“One certificate to rule them all”

L'histoire d'un ORB Chinois

JPCERT CC

JPCERT/CC Eyes

Top > List of "Malware" > GobRAT malware written in Go language targeting Linux routers

増渕 維摩(Yuma Masubuchi)

May 29, 2023

GobRAT malware written in Go language targeting Linux routers

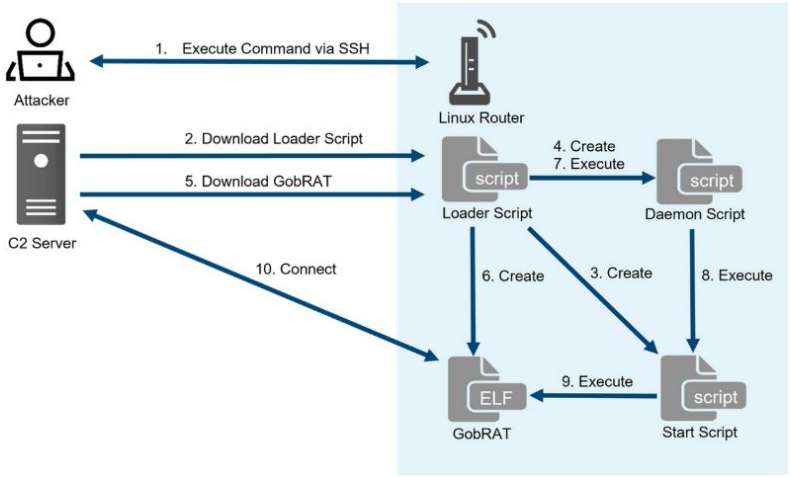
Tool

X Post Email

JPCERT/CC has confirmed attacks that infected routers in Japan with malware around February 2023. This blog article explains the details of the attack confirmed by JPCERT/CC and GobRAT malware, which was used in the attack.

Attack flow up to malware execution

Initially, the attacker targets a router whose WEBUI is open to the public, executes scripts possibly by using vulnerabilities, and finally infects the GobRAT. Figure 1 shows the flow of the attack until GobRAT infects the router.



Commands executed

GobRAT has 22 commands that are executed by the commands from the C2 server, and we have identified the following commands. Since the malware targets routers, you can see that most functions are related to communication, such as frpc, socks5, and reconfiguration of C2. See Appendix A for command details.

- Obtain machine Information
- Execute reverse shell
- Read/write files
- Configure new C2 and protocol
- Start socks5
- Execute file in /zone/frpc
- Attempt to login to sshd, Telnet, Redis, MySQL, PostgreSQL services running on another machine

GobRAT Analysis Tools

Since GobRAT uses gob for communication, if you want to emulate its communication with C2 to check commands, you need to create a program using Go language. Our C2 emulation tool that supports GobRAT analysis is available on GitHub. Please download it from the following webpage for your analysis.

JPCERTCC/aa-tools/GobRAT-Analysis - GitHub
https://github.com/JPCERTCC/aa-tools/tree/master/GobRAT-Analysis

In Closing

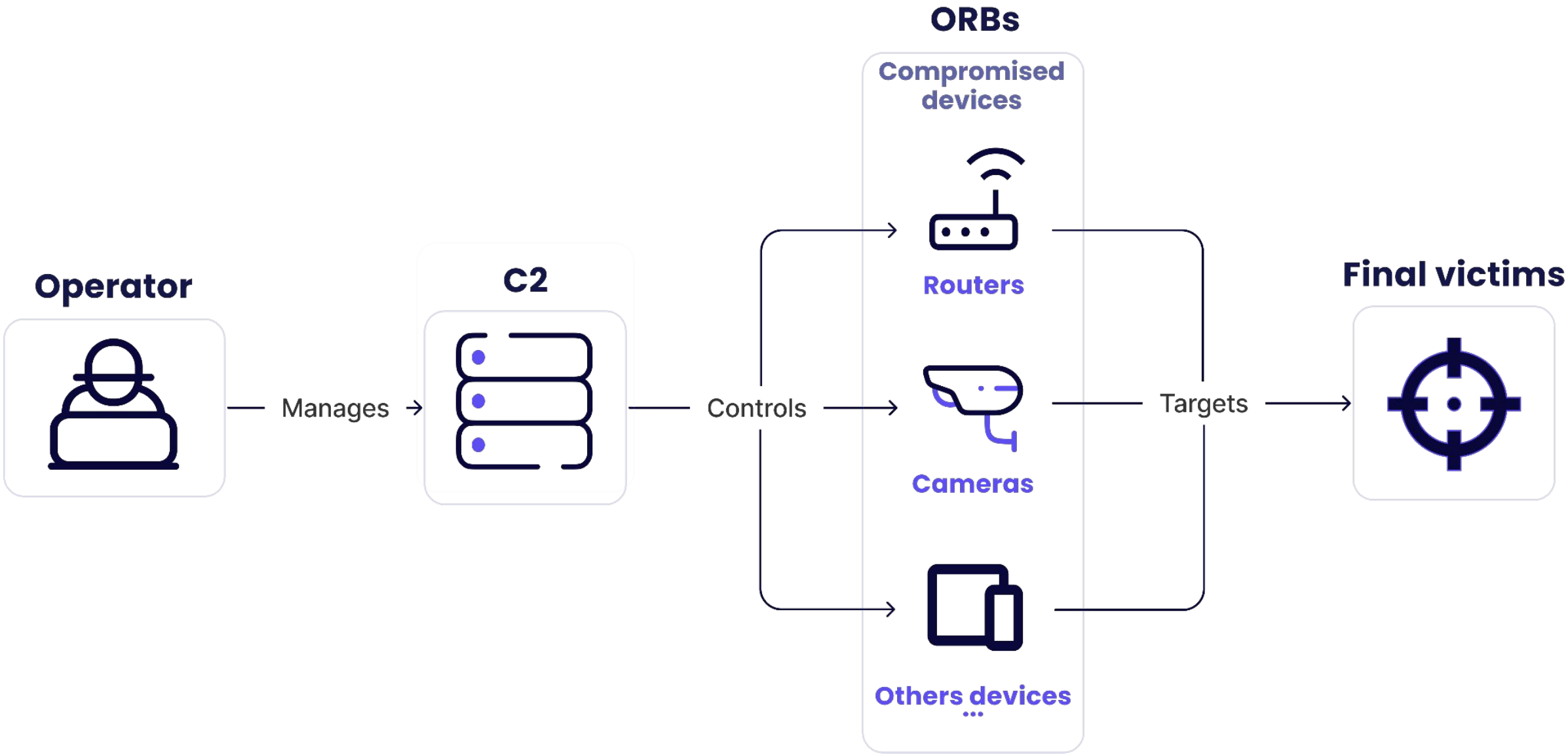
In recent years, different types of malware using Go language have been confirmed, and the GobRAT malware confirmed this time uses gob, which can only be handled by Go language, for communication. Please continuously beware of malware that infects routers, not limited to GobRAT, since they are difficult to detect. Please refer to Appendix B for C2 of the malware, Appendix C for the hash value of the script, and Appendix D for the hash value of the malware.

Yuma Masubuchi

Translated by Takumi Nakano

https://blogs.jpcert.or.jp/en/2023/05/gobrat.html

Operational Relay Boxes



Appendix B: C2

- https://su.vealcat.com
- http://su.vealcat.com:58888
- https://ktlvz.dnsfailover.net
- http://ktlvz.dnsfailover.net:58888
- su.vealcat.com
- ktlvz.dnsfailover.net
- wpksi.mefound.com

Appendix C: Hash values of the scripts

- 060acb2a5df6560acab9989d6f019fb311d88d5511f3eda0effcbd9fc6bd12bb
- feaef47defd8b4988e09c8b11967e20211b54e16e6df488780e2490d7c7fa02a
- 3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1
- 60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3

Appendix D: Hash values of the malware

- a8b914df166fd0c94106f004e8ca0ca80a36c6f2623f87a4e9afe7d86b5b2e3a
- aeed77896de38802b85a19bfcb8f2a1d567538ddc1b045bcdb29cb9e05919b60
- 6748c22d76b8803e2deb3dad1e1fa7a8d8ff1e968eb340311fd82ea5d7277019
- e133e05d6941ef1c2e3281f1abb837c3e152fdeaffefde84ffe25338fe02c56d
- 43dc911a2e396791dc5a0f8996ae77ac527add02118adf66ac5c56291269527e
- af0292e4de92032ede613dc69373de7f5a182d9cbba1ed49f589ef484ad1ee3e
- 2c1566a2e03c63b67fbdd80b4a67535e9ed969ea3e3013f0ba503cfa58e287e3
- 98c05ae70e69e3585fc026e67b356421f0b3d6ab45b45e8cc5eb35f16fef130c
- 300a92a67940cfafeed1cf1c0af25f4869598ae58e615ecc559434111ab717cd
- a363dea1efda1991d6c10cc637e3ab7d8e4af4bd2d3938036f03633a2cb20e88
- 0c280f0b7c16c0d299e306d2c97b0bff3015352d2b3299cf485de189782a4e25
- f962b594a847f47473488a2b860094da45190738f2825d82afc308b2a250b5fb
- 4ceb27da700807be6aa3221022ef59ce6e9f1cda52838ae716746c1bbdee7c3d
- 3e1a03f1dd10c3e050b5f455f37e946c214762ed9516996418d34a246daed521
- 3bee59d74c24ef33351dc31ba697b99d41c8898685d143cd48bccdff707547c0
- c71ff7514c8b7c448a8c1982308aaffed94f435a65c9fdc8f0249a13095f665e

Appendix B: C2

- https://su.vealcat.com
- http://su.vealcat.com:58888
- https://ktlvz.dnsfailover.net
- http://ktlvz.dnsfailover.net:58888
- su.vealcat.com
- ktlvz.dnsfailover.net
- wpksi.mefound.com

Appendix C: Hash values of the scripts

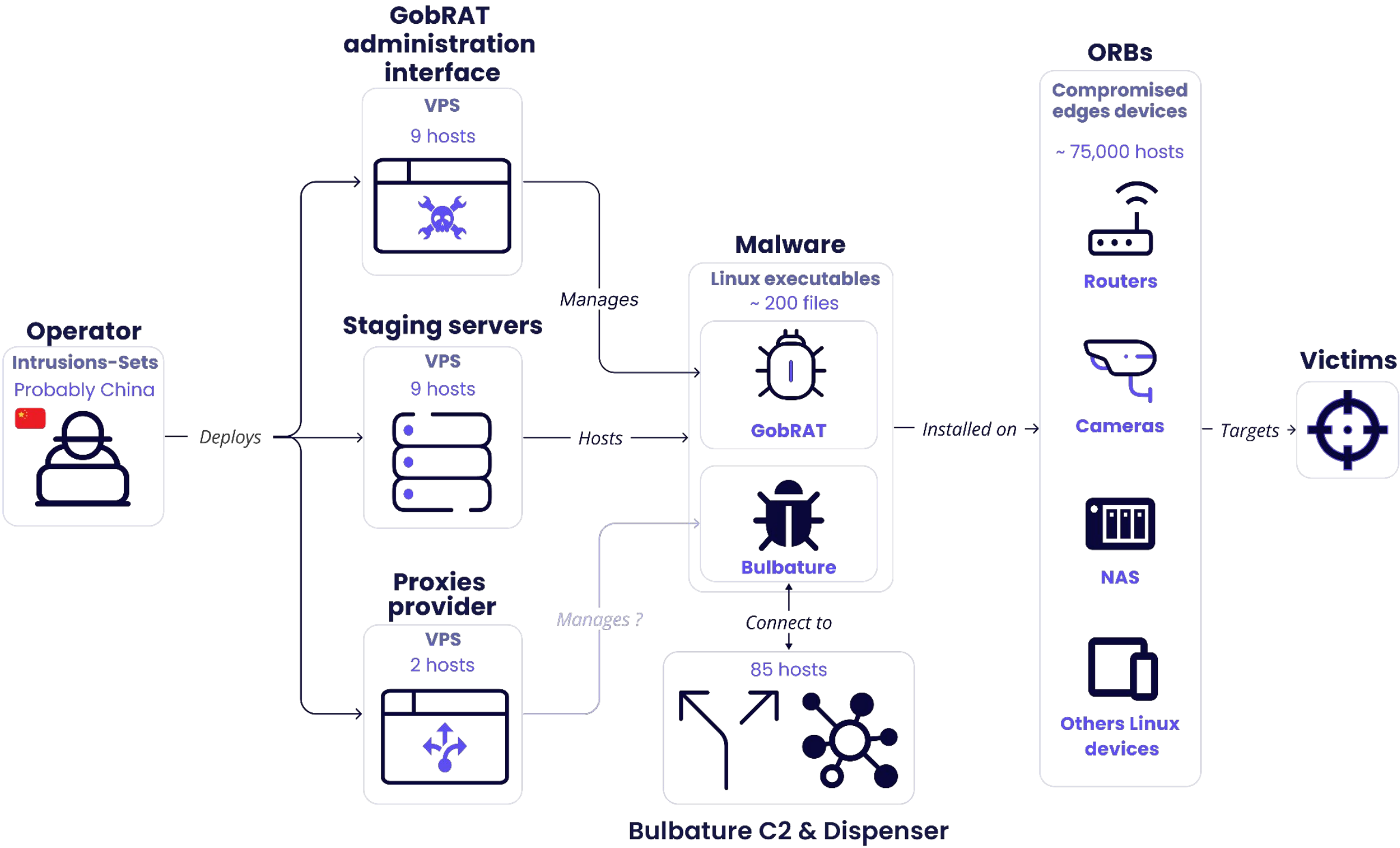
- 060acb2a5df6560acab9989d6f019fb311d88d5511f3eda0effcbd9fc6bd12bb
- feaef47defd8b4988e09c8b11967e20211b54e16e6df488780e2490d7c7fa02a
- 3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1
- 60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3

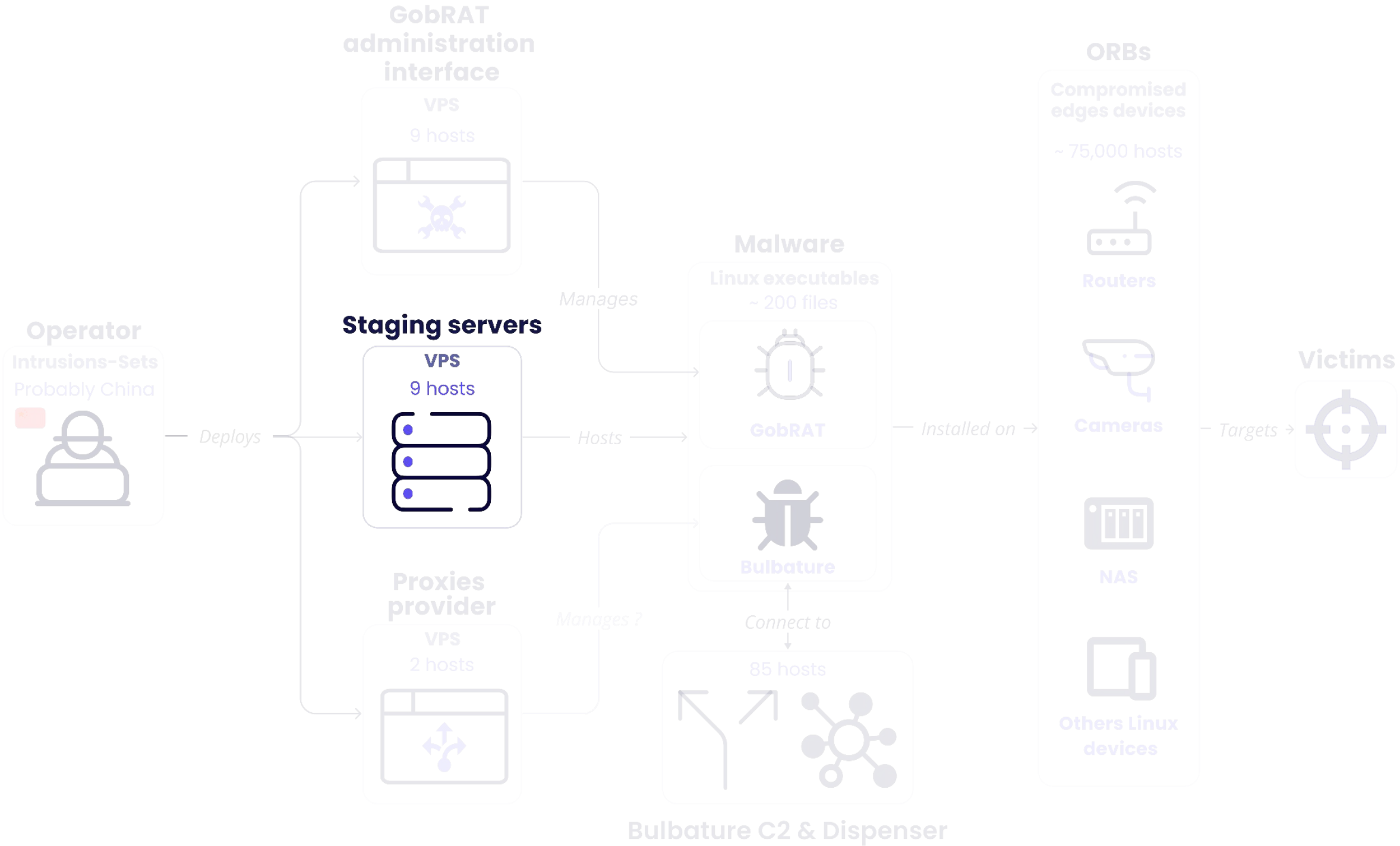
Appendix D: Hash values of the malware

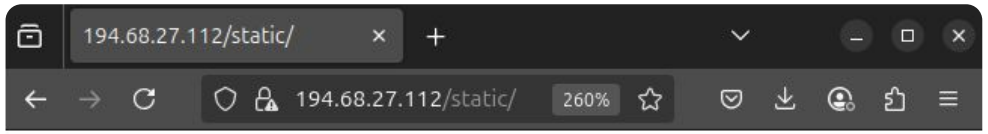
- a8b914df166fd0c94106f004e8ca0ca80a36c6f2623f87a4e9afe7d86b5b2e3a
- aeed77896de38802b85a19bfcb8f2a1d567538ddc1b045bcdb29cb9e05919b60
- 6748c22d76b8803e2deb3dad1e1fa7a8d8ff1e968eb340311fd82ea5d7277019
- e133e05d6941ef1c2e3281f1abb837c3e152fdeaffefde84ffe25338fe02c56d
- 43dc911a2e396791dc5a0f8996ae77ac527add02118adf66ac5c56291269527e
- af0292e4de92032ede613dc69373de7f5a182d9cbba1ed49f589ef484ad1ee3e
- 2c1566a2e03c63b67fbdd80b4a67535e9ed969ea3e3013f0ba503cfa58e287e3
- 98c05ae70e69e3585fc026e67b356421f0b3d6ab45b45e8cc5eb35f16fef130c
- 300a92a67940cfafeed1cf1c0af25f4869598ae58e615ecc559434111ab717cd
- a363dea1efda1991d6c10cc637e3ab7d8e4af4bd2d3938036f03633a2cb20e88
- 0c280f0b7c16c0d299e306d2c97b0bff3015352d2b3299cf485de189782a4e25
- f962b594a847f47473488a2b860094da45190738f2825d82afc308b2a250b5fb
- 4ceb27da700807be6aa3221022ef59ce6e9f1cda52838ae716746c1bbdee7c3d
- 3e1a03f1dd10c3e050b5f455f37e946c214762ed9516996418d34a246daed521
- 3bee59d74c24ef33351dc31ba697b99d41c8898685d143cd48bccdff707547c0
- c71ff7514c8b7c448a8c1982308aaffed94f435a65c9fdc8f0249a13095f665e

SHA1: ***d0d3975b5b900b3af2dce973428475f022b16f60***
Validity period:
2021-05-16 to 2031-05-14
C=*AU,*
ST=*Some-State,*
O=*Internet Widgits Pty Ltd*

SHA1: ***74fe94844a337da4bdc2988609fb3c4df3f3b78d***
Validity period:
2021-12-21 to 2024-03-21
O=*mkcert development CA,*
OU=*a@a-virtual-machine,*
CN=*mkcert a@a-virtual-machine*


GobRAT administration interface
VPS
9 hosts
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Manages
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser


GobRAT administration interface
VPS
9 hosts
Manages
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser



Bulbature

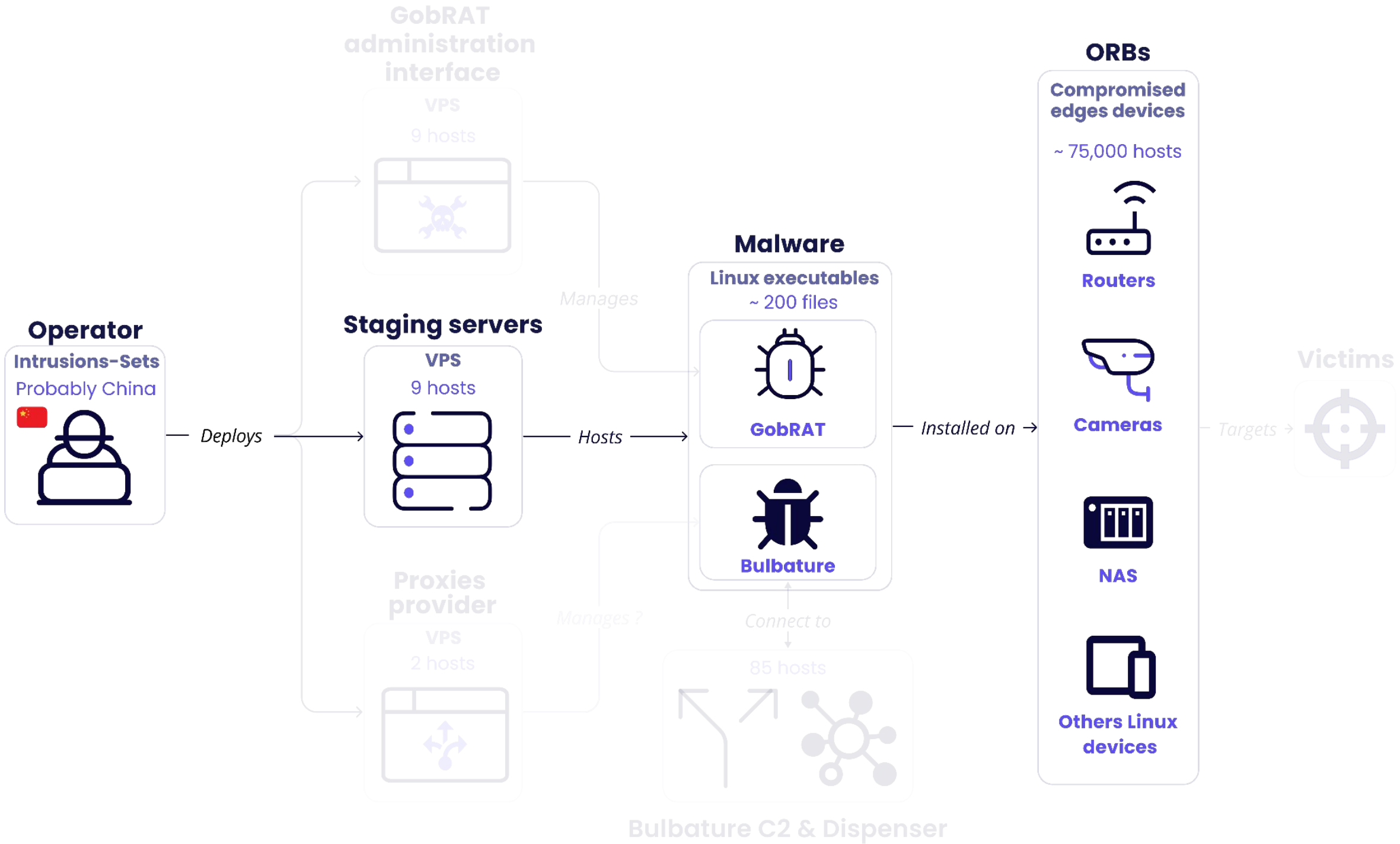
Some tools

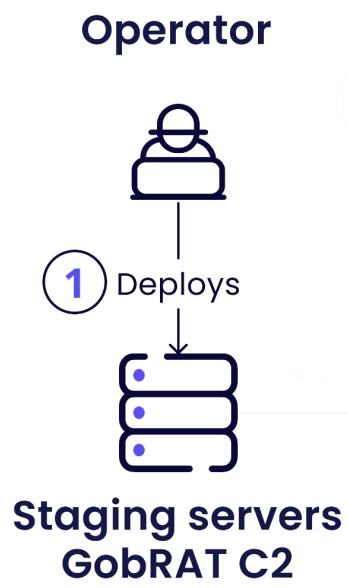
Bash scripts

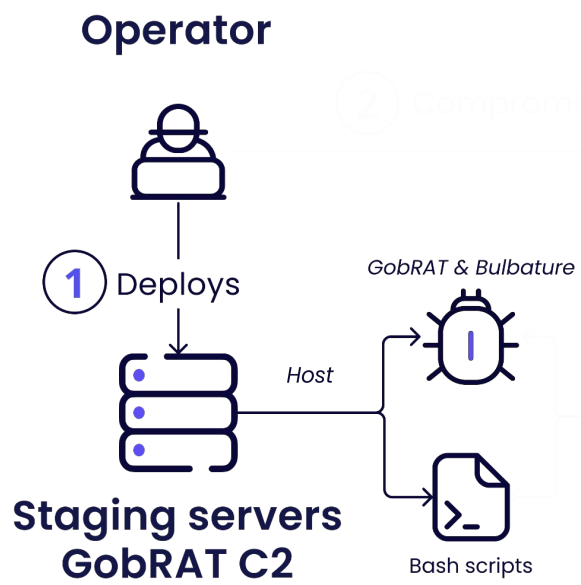
GobRAT

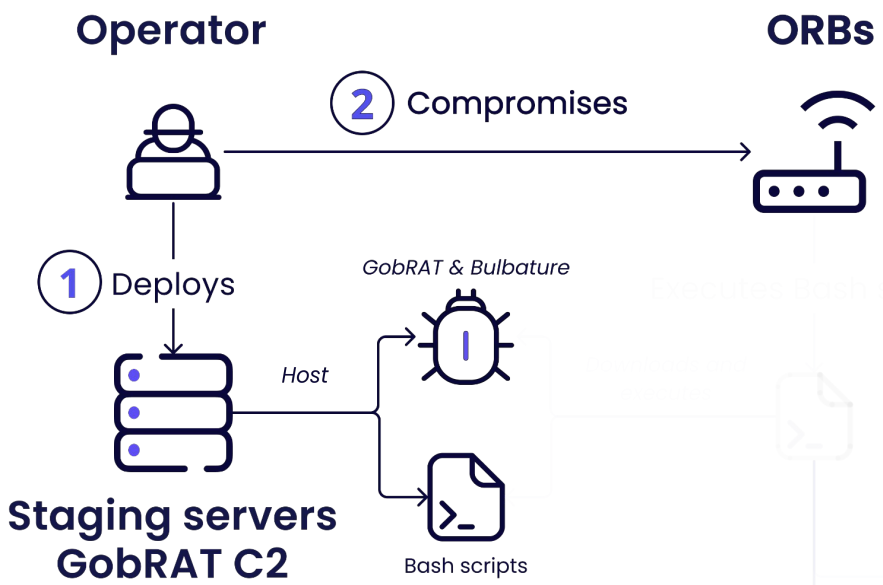
- bulbature
- frpc.arm
- frpc.i686
- frpc.x86_64
- hold_by_bot.sh
- sshdeny1.sh
- zone.arm
- zone.arm64
- zone.i686
- zone.mips
- zone.x86_64
- zoneController.sh
- zoneRestart.sh
- zonedelete.sh
- zonesetup.sh
- zoneupdate.sh

