MEATPISTOL
A Modular Malware Implant Framework

Presented by: @ceyxiest and @fuzzynop
HERE TO TALK ABOUT—
A GUN MADE OF MEAT
...THAT SHOOTS MALWARE BULLETS?
This is a tool for...

RED TEAM
You mean "Pentesting?"
"Fundamentally a framework for creating, managing, and interacting with stealth implants that support persistent adversarial operations"
Red Team Operating Paradigm

Scope: any systems, humans, or processes employed by the company #Yoloscope

We choose the targets, set the rules of engagement, we use as much time as necessary #NoScopeBias

Steal stuff for real, incident responders treat us like we are real, try not to get caught, try to win by any means necessary

Read out our results to large audiences, branded operations, craft propaganda

Have an impact.
Origin Story.

New Job, who dis?

"Hey go hack stuff"

"cause an impact"

"Don't get caught"

"Got shell yet?"
fine.

Just get some malware and SE my target to run it.

System report:
Everything is fine. Nothing is ruined.
ok
Ooops.
All the decent malware was for windows.

Totally not a virus. Trust me... I'm a dolphin.
Snail—

Python Based Reverse SSH Tunneling Tool

Used twitter for C2 resolution based on a lexicon

Crontab or LaunchDaemon persistence

Random scheduling

Obfuscated

Generator script
Worked Good

For like a year.
Problems

Blue Team—
does not like getting wrecked by python
Problems

Blue Team writes specific detections for Red Team
Problems

Attribution of Red Team gets really good.
Problems

Ability to be a good Boogeyman goes down.
Problems

And we have a bunch of spaghetti code.
Time to iterate, write new malware

Turtles:

Fully implemented SSH client and server written in java

Rio:

Another SSH reverse tunneling tool written fully in bash
New malware, new tricks

So great!
But, the status quo was...

We ended up rewriting malware each time we wanted something new.

We had to stand up all our own C2 each time.

We had to manage and configure all our C2.

We had to manage all our keys and certificates for our C2.

It took time and effort, and a lot of it.
AND...

It's prone to errors:

Accidentally reused a C2... which got us attributed

Accidentally connected to C2 from the wrong place

Broken shells and broken dreams

Shell dies and never comes back

Used the same cert across multiple C2s
THIS WAS PAINFUL

Unreliable

Impossible to maintain

Impossible to truly iterate

Really hard to add features
Plus we still have spaghetti code
Wouldn’t it be nice if...
You didn't have to write things from scratch every time...
And cutting a new malware implant took seconds?
And you could pick the features you wanted for that implant...
and C2 server infrastructure spinup happened automagically...
...and each sample was unique...
...and each C2 endpoint was unique
...and you didn’t have to manage keys for each C2 server...
Wouldn’t it be nice if the malware was just super fugging awesome!
So that's what we built.
Core
Essentially a Microkernel
I’m Mr. C2 Module

Job: Provide the mechanism to communicate to the C2
LOOK AT MEEEE!!!

Modules register with the core on startup.
I’ll listen for C2_CONNECT and C2_DISCONNECT events.

If you want to change the state of connection to the meatpistol network then trigger the relevant event.
Core
Event Loop
Scheduler Loop
C2
Persistence
How does everything communicate?
Client to Client
Uni-directional
Persistent
Many Reader
Many Writer
Read()
Write()
Attach()
Detach()
Close()

CHANNEL
NETWORK ARCHITECTURE
DEMO TIME AND POST.
Malware implant creation used to take days.

Now it takes seconds.

Weeks off our operation time.
... once you get locked into a serious malware collection, the tendency is to push it as far as you can.
The best way to increase the arsenal?
Share it.

... or not.
Ok, you are probably wondering about the name.
Meatpistol
Enthralls
Angry
Tyrants

Proposing
Intimate
Sexy-times
Teasing
Oligarch
Llamas
Marginally Erect Alpacas Tactically Pursuing International Slave Trading Oligarch Llamas
Modular Embedded Adversary Tooling
metasploit

meatpistol

meta lot
It's natural to want to compare...
PEOPLE ASK US:
How's this different than metasploit?
PEOPLE ASK US:
Is this the same as Cobalt Strike?
PEOPLE ASK US:
But did you hear about Empire Project?
PEOPLE ASK US:
They dumped fuzzbunch isn't that the same?
MEATPISTOL is not an exploit database.
MEATPISTOL is not click to win.
MEATPISTOL is not a post exploitation agent.
MEATPISTOL is not a bag of cool tricks.
MEATPISTOL is a MEAT CANNON THAT SHOOTS OUT MALWARE IMPLANTS
MEATPISTOL is a framework for Red Teams to create better implants.
MEATPISTOL is multi-user implant management and interaction portal
MEATPISTOL is an offensive infrastructure automation tool.
MEATPISTOL is something that has saved us a lot of time and pain.
Now it’s yours.

#SOON
THANK YOU
Questions?

SKURRT SKURRRT Good Sir.