



CYSLAB

CGI Business Consulting

RedTeam & Tunneling Stop using Raspis

Nicolas Chatelain – Nicocha30

Who am I ?

Nicolas Chatelain (@Nicocha30)

- Director @ CGI Business Consulting / CysLab
- Author of Ligolo, Chashell, Ligolo-ng

01

Implant level 00

Sure, your Raspberry Pi is nice. But can you do better?

02

Solving issues

Open Source, cheap, secure and stealthy solutions

03

PoC || GTFO

A PoC that requires \$20k to go live.



01

Implant level 00

I hate Raspberry Pi-based implants



CYSLAB

CGI Business Consulting

**“Yes! I did an implant at
my former company! It
was based on a
Raspberry Pi!”**

—Someone from my team whom I
unfortunately recruited.



Type of implants



Hardware

A device that you physically connect during a RedTeam on the client network.



Software

A program that runs on a compromised workstation, giving you access to the internal network.



CYSLAB

CGI Business Consulting

What are the constraints of a RedTeam implant?

Internet Access

Must be able to access Internet in complex environments (802.1x, Proxies...)

Stealth

The implant must be stealthy, compact and easily concealed.

Layer 2

Pentesters should be able to perform L2 attacks (ARP Cache Poisoning)

Cheap

We don't have the same budget as CIA

Secure

Inforsenic analysis of the implant must be complex

Anonymous

The implant must not allow the attacker to be identified



Hardware Implant Level 00

Step 1: Take a Raspberry Pi



« Internet? Easy bro, just add a 4G USB Antenna! »

« Oh, we don't have a static public IP? Just setup an OpenVPN Gateway »

Hardware Implant Level 00

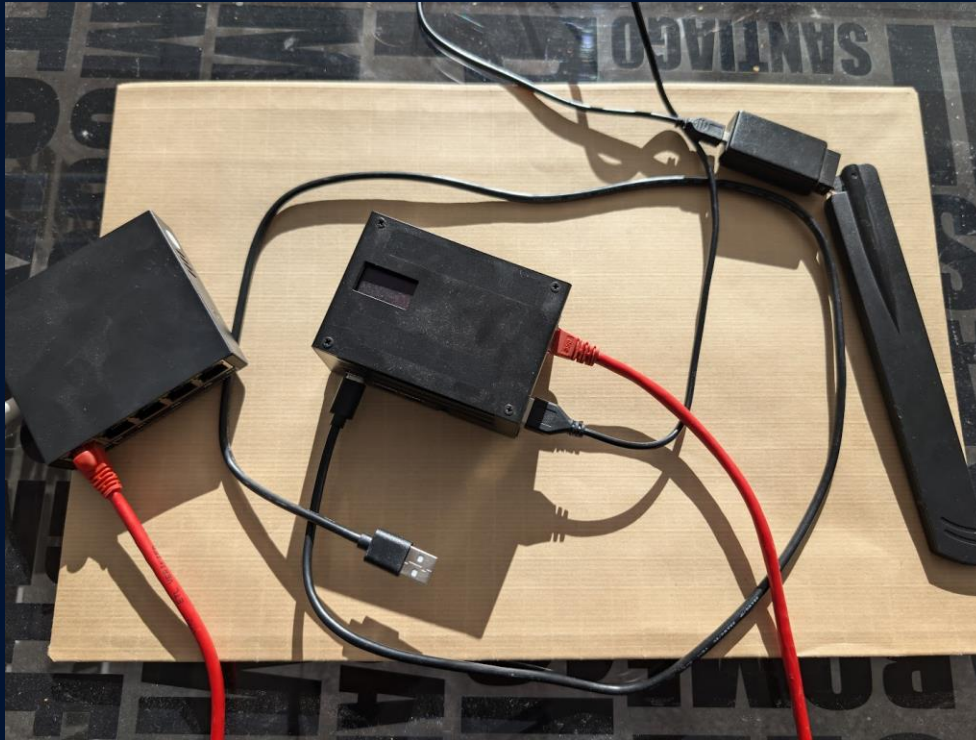
Step 2: Add Internet !