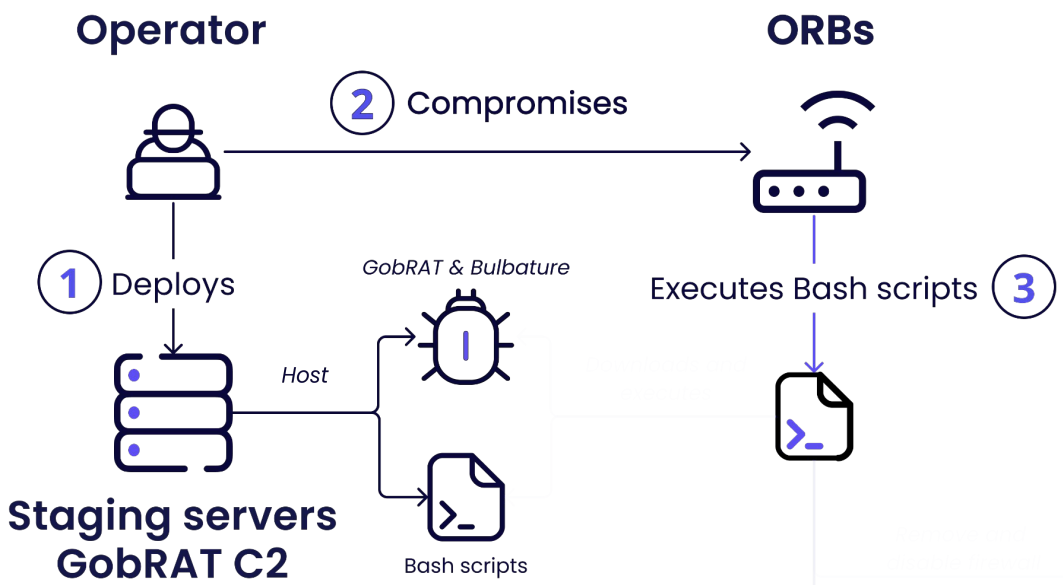
Exemple actif : hxxps://38.60.212[.]187/static

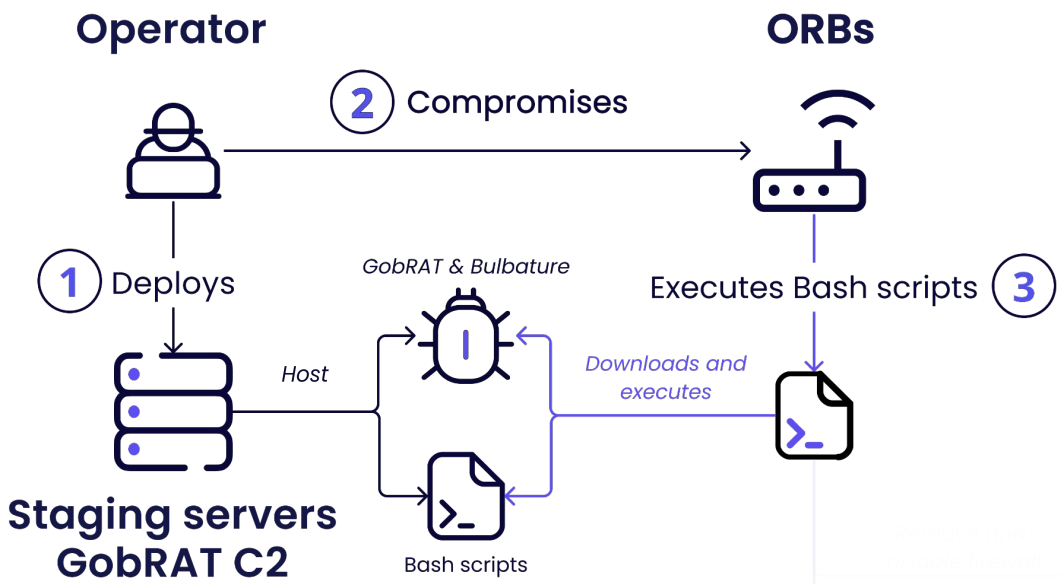

GobRAT administration interface
VPS
9 hosts
Manages
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser

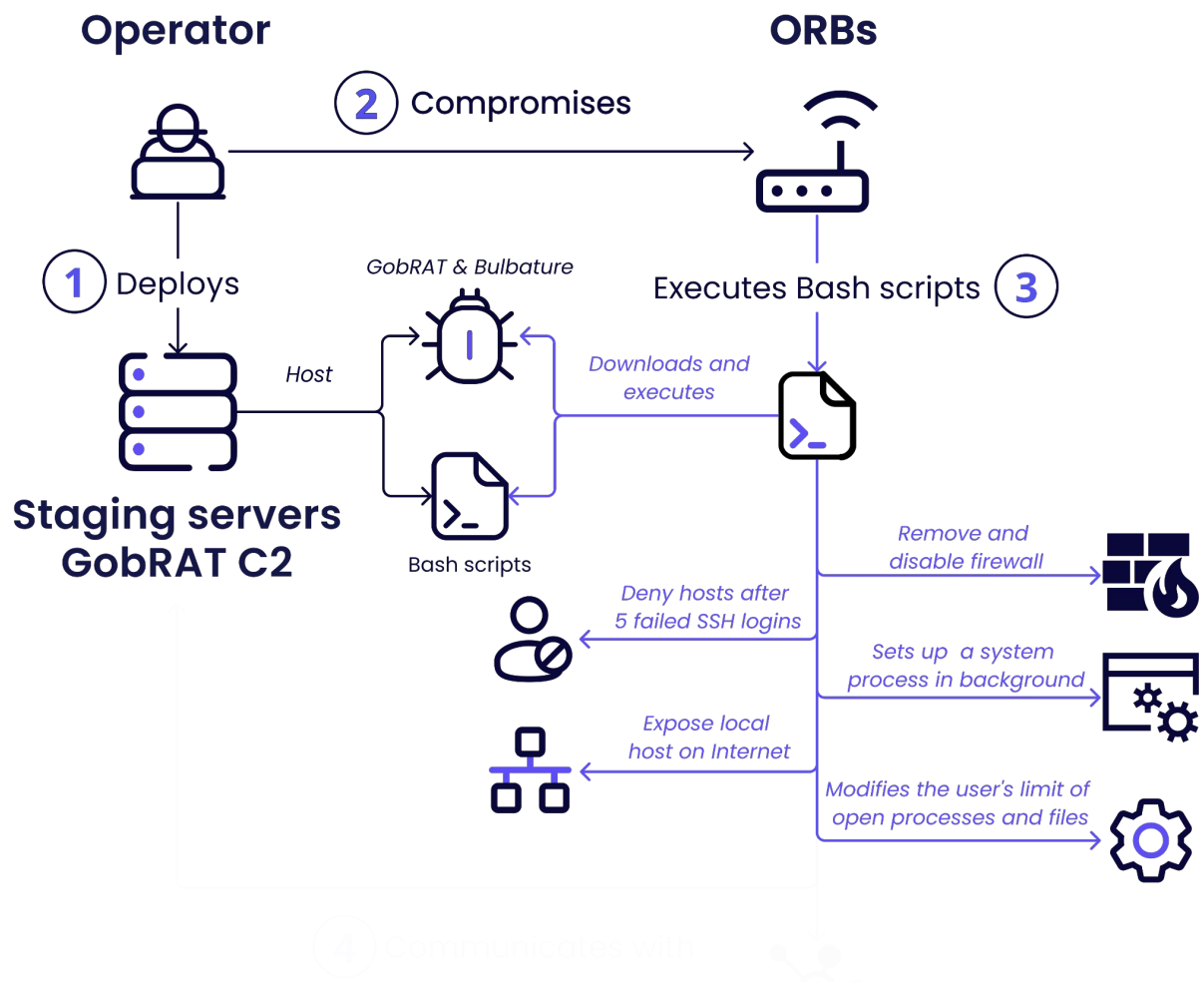

Operator
1 Deploys
Staging servers
GobRAT C2

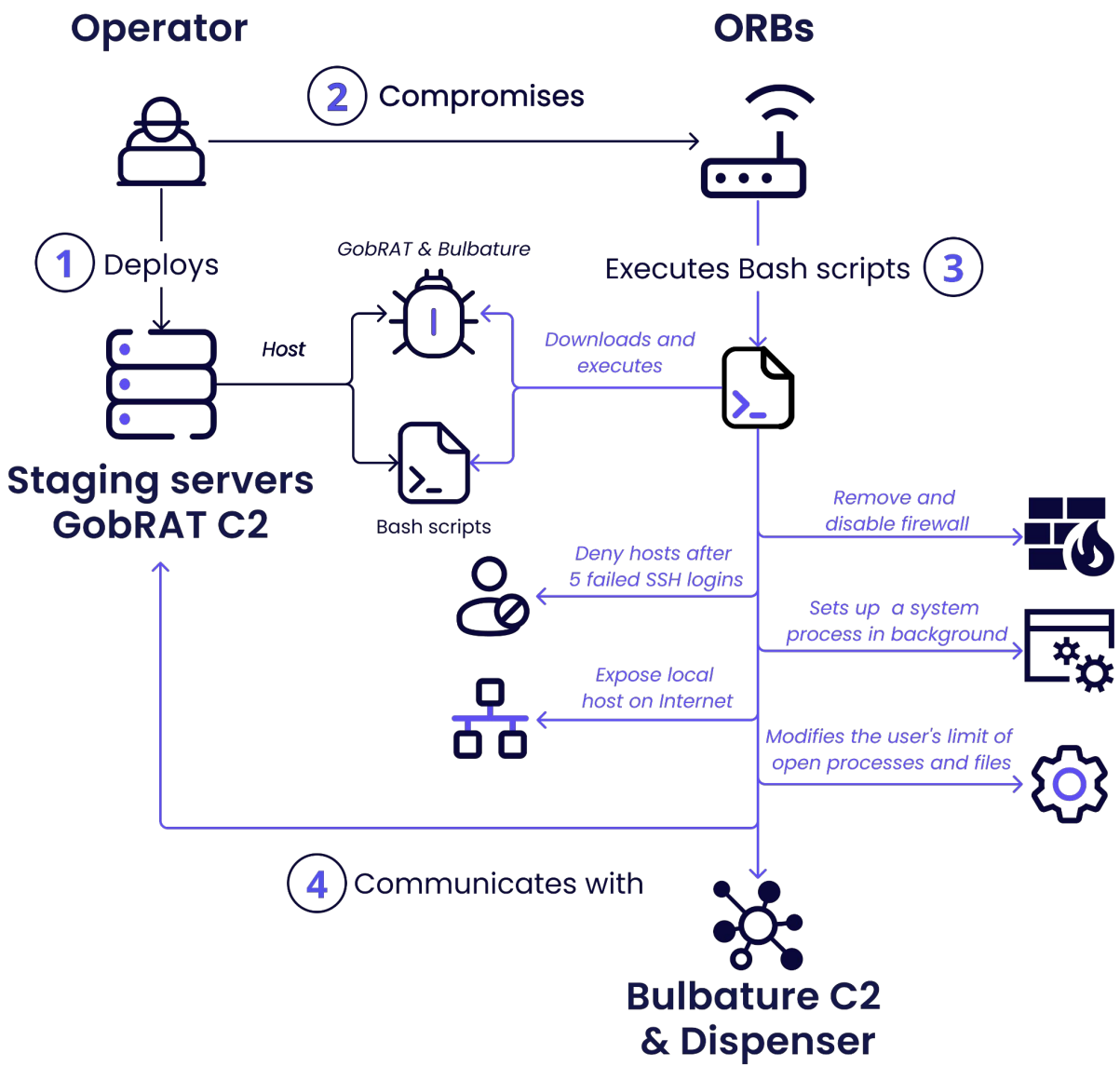

Operator
1 Deploys
GobRAT & Bulbature
Host
Staging servers
GobRAT C2
Bash scripts

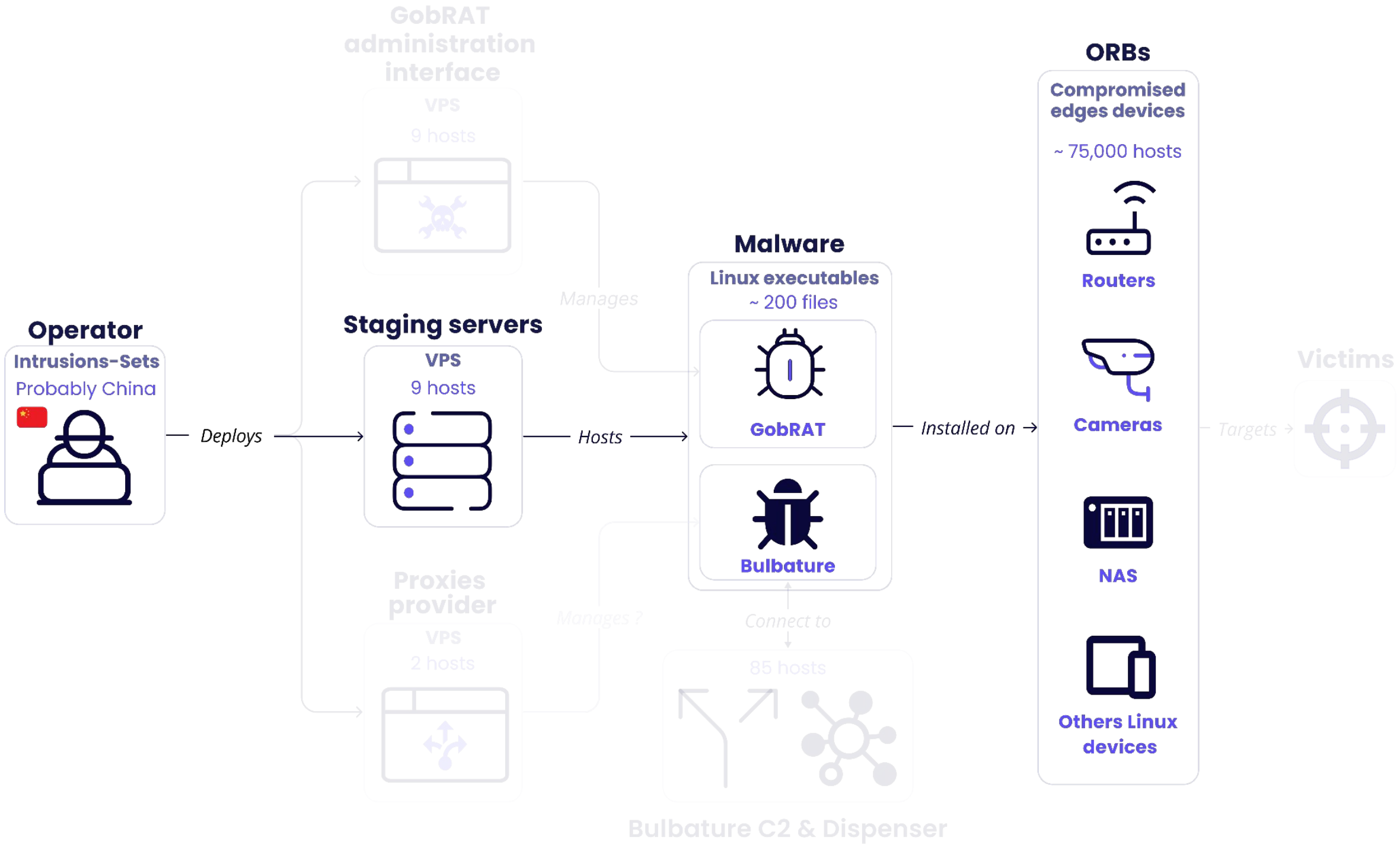

Operator
ORBs
2 Compromises
1 Deploys
GobRAT & Bulbature
Host
Staging servers
GobRAT C2
Bash scripts

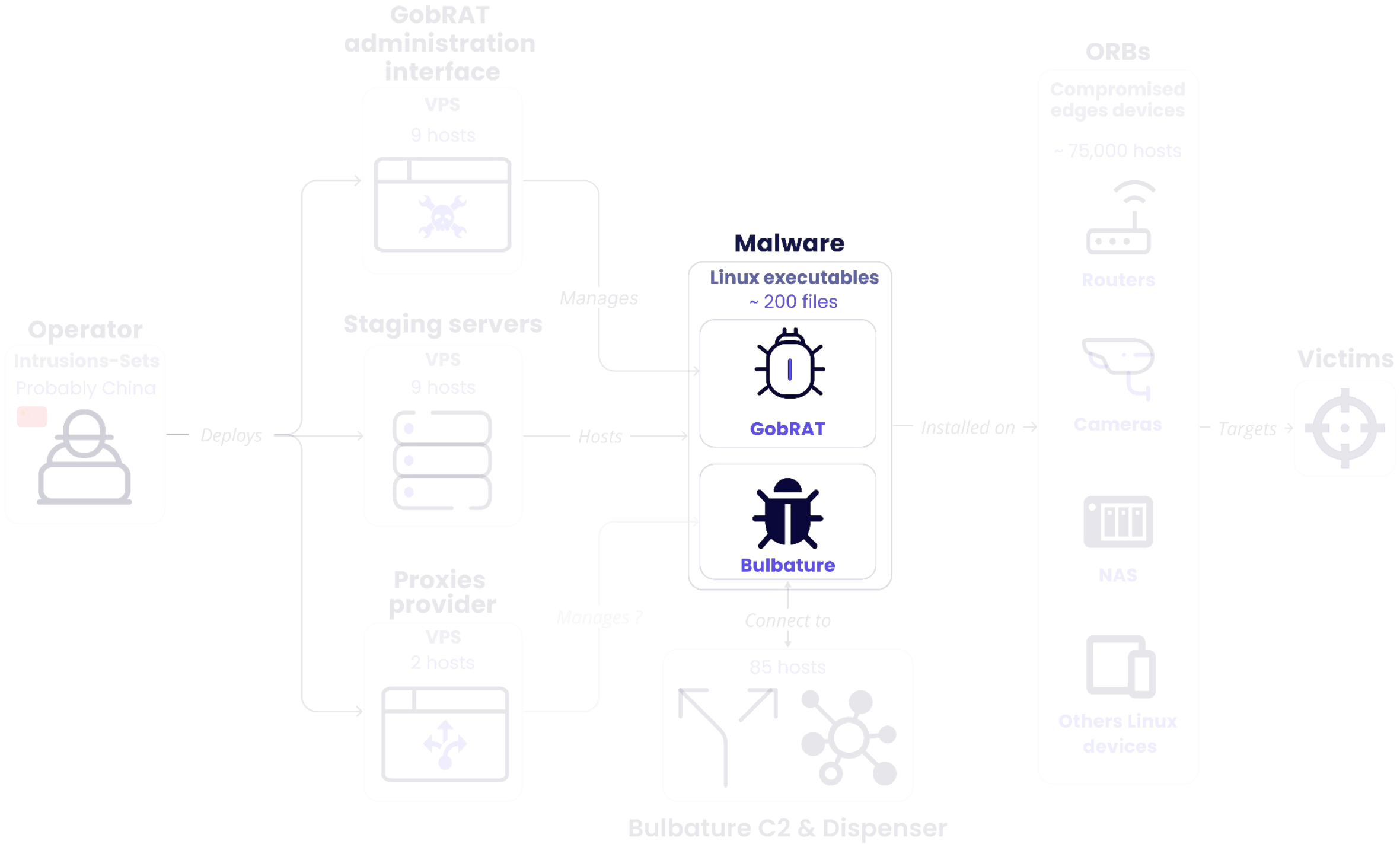

Operator
ORBs
2 Compromises
1 Deploys
GobRAT & Bulbature
Executes Bash scripts 3
Host
Staging servers
GobRAT C2
Bash scripts

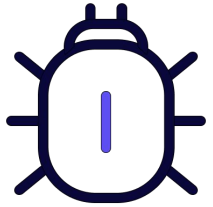

Operator
ORBs
2 Compromises
1 Deploys
GobRAT & Bulbature
Executes Bash scripts 3
Host
Downloads and executes
Staging servers
GobRAT C2
Bash scripts


Operator
ORBs
2 Compromises
1 Deploys
GobRAT & Bulbature
Executes Bash scripts 3
Host
Downloads and executes
Staging servers GobRAT C2
Bash scripts
Remove and disable firewall
Deny hosts after 5 failed SSH logins
Sets up a system process in background
Expose local host on Internet
Modifies the user's limit of open processes and files
4 Communicates with
Bulbature C2 & Dispenser


Operator
ORBs
2 Compromises
1 Deploys
GobRAT & Bulbature
Executes Bash scripts 3
Host
Downloads and executes
Staging servers GobRAT C2
Bash scripts
Remove and disable firewall
Deny hosts after 5 failed SSH logins
Sets up a system process in background
Expose local host on Internet
Modifies the user's limit of open processes and files
4 Communicates with
Bulbature C2 & Dispenser


GobRAT administration interface
VPS
9 hosts
Manages
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser


GobRAT administration interface
VPS
9 hosts
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Proxies provider
VPS
2 hosts
Manages
Hosts
Manages ?
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Connect to
85 hosts
Bulbature C2 & Dispenser
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims



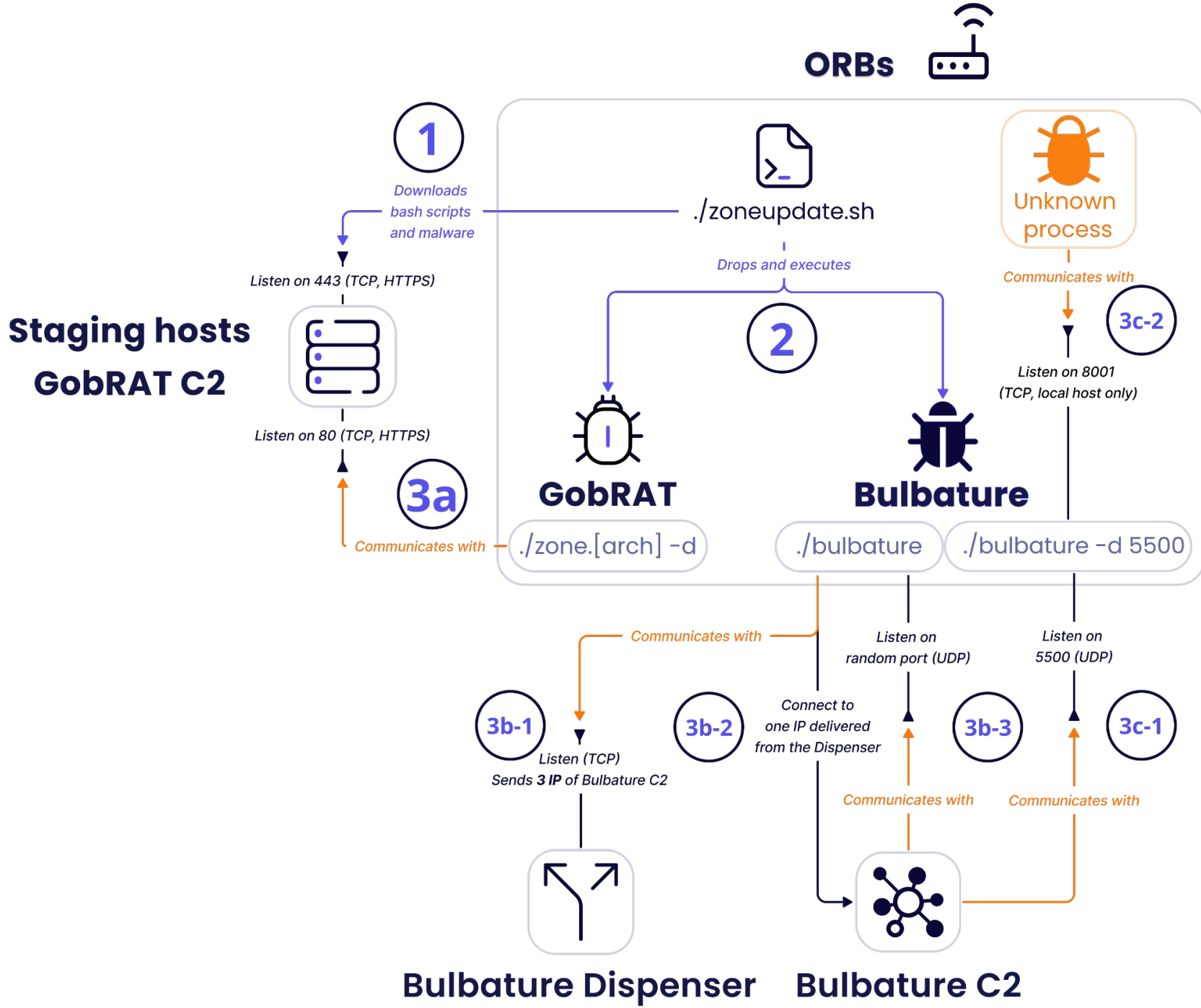
GobRAT

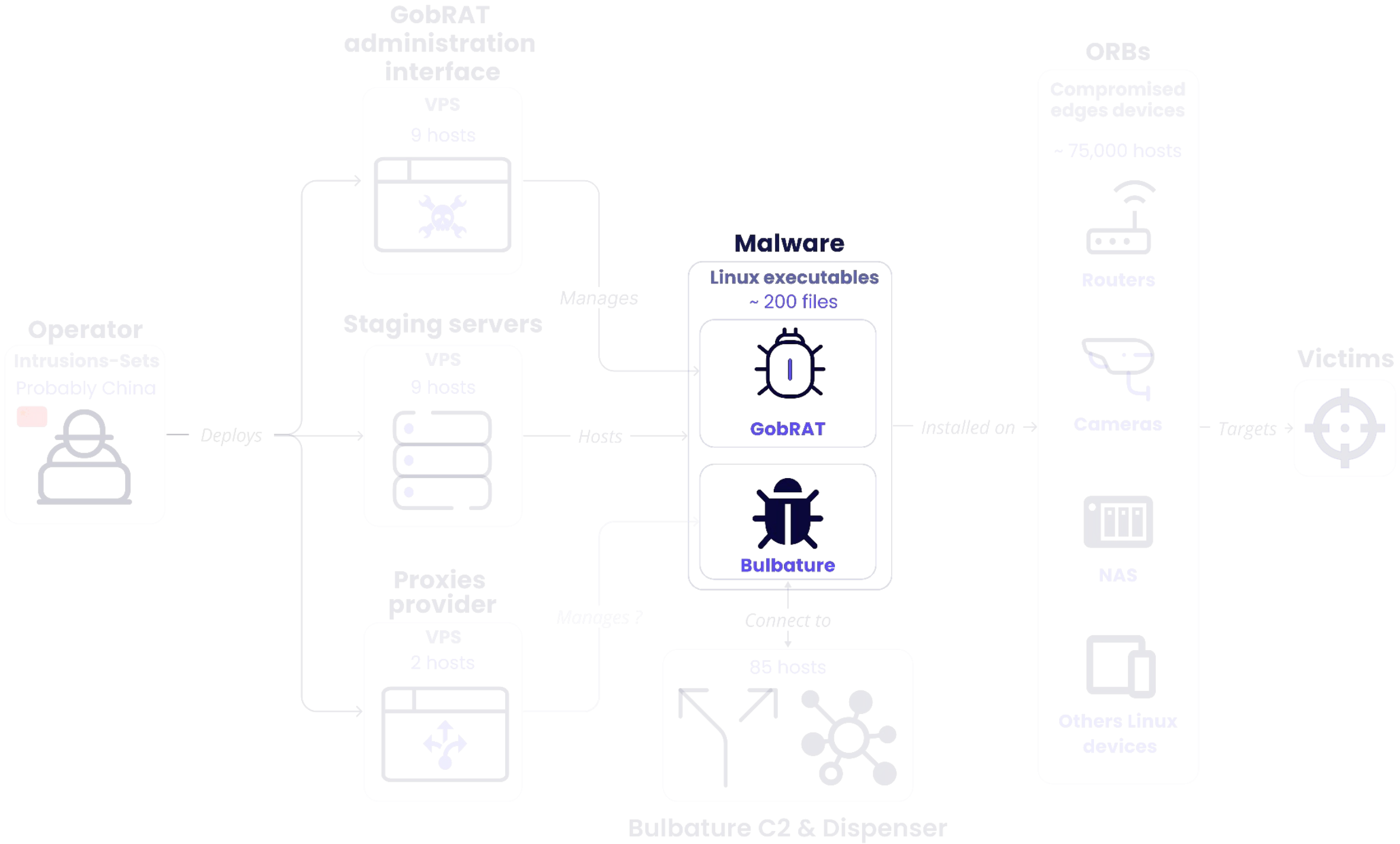
- Démarrer/arrêter un revershell
- Exécuter des commandes shell
- Fingerprint de l'hôte

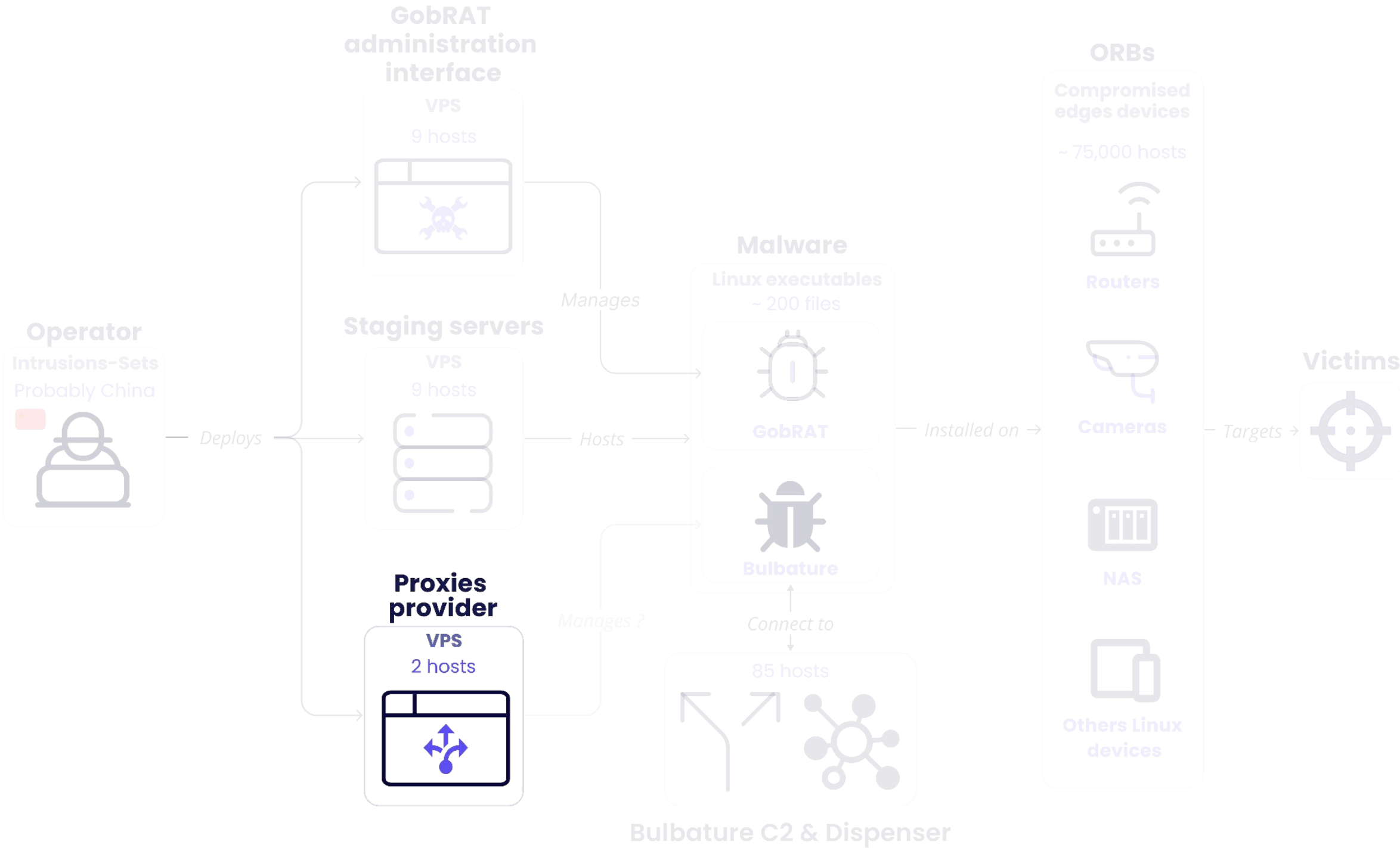
- Tentatives de connexion à des services **SSH, Telnet, Redis, MySQL ou PostgreSQL**
- **Attaques par dictionnaire** HTTP/HTTPS sur une adresse IP
- **Attaques DDoS** via SYN, TCP, UDP, HTTP, ICMP
- Créer un **proxy SOCKS5**

Bulbature

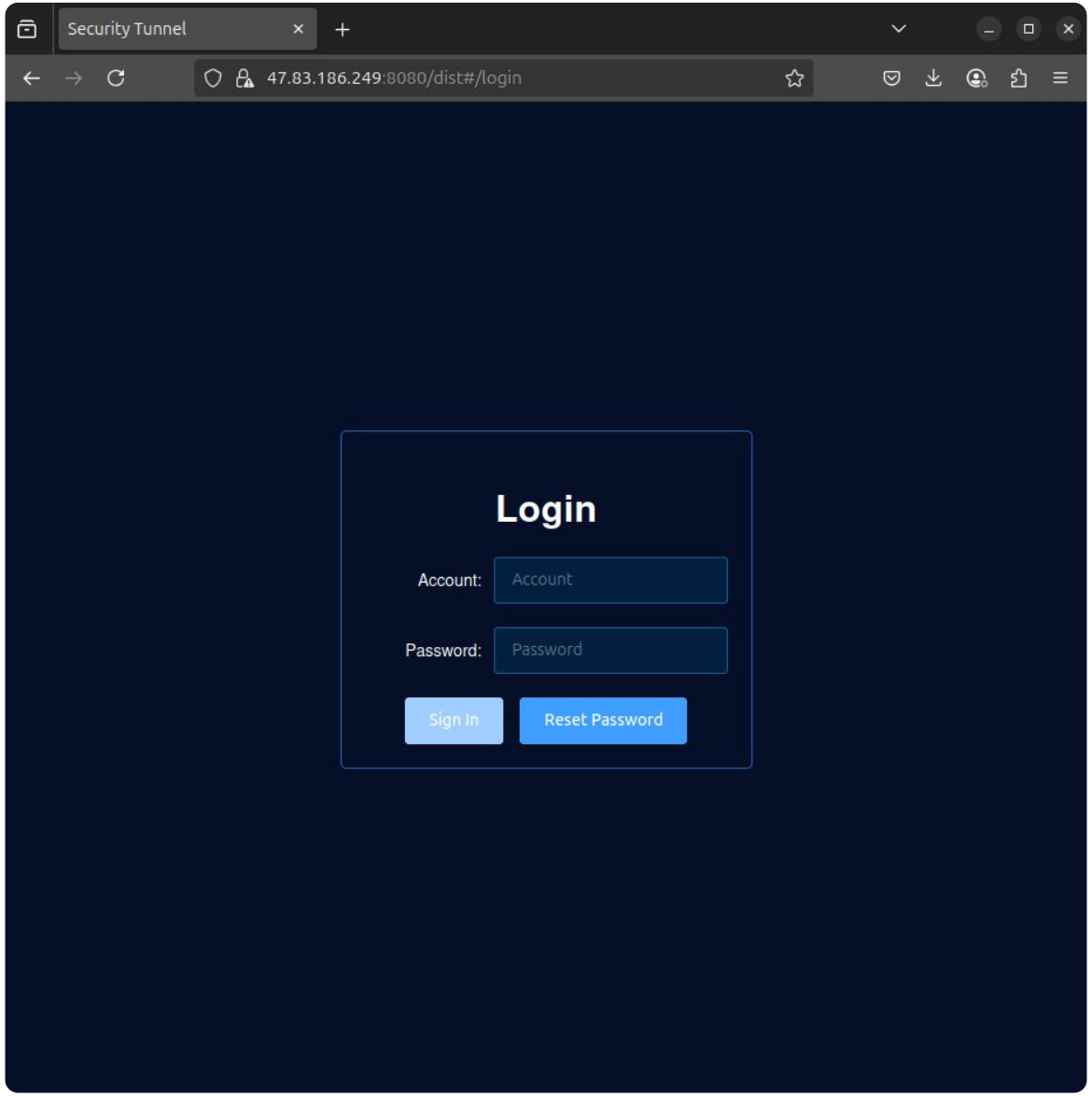
- Anti-analysis (Control Flow Flattening)
- Contient plus de 1 000 fonctions
- Utilisation intensive de programmation async
- Fonctionnalités plutôt liées au réseau


ORBs
1
Downloads
bash scripts
and malware
./zoneupdate.sh
Unknown
process
Listen on 443 (TCP, HTTPS)
Staging hosts
GobRAT C2
Drops and executes
2
Communicates with
3c-2
Listen on 8001
(TCP, local host only)
Listen on 80 (TCP, HTTPS)
3a
GobRAT
Bulbature
Communicates with
./zone.[arch] -d
./bulbature
./bulbature -d 5500
Communicates with
Listen on
random port (UDP)
Listen on
5500 (UDP)
3b-1
3b-2
Connect to
one IP delivered
from the Dispenser
3b-3
3c-1
Listen (TCP)
Sends 3 IP of Bulbature C2
Communicates with
Communicates with
Bulbature Dispenser
Bulbature C2

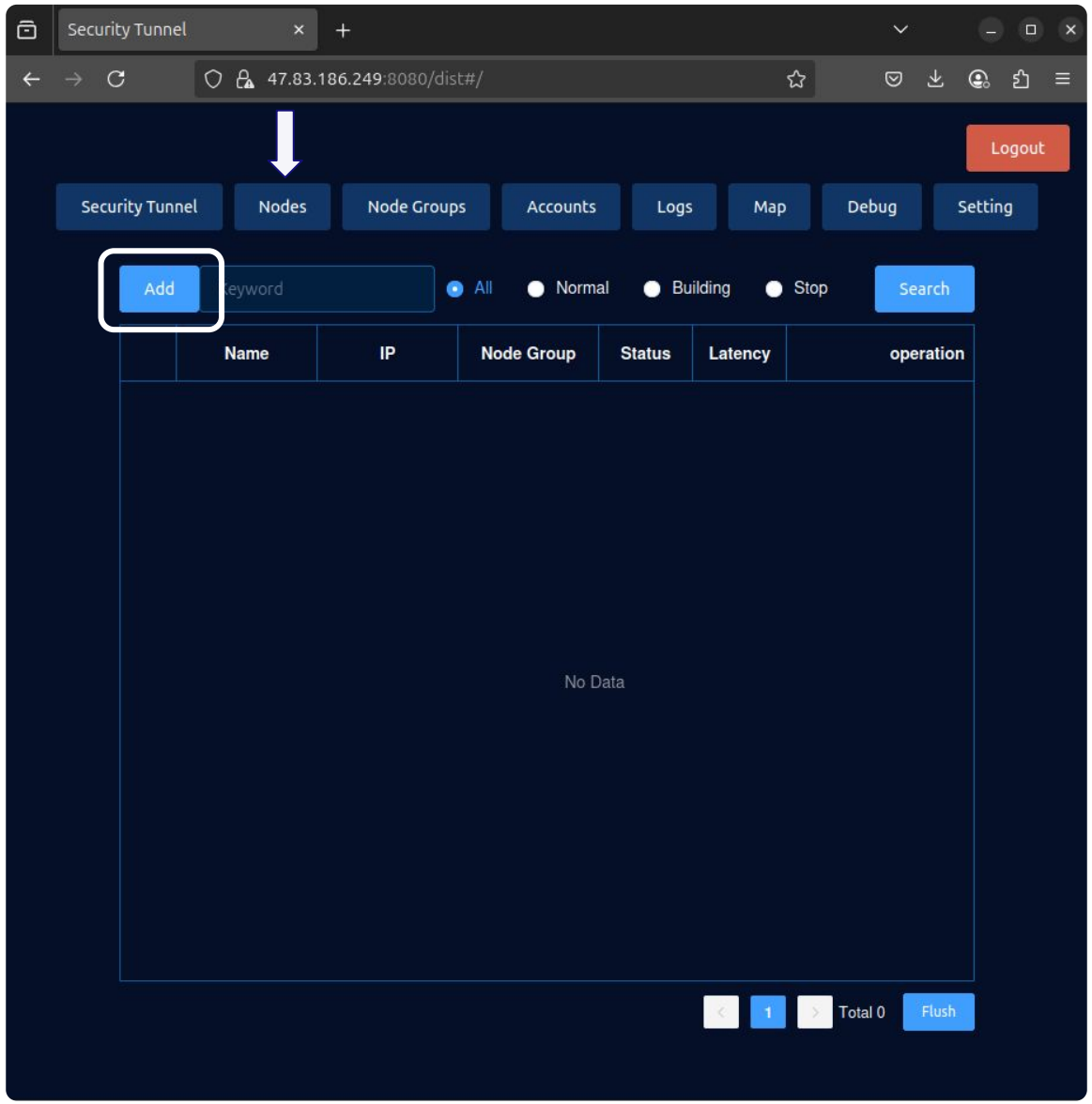

GobRAT administration interface
VPS
9 hosts
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Proxies provider
VPS
2 hosts
Manages
Hosts
Manages ?
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Connect to
85 hosts
Bulbature C2 & Dispenser
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims

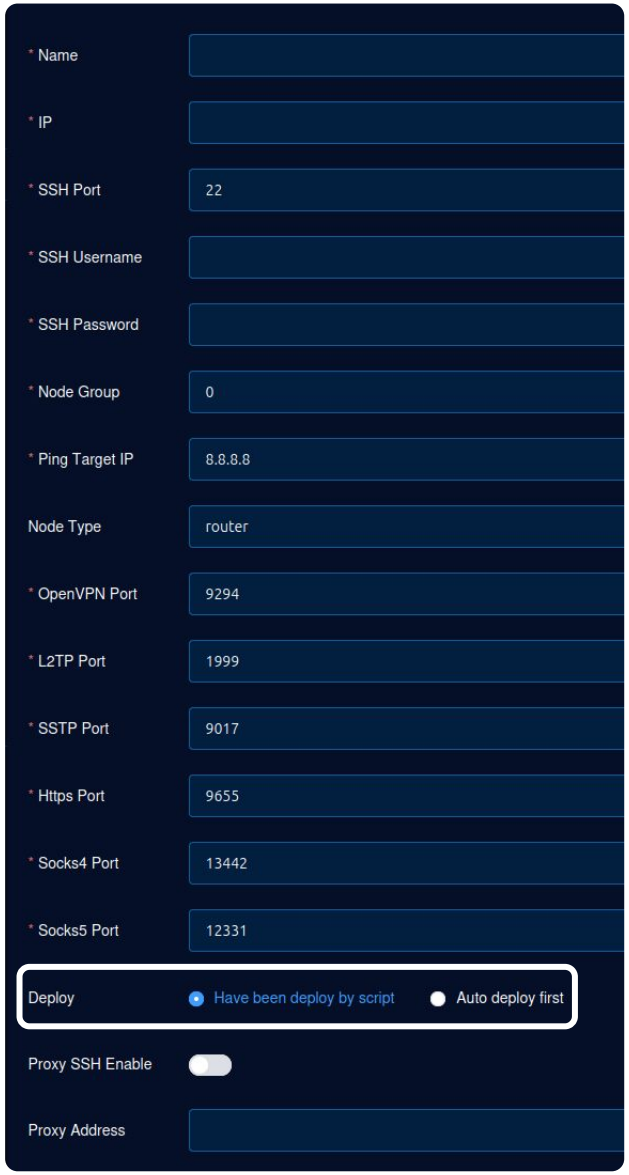

GobRAT administration interface
VPS
9 hosts
Manages
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser

Exemple actif: hxxps://47.238.154[.]134:8080/dist#/login

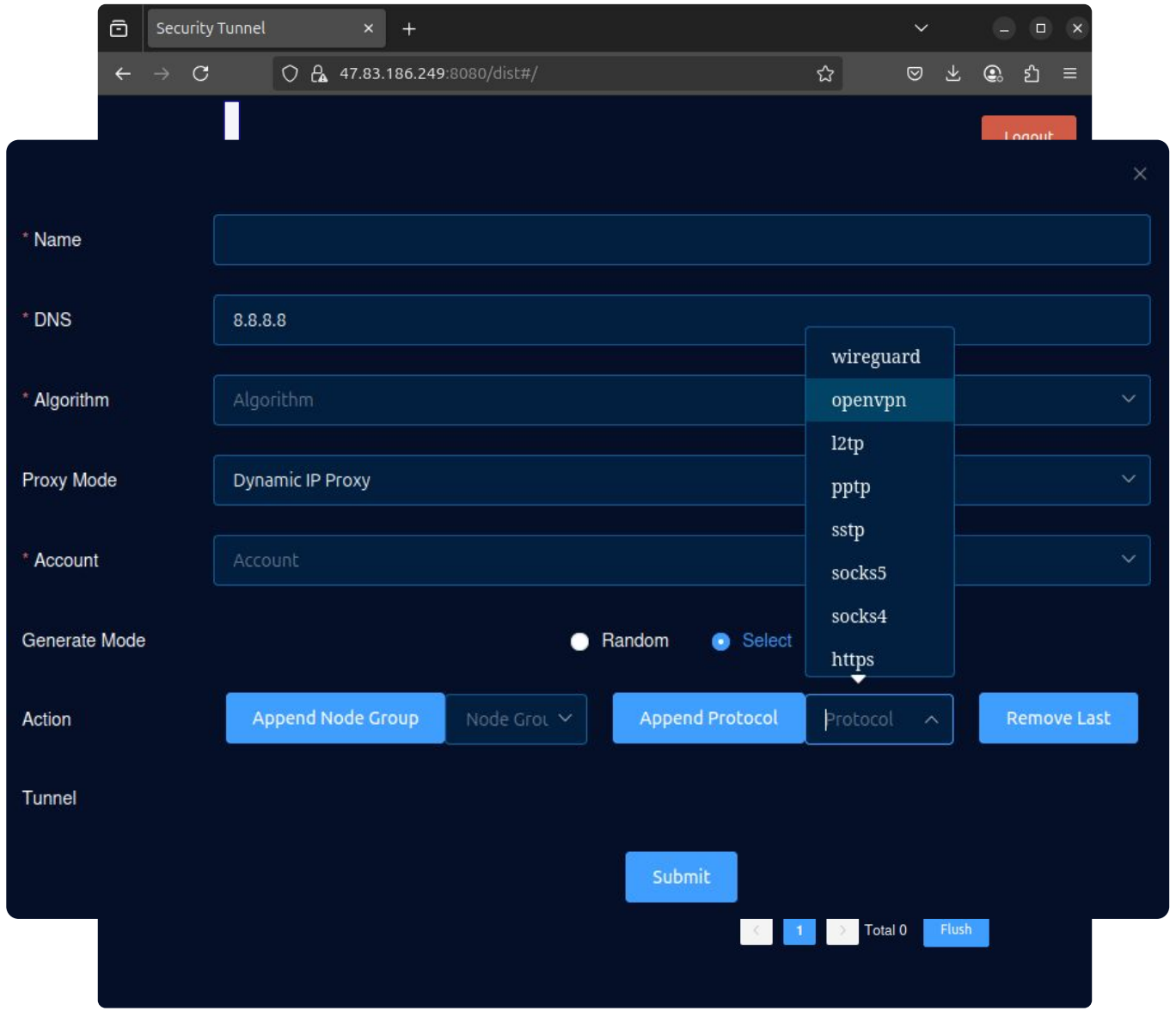


Exemple actif: hxxps://47.238.154[.]134:8080/dist#/login

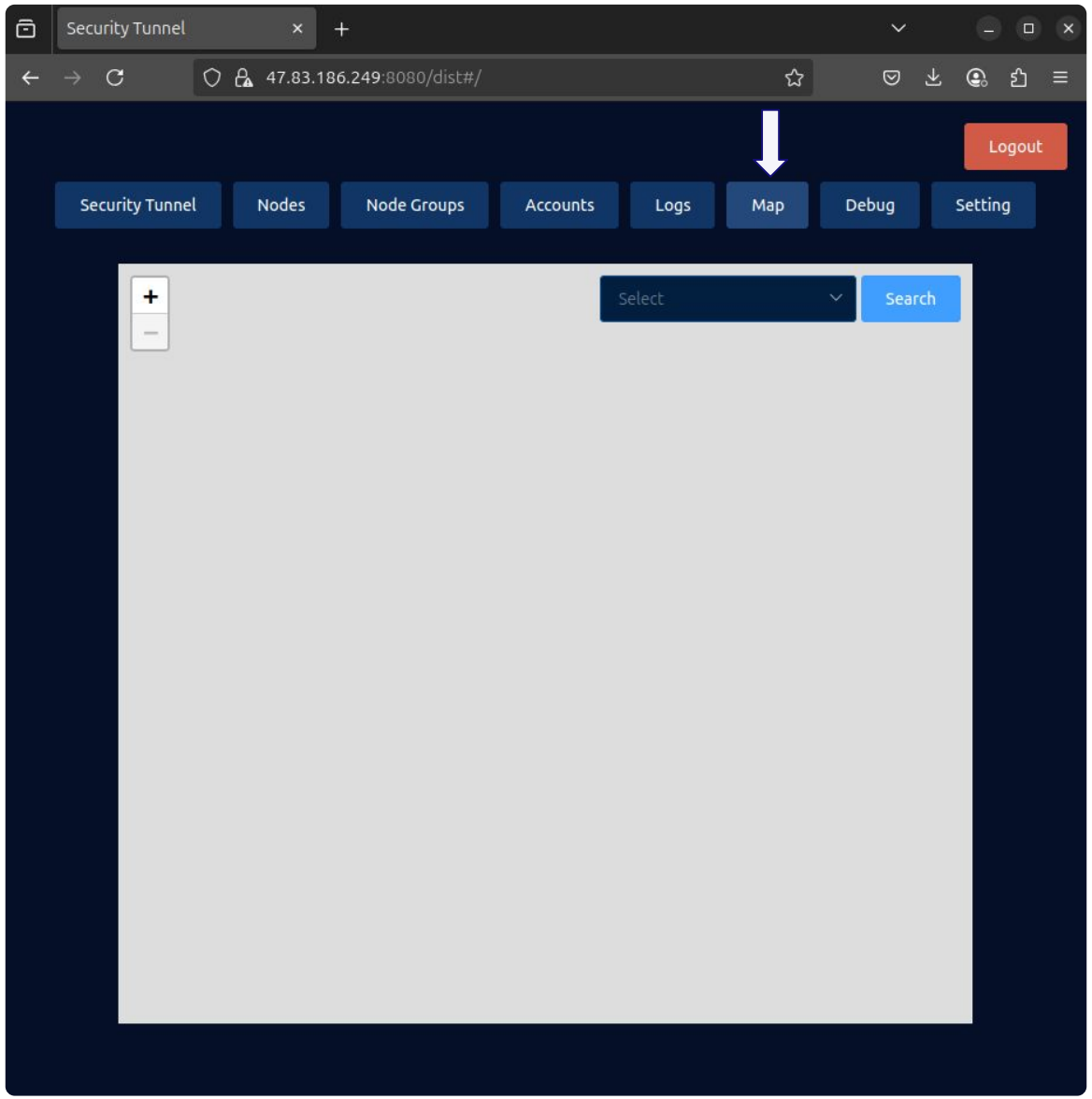




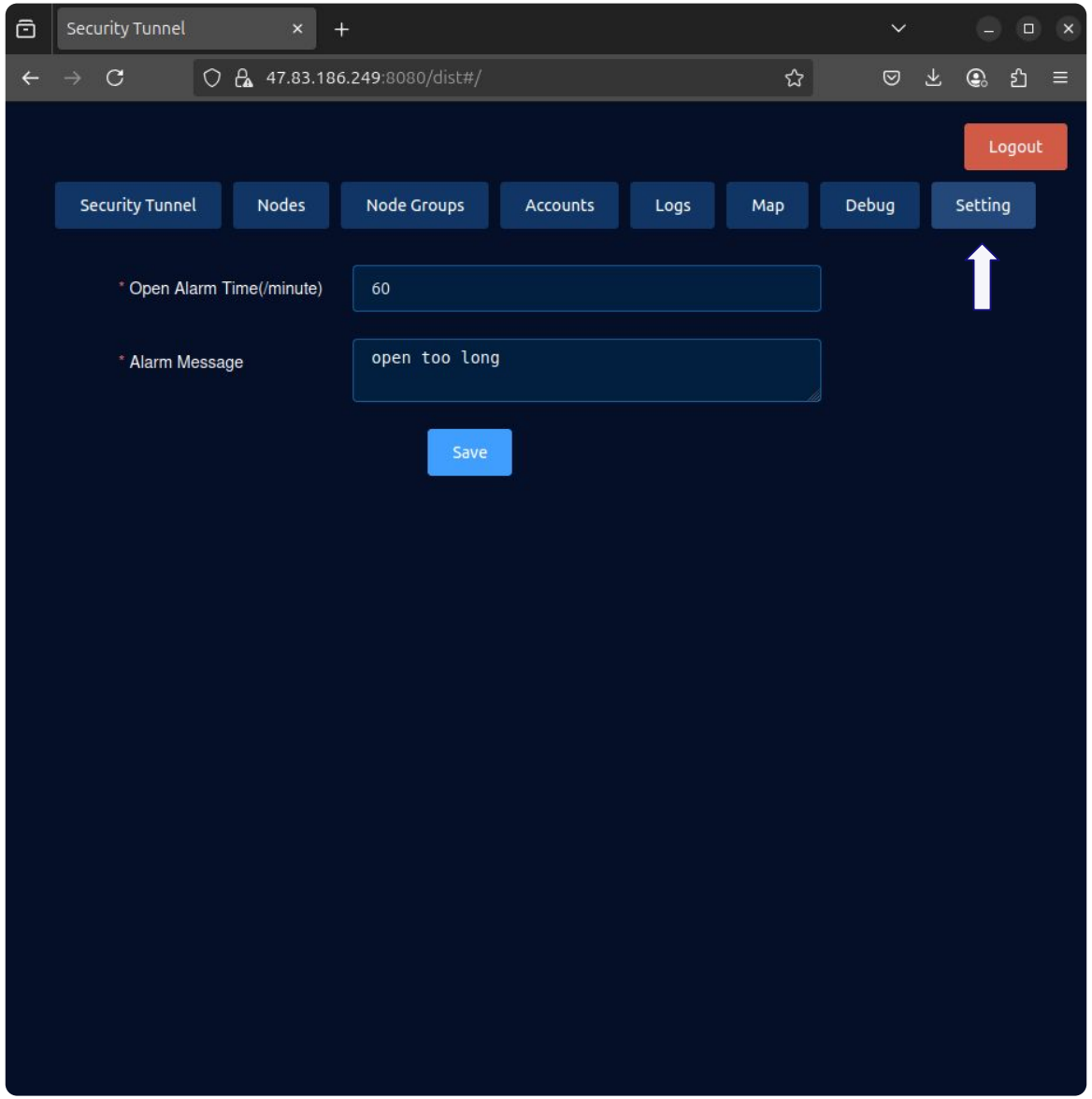
Exemple actif: hxxps://47.238.154[.]134:8080/dist#/login

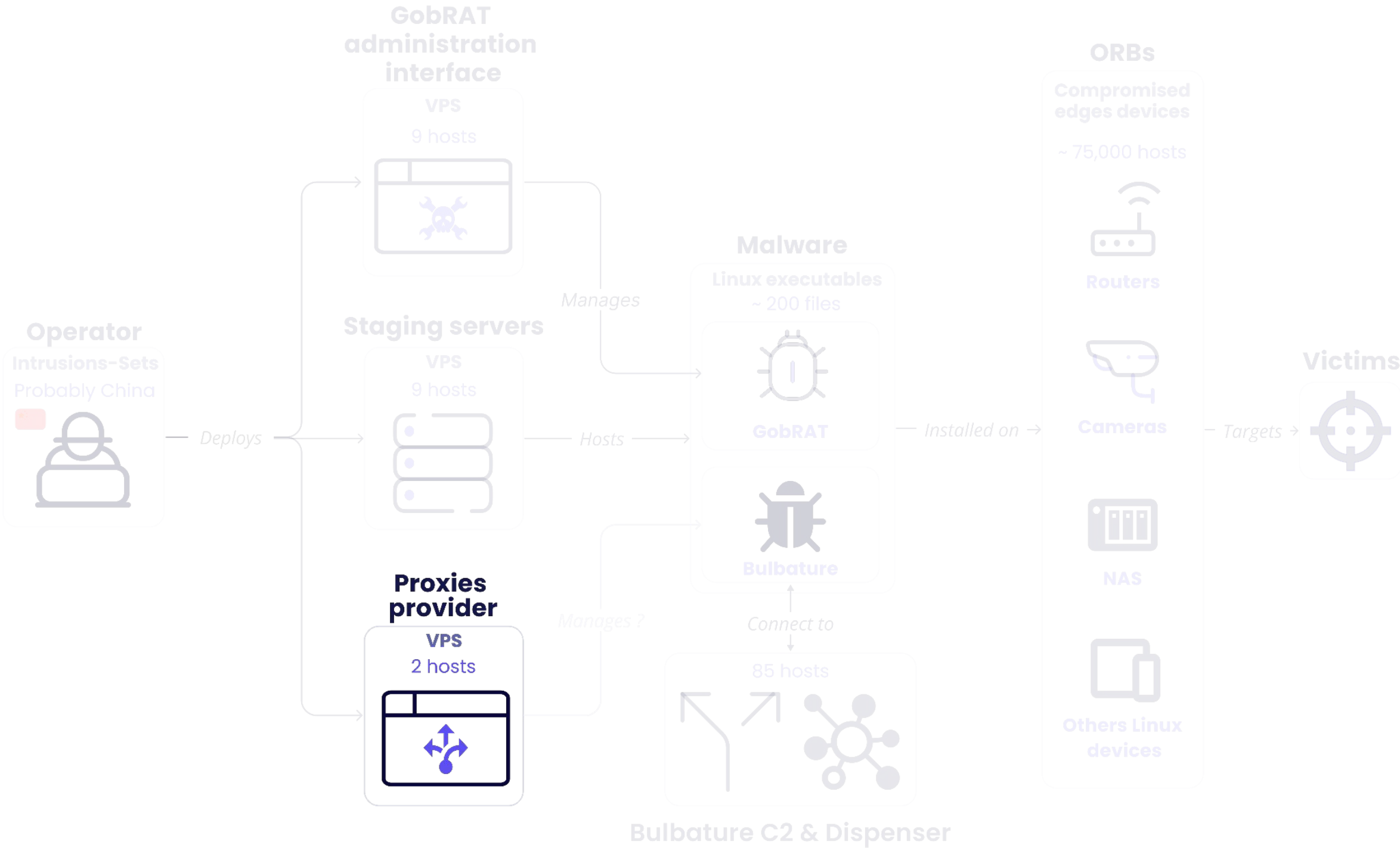


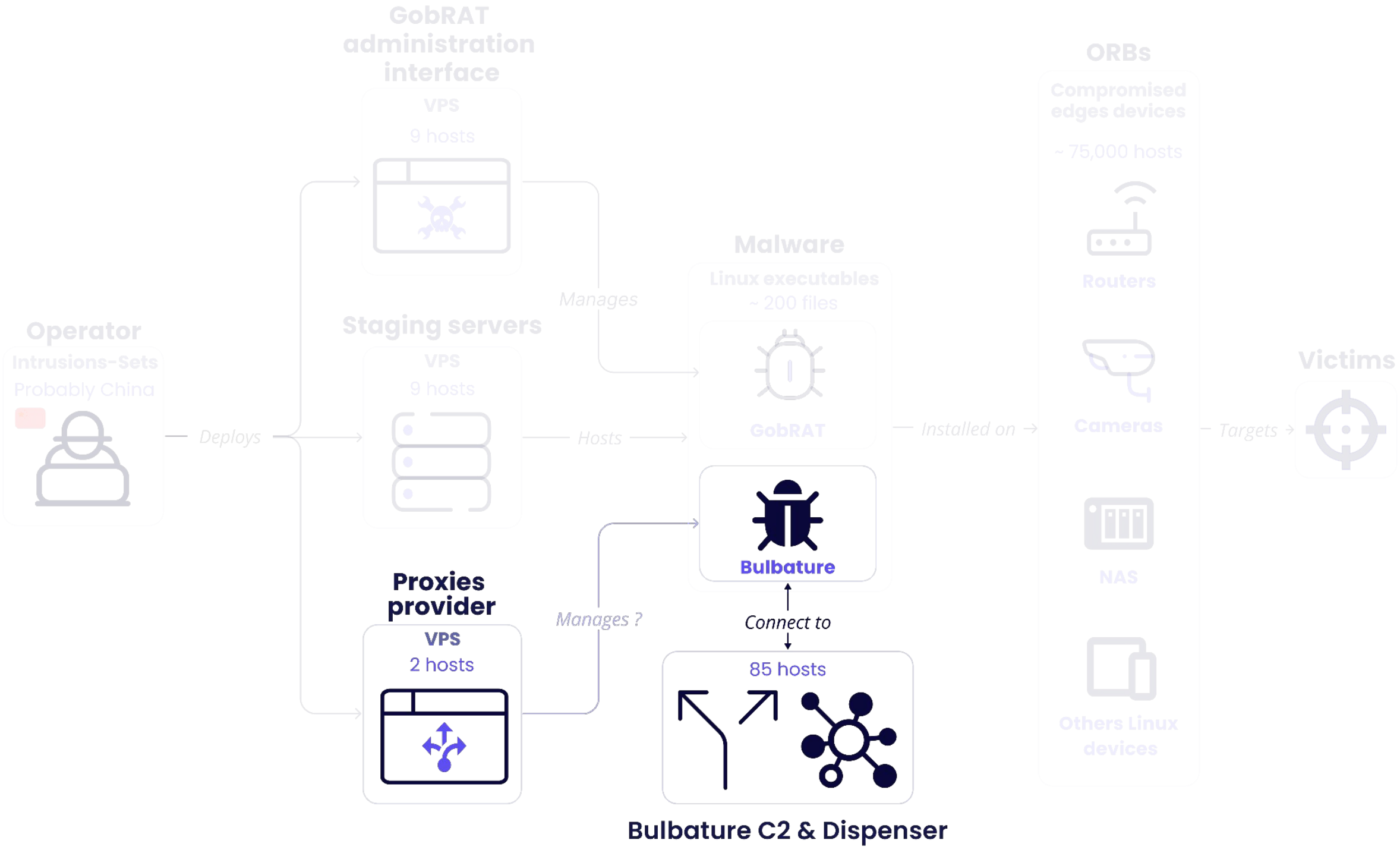
Exemple actif: hxxps://47.238.154[.]134:8080/dist#/login

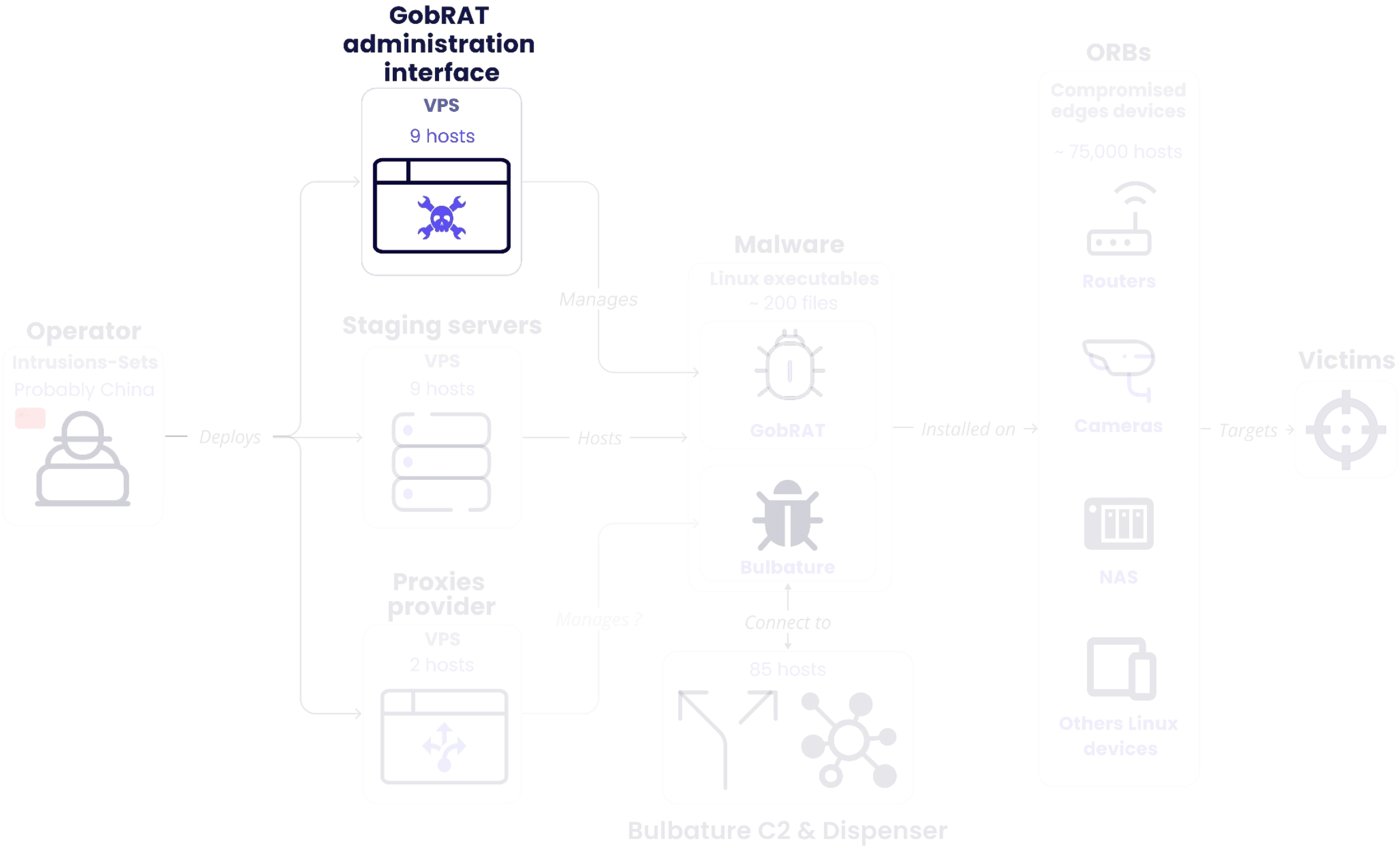


Exemple actif: hxxps://47.238.154[.]134:8080/dist#/login

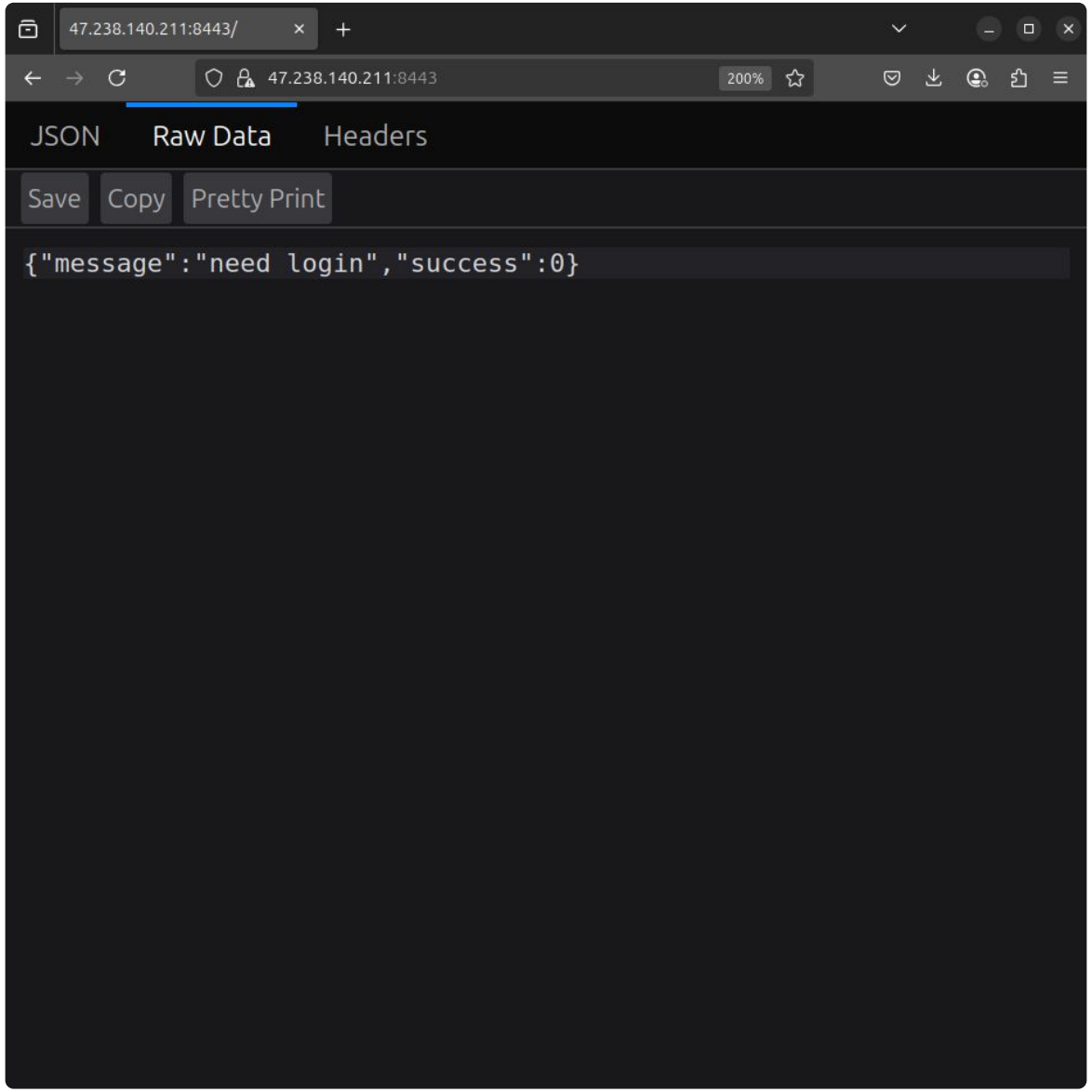



GobRAT administration interface
VPS
9 hosts
Manages
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser

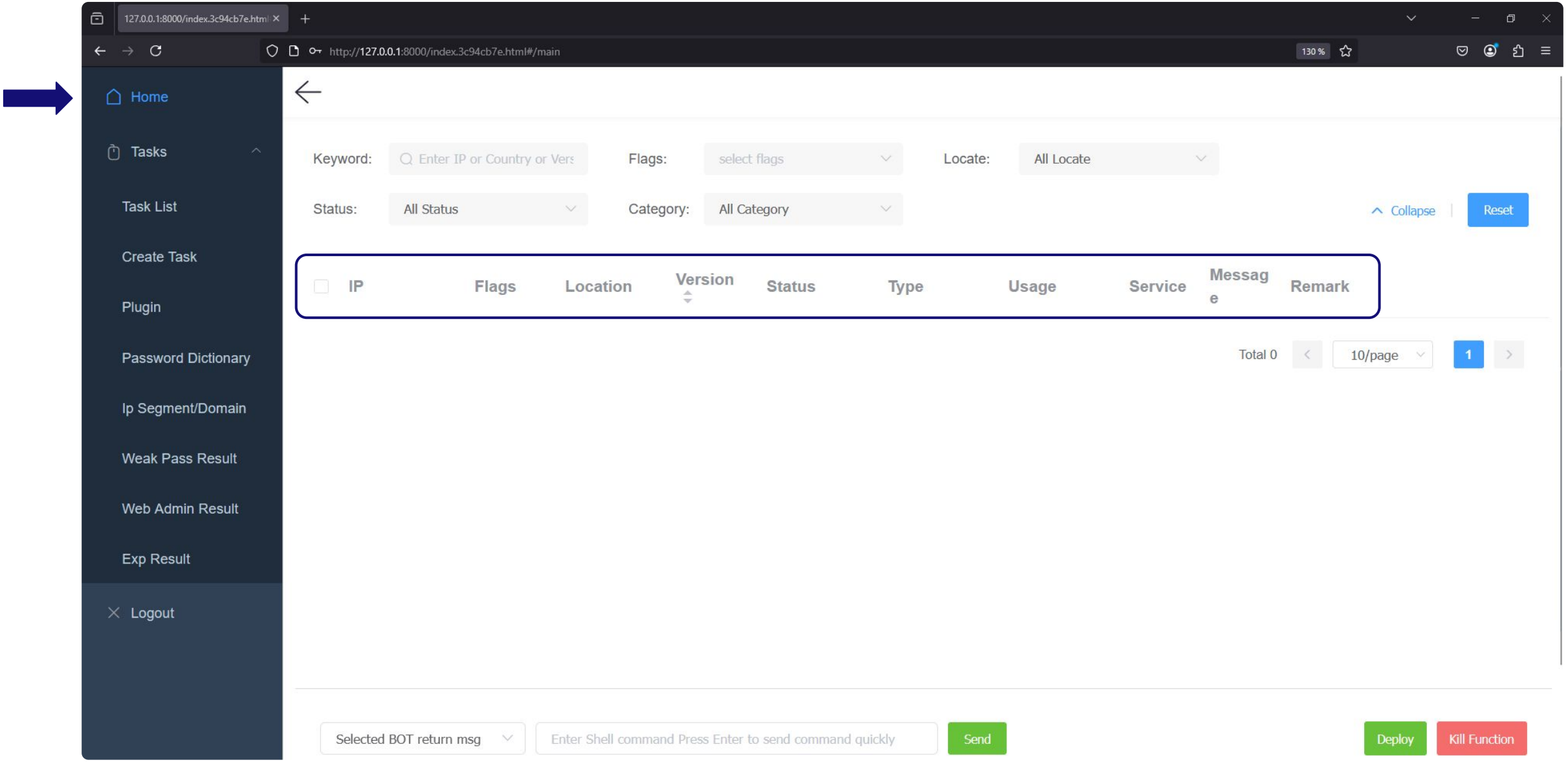

GobRAT administration interface
VPS
9 hosts
Manages
Malware
Linux executables
~ 200 files
GobRAT
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Installed on
Targets
Victims
Bulbature
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser


GobRAT administration interface
VPS
9 hosts
Manages
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser

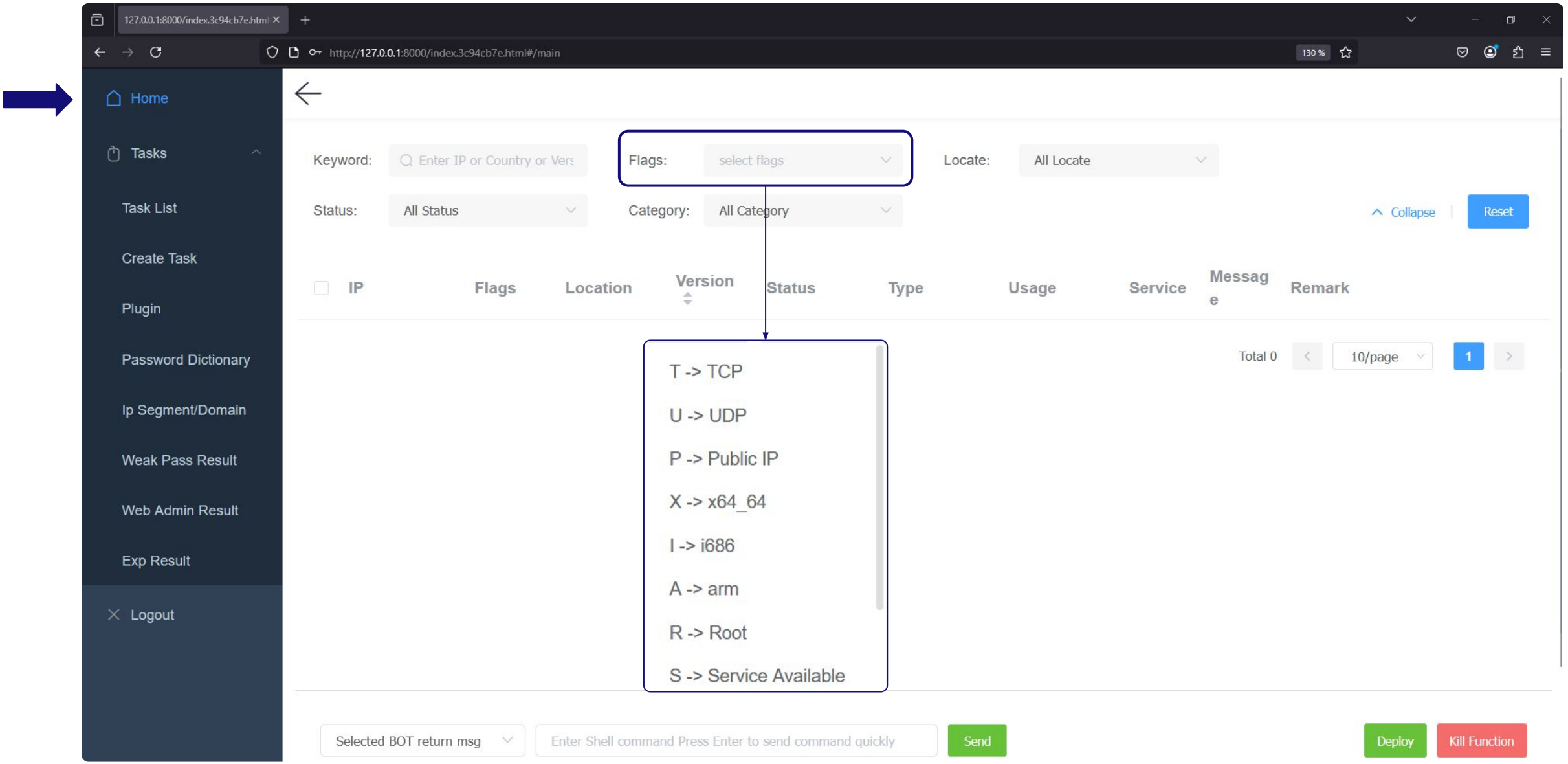
Exemple actif: hxxps://158.255.208[.]85:42208/assets/



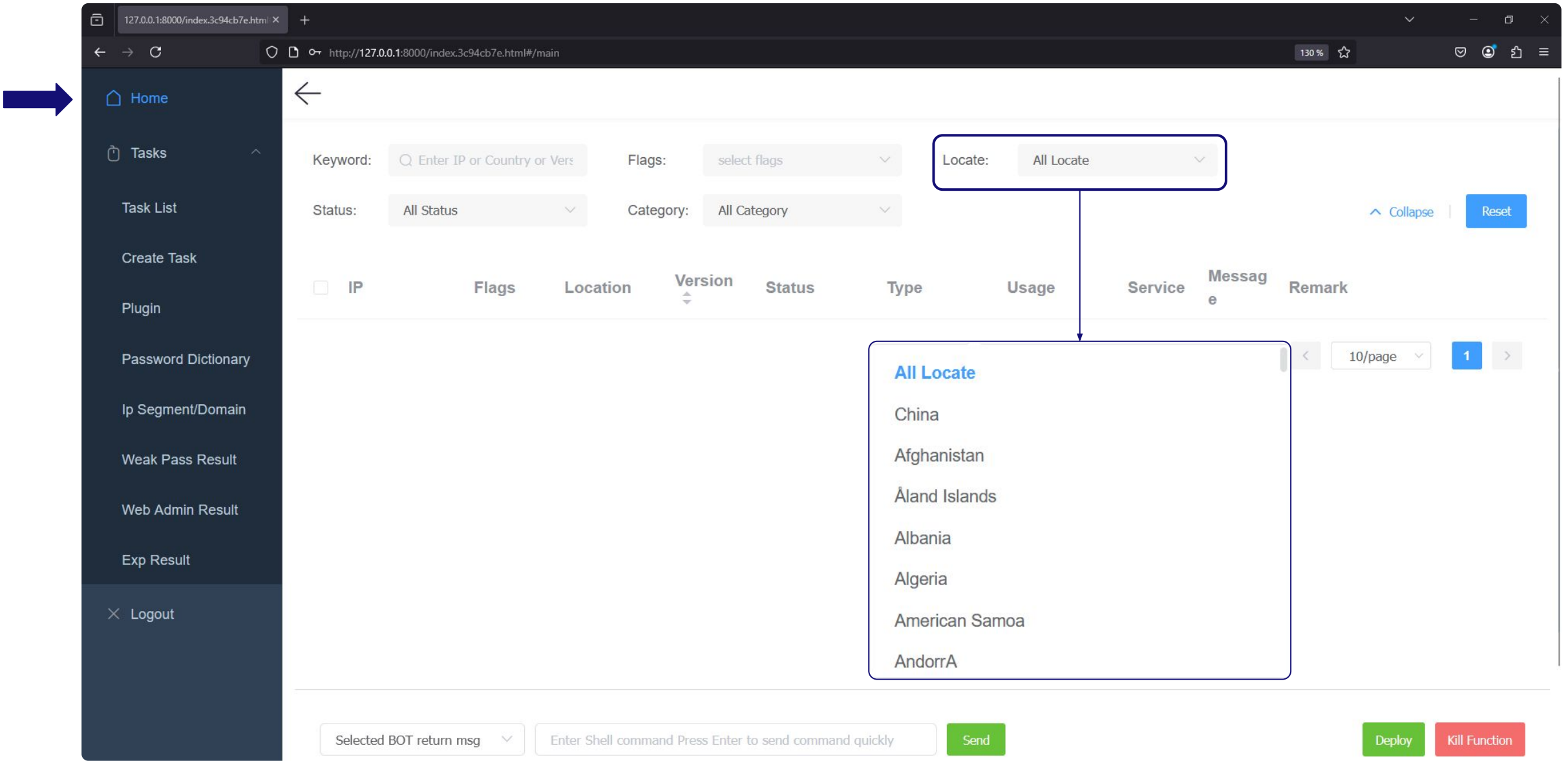
Exemple actif: hxxps://158.255.208[.]85:42208/assets/



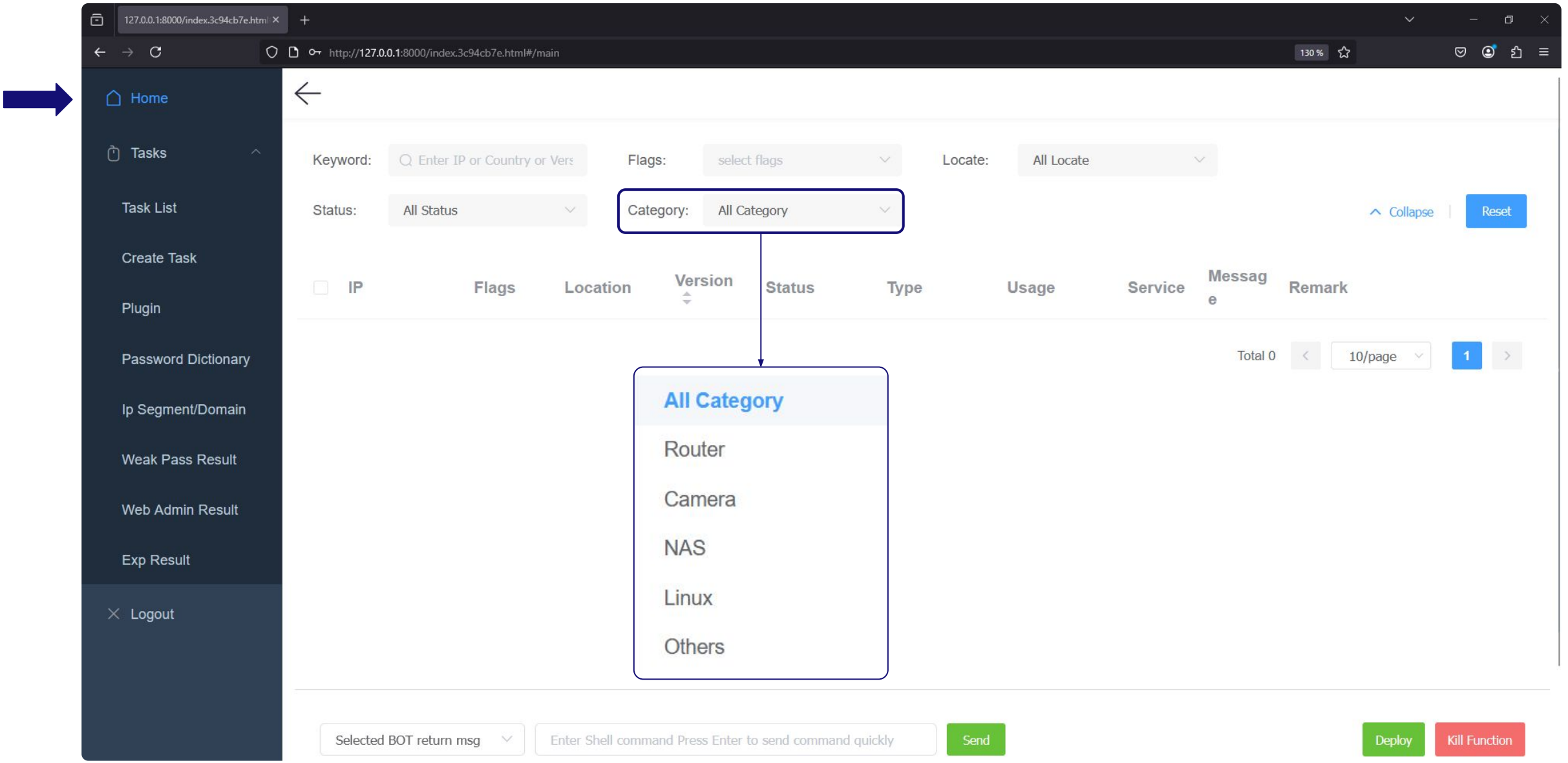
Exemple actif: hxxps://158.255.208[.]85:42208/assets/



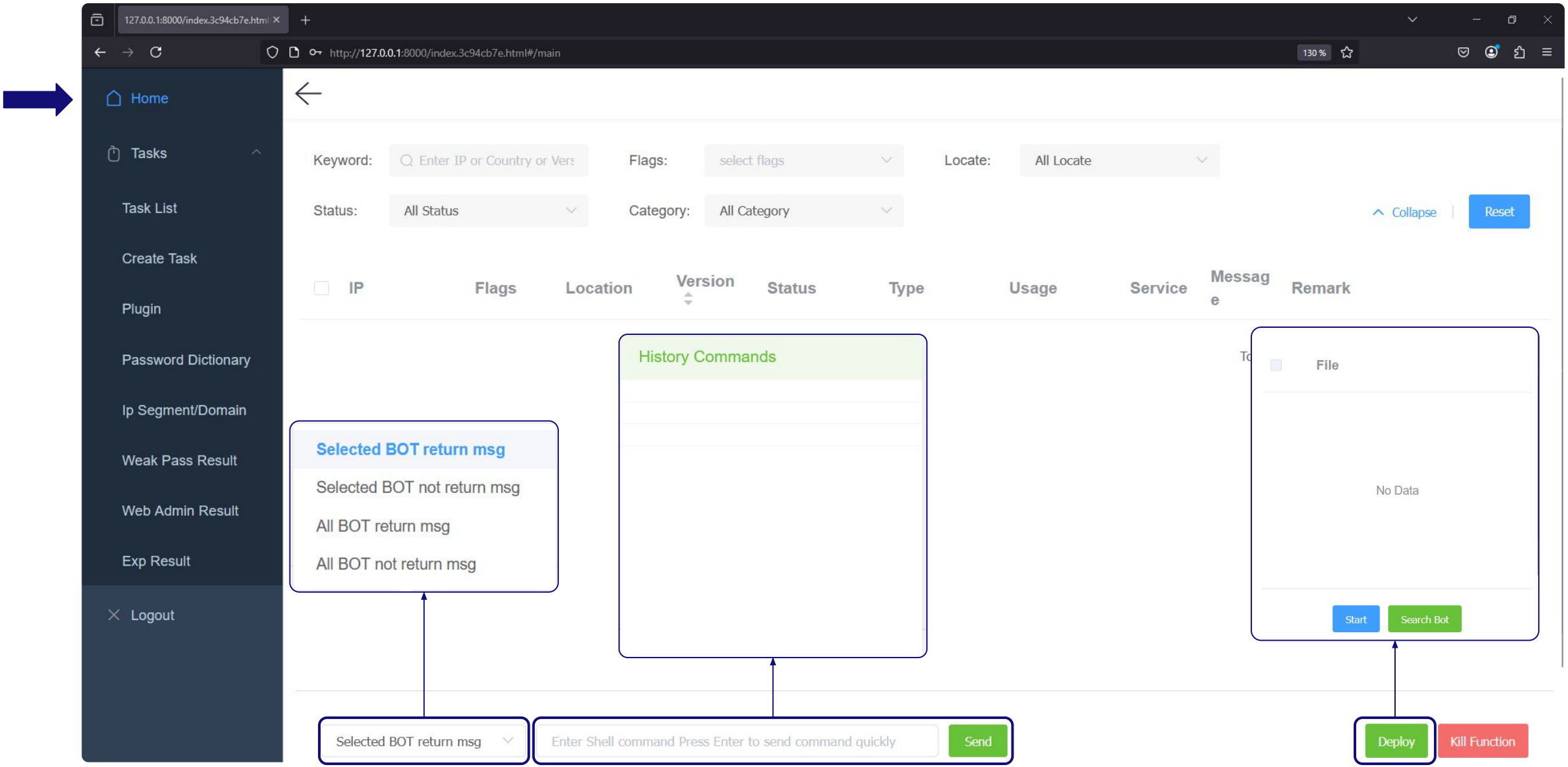
Exemple actif: hxxps://158.255.208[.]85:42208/assets/



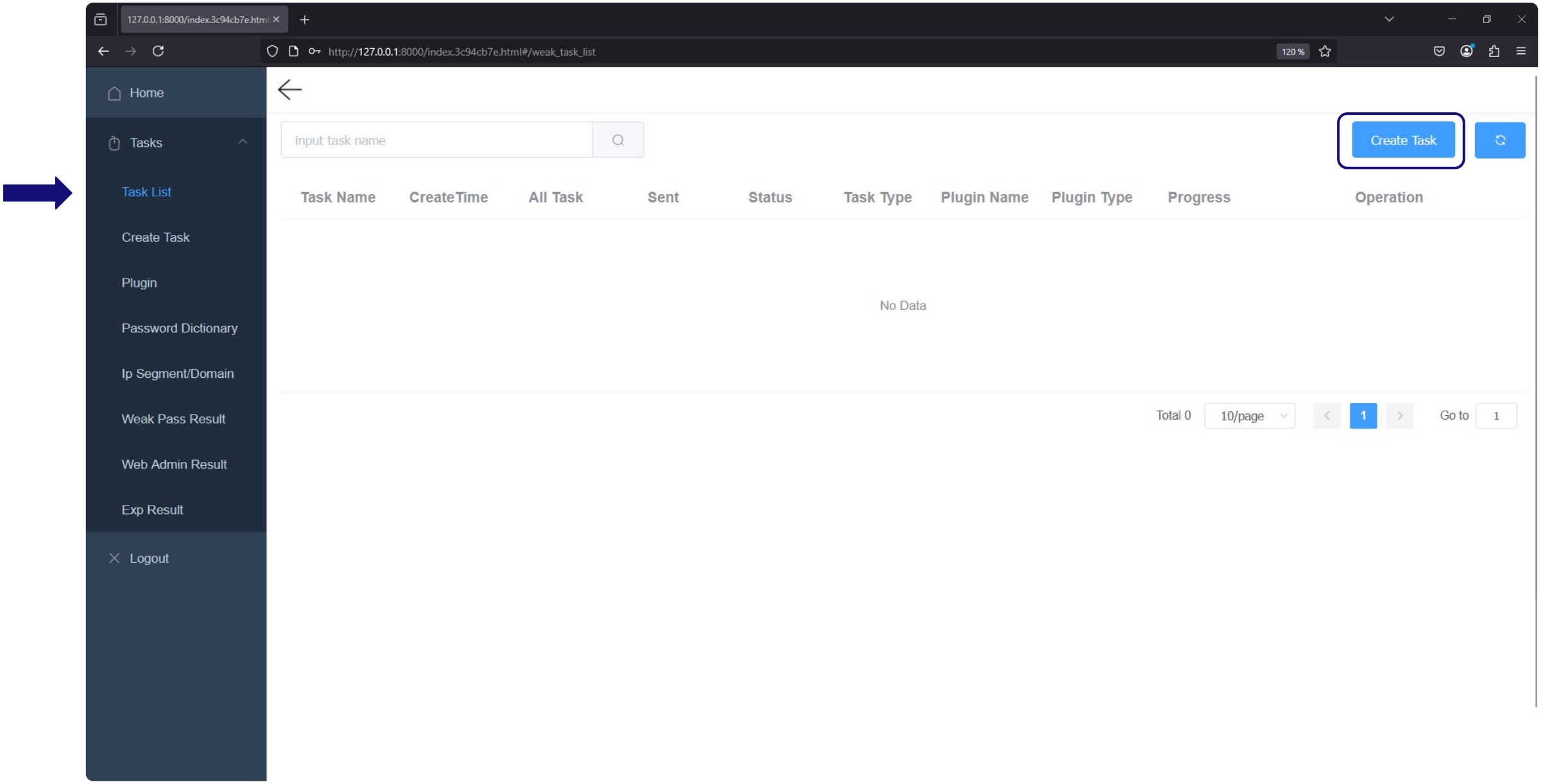
Exemple actif: hxxps://158.255.208[.]85:42208/assets/

