


# CROZONO

---

Leveraging autonomous devices as an attack vector on industrial networks

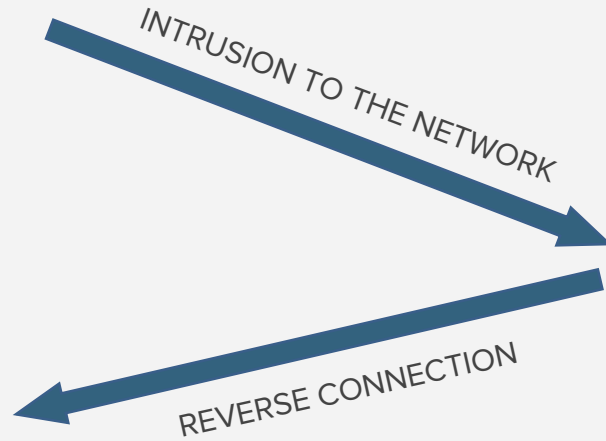
# \$ whoami

- Sheila A. Berta  
Security researcher & Exploit Writer  
CROZONO core developer
- Nicolas S. Villanueva  
DevOps Engineer at redbee studios   
CROZONO core developer
- Pablo Romanos  
Hardware & electronics design
- Demian Benitez  
CROZONO developer
- Manuel Pepe  
CROZONO developer

# What is CROZONO?

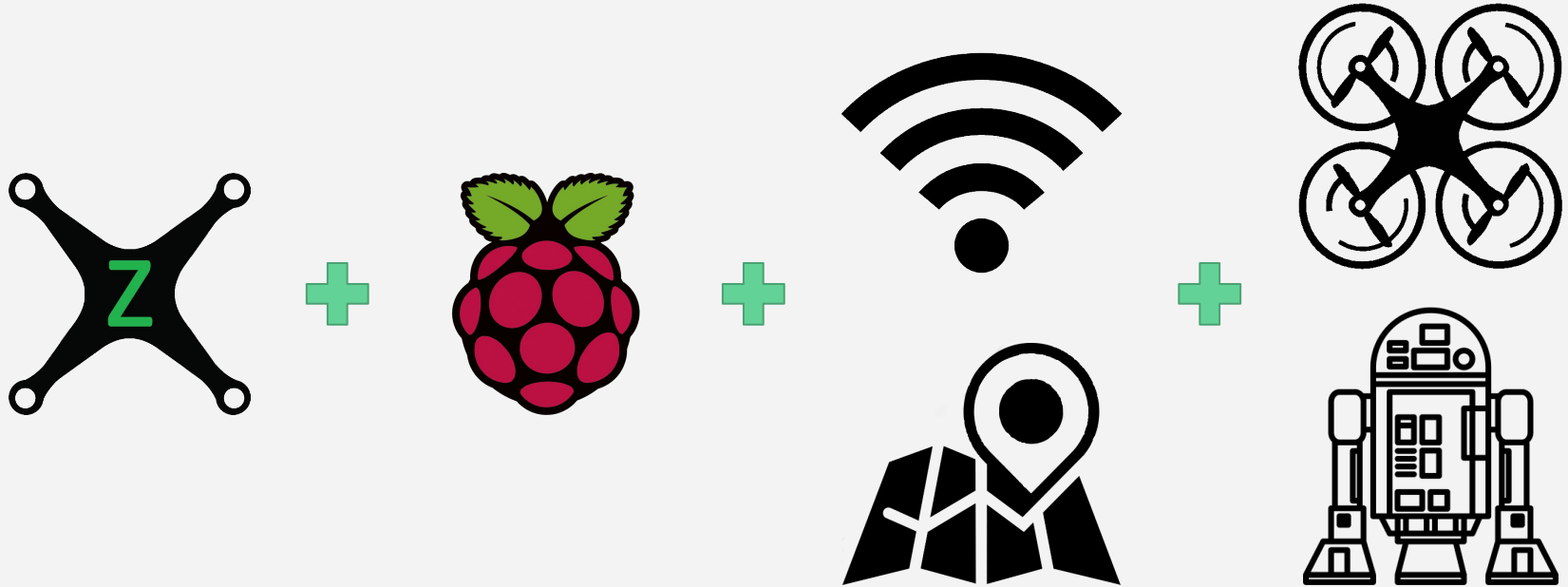
- Open source framework designed to be used on autonomous devices.
- Core and modules developed in Python 3.
- It takes decisions by itself – it is not necessary control it remotely.
- Fully automated attacks to WLAN and LAN networks.
- Attacks may be extended through modules and parameters.