« Yea, the *Raspi* only have one *Ethernet* port, but don't worry, let's add a *Switch*! »

Hardware Implant Level 00

Step 3: Add a Switch



« Ok, we might need a power-strip to connect the Raspberry Pi and the switch. »

Hardware Implant Level 00

Step 4: Add a Power-Strip



« Let's add a battery so that if we don't have access to a power outlet, it can still work! »

Hardware Implant Level 00

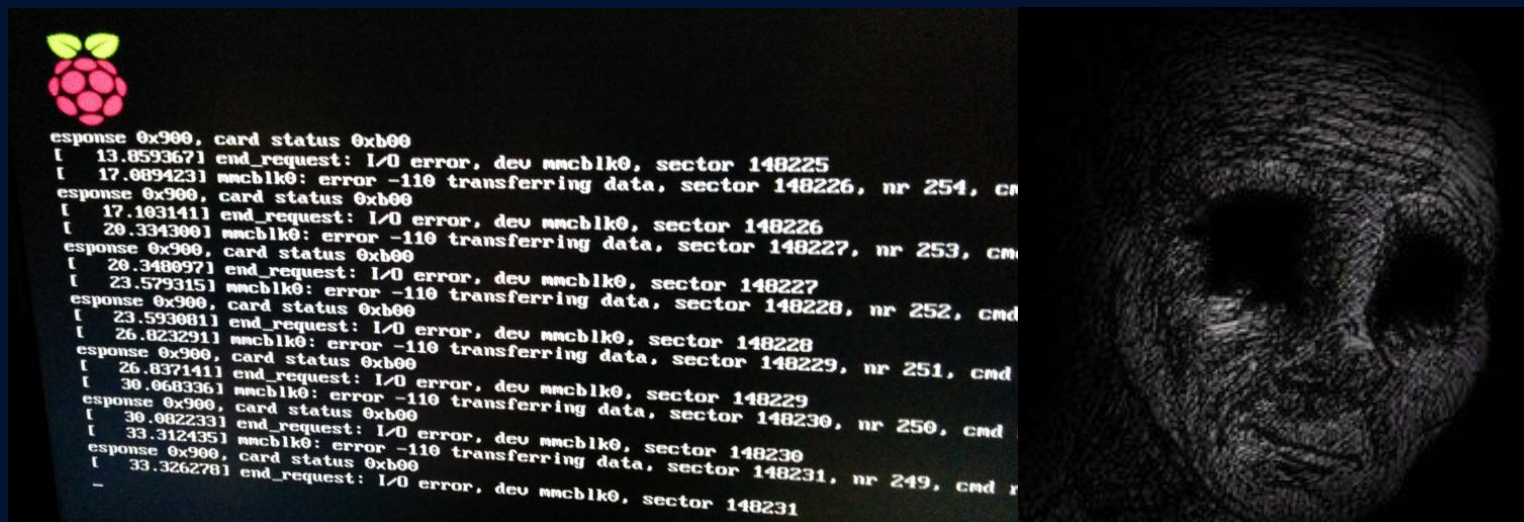
Step 5: Add a powerbank



« Yea bro, perfect, it will work. I hope the SD card doesn't get corrupted, and that the blueteam doesn't decide to extract it. »

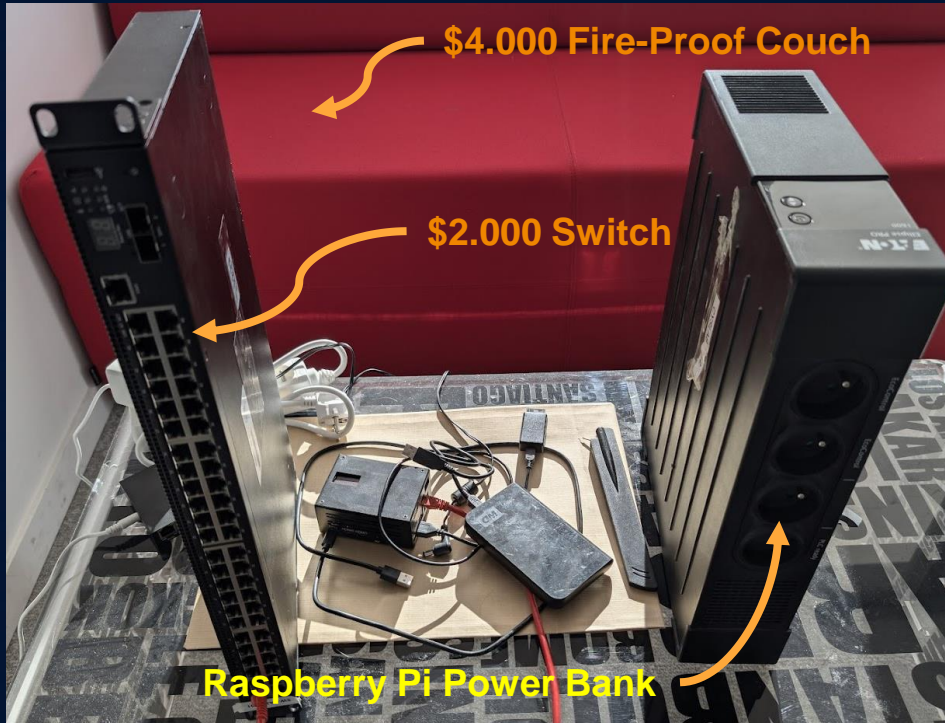
Hardware Implant Level 00

Step 6: Ruin your RedTeam



Hardware Implant Level 00

Pros & Cons



Pros :

- Can add a 2.000\$ 48 Port POE++ Managed Switch
- Can add an EATON Backup Power Supply
- Looks totally legit

Cons :

- A bit heavy

Congratulations! ***You've done it!***

Any similarity with fictitious events or
characters was purely coincidental.