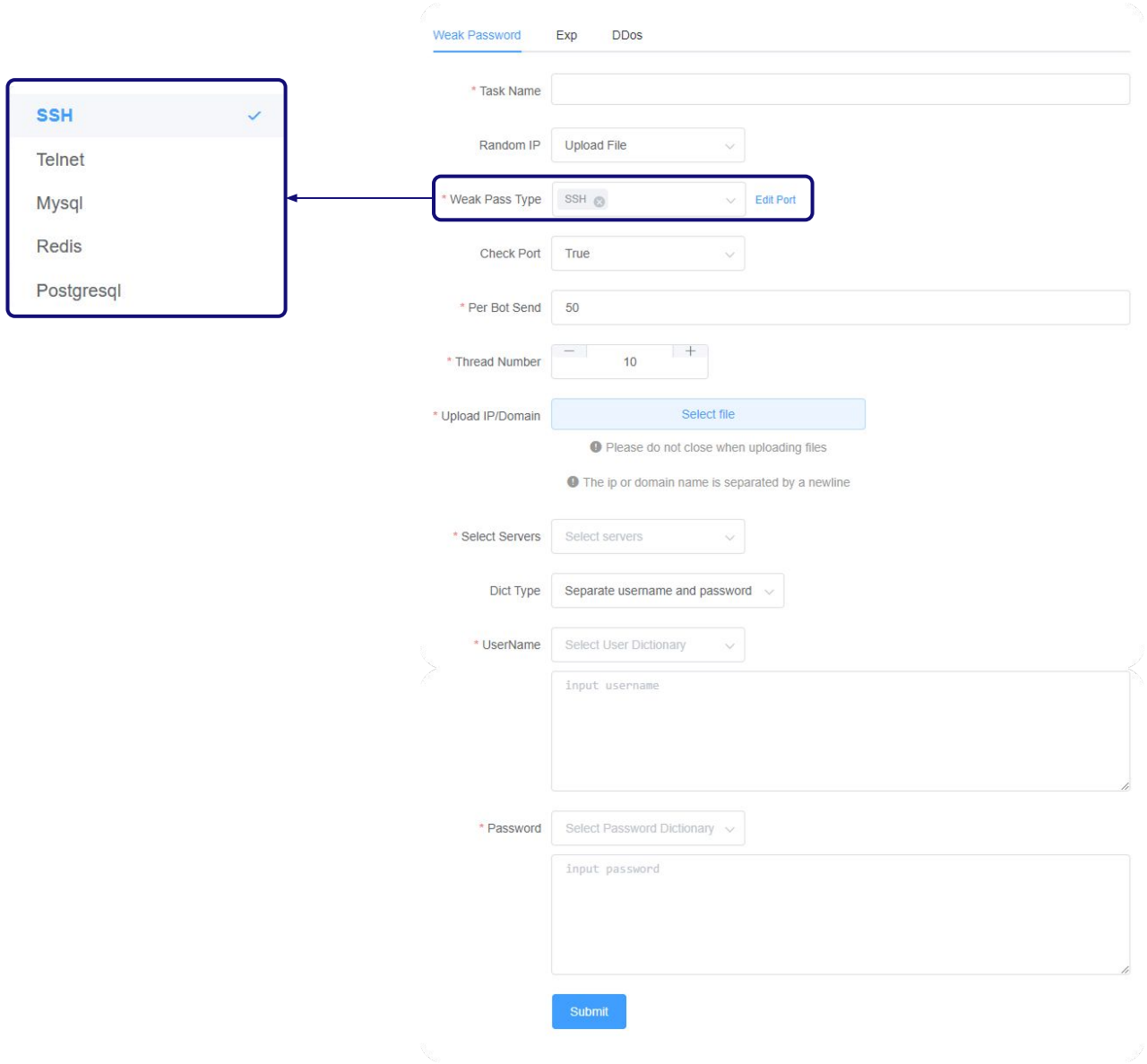


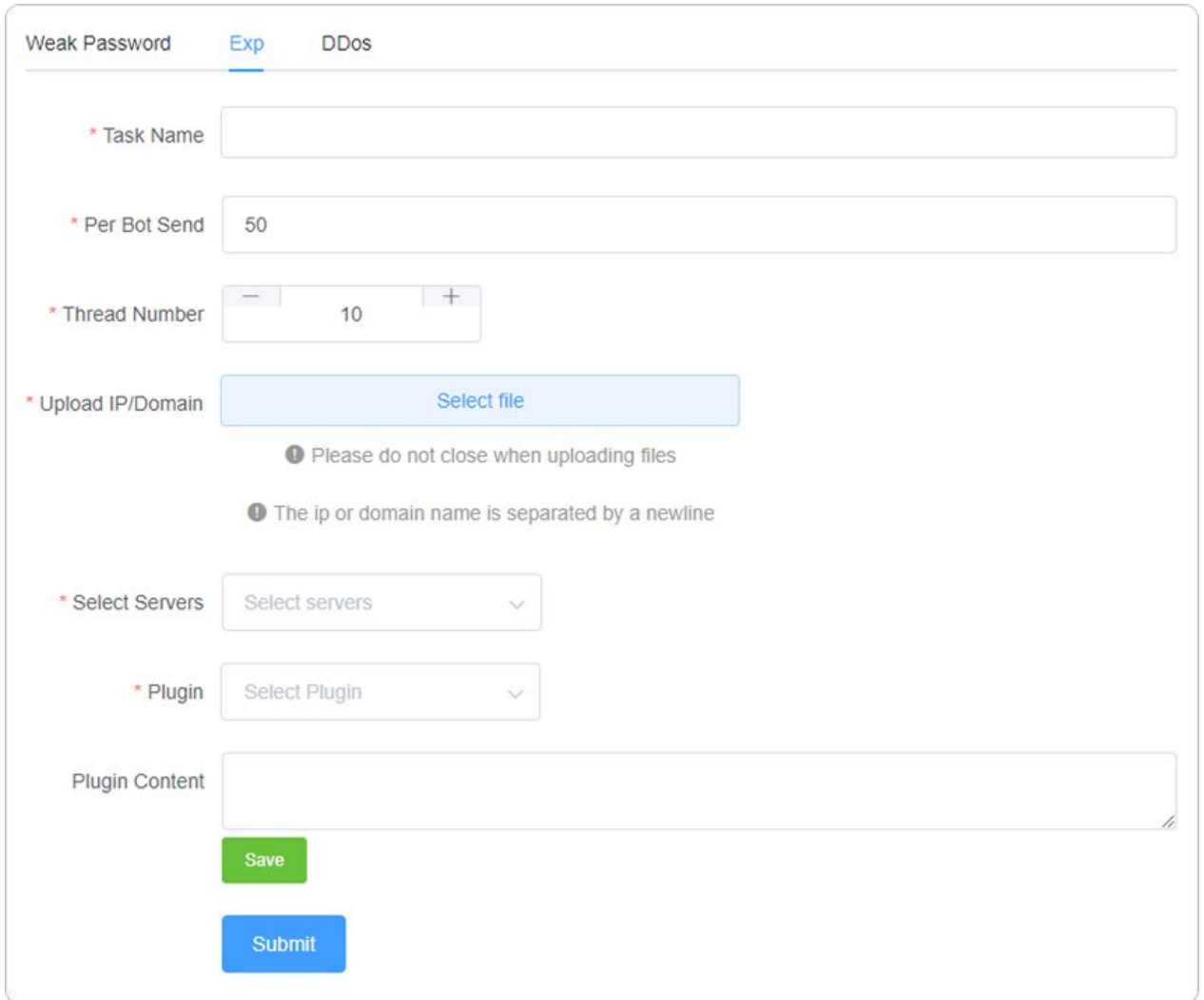
Exemple actif: hxxps://158.255.208[.]85:42208/assets/

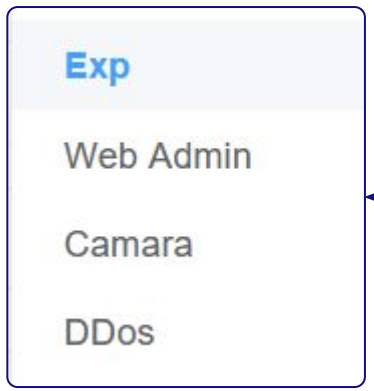


Exemple actif: hxxps://158.255.208[.]85:42208/assets/




SSH
Telnet
Mysql
Redis
Postgresql
Weak Password
Exp
DDos
* Task Name
Random IP
Upload File
* Weak Pass Type
SSH
Edit Port
Check Port
True
* Per Bot Send
50
* Thread Number
10
* Upload IP/Domain
Select file
Please do not close when uploading files
The ip or domain name is separated by a newline
* Select Servers
Select servers
Dict Type
Separate username and password
* UserName
Select User Dictionary
input username
* Password
Select Password Dictionary
input password
Submit


Weak Password
Exp
DDos
* Task Name
* Per Bot Send
50
* Thread Number
10
* Upload IP/Domain
Select file
Please do not close when uploading files
The ip or domain name is separated by a newline
* Select Servers
Select servers
* Plugin
Select Plugin
Plugin Content
Save
Submit



Add New Plugin

* Plugin Name: NorthSec 2025 🚀 : my plugin

* Plugin Type: Exp

step1 × | step2 | step3 | step4

Exp Name: exp1

Uri: /result

Method: POST

Packet Format: example:{{username}}:{{ password }}

Headers: header key | header value | Add

Success Http Code: 200

Code With Other Relation: and

Success Body Contains: dashbord

Success Headers Contains: dashbord

Contains Relation: and

Success Body Regular: (?i)(dashboard)

Success Header Regular: (?i)(content-type)

Regular Relation: and

Failed Body Contain: 401

Return Body Contain: (?i)(router)

Return Headers Contain: (?)(content-type:())

Get Cookie First

Continue Next Step

Sleep(s): 0

Cancel | Confirm

Weak Password | Exp | DDos

* Task Name

* Target

Select Ip Segment

Multiple ip/domain segments are separated by newlines

Ports

Except http type, others are required,Multiple ports are separated by commas

* Thread Number

10

* Start Time

2025-04-27 22:18:10

Duration(unit:s)

10

* Select Servers

Select servers

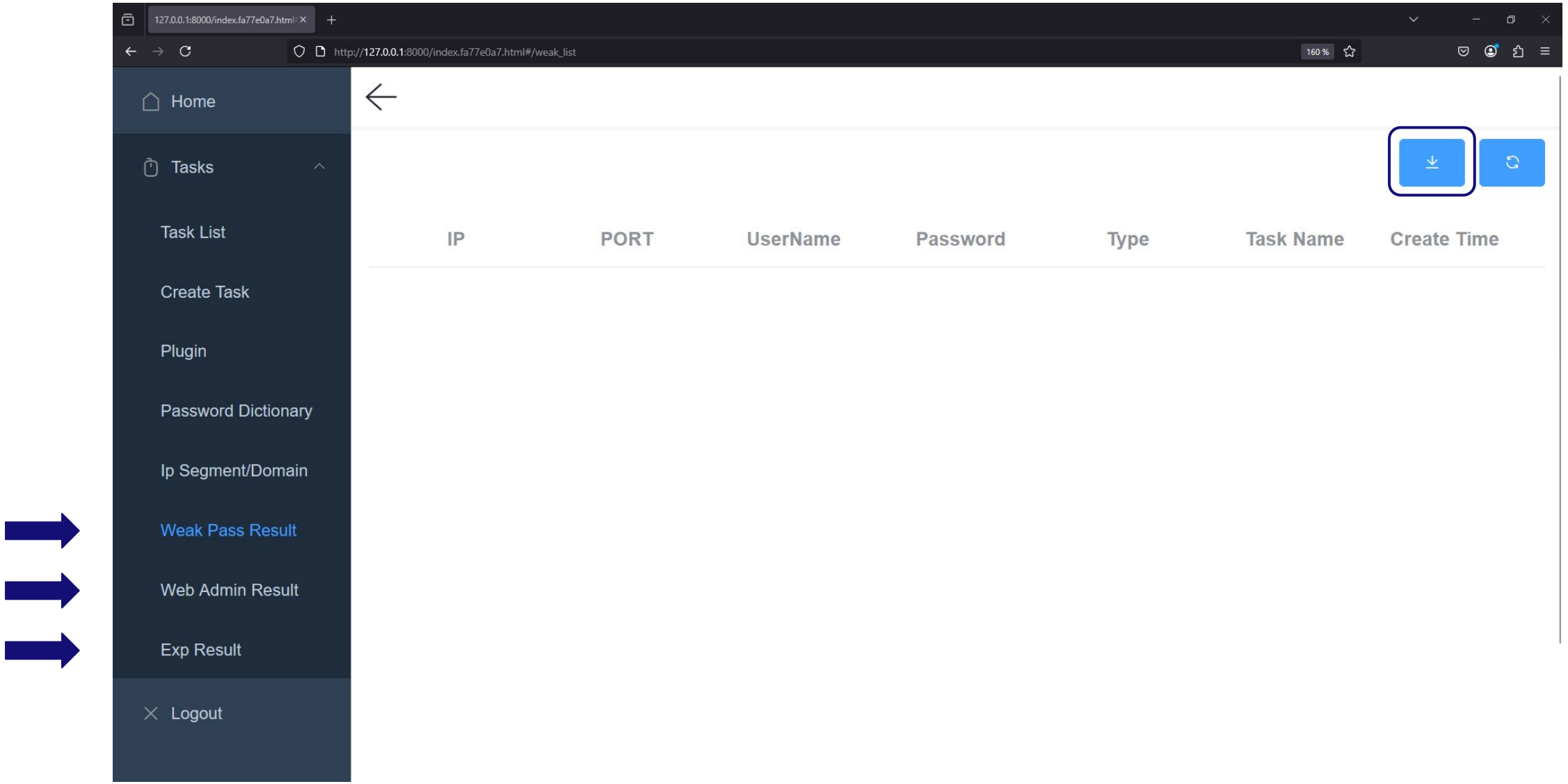
* Plugin

Select Plugin

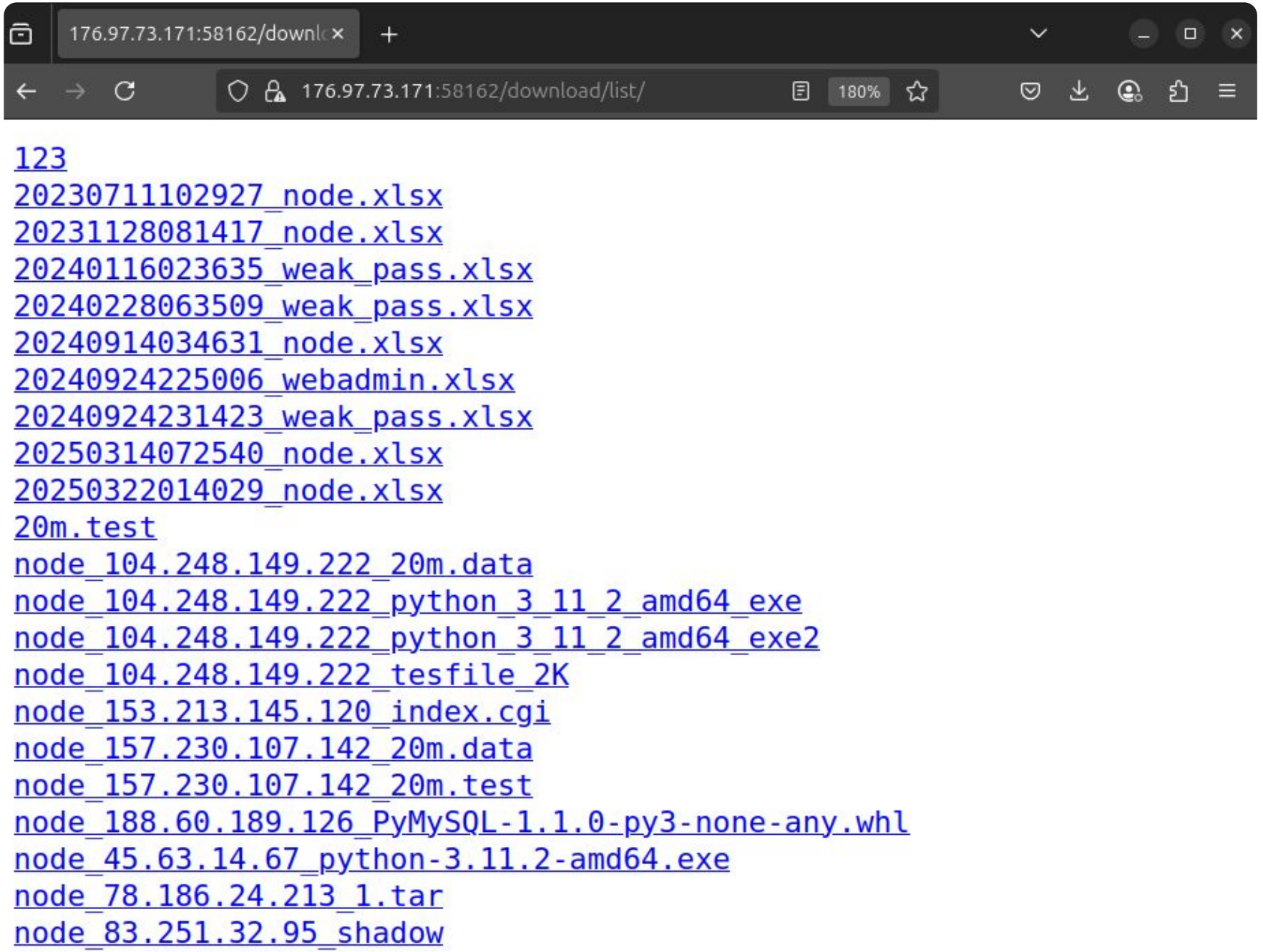
Plugin Content

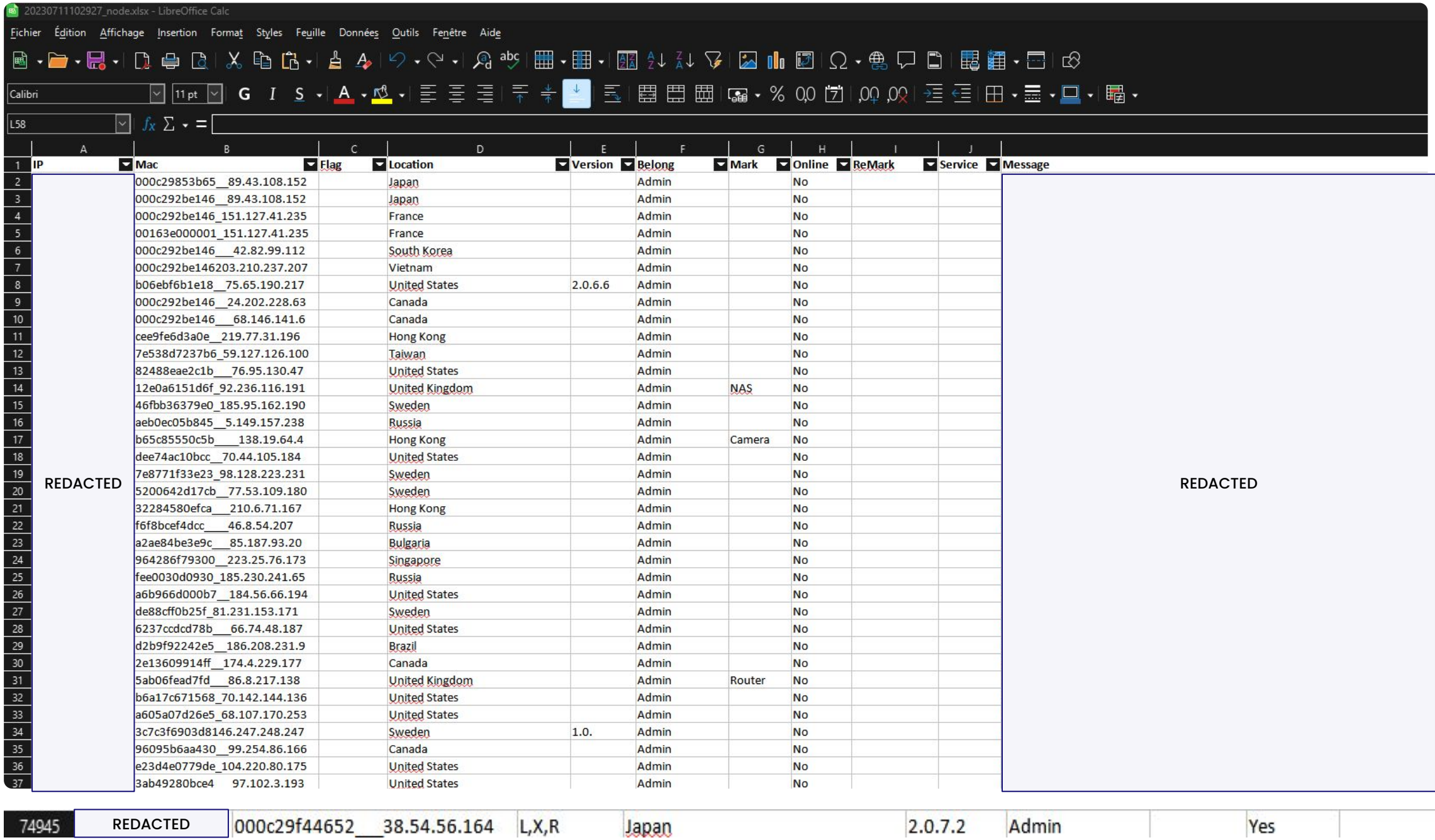
Save

Submit


127.0.0.1:8000/index.fa77e0a7.html
http://127.0.0.1:8000/index.fa77e0a7.html#/weak_list
160 %
Home
Tasks
Task List
Create Task
Plugin
Password Dictionary
Ip Segment/Domain
Weak Pass Result
Web Admin Result
Exp Result
Logout
IP
PORT
UserName
Password
Type
Task Name
Create Time

Export via l'interface avec timestamp




20230711102927_node.xlsx - LibreOffice Calc

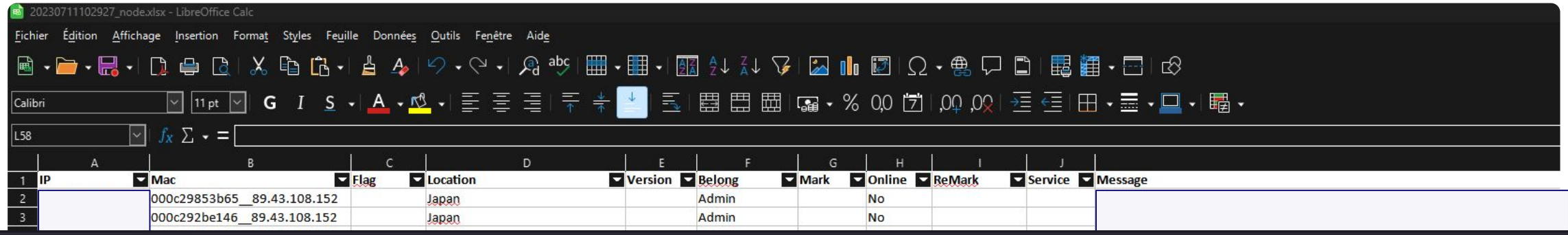
Fichier Édition Affichage Insertion Format Styles Feuille Données Outils Fenêtre Aide

