0 00 64 01 74 01 00 00 00 00 22 00 00 00 00 00 00 .....
```

Re-read Write Go to... 16 bytes per row Save... Close

```
monarch.x64.exe (7148) (0x7ff704090000 - 0x7ff704199000)  
00000000 3e 51 23 45 e0 d7 f1 70 99 59 95 79 b3 c9 d1 dd >Q#E...p.Y.y....  
00000010 a2 c9 0d c7 5c bb 76 0b bc 1f 26 4d 61 ae ae 47 .....v...&Ma..G  
00000020 0a df 54 4a e2 88 ce 52 63 b8 a5 56 7a dc 2d c6 ..TJ..Rc..Vz.-.  
00000030 cb 5c 06 b0 05 7f cc 41 ec a9 28 5c 2a aa d9 53 .\.....A..(\^..S  
00000040 47 f5 4d ec ae 79 22 02 a3 d1 0c 30 0d 8c a7 f1 G.M.y"....0....  
00000050 85 05 e8 64 d5 98 3e 56 bc 4f 10 4b d3 ec 20 69 ...d..>V.O.K.. i  
00000060 89 93 4d 37 6a 75 31 56 d0 28 ff a0 56 b8 94 40 ..M7julV.(..V..@  
00000070 59 68 cf 19 eb 24 05 75 12 3e cf c3 df 8a 63 cc Yh...$.u.>....c.  
00000080 32 9e 77 db cl 0f c6 99 53 57 64 bc 5c al 4b bd 2.w....SWd.\.K.  
00000090 62 c7 f9 b8 cf cd 24 c1 0d dc 1f 00 c4 f2 6e 1e b.....$.....n.  
000000a0 49 2b 3b 76 d3 a9 17 e2 34 11 b3 a7 23 09 f0 f5 I+;v....4....#...  
000000b0 ed ce 65 4d 4a 25 5c d0 34 fd ea 19 4a b4 b6 bb ..eMJ%\..4....J...  
000000c0 7e 65 0c ac 77 ff 79 d0 e6 0d a3 la b3 ba 2c 6f ~e..w.y.....,o  
000000d0 de 23 c9 9e 7a 48 05 64 ad 85 48 b9 60 c6 fe 66 .#.zH.d..H.^..f  
000000e0 e9 2c d5 f0 3d bl ba 0f fd 15 98 6a c0 a1 7c 39 ,.=.....j..|9  
000000f0 b6 ac 45 99 97 f3 ce 91 ef 69 a5 aa 49 31 fb f2 ..E.....i..Il..  
00000100 28 6d 4c bd 00 8d 84 db 8d 85 a4 f3 5c 61 e0 51 (mL.....\a.Q  
00000110 b3 99 ce a4 66 9e 2a 1e e5 5e 2d 19 f4 f5 5b 2e ....f.*..^...[.  
00000120 ba 58 17 dd 23 14 b9 37 62 e4 8b dc cf 46 5f 9c .X..#..7b....F_.  
00000130 1e 12 f6 b9 51 ee 46 0d f5 5a 9e fa 90 52 d8 86 ....Q.F..Z..R..  
00000140 75 fa 24 63 f3 ee 7d 2e ab 05 1d e5 3e bf d9 a3 u.$c...).....>...  
00000150 17 5f a3 la 1c c9 0d 18 33 75 27 17 6c 11 81 c4 .._.....3u'.1...  
00000160 7a 19 11 a5 e9 92 d5 5c bd 72 9b 78 f7 53 14 c8 z.....\r.x.S..  
00000170 92 7b 26 31 24 63 a4 05 7e bf 47 3f 23 75 34 d9 .{&1$c..~.G?#u4..  
00000180 3f ff e4 5b c4 6b 1e 98 b3 a7 7d 5a 4e b0 d3 2b ?..[.k....}ZN...+  
00000190 b2 6f 8a cf ba 9f af 6b c8 29 0b 53 0b fc 38 8d .o.....k.).S..8.  
000001a0 dd af 7e 27 f0 1c 45 d4 39 25 aa 94 fd a7 ac 00 ...~'..E.9%.....  
000001b0 05 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Re-read Write Go to... 16 bytes per row Save... Close