# What is the purpose of CROZONO?



TARGET

# How to make a CROZONO device?



# CROZONO's flavors

## CROZONO Attacker

Perform automated attacks on specific networks.

Auto-determine security level, and act accordingly.

Even if the breach is unsuccessful, bring back useful information to the operator, for later offline attack.

## CROZONO Explorer

Gather information about an area's wireless networks.

AP's power, security protocol, etc.

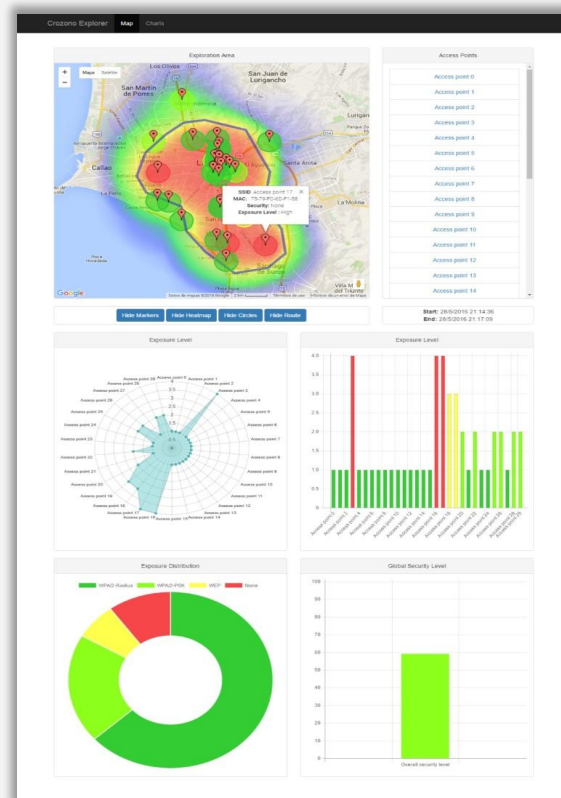
Get network's coverage map.

Generate reports.

No network intrusion attempted.

# CROZONO Explorer

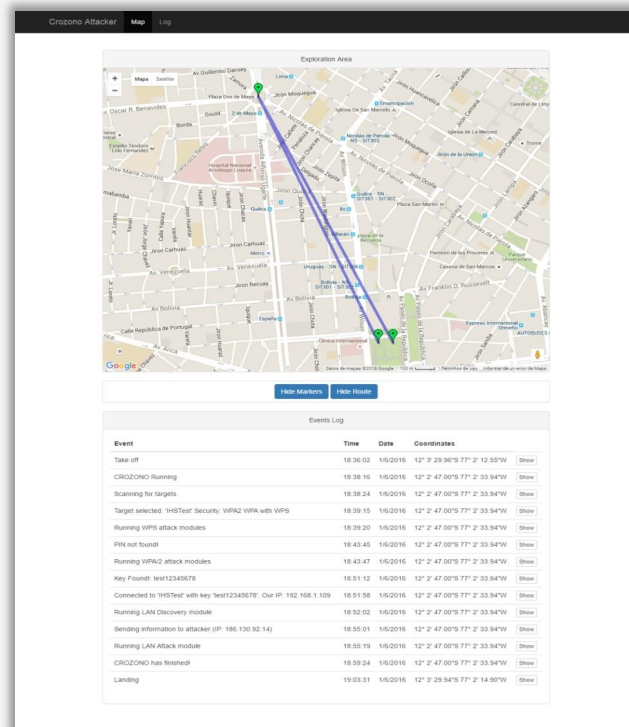
- Information of the area's APs
- Access point's power and reach
- Type of security protocol used
  - Can give an assessment of the overall security of the network
  - Pinpoint insecure access points
- Find out about areas with poor connection, or overlapping, strong signals.