Calibri 11 pt

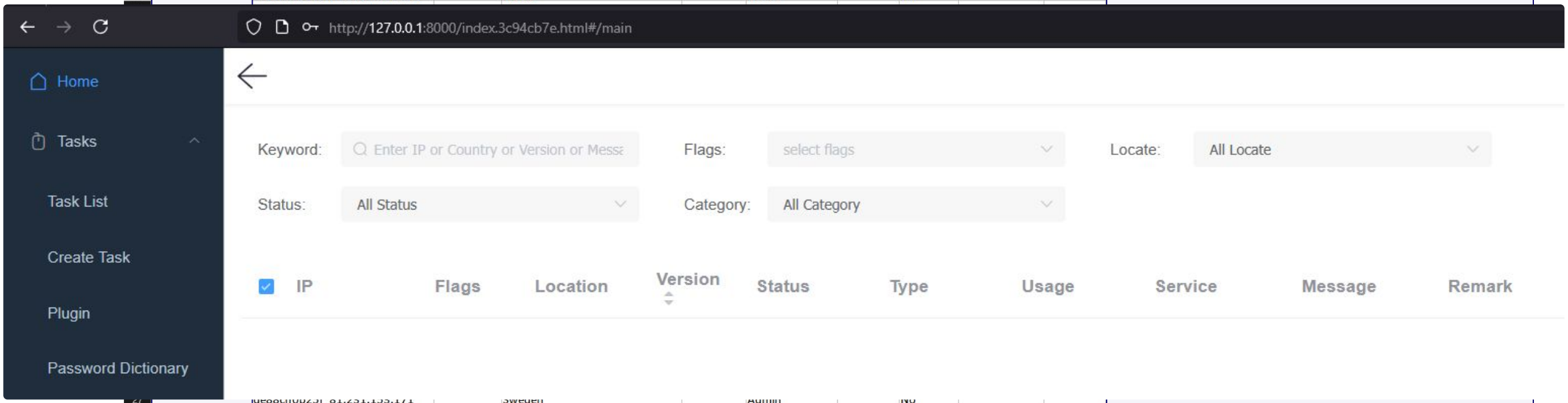
L58

	A	B	C	D	E	F	G	H	I	J	
1	IP	Mac	Flag	Location	Version	Belong	Mark	Online	ReMark	Service	Message
2	REDACTED	000c29853b65__89.43.108.152		Japan		Admin		No			REDACTED
3		000c292be146__89.43.108.152		Japan		Admin		No			
4		000c292be146_151.127.41.235		France		Admin		No			
5		00163e000001_151.127.41.235		France		Admin		No			
6		000c292be146___42.82.99.112		South Korea		Admin		No			
7		000c292be146203.210.237.207		Vietnam		Admin		No			
8		b06ebf6b1e18__75.65.190.217		United States	2.0.6.6	Admin		No			
9		000c292be146__24.202.228.63		Canada		Admin		No			
10		000c292be146___68.146.141.6		Canada		Admin		No			
11		cee9fe6d3a0e__219.77.31.196		Hong Kong		Admin		No			
12		7e538d7237b6_59.127.126.100		Taiwan		Admin		No			
13		82488eae2c1b___76.95.130.47		United States		Admin		No			
14		12e0a6151d6f_92.236.116.191		United Kingdom		Admin	NAS	No			
15		46fbb36379e0_185.95.162.190		Sweden		Admin		No			
16		aeb0ec05b845__5.149.157.238		Russia		Admin		No			
17		b65c85550c5b____138.19.64.4		Hong Kong		Admin	Camera	No			
18		dee74ac10bcc__70.44.105.184		United States		Admin		No			
19		7e8771f33e23_98.128.223.231		Sweden		Admin		No			
20		5200642d17cb__77.53.109.180		Sweden		Admin		No			
21		32284580efca___210.6.71.167		Hong Kong		Admin		No			
22		f6f8bcef4dcc____46.8.54.207		Russia		Admin		No			
23		a2ae84be3e9c___85.187.93.20		Bulgaria		Admin		No			
24		964286f79300__223.25.76.173		Singapore		Admin		No			
25		fee0030d0930_185.230.241.65		Russia		Admin		No			
26		a6b966d000b7__184.56.66.194		United States		Admin		No			
27		de88cff0b25f_81.231.153.171		Sweden		Admin		No			
28		6237ccdcd78b___66.74.48.187		United States		Admin		No			
29		d2b9f92242e5__186.208.231.9		Brazil		Admin		No			
30		2e13609914ff__174.4.229.177		Canada		Admin		No			
31		5ab06fead7fd___86.8.217.138		United Kingdom		Admin	Router	No			
32		b6a17c671568_70.142.144.136		United States		Admin		No			
33		a605a07d26e5_68.107.170.253		United States		Admin		No			
34		3c7c3f6903d8146.247.248.247		Sweden	1.0.	Admin		No			
35		96095b6aa430__99.254.86.166		Canada		Admin		No			
36		e23d4e0779de_104.220.80.175		United States		Admin		No			
37		3ab49280bce4 97.102.3.193		United States		Admin		No			

74945	REDACTED	000c29f44652___38.54.56.164	L,X,R	Japan		2.0.7.2	Admin		Yes

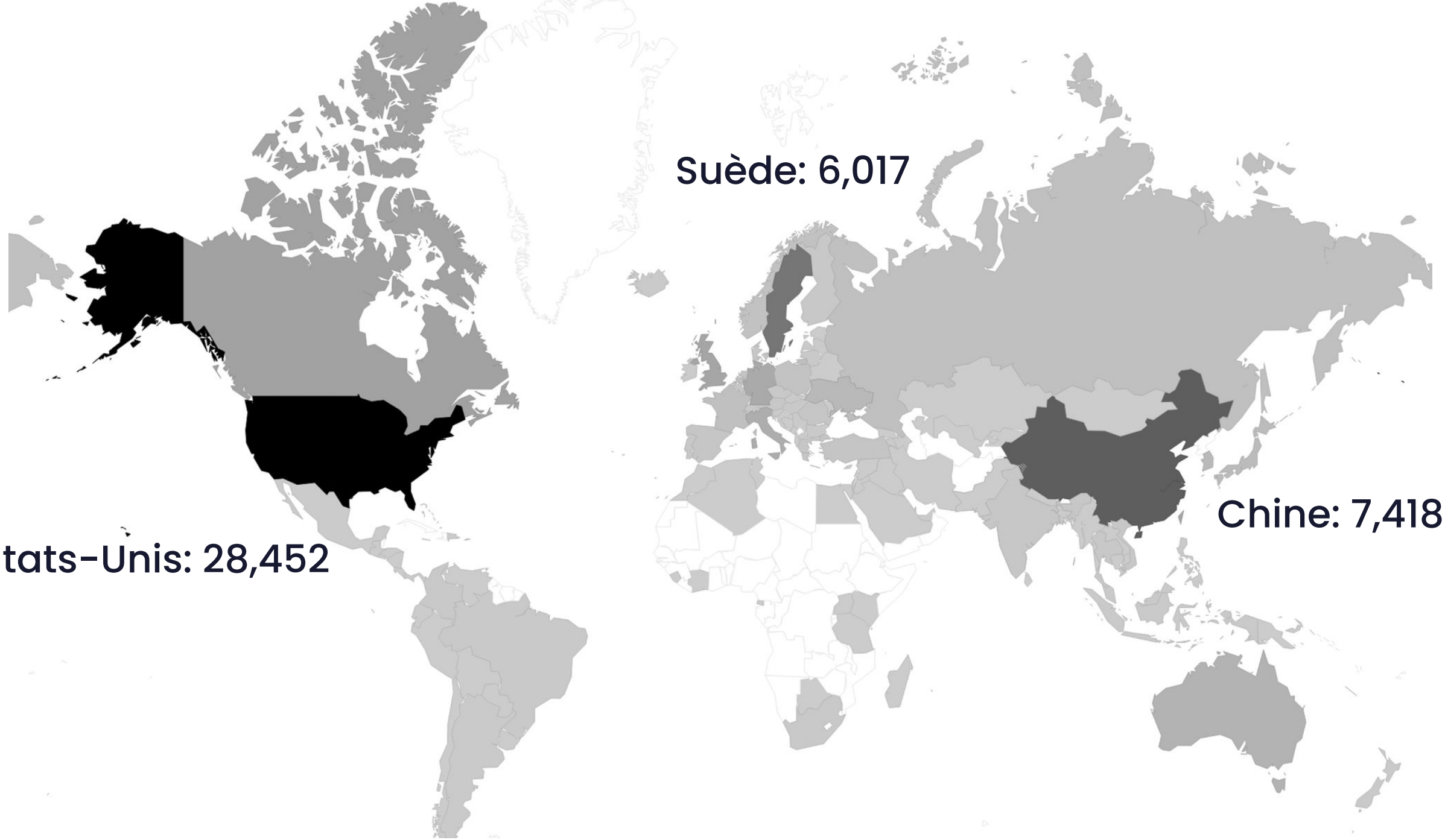


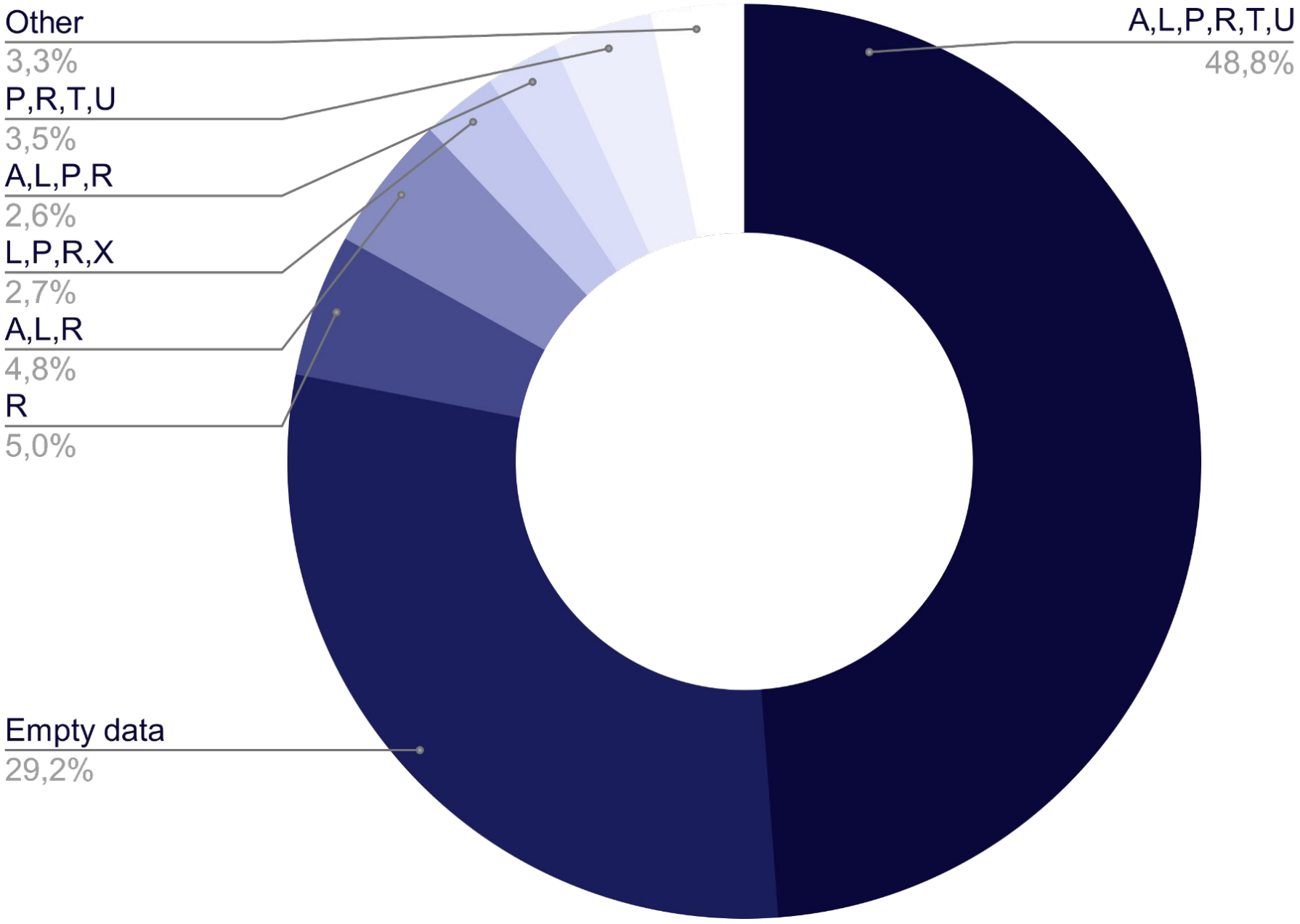
	IP	Mac	Flag	Location	Version	Belong	Mark	Online	ReMark	Service	Message
2		000c29853b65__89.43.108.152		Japan		Admin		No			
3		000c292be146__89.43.108.152		Japan		Admin		No			



	IP	Mac	Flag	Location	Version	Belong	Mark	Online	ReMark	Service	Message
28		6237ccdcd78b___66.74.48.187		United States		Admin		No			
29		d2b9f92242e5__186.208.231.9		Brazil		Admin		No			
30		2e13609914ff__174.4.229.177		Canada		Admin		No			
31		5ab06fead7fd___86.8.217.138		United Kingdom		Admin	Router	No			
32		b6a17c671568_70.142.144.136		United States		Admin		No			
33		a605a07d26e5_68.107.170.253		United States		Admin		No			
34		3c7c3f6903d8146.247.248.247		Sweden	1.0.	Admin		No			
35		96095b6aa430__99.254.86.166		Canada		Admin		No			
36		e23d4e0779de_104.220.80.175		United States		Admin		No			
37		3ab49280bce4 97.102.3.193		United States		Admin		No			

74945	REDACTED	000c29f44652___38.54.56.164	L,X,R	Japan		2.0.7.2	Admin		Yes


Suède: 6,017
Chine: 7,418
Etats-Unis: 28,452

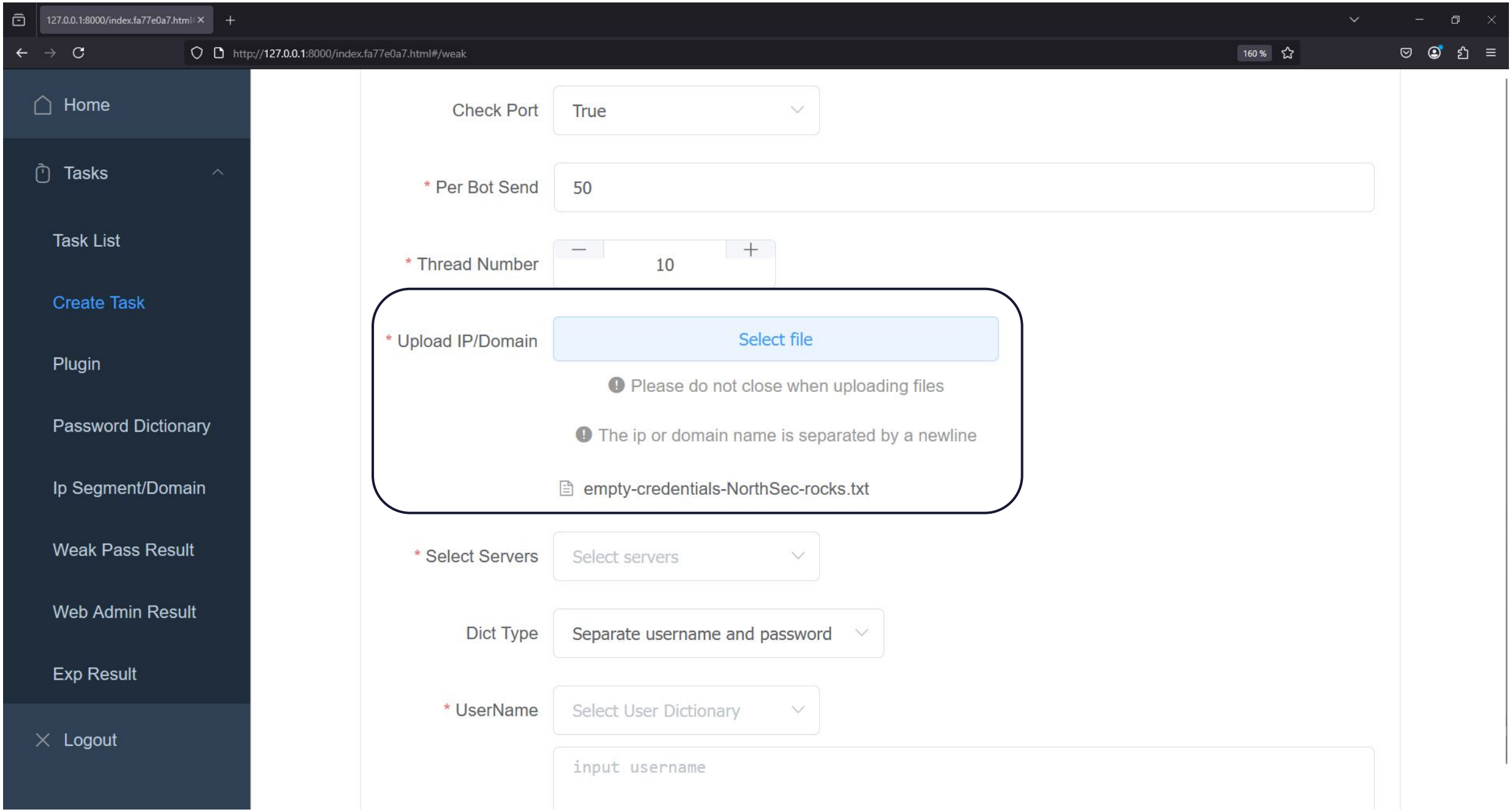


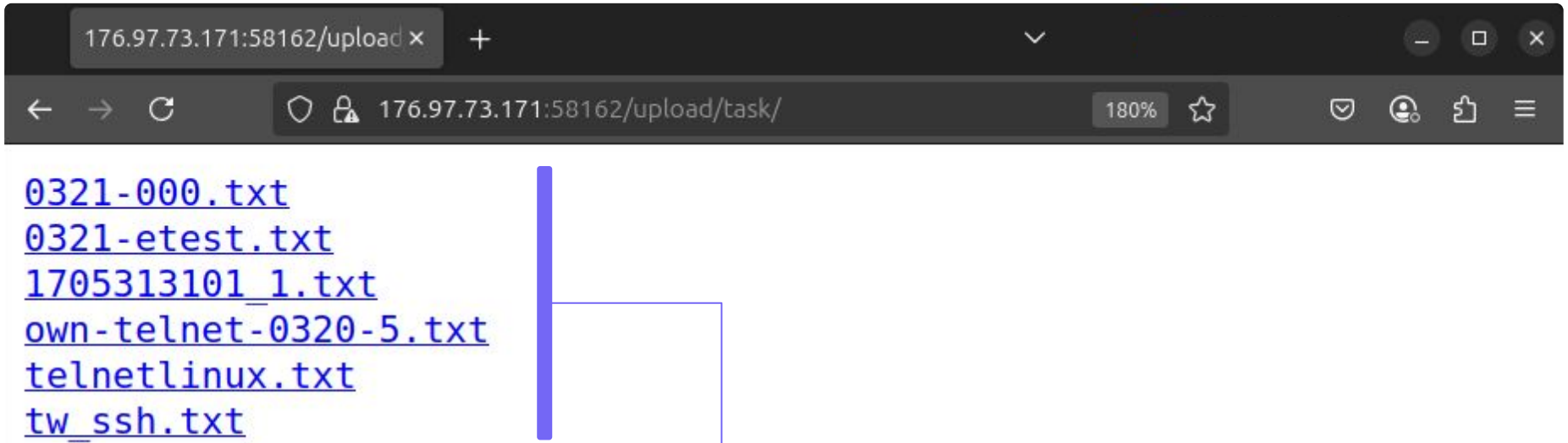
T: TCP
U: UDP
P: Public IP

X: x86_64
I: i686
A: ARM

R: Root

L: Linux
W: Windows


127.0.0.1:8000/index.fa77e0a7.html#/weak
http://127.0.0.1:8000/index.fa77e0a7.html#/weak
160 %
Home
Tasks
Task List
Create Task
Plugin
Password Dictionary
Ip Segment/Domain
Weak Pass Result
Web Admin Result
Exp Result
Logout
Check Port
True
* Per Bot Send
50
* Thread Number
10
* Upload IP/Domain
Select file
Please do not close when uploading files
The ip or domain name is separated by a newline
empty-credentials-NorthSec-rocks.txt
* Select Servers
Select servers
Dict Type
Separate username and password
* UserName
Select User Dictionary
input username