CYSLAB

CGI Business Consulting



02

Solving issues

Let's not reinvent the wheel



CYSLAB

CGI Business Consulting

First issue: The Hardware

The Hardware : *GL-iNet Puli X300*

Pros:

- *Cheap and fit in your pocket*
- *Reliable*
- *Open Software (OpenWRT)*
- *4G*
- *Dual Ethernet*
- *Battery Backup*

Cons:

- *Performance ?*



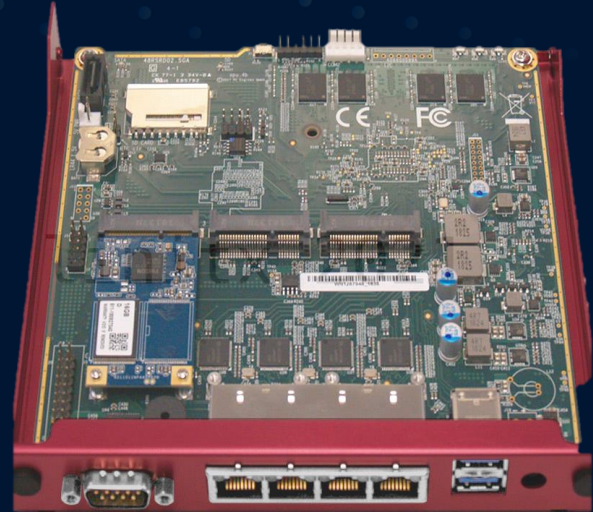
The Hardware : PC Engine APU

Pros:

- *Fast*
- *Reliable*
- *Open Software & BIOS (+ hardware schematics)*
- *Can add mPCIe Modules (4G/5G)*
- *4x Gigabit Ethernet*

Cons:

- *AMD SoC EOL*
- *Does not fit in your pocket*



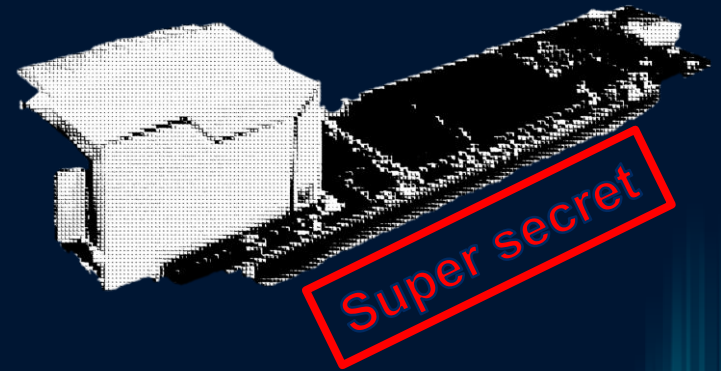
The Hardware : the project I need \$20k to release

Pros:

- *Stealth*
- *Secure as hell*
- *Hackable*
- *Ligolo-ng Wat?*

Cons:

- *Need to find \$20k for a completely ill-conceived idea.*



Solved issues

Internet Access

Must be able to
access Internet in
complex
environments
(802.1x, Proxies...)

OK

Stealth

The implant must be
stealthy, compact
and easily
concealed.

OK

Layer 2

Pentesters should
be able to perform
L2 attacks (ARP
Cache Poisoning)

Cheap

We don't have the
same budget as CIA

OK

Secure

Infomsec analysis of
the implant must be
complex

Mostly OK

Anonymous





The implant must
not allow the
attacker to be
identified

Second issue: The Software

VPN/Tunneling technologies

| | Simple to setup | Anonymous | Layer 2 Support | Fast |
|------------|-----------------|-----------|-----------------|------|
| OpenVPN | ✓ | ✗ | ✓ | ✗ |
| Wireguard | ✓ | ✗ | ✗ | ✓ |
| L2TP/IPSEC | ✗ | ✗ | ✓ | ✓ |
| Tailscale | ✓ | ✗ | ✗ | ✓ |
| Ligolo-ng | ✓ | ✗ | ✗ | ✗ |

THE CHOSEN ONE

| | Simple to setup | Anonymous | Layer 2 Support | Fast |
|----------|---|---|---|---|
| Zerotier |  |  |  |  |

The software

Simple to setup:

- *zerotier-cli join [network id]*

Anonymous:


- Config file only contains network id
- Communications expose IP Addresses 

Layer 2 Support : *literally a virtual network switch*

Fast:


- *Developed in C++, very small binary, can run on low power devices*

ZT Setup: Join & Authorize hosts



ZEROTIER
Download Documentation

← Networks

intruder



Network ID:



Included Devices: **8 / 25**
Upgrade to Essential for more networks/admins/sso

Members

5 total members

5 filtered members

AUTHORIZATION

All ☒
Authorized ☐ (3)
Not authorized ☐ (2)

ACTIVITY

All ☒
Inactive ☐ (3)
Active ☐ (2)

MISC

Bridges ☐ (5)

Reset Filters

Refresh

| <input type="checkbox"/> | Edit | Auth | Address | Name/Desc | Managed IPs | Last Seen | Version | Physical IP |
|--------------------------|------|------|-------------|---------------|----------------|-----------|---------|-------------|
| <input type="checkbox"/> | | | 11 1a... | nworkstation2 | | 1 minute | 1.14.1 | |
| <input type="checkbox"/> | | | 71 1a... | vtr | | 4 months | 1.14.0 | |
| <input type="checkbox"/> | | | 76 1a... | intruder | 1...168.192.10 | 2 minutes | 1.14.0 | |
| <input type="checkbox"/> | | | 7B 1a... | vsphere | | 7 months | 1.12.2 | |
| <input type="checkbox"/> | | | A3 1a... | nworkstation | | 8 months | 1.12.2 | |

RedTeam operator

Implant

`zerotier-cli join [network id]`

ZT Setup: Allow device bridging

76

Authorized

Authorized ☒

Name

intruder

Description

IP Assignments

192.168.192.10

Add IP

▼ Advanced

Exclude from SSO ☐

Allow Ethernet Bridging ☒

Do Not Auto-Assign IPs ☐

Save

Don't forget to bridge interfaces on the implant!

ztXXXXXX ⇔ eth0 ⇔ eth1

ZT Setup: Check if L2 is working

| Appliquer un filtre d'affichage ... <Ctrl-/> | | | | | | |
|--|---------------|--------|-----------------|----------|--------|---|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 201 | 250.690997192 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 202 | 258.720543188 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 203 | 259.693985608 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 204 | 261.559489732 | 0. | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0x5be5e454 |
| 205 | 261.561014295 | 0. | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x5be5e454 |
| 206 | 261.673112609 | Re | Broadcast | ARP | 60 | Who has 172.16.32.1? Tell 172.16.32.10 |
| 207 | 261.827895864 | 17. | 239.255.255.250 | SSDP | 179 | M-SEARCH * HTTP/1.1 |
| 208 | 262.695400469 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 209 | 263.633696905 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 210 | 264.351424490 | fe | ff02::2 | ICMPv6 | 62 | Router Solicitation |
| 211 | 265.746569434 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 212 | 267.010023000 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 213 | 268.449515780 | 17. | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 214 | 268.761589044 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 215 | 269.450966282 | 17. | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 216 | 270.451477564 | 17. | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 217 | 271.144008665 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 218 | 271.452685268 | 17. | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 219 | 271.763672120 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |
| 220 | 272.771256796 | Qo | Broadcast | ARP | 60 | Who has 172.16.32.14? Tell 172.16.32.1 |

ZT Setup: Bridge VM Net to ZT

Virtual Network Editor

| Name | Type | External Connection | Host Connection | DHCP | Subnet IP Address | MTU |
|--------|-----------|---------------------|-----------------|------|-------------------|-----|
| vmnet0 | bridged | ztdwjhzvbm | — | — | — | — |
| vmnet1 | host-only | none | vmnet1 | yes | 172.16.47.0 | — |
| vmnet8 | NAT | NAT | vmnet8 | yes | 192.168.57.0 | — |

+ Add Network...

- Remove Network

vmnet0

☒ Bridged (connect VMs directly to the external network)

Bridged to:

ztdwjhzvbm

Automatic Settings...

☐ NAT (share host's IP address with VMs)

NAT Settings...

☐ Host-only (connect VMs internally in a private network)

☐ Use local DHCP service to distribute IP addresses to VMs

☐ Connect a host virtual adapter (vmnet0) to this network

Subnet IP:

.

.

.

Subnet mask:

.

.

.

⚡

 Leave blank to automatically select an unused subnet IP.

MTU*:

Help

Cancel

Save

ZT Setup: Enjoy L2 VPN over ZT

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo dhclient -v eth0  
Internet Systems Consortium DHCP Client 4.4.3-P1  
Copyright 2004-2022 Internet Systems Consortium.  
All rights reserved.  
For info, please visit https://www.isc.org/software/dhcp/  
  
Listening on LPF/eth0/00:0c:  
Sending on   LPF/eth0/00:0c:  
Sending on   Socket/fallback  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5  
DHCPOFFER of 172.16.32.106 from 172.16.32.1  
DHCPREQUEST for 172.16.32.106 on eth0 to 255.255.255.255 port 67  
DHCPACK of 172.16.32.106 from 172.16.32.1  
Error: ipv4: Address already assigned.  
bound to 172.16.32.106 -- renewal in 2852 seconds.  
  