# CROZONO Attacker

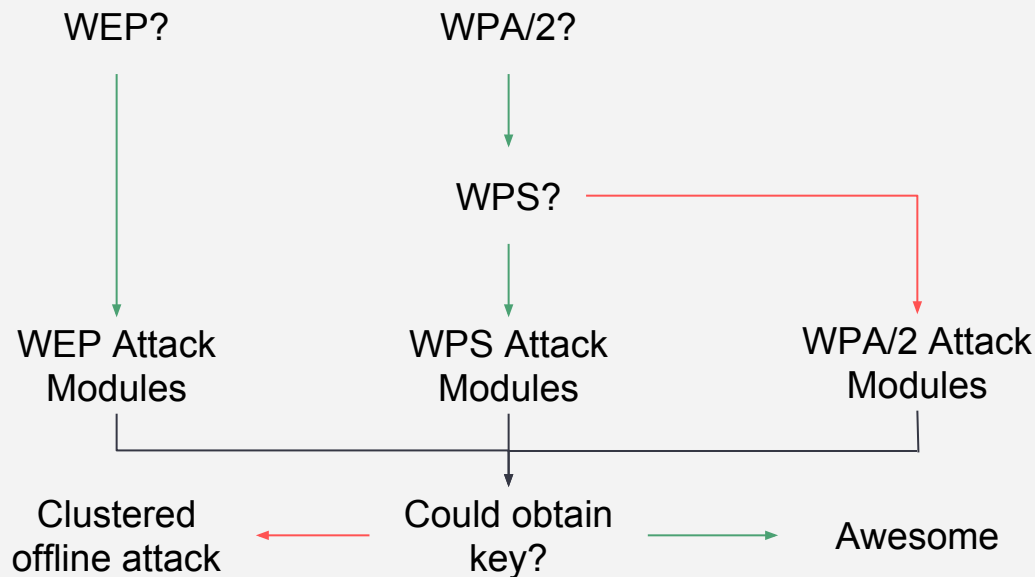
1. Attack a target, breaching its security protocol.
2. Once inside the network, perform a reverse connection to the operator leveraging the victim's internet connection.
3. Analyze the network by running “LAN discovery” modules, and sending the results back to the operator in real-time.
4. Run “LAN attack” modules to gather specific information, leave backdoors, etc.

New modules can be created and easily integrated to the framework.

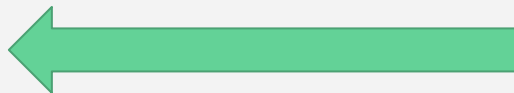




# How does it automatically crack the network?



# After attacking...



Reverse connection, gather info  
about the target, execution of  
LAN-based attacks, etc...



# What LAN attacks can it perform?

- Metasploit
- Packet sniffing
- MITM
- and more...