Activity 2: Requesting

- C2 Network traffic can be customized using C2 profiles
 - User-agents
 - HTTP endpoints
 - Headers
 - GET Parameters
 - ...

```
# Defines URI endpoints for HTTP GET requests
# This has to be an array, even if it only has one member
endpoints = [
    "/get",
    "/api/v1.2/status.js"
]

# Defines arbitrary URI parameters that are added to the request
[http-get.agent.parameters]
id = "#####-#####"
lang = [
    "en-US",
    "de-AT"
]

# Defines arbitrary headers that are added by the agent when performing a HTTP GET request
[http-get.agent.headers]
Host = [
    "wikipedia.org",
    "google.com",
    "127.0.0.1"
]
Connection = "Keep-Alive"
Cache-Control = "no-cache"
```

Activity 2: Requesting

- C2 Network traffic can be customized using C2 profiles
 - User-agents
 - HTTP endpoints
 - Headers
 - GET Parameters
- ...

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|--|
| 8 | 0.017898 | 172.29.176.1 | 172.29.177.43 | HTTP | 446 | POST /api/v2/get.js?lang=en-US&page=16 HTTP/1.1 (text/plain) |
| 10 | 0.189483 | 172.29.177.43 | 172.29.176.1 | HTTP | 91 | HTTP/1.1 200 |
| 17 | 0.222307 | 172.29.176.1 | 172.29.177.43 | HTTP | 541 | GET /api/v1.2/status.js?id=b3AKO-7fE90&lang=en-US HTTP/1.1 |
| 19 | 0.352693 | 172.29.177.43 | 172.29.176.1 | HTTP | 89 | HTTP/1.1 200 |
| 26 | 5.557146 | 172.29.176.1 | 172.29.177.43 | HTTP | 524 | GET /get?id=lAUQk-LStob&lang=de-AT HTTP/1.1 |
| 28 | 5.688683 | 172.29.177.43 | 172.29.176.1 | HTTP | 89 | HTTP/1.1 200 |
| 35 | 11.384841 | 172.29.176.1 | 172.29.177.43 | HTTP | 508 | GET /get?id=zWgyL-eAVDN&lang=en-US HTTP/1.1 |
| 37 | 11.479281 | 172.29.177.43 | 172.29.176.1 | HTTP | 89 | HTTP/1.1 200 |
| 44 | 17.036604 | 172.29.176.1 | 172.29.177.43 | HTTP | 551 | GET /api/v1.2/status.js?id=VnQ4B-o5b5k&lang=de-AT HTTP/1.1 |
| 46 | 17.161741 | 172.29.177.43 | 172.29.176.1 | HTTP | 275 | HTTP/1.1 200 |
| 54 | 17.189807 | 172.29.176.1 | 172.29.177.43 | HTTP | 1526 | PUT /api/v2/get.js?lang=de-AT&page=17 HTTP/1.1 (text/plain) |
| 57 | 17.243284 | 172.29.177.43 | 172.29.176.1 | HTTP | 91 | HTTP/1.1 200 |
| 64 | 21.884782 | 172.29.176.1 | 172.29.177.43 | HTTP | 539 | GET /api/v1.2/status.js?id=vkXB2-btoZb&lang=de-AT HTTP/1.1 |
| 66 | 21.998057 | 172.29.177.43 | 172.29.176.1 | HTTP | 89 | HTTP/1.1 200 |

Data transformation

- Customize how packet data is represented

1. Encoding
2. Append/prepend strings
3. Placement

```
[http-get.agent.heartbeat]
placement = { type = "header", name = "Authorization" }
encoding = { type = "base64", url-safe = true }
prefix = "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9."
suffix = ".#####-#####"
```