(kali@kali)-[~]  
$ sudo arping 172.16.32.9  
ARPING 172.16.32.9  
60 bytes from 38:f3: (172.16.32.9): index=0 time=43.759 msec  
60 bytes from 38:f3: (172.16.32.9): index=1 time=45.701 msec  
60 bytes from 38:f3: (172.16.32.9): index=2 time=45.086 msec  
^C  
— 172.16.32.9 statistics —  
3 packets transmitted, 3 packets received, 0% unanswered (0 extra)  
rtt min/avg/max/std-dev = 43.759/44.849/45.701/0.810 ms
```

Third issue : Improving efficiency and stability

What if something goes wrong?

*We need additional communications methods if 4G or
Zerotier fails for whatever reason.*

Using GSM AT MODEM

```
ttyUSB3
ttyUSB4
ubi0
ubi0_0
ubi0_1
ubi_ctrl
ubiblock0_0
urandom
watchdog
zero

qmicli -p -d /dev/cdc-wdm0 --
uim-read-
transparent=0x3F00,0x2FE2

qmicli -p -d /dev/cdc-wdm0 --
uim-read-
transparent=0x3F00,0x2FE2

id

id

uid=0(root) gid=0(root)
```

- C&C (Authenticated) over SMS
- If the power supply is disconnected, an alert is sent

Using LoRaWAN



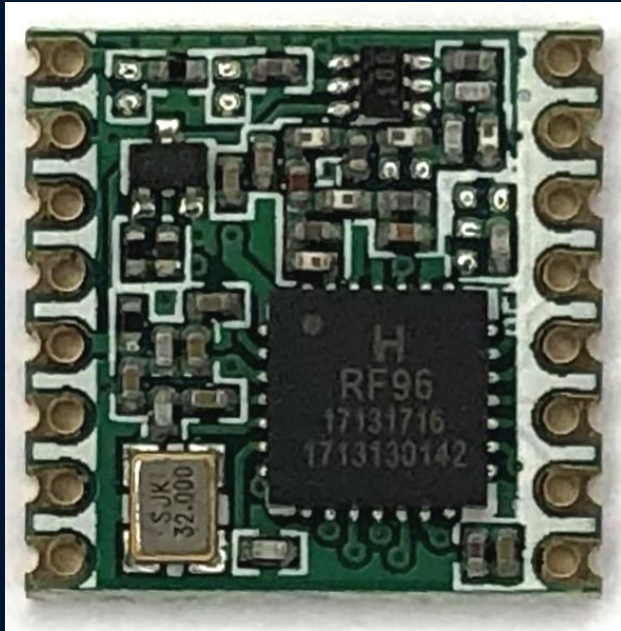
- Free, collaborative LoRaWAN Network
- You can add LoRaWAN Gateways and end devices (very) easily!

The hardware : TTGO LORA32



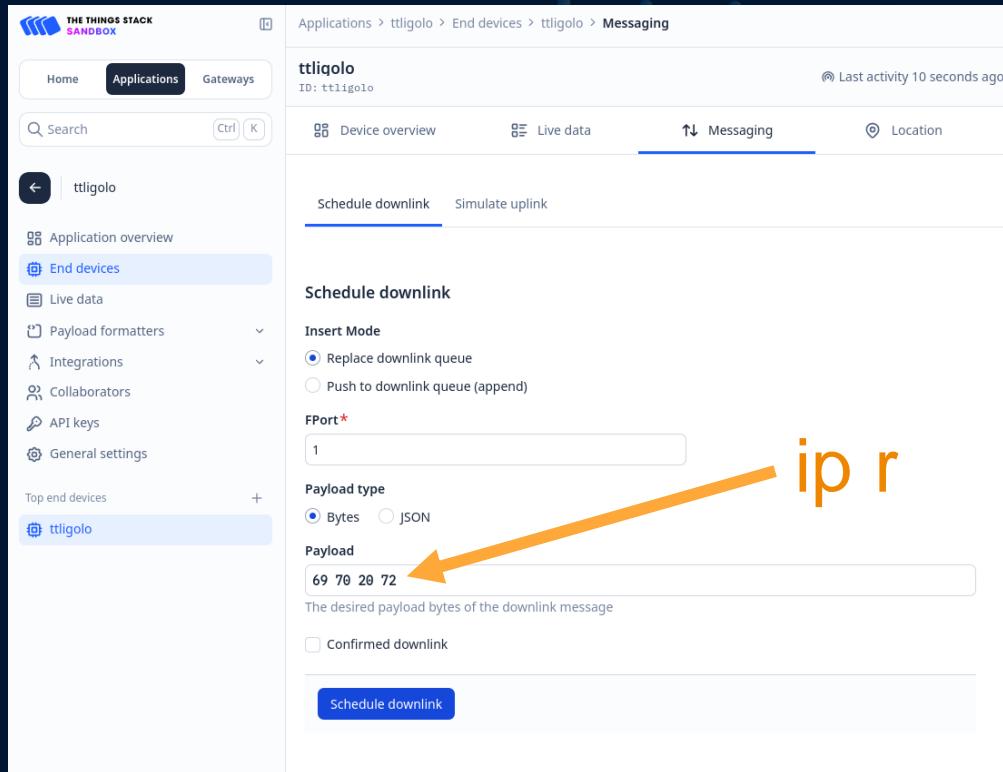
- TTGO LORA32 : Low power ESP32
- ~14€ on AliExpress
- Can be battery powered
- Wi-Fi / BLE Support

The hardware : HOPERF RFM95W



- HopeRF – 3,80€ on AliExpress

Quick POC : C2 over LoRaWAN



The screenshot shows the 'The Things Stack Sandbox' interface. The left sidebar contains navigation links: Home, Applications, Gateways, Search, and a list of end devices including 'ttlqolo'. The main panel is titled 'Applications > ttlqolo > End devices > ttlqolo > Messaging'. It features tabs for 'Device overview', 'Live data', 'Messaging' (selected), and 'Location'. Under