Plug-and-play modules  
written in Python

```
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

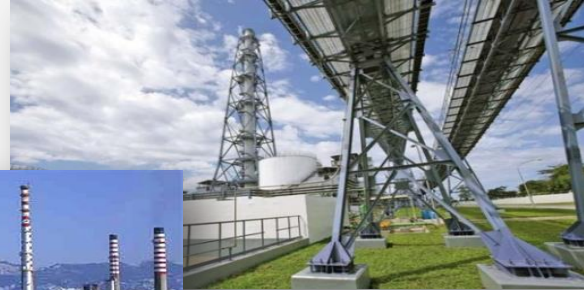
knock, knock, Neo.

http://metasploit.com

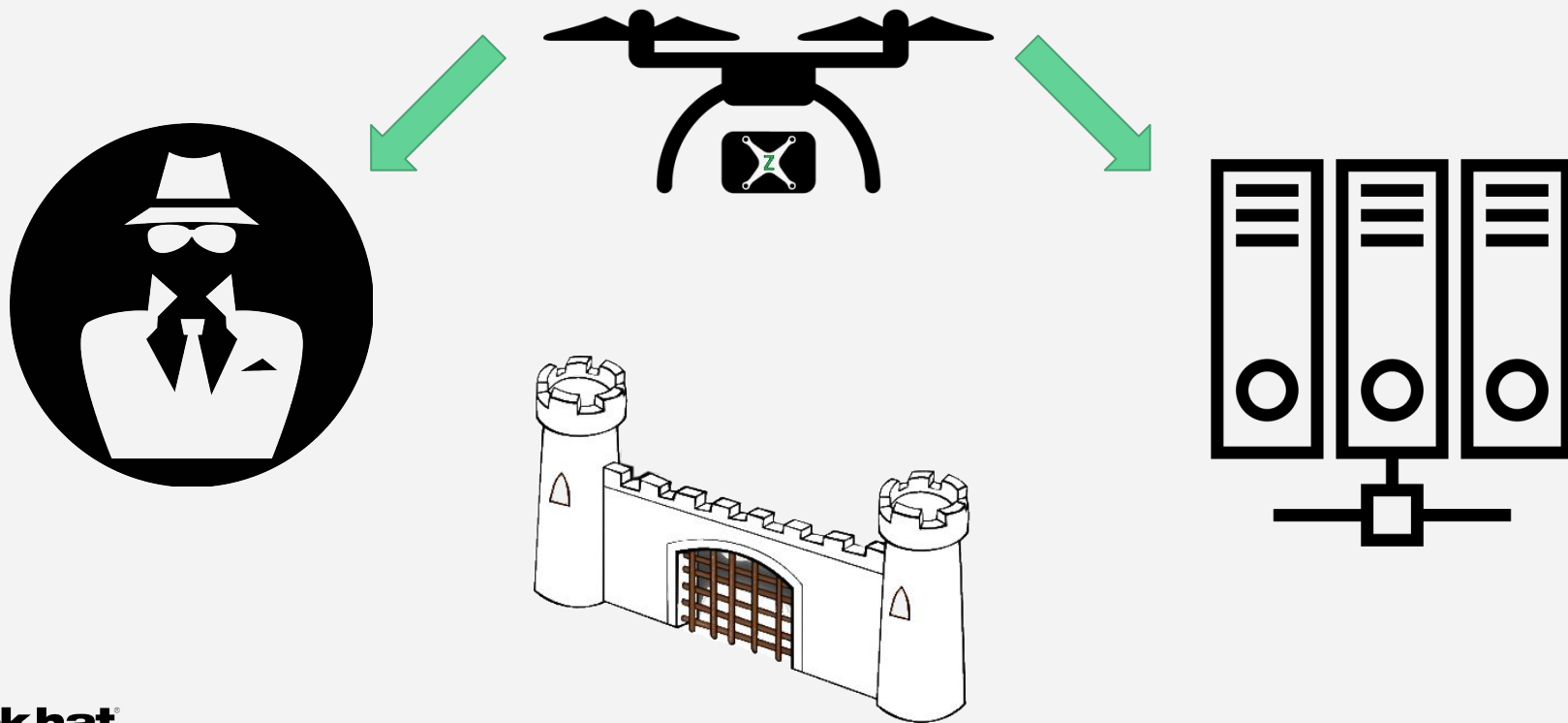
=[ metasploit v4.12.24-dev-92dba8f
+ -- ==[ 1577 exploits - 907 auxiliary - 272 post
+ -- ==[ 455 payloads - 39 encoders - 8 nops
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > █
```

# Why use CROZONO on industrial networks?



# Evade the target's physical security



# Simple setup

- Low weight added
- Flight capability undisturbed
- Easy to attach
- Compatible with all major drone manufacturers