Data transformation

```
Frame 73: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface \Device\NPF_{42402AF3-E76F-4A86-9807-322510CEA966}, id 0
  Ethernet II, Src: Microsoft_16:13:82 (00:15:5d:16:13:82), Dst: Microsoft_16:1b:44 (00:15:5d:16:1b:44)
  Internet Protocol Version 4, Src: 172.29.176.1, Dst: 172.29.177.43
  Transmission Control Protocol, Src Port: 53612, Dst Port: 8080, Seq: 1, Ack: 1, Len: 455
  Hypertext Transfer Protocol
    GET /get?id=7cyub-sHSoi&lang=de-AT HTTP/1.1\r\n
      Request Method: GET
    Request URI: /get?id=7cyub-sHSoi&lang=de-AT
      Request URI Path: /get
    Request URI Query: id=7cyub-sHSoi&lang=de-AT
      Request Version: HTTP/1.1
    connection: Keep-Alive\r\n
    authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.QzBOUQFkAQAkAAAAID5E6AAAAAAQbtndlhTVRrVaa6bIypGtjDLo3iKTqljRydyajCMPceUS1XA_bkIQSVDmNv5
    host: 127.0.0.1\r\n
    cache-control: no-cache\r\n
    user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36\r\n
\r\n
[Response in frame: 75]
[Full request URL: http://127.0.0.1/get?id=7cyub-sHSoi&lang=de-AT]
```

Data transformation

Frame 73: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface \Device\NPF_{42402AF3-E76F-4A86-9807-322510CEA966}, id 0
Ethernet II, Src: Microsoft_16:13:82 (00:15:5d:16:13:82), Dst: Microsoft_16:1b:44 (00:15:5d:16:1b:44)

The screenshot shows a NetworkMiner interface with a "Recipe" panel on the left and an "Input" and "Output" panel on the right.

Recipe:

- From Base64
- Alphabet: A-Za-z0-9+=
- Remove non-alphabet chars (checked)

Input: QzBOUQFkAQAkAAAAID5E6AAAAAAQbtndlhTVRrVaa6bIypGtjDLo3iKTqljRydyajCMPceUS1XA_bkIQSVDmNv
start: 112 end: 112 length: 0

Output: C0NQ.d...\$.>Dè.....n×m..ÑFµZk!ÈÈ...2èp".¤XÑÉÜ..#.qå.Öp....T9.¿.ÚåþTB¡..%.~.£.!
X.

start: 84 end: 84 length: 0

[Response in frame: 75]
[Full request URL: http://127.0.0.1/get?id=7cyub-sHSoi&lang=de-AT]

Activity 3: Executing

Command
execution

Screenshots

File upload &
download

BOF
execution

.NET
execution

Token
manipulation

Conquest

Options Views

Sessions [Table View] X Eventlog X

| AgentID | IP (Internal) | Username | Hostname | Domain | OS | Process | PID | First seen | Last seen |
|---------|---------------|----------|----------|--------|----|---------|-----|------------|-----------|
| | | | | | | | | | |

[+] Connected to Conquest team server.

Listeners X

Start Listener Generate Payload

| ListenerID | Address | Port | Callback Hosts | Protocol |
|------------|---------|------|----------------|----------|
| | | | | |

Chapter 4

Should I build a C2 framework?

It depends...



Should I build a C2 framework?

YES, because ...

- ... you want to **learn how C2 frameworks work** in detail
- ... you want **full control** over capabilities and features
- ... you can spend time and energy on **designated malware/tool development**
- ... you want to fill a **market or research gap**
- ... you want to **challenge** yourself

NO, because...

- ... it takes a lot of **effort**
- ... you don't want to **reinvent the wheel**
- ... building a **custom agent/module** also gets the job done
- ... **time is money**. You get paid for doing engagements, not writing a C2

What's next for Conquest?

- *The more you know, the more you know that you don't know*
- More listener & payload types
- Modular plugin system
- Stability - Usability - Functionality



<https://github.com/jakobfriedl/conquest>

Thank you!

 jakobfriedl.github.io