the 'Messaging' tab, there are two sub-tabs: 'Schedule downlink' (selected) and 'Simulate uplink'. The 'Schedule downlink' section includes an 'Insert Mode' dropdown with 'Replace downlink queue' selected, an 'FPort*' input field with the value '1', a 'Payload type' dropdown with 'Bytes' selected, and a 'Payload' input field containing the hex string '69 70 20 72'. An orange arrow points from the text 'ip r' to the 'Payload' field. Below the payload field is a checkbox for 'Confirmed downlink' and a 'Schedule downlink' button.

Applications > ttlqolo > End devices > ttlqolo > Messaging

ttlqolo
ID: ttlqolo

Device overview Live data **Messaging** Location

Schedule downlink Simulate uplink

Schedule downlink

Insert Mode

- ☒ Replace downlink queue
- ☐ Push to downlink queue (append)

FPort*

1

Payload type

- ☒ Bytes ☐ JSON

Payload



69 70 20 72

The desired payload bytes of the downlink message

☐ Confirmed downlink


Schedule downlink


Quick POC : C2 over LoRaWAN





Home Applications Gateways


Search Ctrl K


 ttligolo


 Application overview


 End devices


 Live data

 Payload formatters


 Integrations

 Collaborators

 API keys

 General settings

Top end devices +

 ttligolo

Applications > ttligolo > End devices > ttligolo > Live data

ttligolo

ID: ttligolo

Last activity 12 seconds ago • 75 up / 19 (App), 16 (Nwk) down

 Device overview

 Live data

 Messaging

 Location

 Payload formatters

 Settings

Verbose stream    

ip route result

Testing the final implant

The test

Both implants tested during a real RedTeam engagement

- Network throughput about 20Mbit/s (mostly due to bad 4G network)
- Latency between 30ms (APU) and 80ms (Puli)
- ARP Attacks / LLMNR Poisoning, everything worked