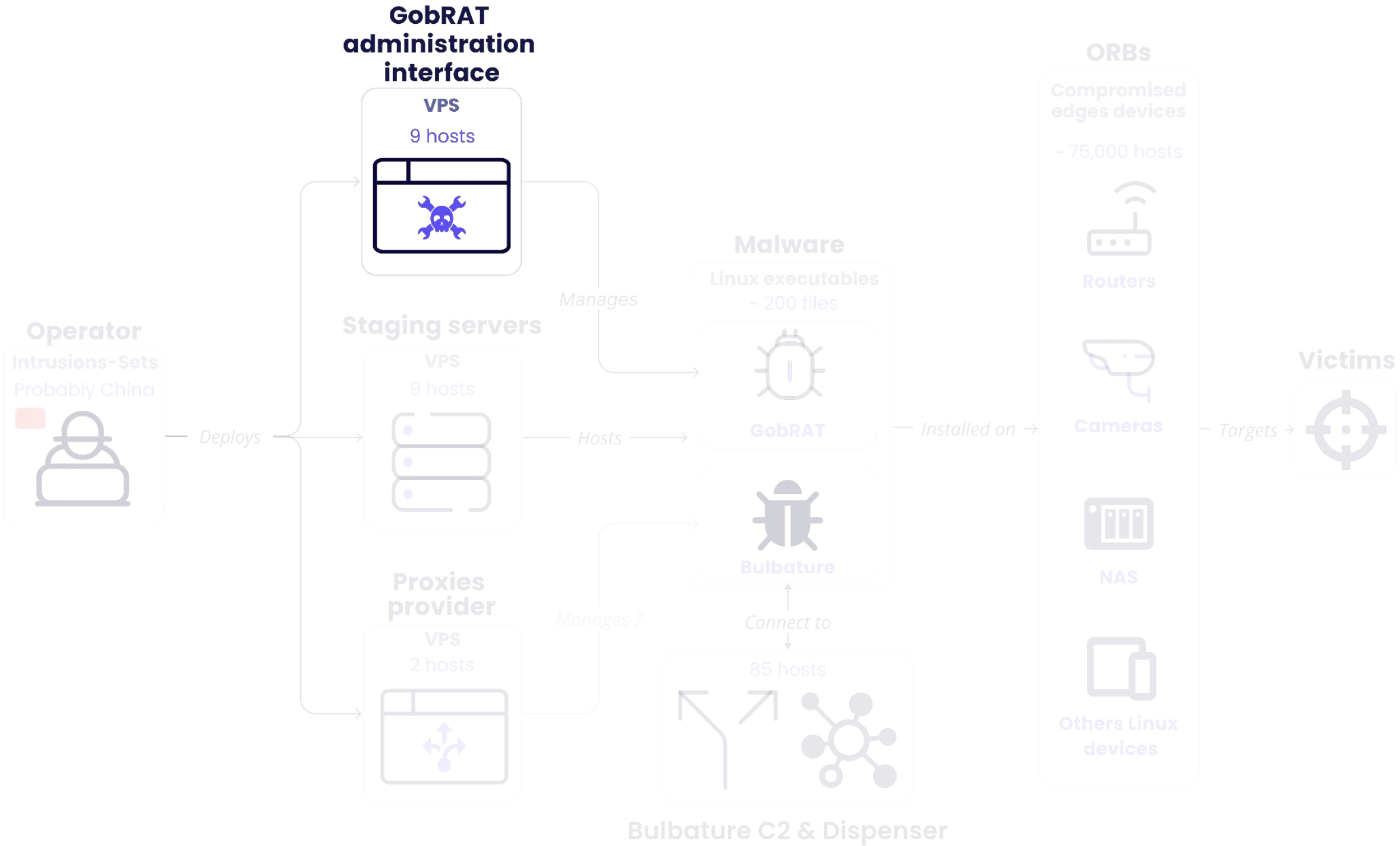


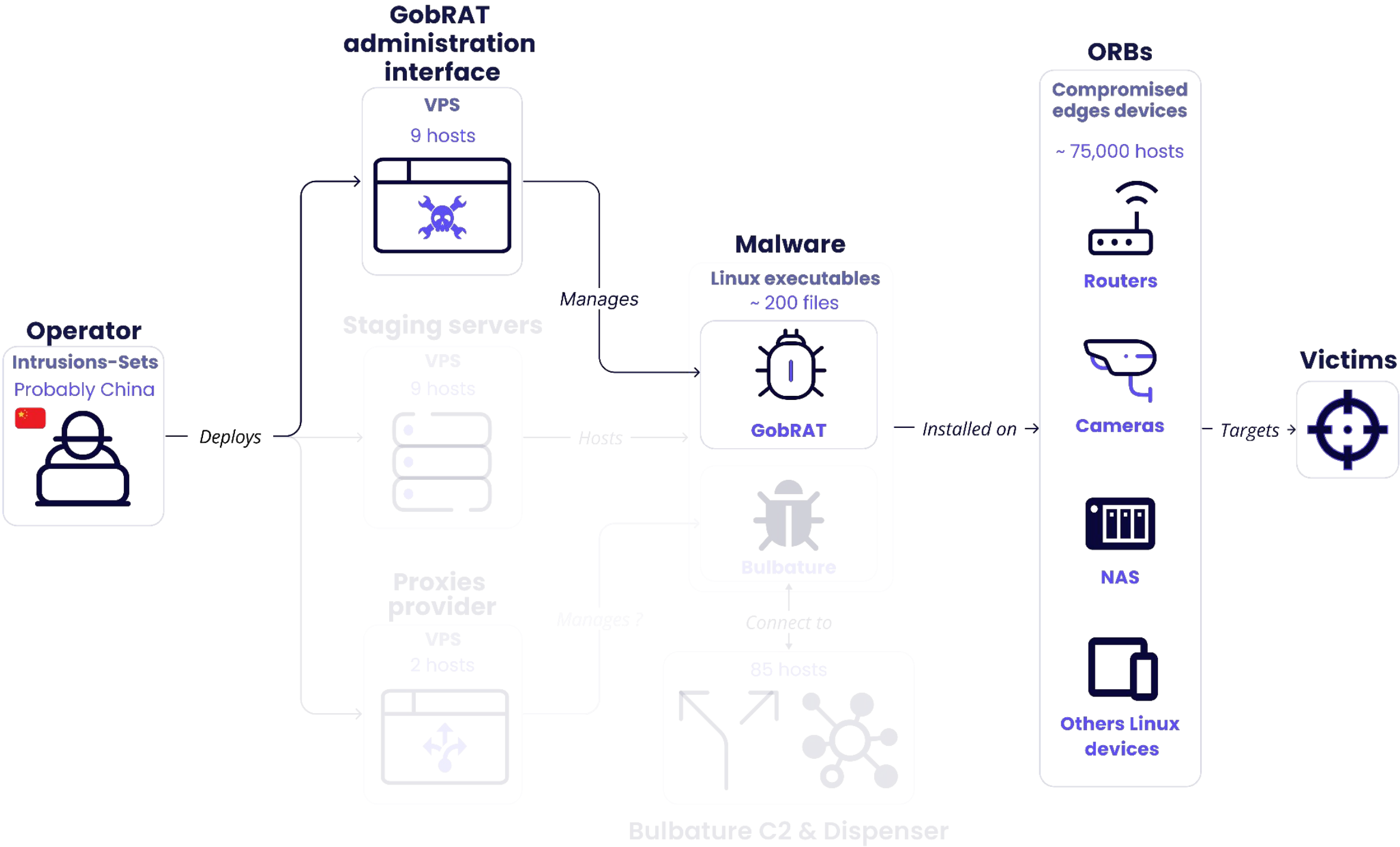
Sauvegarde des fichiers uploadés

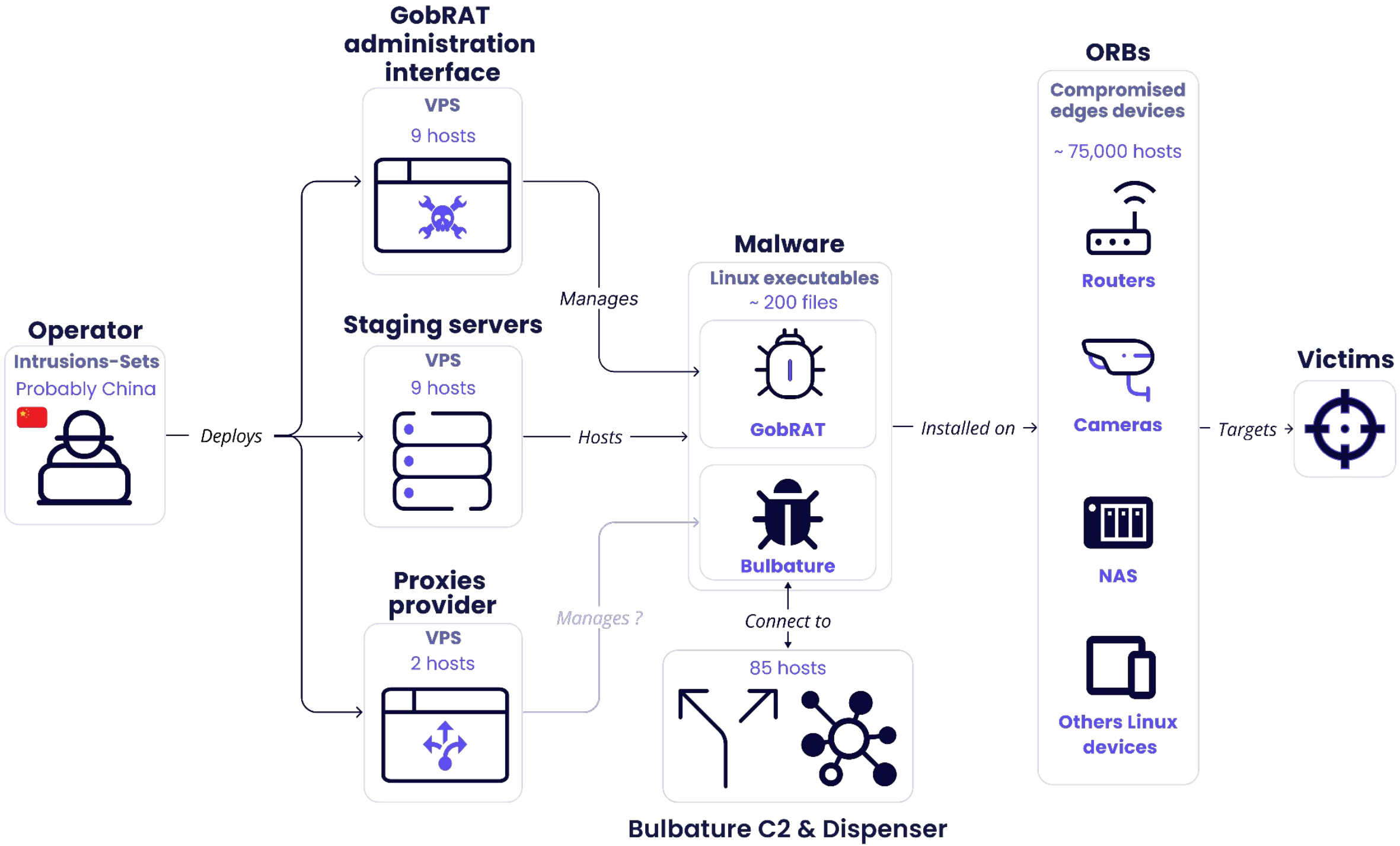
Filename	Number of rows
[ok]**【CVE-2019-9082】**Thinkphp5.txt	355,149
[ok]**【CVE-2019-13956】**discuz mlv3.txt	118,474
[ok]**【CVE-2017-5638】**S2-045 远程代码执行漏洞 2.txt	325,963
1705313101_1.txt	500,001
telnetlinux.txt	800
tw_ssh.txt	842,457
own-0209-7.txt	131,071
own-0209-10.txt	133,621
own-0209-11.txt	3,061
own-0209-41.txt	68,341
own-shiz-0214-0.txt	0
own-telnet-0222-0.txt	308,551
own-telnet-sz-02.txt	11,133,553
ssdaf0222.txt	308,551
own-telnet-0320-5.txt	352,085

Filename	Number of rows
test_ip_range1.txt	0
test_range_ip.txt	65,536
wys_test_range_ip.txt	65,536
lilin-38w-ip.txt	396,874
ssh-ip-500k.txt	500
dlink-20221208.txt	64,399
draytek1.txt	42,699
drapal7-30w.txt	600,599
ssh-ip.txt	500
iot-telnet-50k.txt	499,999
tw-telnet-60w-quchong.txt	625,333
qnap-all-**fofa**.txt	1,377,93
drupal-ip-60w.txt	600,599
0321-000.txt	1,488,18
0321-etest.txt	448,876

Total: + 22 million d'IP

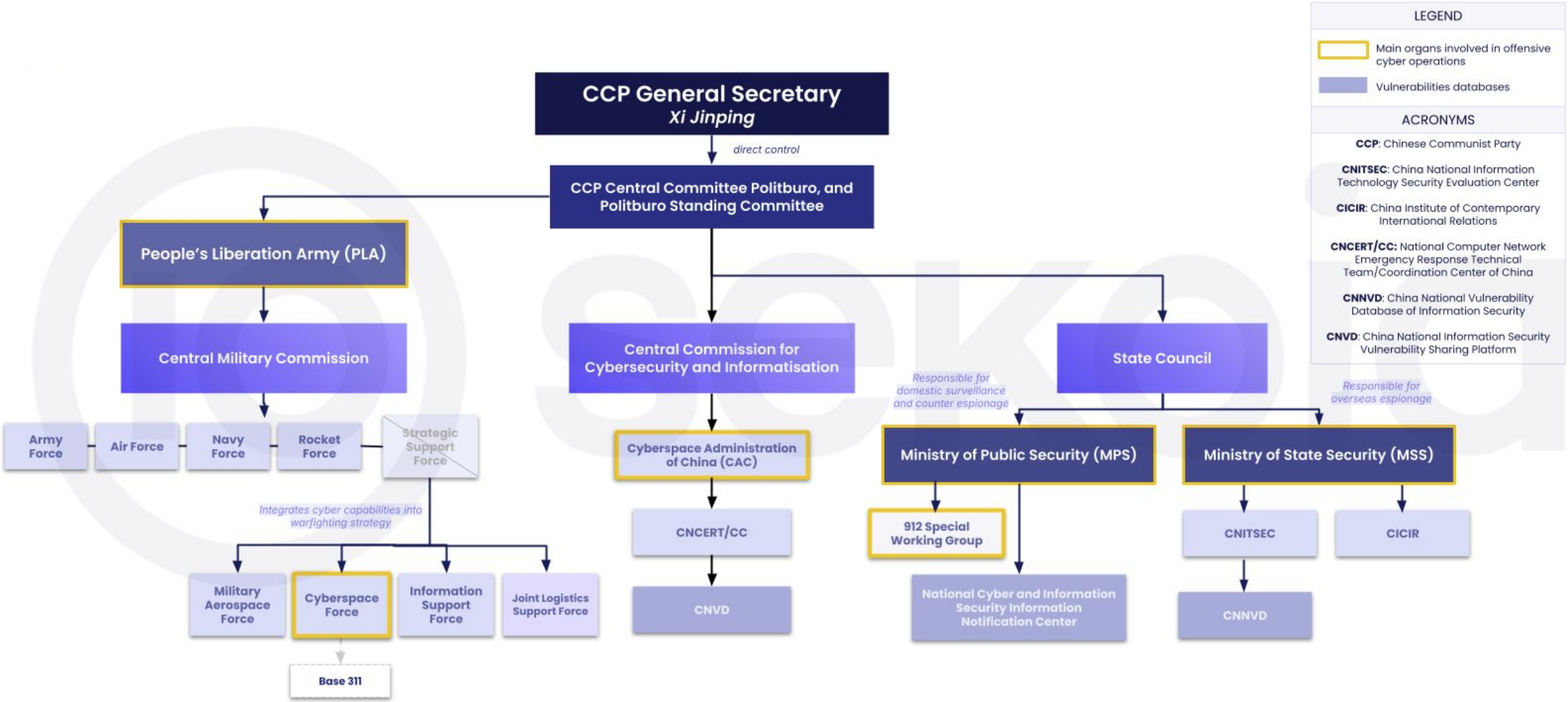

GobRAT administration interface
VPS
9 hosts
Manages
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser


GobRAT administration interface
VPS
9 hosts
Manages
Malware
Linux executables
~ 200 files
GobRAT
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Victims
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Installed on
Targets
Bulbature
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser


GobRAT administration interface
VPS
9 hosts
Operator
Intrusions-Sets
Probably China
Deploys
Staging servers
VPS
9 hosts
Hosts
Manages
Malware
Linux executables
~ 200 files
GobRAT
Bulbature
Installed on
ORBs
Compromised edges devices
~ 75,000 hosts
Routers
Cameras
NAS
Others Linux devices
Targets
Victims
Proxies provider
VPS
2 hosts
Manages ?
Connect to
85 hosts
Bulbature C2 & Dispenser

Qui fait ça ?

TTPs : Écosystème étatique chinois



TTPs : Écosystème étatique chinois

Trace de code et interface en chinois

Proxies provider en date du 3 septembre 2023

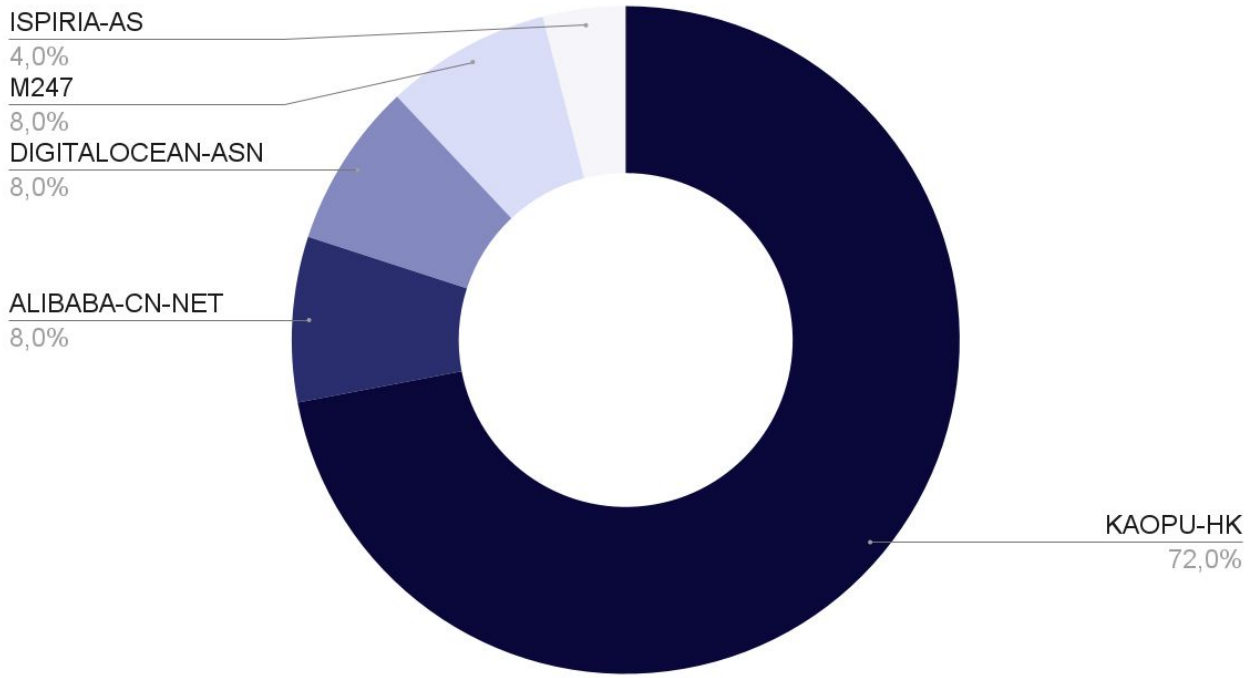
Code Bash trouvé dans les Staging servers

```
# 检测是否存在指定命令  = Vérifie si la commande spécifiée existe
if ! grep -q "(/zone/hold_by_bot.sh &)" /etc/rc.d/rc.local; then
    # 添加指定命令到 /etc/rc.d/rc.local 文件末尾   = Ajoute la commande spécifiée [...] à la fin du fichier
    echo "(/zone/hold_by_bot.sh &)" >> /etc/rc.d/rc.local
fi
```

TTPs : Écosystème étatique chinois

Trace de code et interface en chinois

Utilisation répétée de AS138915 « **KAOPU-HK Kaopu Cloud HK Limited** »

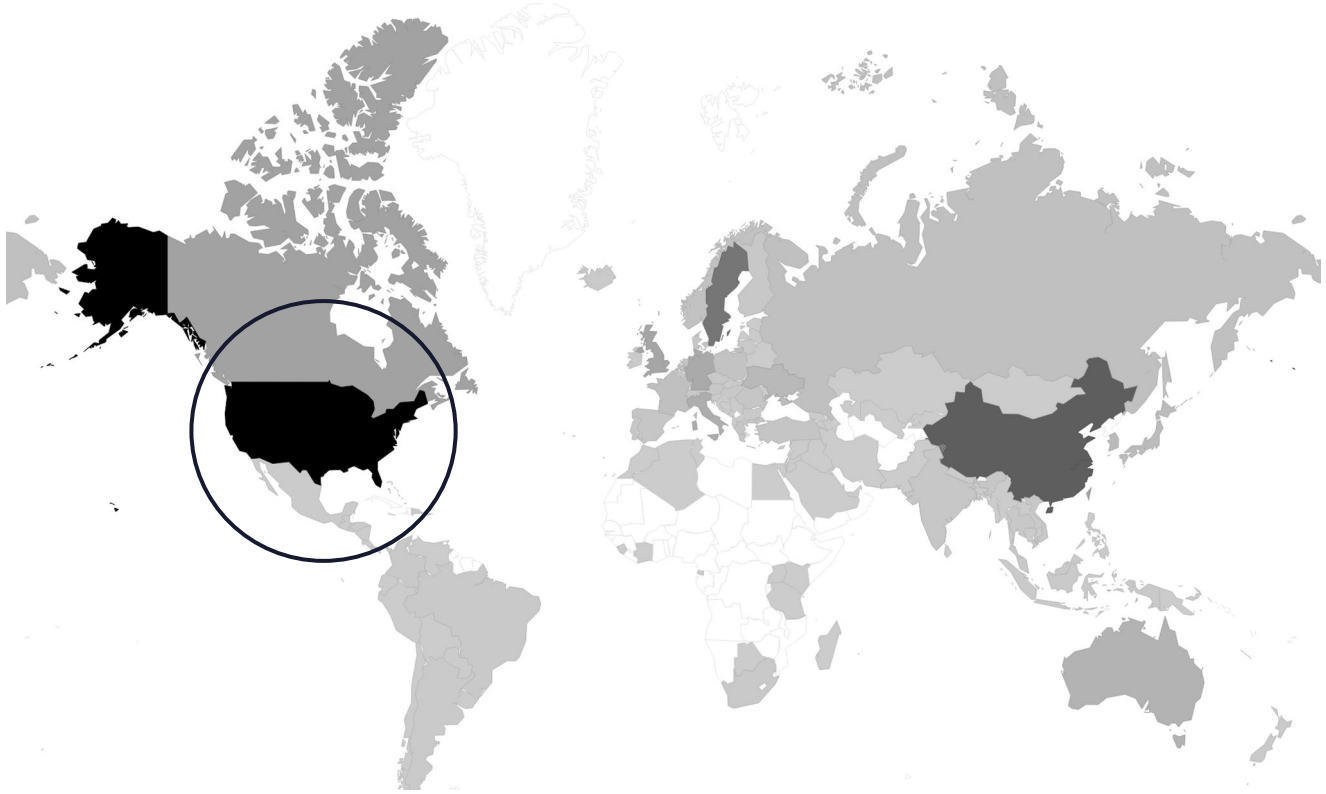


TTPs : Écosystème étatique chinois

Trace de code et interface en chinois

Utilisation répétée de AS138915 « **KAOPU-HK Kaopu Cloud HK Limited** »

Ciblage principalement **nord-américain**



TTPs : Écosystème étatique chinois

Trace de code et interface en chinois

Utilisation répétée de AS138915 « **KAOPU-HK Kaopu Cloud HK Limited** »

Ciblage principalement **nord-américain**

GoogleCloud - Mandiant: publication ***China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders*** *(22 Mai 2024)*

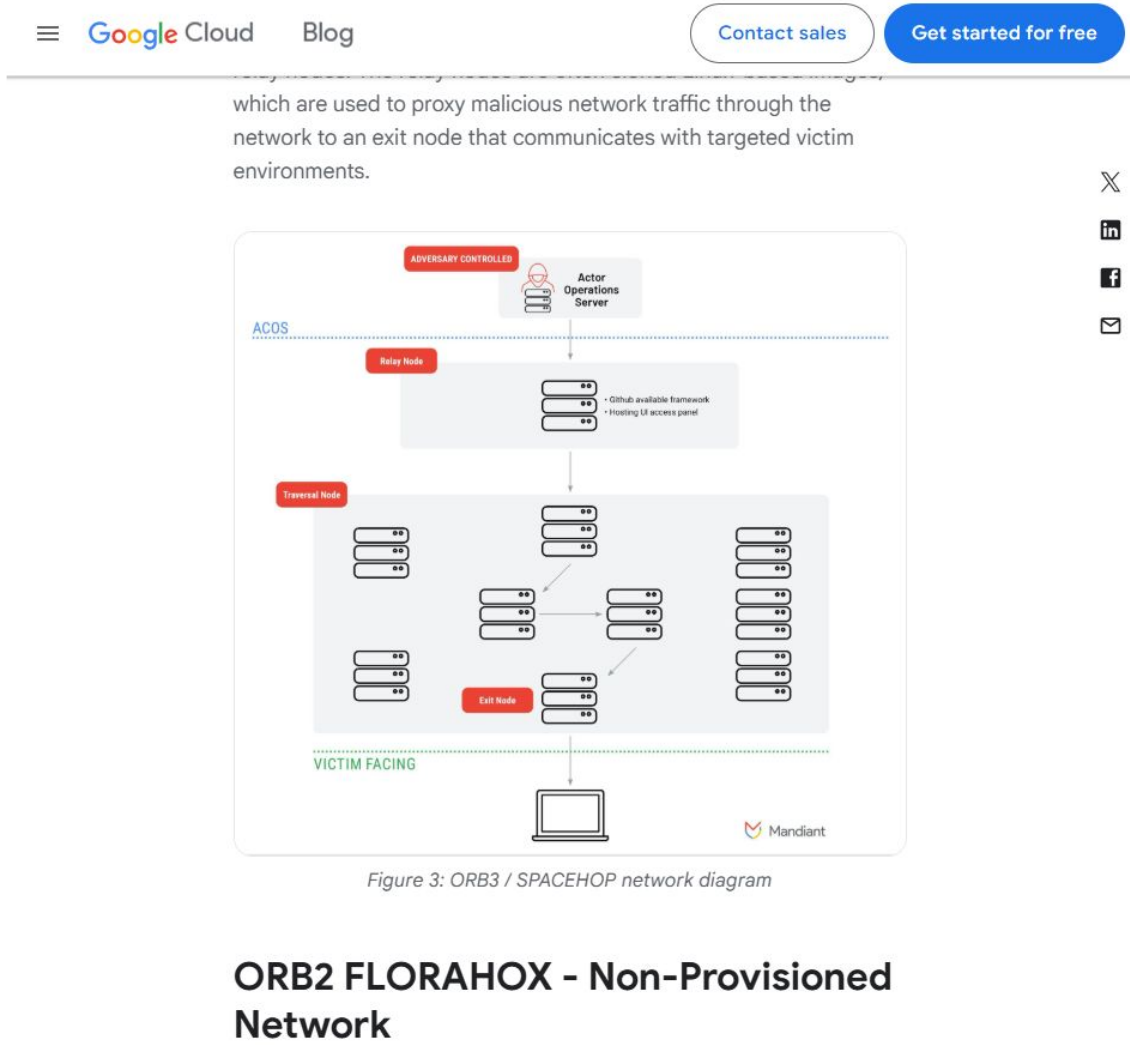


Figure 3: ORB3 / SPACEHOP network diagram

ORB2 FLORAHOX - Non-Provisioned Network

TTPs : Écosystème étatique chinois

Trace de code et interface en chinois

Utilisation répétée de AS138915 « **KAOPU-HK Kaopu Cloud HK Limited** »

Ciblage principalement **nord-américain**

GoogleCloud - Mandiant: publication ***China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders*** *(22 Mai 2024)*

GoogleCloud - Mandiant: publication ***China-Nexus Espionage Actor UNC3886 Targets Juniper Routers*** *(12 Janvier 2025)*

Malware Analysis

appid — TINYSHELL-Based Active Backdoor

Sample one, named `appid`, is an active backdoor written in C. It is derived from the publicly available TINYSHELL source code with additional supported commands. It is an active backdoor that communicates to the following hardcoded command and control (C2) servers:

- `TCP://129[.]126[.]109[.]50:22`
- `TCP://116[.]88[.]34[.]184:22`
- `TCP://223[.]25[.]78[.]136:22`
- `TCP://45[.]77[.]39[.]28:22`

Mandiant believes these IPs are staging nodes of a GOBRAT ORB network, eventually leading to a single, backend Adversary Controlled Operations Server ("ACOS").

Merci

Signal : amaury.42