- 6 simultaneous RedTeam operators, 0 downtime
- **Bonus:** even if the BlueTeam disconnected our implant, the battery powered implant allowed us to continue the tests by connecting to the Corporate Wi-Fi Network with stolen credentials 😊



03

PoC || GTFO

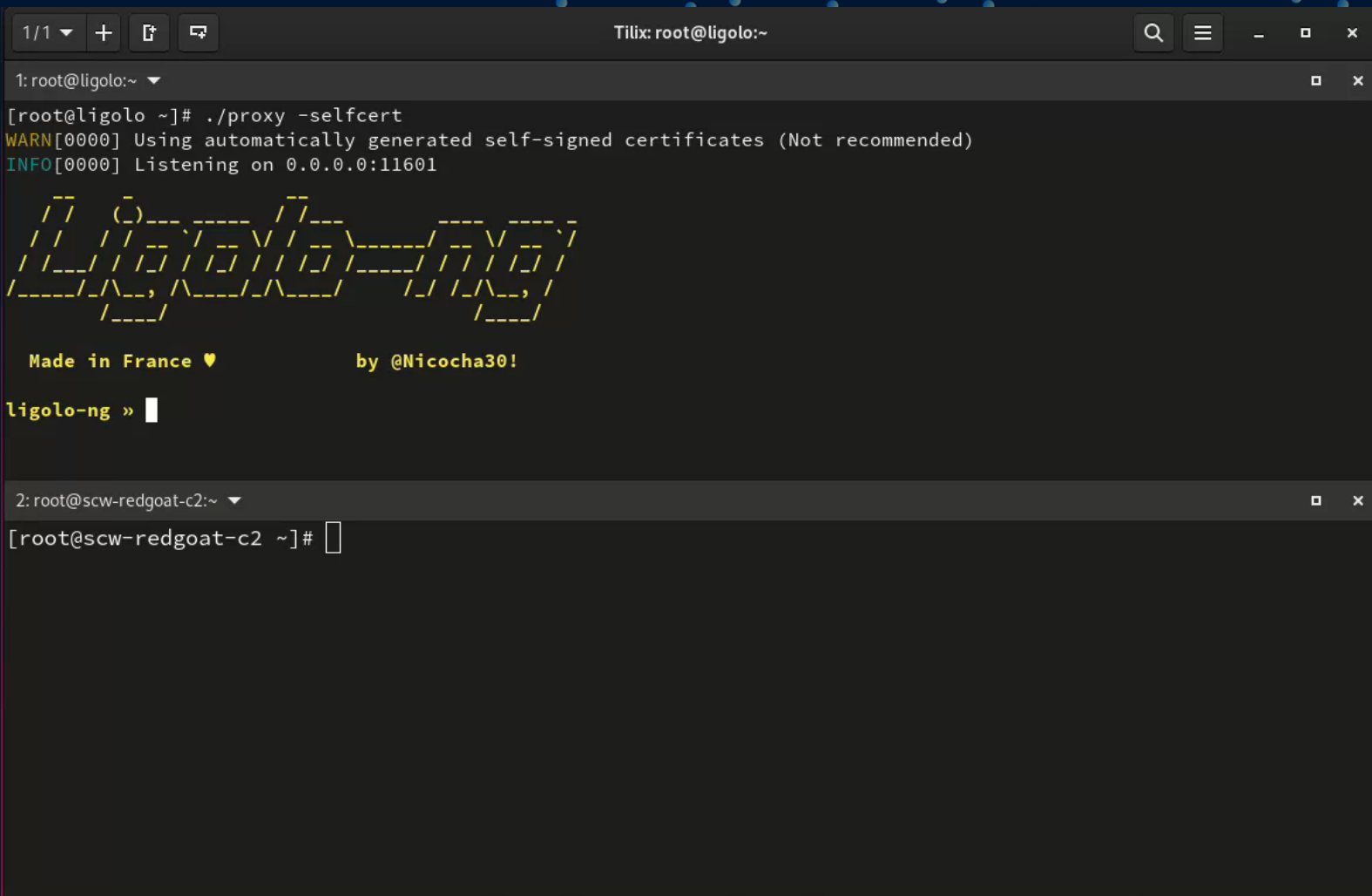
The \$20k ill-conceived idea

Reminder: What is Ligolo-ng

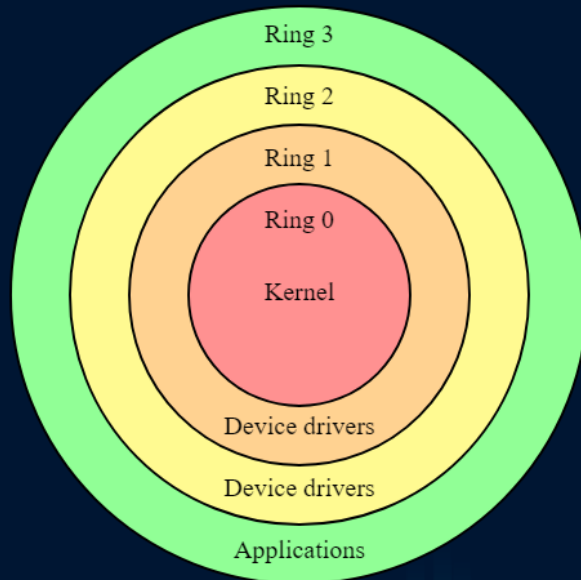
- You have a remote access to a computer, on another LAN network (malware, RCE on a server, ...)
- You need to use your own tools to target other LAN machines (NetExec, nmap, xfreerdp, ...)
- **You don't have root/admin privileges on the remote machine**
- **You don't/can't install tools on the remote machine**
- **You don't want to struggle with SOCKS Proxy/Port Forwarding**

Reminder: What is Ligolo-ng

- <https://github.com/nicocha30/ligolo-ng>
- Allows you to **access remote network** using an **unprivileged** agent, from a reverse connection (the “VPN Server” connects to you!)
- Like chisel, but **without the need of proxychains**
- Works like a **Layer 3 VPN**, with a **tuntap** interface
- Yes, you can do **nmap scans, access all TCP/UDP services without modifying any software settings (like proxy settings).**
- Agent works almost everywhere



“Agent works almost everywhere, but ...”

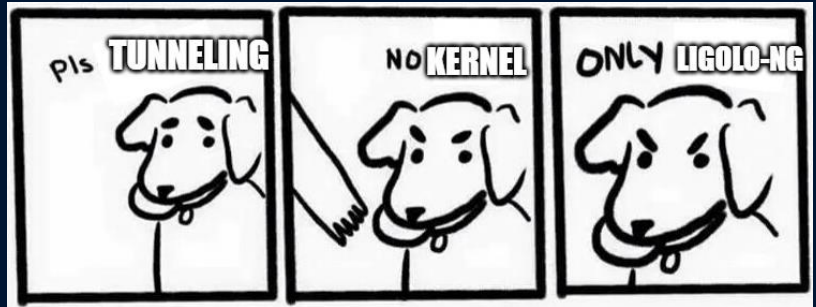


- Too much overlay
- All this to manage two, three network packets with Ligolo-ng
- Linux is overrated
- All of this to say “I use Arch btw”

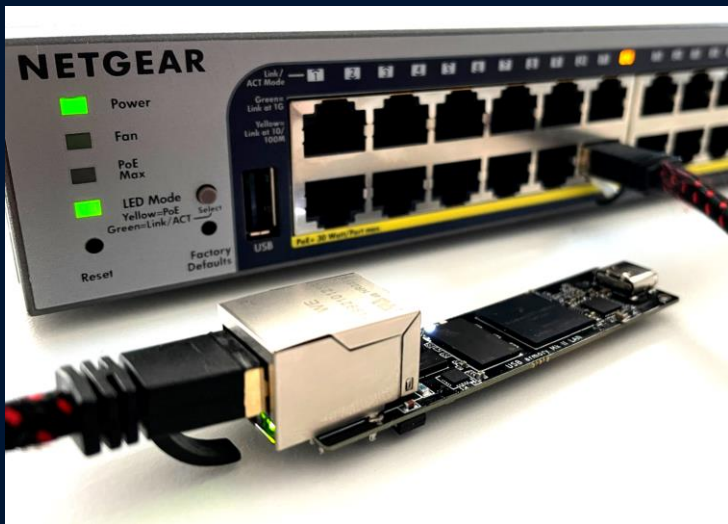
Introducing: Ligolo-baremetal

Ring 0

Ligolo-baremetal



Ligolo-baremetal (Ligolo-ng on a stick)



- Based on USB Armory MKII
- Include more security features than your ArchLinux ThinkPad laptop
- I only need \$20k to buy the minimum orderable units (100)
- Tamago framework allows to run baremetal Go applications
- If you didn't know (there might be clues) Ligolo-ng is developed in Go.

Ligolo-baremetal (Ligolo-ng on a stick)

- Secure Boot (HABv4)
- Hardware RNG
- Cryptographic Accelerator
- Secure Non-Volatile Storage (Protection against CLK glitching, voltage glitching...)
- NXP SE050 Secure Element (Hardware accelerator for AES + Secure Key State)

Ligolo-baremetal (Ligolo-ng on a stick)

Pros :

- Stealth
- Secure
- Easy to setup
- Customizable

Cons :

- One Ethernet port

Step 1: Build & Flash Ligolo-baremetal.

Ligolo-baremetal: Insert implant



Step 2: Plug.

Step 3: Profit.

Ligolo-baremetal: Next steps

- Implement DHCP Client on Pure-Go
- Get the PoE version (currently using the USB-C version with USB Ethernet)
- Implement Layer 2 Communication Mode
- Use the Hardware Dedicated Cryptographic Processor (DCP)
- Implement LPWAN Communications


SURPRISE! Thanks WithSecure !

Re: USBArmory MKII LAN Model



Andrea Barisani <andrea.barisani@withsecure.com>

À  CHATELAIN, Nicolas

Cc  usbarmory



Vous avez répondu à ce message le 24/10/2024 15:09.

Nous avons supprimé les sauts de ligne en surnombre dans ce message.



↳ Répondre

↳ Répondre à tous

→ Transférer



jeu. 24/10/2024 14:5

Hello,

given that you are making a public presentation about it we would happy to sell up to two units from our private stock and make an exception on the bulk/OEM rule.

Kindly send us invoicing details so that we can prepare a quote.

Thanks

Roadmap: Release on GitHub!

THANKS!

To all my colleagues from



And my fellas from other companies.

Do you have any questions?

Nicocha30 on Twitter/Discord

Liked the talk? [Buy a drink to my colleagues!](#)